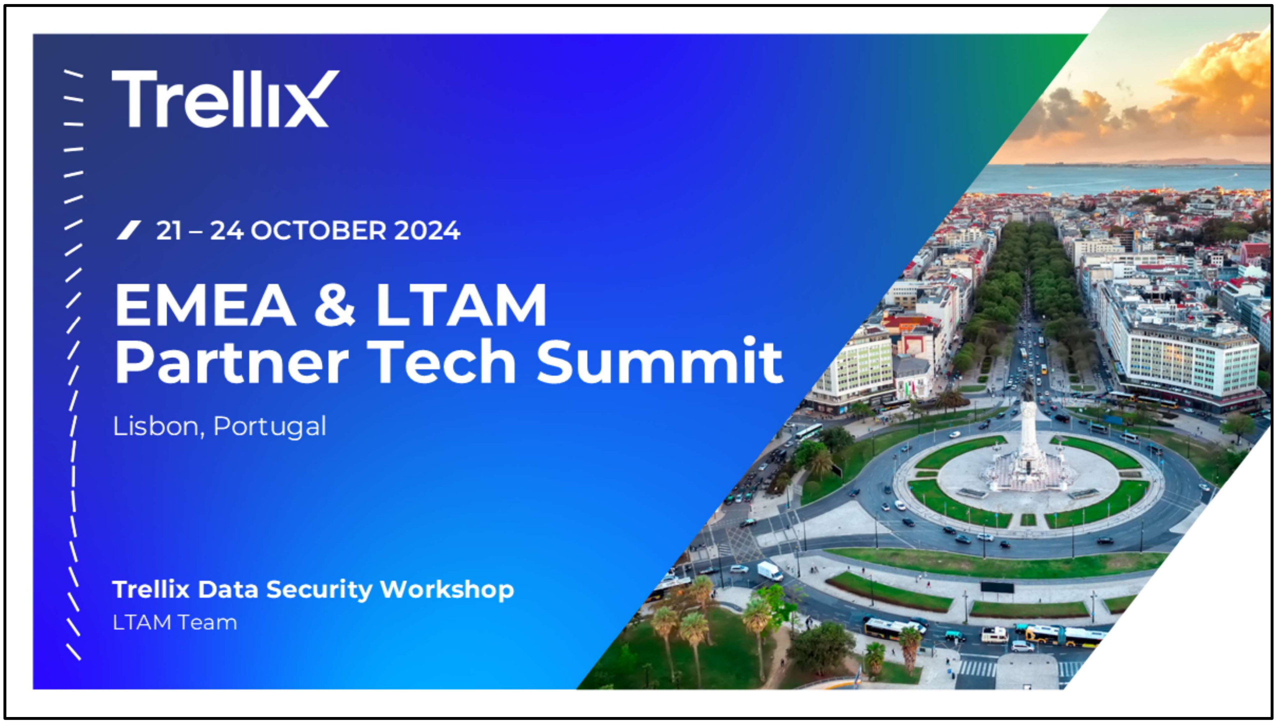


Trellix

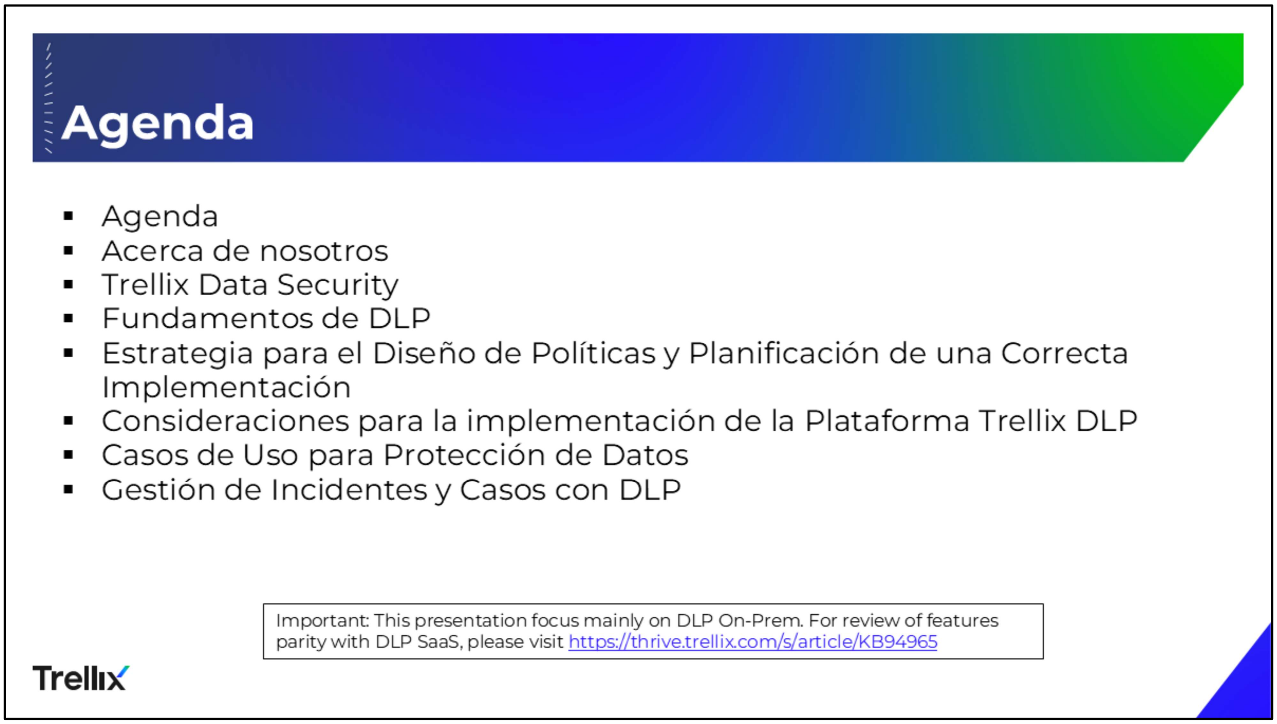
21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Trellix Data Security Workshop

LTAM Team



Agenda

- Agenda
- Acerca de nosotros
- Trellix Data Security
- Fundamentos de DLP
- Estrategia para el Diseño de Políticas y Planificación de una Correcta Implementación
- Consideraciones para la implementación de la Plataforma Trellix DLP
- Casos de Uso para Protección de Datos
- Gestión de Incidentes y Casos con DLP

Important: This presentation focus mainly on DLP On-Prem. For review of features parity with DLP SaaS, please visit https://thrive.trellix.com/s/article/KB94965

Acerca de nosotros

Julio Quinteros

Director Trellix Professional Services

David Nieto

Senior Sales Engineer

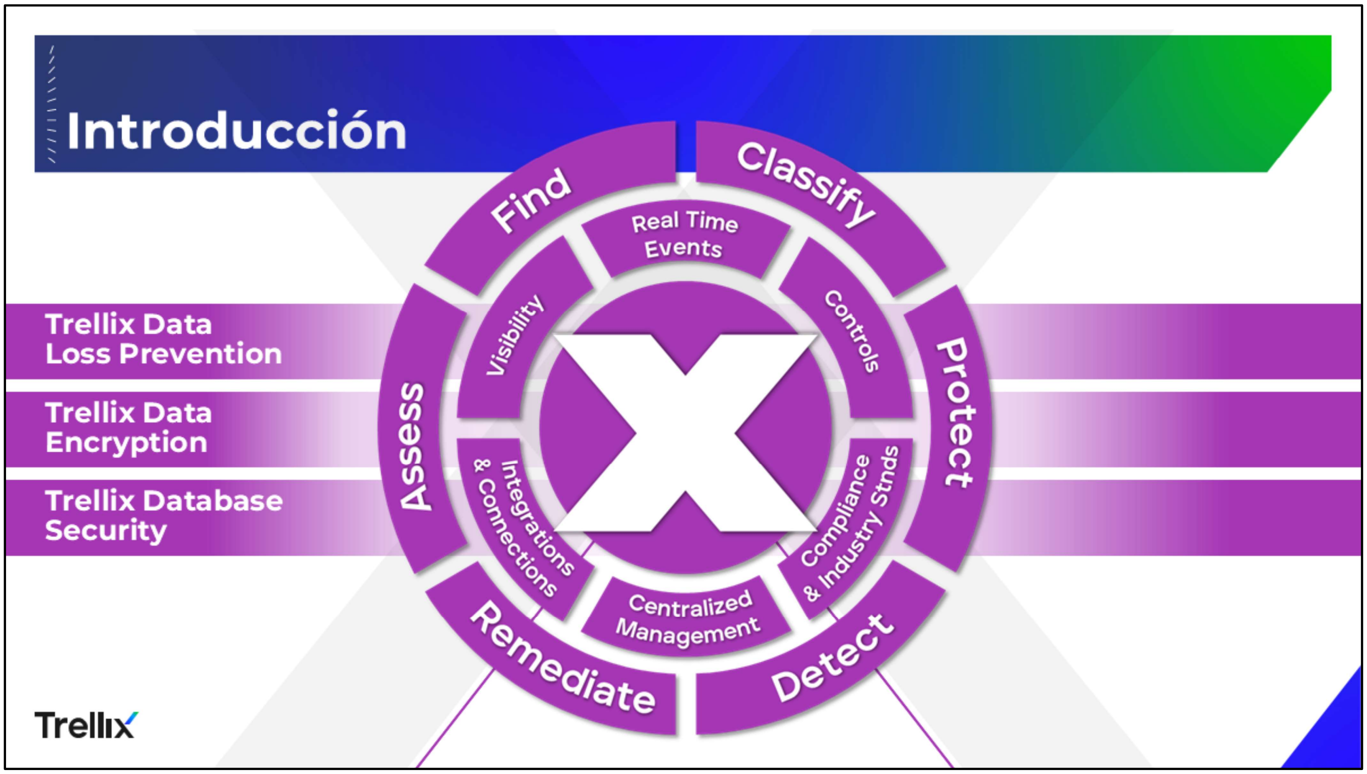
Trellix

Trellix Data Security

Workshop

Julio Quinteros

Director Trellix Professional Services
October, 2024



In the past, Trellix mostly focused on the Data Loss Prevention products - sometimes to the detriment of our other products in this line of business. And we had gained a reputation for being legacy in the market. After examining our market opportunities for the next few years, we decided to undertake a repositioning and rebranding that would focus on our abilities as a set of solutions rather than an individual product.

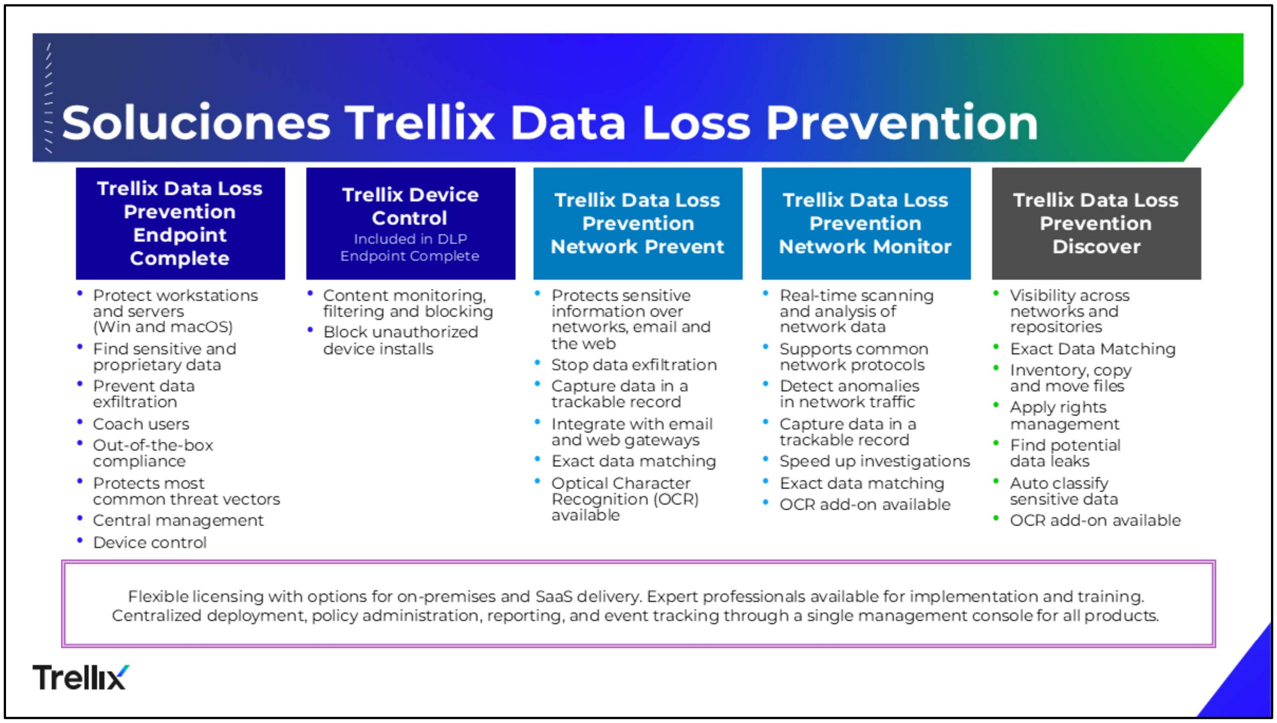
As part of this initiative, Trellix Data Protection became Trellix Data Security. The more accepted and widely recognized industry term - especially with analysts. And as we left legacy behind, we determined that we needed to be more flexible with how we sell our products and bundle our packages.

To achieve flexibility and competitiveness, sellers now have access to our full line of encryption products as individual offerings or in our various packages. And we updated our Database Security product into a single comprehensive offering - and more on the investments in that later.

We also refreshed all our package and product names to better reflect what is included in the solutions. But we didn't change the SKUs so that existing customers didn't experience any disruption.

And we created a new SKU to deliver the most end-to-end data security solution possible - the Data Security Suite. This new package is designed to solve our customers biggest challenges, take on our competitors head to head, and make it easy to up-sell current customers who want more comprehensive protection.

- Trellix Data Protection is now **Trellix Data Security**
- Trellix Data Encryption products are **available individually**
- Trellix Database Security is sold only as a **single offering**
- Some Data Security packages (suites) were **re-named**
  - SKUs were not changed
- Minor **product re-naming**
  - Trellix Native Drive Encryption
  - Trellix DLP Discover
  - Trellix DLP Endpoint Complete,
  - Trellix DLP Network
- **Trellix Data Security Suite** was created with DLP and Encryption - add on for Database Security



Soluciones Trellix Data Loss Prevention

Trellix Data Loss Prevention Endpoint Complete

- Protect workstations and servers (Win and macOS)
- Find sensitive and proprietary data
- Prevent data exfiltration
- Coach users
- Out-of-the-box compliance
- Protects most common threat vectors
- Central management
- Device control

Trellix Device Control
Included in DLP Endpoint Complete

- Content monitoring, filtering and blocking
- Block unauthorized device installs

Trellix Data Loss Prevention Network Prevent

- Protects sensitive information over networks, email and the web
- Stop data exfiltration
- Capture data in a trackable record
- Integrate with email and web gateways
- Exact data matching
- Optical Character Recognition (OCR) available

Trellix Data Loss Prevention Network Monitor

- Real-time scanning and analysis of network data
- Supports common network protocols
- Detect anomalies in network traffic
- Capture data in a trackable record
- Speed up investigations
- Exact data matching
- OCR add-on available

Trellix Data Loss Prevention Discover

- Visibility across networks and repositories
- Exact Data Matching
- Inventory, copy and move files
- Apply rights management
- Find potential data leaks
- Auto classify sensitive data
- OCR add-on available

Flexible licensing with options for on-premises and SaaS delivery. Expert professionals available for implementation and training.
Centralized deployment, policy administration, reporting, and event tracking through a single management console for all products.

Trellix

Trellix Data Loss Prevention (DLP) delivers exceptional visibility across data types and throughout the data lifecycle so that organizations can find sensitive information and intellectual property, classify only the data that requires added protection, determine policies to be applied across the environment, and detect inappropriate activity for remediation.

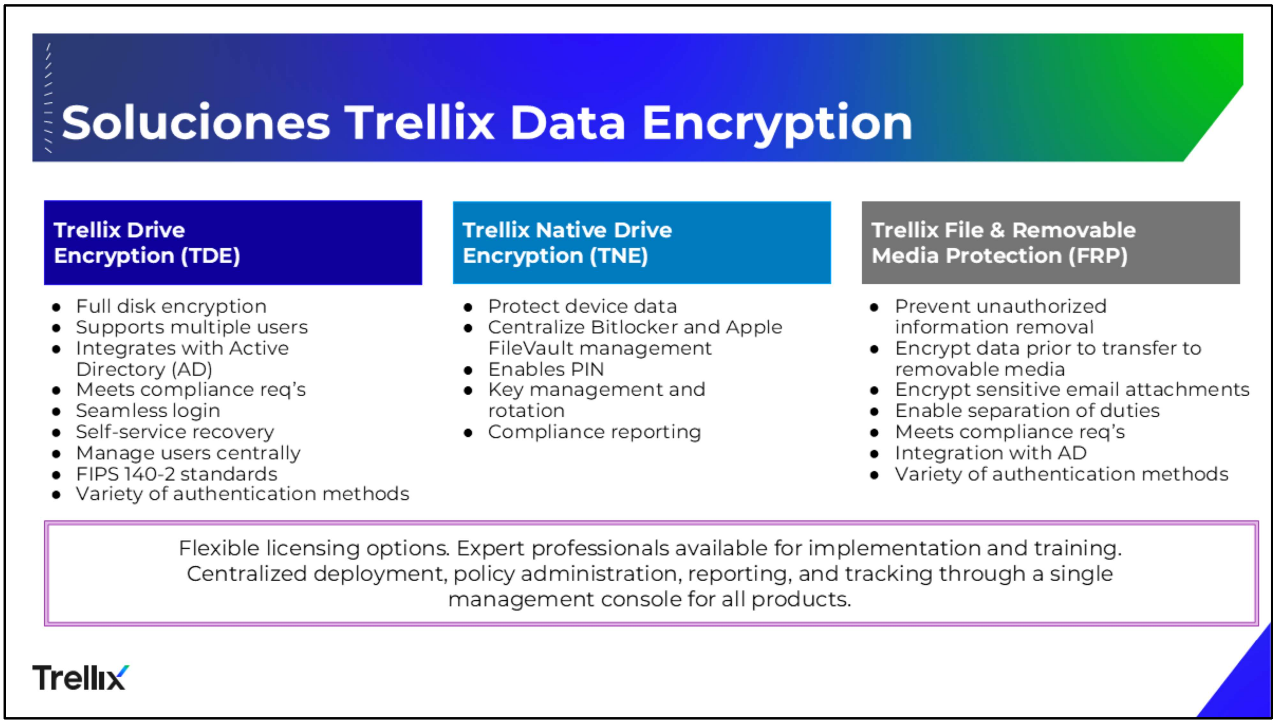
Trellix DLP products fall into three categories - (CLICK) Trellix Data Loss Prevention Endpoint, (CLICK) Trellix Data Loss Prevention Network and (CLICK) Trellix Data Loss Prevention Discover. You can see some of the key features of each here. One of Trellix DLP's greatest strengths is the ability to stop data leakage. But that's dependent on knowing what data to protect. Our products offer extensive data discovery that searches out the data that matters and limits false positives.

Our products are available on-prem and via SaaS. DLP is deployed from the ePO console. We can protect data on both Windows operating systems and macOS workstations and laptops with our DLP Endpoint products. We also offer add-on products like Optical Character Recognition (OCR) that enhance capabilities to track and retain sensitive data for forensics and investigations.

We updated naming for a few of these products in 2024, including Trellix Data Loss Prevention Endpoint Complete. In the case of DLP Endpoint, we wanted to emphasize that it includes our Device Control capabilities, as well as versions for Windows and Mac endpoints. As you probably know, Device Control is also available as a stand-alone product and is included in many Endpoint Security product bundles which makes DLP and Endpoint excellent cross-sell partners.

All DLP products identify sensitive data or user activity, take action on policy violations, and create incidents of violations.

- **Detect and identify**
  - DLP identifies data on your network when that data:
  - Is used or accessed by a user
  - Is in transit across or outside your network
  - Resides on a local file system or shared repository
- **React and protect**
  - The software can take different actions on sensitive data, such as:
  - Report an incident
  - Block User Access
  - Move or encrypt files
  - Quarantine emails that contain the data
- **Monitor and report:** When policy violations are discovered, DLP creates an incident with details of the violation.
- **Categorize:** DLP collects data and categorizes it by vectors: Data-in-Motion, Data-at-Rest, and Data- in-Use.



Soluciones Trellix Data Encryption

Trellix Drive Encryption (TDE)

- Full disk encryption
- Supports multiple users
- Integrates with Active Directory (AD)
- Meets compliance req's
- Seamless login
- Self-service recovery
- Manage users centrally
- FIPS 140-2 standards
- Variety of authentication methods

Trellix Native Drive Encryption (TNE)

- Protect device data
- Centralize Bitlocker and Apple FileVault management
- Enables PIN
- Key management and rotation
- Compliance reporting

Trellix File & Removable Media Protection (FRP)

- Prevent unauthorized information removal
- Encrypt data prior to transfer to removable media
- Encrypt sensitive email attachments
- Enable separation of duties
- Meets compliance req's
- Integration with AD
- Variety of authentication methods

Flexible licensing options. Expert professionals available for implementation and training. Centralized deployment, policy administration, reporting, and tracking through a single management console for all products.

Trellix

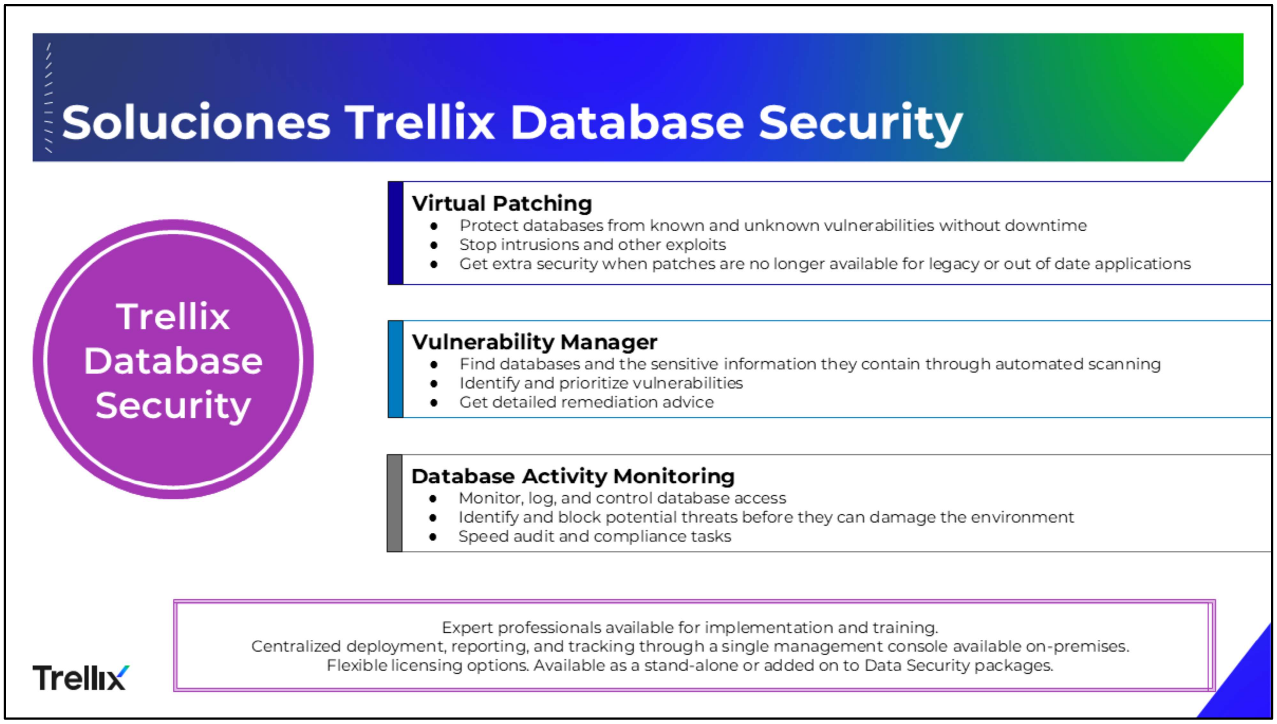
Trellix offers three encryption products and as we mentioned earlier Drive Encryption, Native Drive Encryption, and File & Removable Media Protection. They can be sold together as part of our popular packages or now are offered individually.

Our new strategy to offer our products individually and in packages is designed to give sellers flexibility to combat competitors like Microsoft who may offer just Bitlocker at a lower price. Now, we can counter with Trellix Native Drive Encryption (TNE) which will manage Bitlocker and Apple FileVault in a single location.

Our Encryption offerings are designed to meet customers where they are. For a complex, highly regulated organization it's likely they might need the full disk encryption protection provided by Trellix Drive Encryption. This also offers organizations that need it the ability to authenticate multiple users on the same device.

For organizations concerned with data security but who may not need full disk protection and pre-boot authentication, consider positioning Native Drive Encryption (which was previously named Management of Native Encryption). Organizations that have mixed operating systems in their ecosystem will benefit from streamlined administration and reporting, along with the automatic recognition of the OS.

File and removable Media Protection (FRP) can be a game change for organizations that require 'separation of duties' for compliance or who need the added security of file level protection automatically applied based on policies built in their DLP rules. FRP prevents unauthorized access to and transfers of data across some of the most vulnerable leakage points in an organization.



Soluciones Trellix Database Security

Trellix Database Security

Virtual Patching

- Protect databases from known and unknown vulnerabilities without downtime
- Stop intrusions and other exploits
- Get extra security when patches are no longer available for legacy or out of date applications

Vulnerability Manager

- Find databases and the sensitive information they contain through automated scanning
- Identify and prioritize vulnerabilities
- Get detailed remediation advice

Database Activity Monitoring

- Monitor, log, and control database access
- Identify and block potential threats before they can damage the environment
- Speed audit and compliance tasks

Expert professionals available for implementation and training.
Centralized deployment, reporting, and tracking through a single management console available on-premises.
Flexible licensing options. Available as a stand-alone or added on to Data Security packages.

Trellix

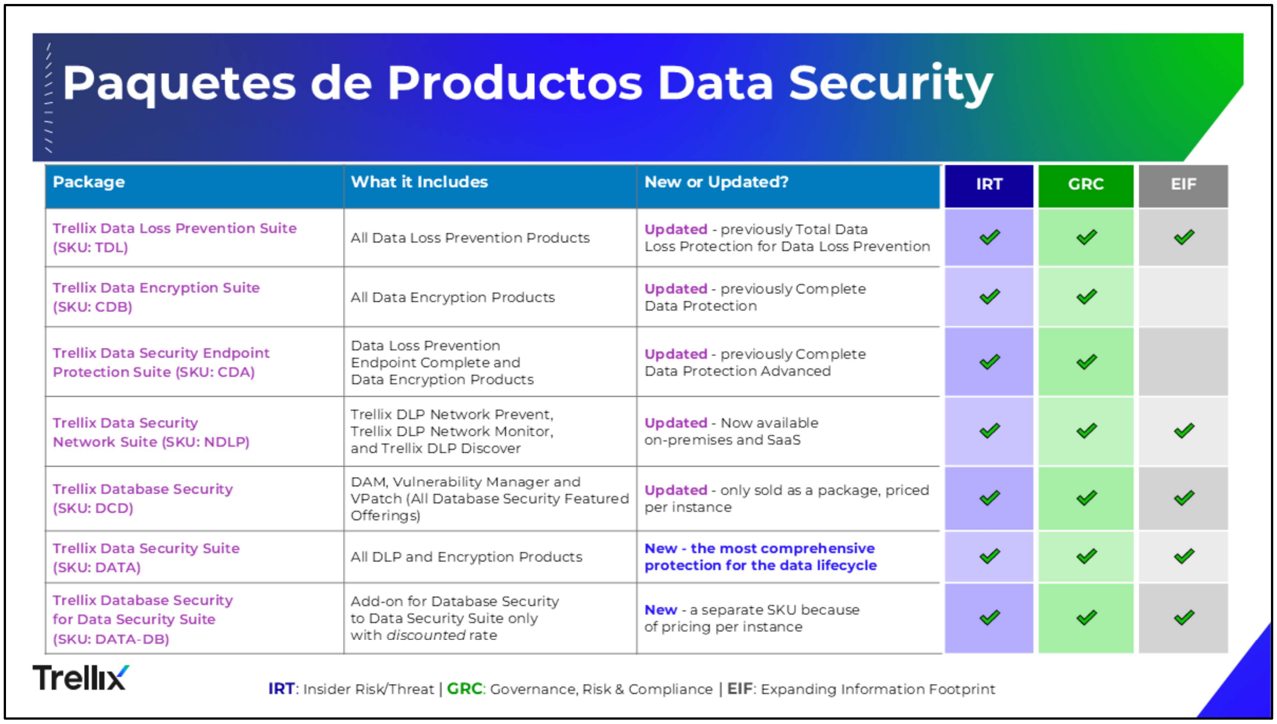
Customers that don't have database security tools in place experience challenges finding rogue databases and tracking down all the sensitive information across their database ecosystem. It's hard to control access to data within databases and keep their security up to date - not to mention ensuring that they are properly configured as many organizations are running different version of databases. And as regulations and laws evolve, compliance tasks are probably difficult for organizations without a tool to manage.

We relaunched the updated Trellix Database Security to help! This solution finds databases and the information they contain, ensures that appropriate access is maintained and scans / patches databases automatically with rules that can provide extra security if no patches are available for a security gap - along with centralized reporting to simplify compliance activities. We protect all leading database types with this comprehensive offering.

If you think this offering sounds familiar - it probably does. Trellix Database Security was formerly a set of McAfee products - you see them now as features here within our new single offering. While we have many existing customers, it was not until March 2024 when these customers transitioned to a Trellix-branded platform with an upgraded experience. We've invested in a development team for this product and have many exciting innovations planned.

There are three key feature sets within Database Security –

1. Database Activity Monitoring: which will safeguard databases against leaks by actively monitoring, logging, and detecting database access and irregularities, while preemptively blocking potential threats before they impact the environment
2. Vulnerability Manager: automates scanning activities to find supported databases and their sensitive information. It will identify and prioritize known vulnerabilities to expedite detailed remediation, swiftly addressing security gaps.
3. Virtual Patching: stops intrusions and other exploits before they breach the database. When available, Trellix's virtual patches are automatically applied without impacting database availability. When vendor patches aren't available, extra security is applied to keep it secure. This is a big differentiating factor for customers who invest in this technology.



Paquetes de Productos Data Security

Package	What it Includes	New or Updated?	IRT	GRC	EIF
Trellix Data Loss Prevention Suite (SKU: TDL)	All Data Loss Prevention Products	**Updated** - previously Total Data Loss Protection for Data Loss Prevention	✓	✓	✓
Trellix Data Encryption Suite (SKU: CDB)	All Data Encryption Products	**Updated** - previously Complete Data Protection	✓	✓	
Trellix Data Security Endpoint Protection Suite (SKU: CDA)	Data Loss Prevention Endpoint Complete and Data Encryption Products	**Updated** - previously Complete Data Protection Advanced	✓	✓	
Trellix Data Security Network Suite (SKU: NDLP)	Trellix DLP Network Prevent, Trellix DLP Network Monitor, and Trellix DLP Discover	**Updated** - Now available on-premises and SaaS	✓	✓	✓
Trellix Database Security (SKU: DCD)	DAM, Vulnerability Manager and VPatch (All Database Security Featured Offerings)	**Updated** - only sold as a package, priced per instance	✓	✓	✓
Trellix Data Security Suite (SKU: DATA)	All DLP and Encryption Products	**New - the most comprehensive protection for the data lifecycle**	✓	✓	✓
Trellix Database Security for Data Security Suite (SKU: DATA-DB)	Add-on for Database Security to Data Security Suite only with *discounted* rate	**New** - a separate SKU because of pricing per instance	✓	✓	✓

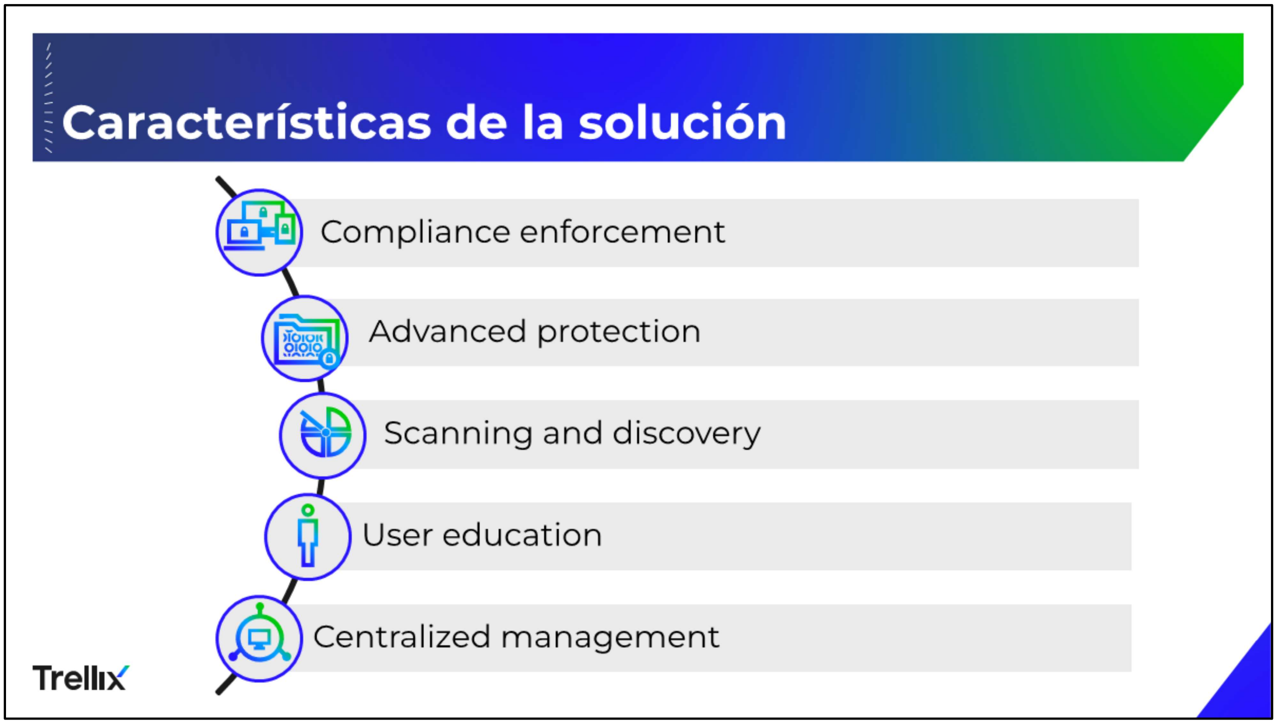
Trellix

IRT: Insider Risk/Threat | **GRC**: Governance, Risk & Compliance | **EIF**: Expanding Information Footprint

Most Trellix customers purchase our products in the form of packages or bundles. While all the Data Security products we have reviewed in this section are available as stand-alone offerings, they're are also all available in combinations we feel will help solve our customers problems. Here you see a grid of our packages - note where we've made some updates to the names of the packages (but SKUs were not changed). You can also see how our packages map to the biggest challenges our customers face - as we talked about in other training modules. This refreshed approach already seems to be catching on as we have started 2024 very strong, including with opportunities in our new full line package.

The likely package targets for most of our customers new to data security are Trellix Data Loss Prevention Suite (SKU: TDL), Trellix Data Security Endpoint Protection Suite (SKU: CDA) - while we will likely upsell to Trellix Data Security Suite (SKU: DATA) - and if the customer has databases (most do) we want to position Trellix Database Security* (SKU: DCD).

Please note that while most of our products and packages are priced by endpoints, Database Security is priced by number of databases. DCD and DATA-DB skus can be added to any deal with the packages you see here but if you need pricing advice contact your SE or a member of our product team. And please note that Trellix Database Security for Data Security Suite (DATA-DB) has an automatic discount applied when sold with the Data Security Suite as an incentive to showcase our new full-line package and help you close those deals.



Características de la solución

- Compliance enforcement
- Advanced protection
- Scanning and discovery
- User education
- Centralized management

Data Loss Prevention is a suite of products that protects against data loss by identifying and securing data within your network and offline. DLP policies help you understand the types of data on your network, how the data is accessed and transmitted, and if the data contains sensitive or confidential information. Use DLP to build and implement effective protection policies while reducing the need for extensive trial and error.

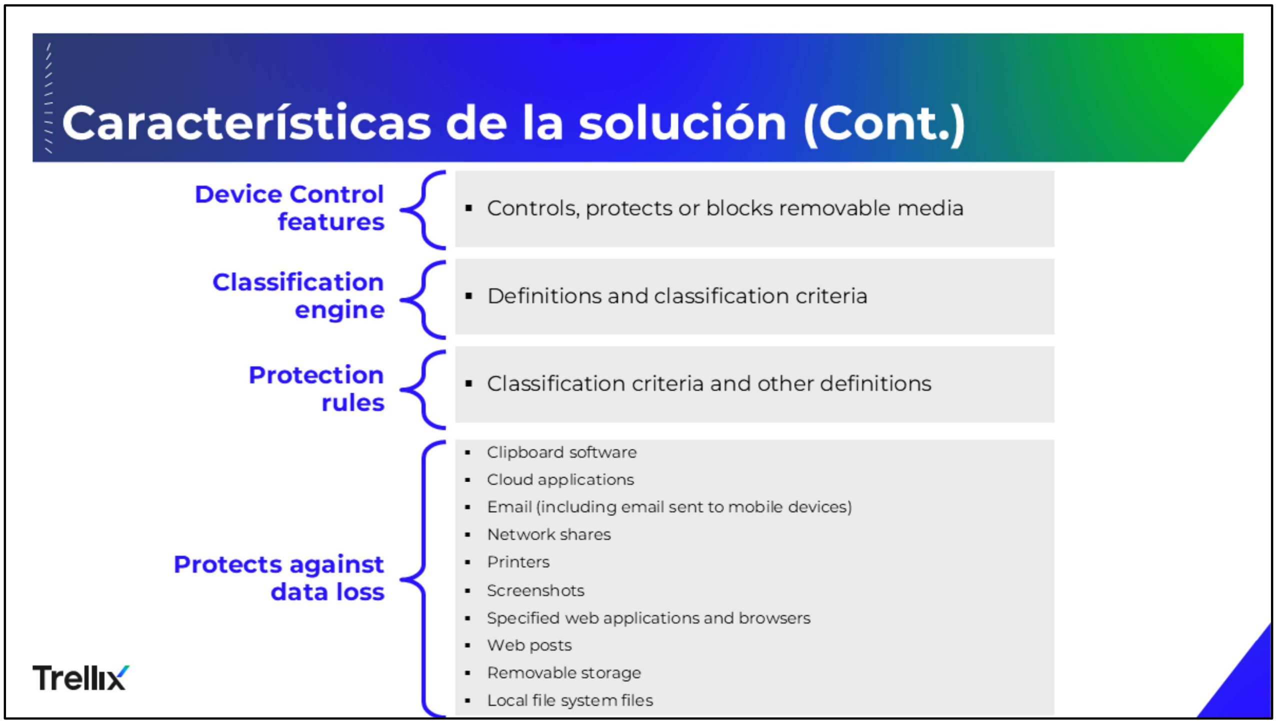
Data Loss Prevention Endpoint (DLP Endpoint) for Windows — Content-based agent solution that inspects user actions. It scans data-in-use on endpoints and blocks or encrypts unauthorized transfer of data identified as sensitive or confidential. The Endpoint Discovery feature scans local file system and email storage files and applies rules to protect sensitive content.

Data Loss Prevention Endpoint for Mac (DLP Endpoint for Mac) — Offers similar protection for Macintosh computers running macOS operating systems.

DLP Endpoint provides comprehensive protection for all potential leaking channels, including removable storage devices, the cloud, email, instant messaging, web, printing, clipboard, screenshot, and file-sharing applications.

- **Compliance enforcement:** Ensure compliance by addressing day-to-day user actions, such as emailing, cloud posting, and downloading to removable media devices.
- **Advanced protection:** Apply fingerprinting, classification, and file tagging to secure sensitive, unstructured data, such as intellectual property and trade secrets.
- **Scanning and discovery:** Scan files and databases stored on local endpoints, shared repositories, or the cloud to identify sensitive data.
- **User education:** Provide real-time feedback through educational pop-up messages to help shape corporate security awareness and culture.
- **Centralized management**: Integrate with ePO software to streamline policy

and incident management.



Características de la solución (Cont.)

Device Control features

- Controls, protects or blocks removable media

Classification engine

- Definitions and classification criteria

Protection rules

- Classification criteria and other definitions

Protects against data loss

- Clipboard software
- Cloud applications
- Email (including email sent to mobile devices)
- Network shares
- Printers
- Screenshots
- Specified web applications and browsers
- Web posts
- Removable storage
- Local file system files

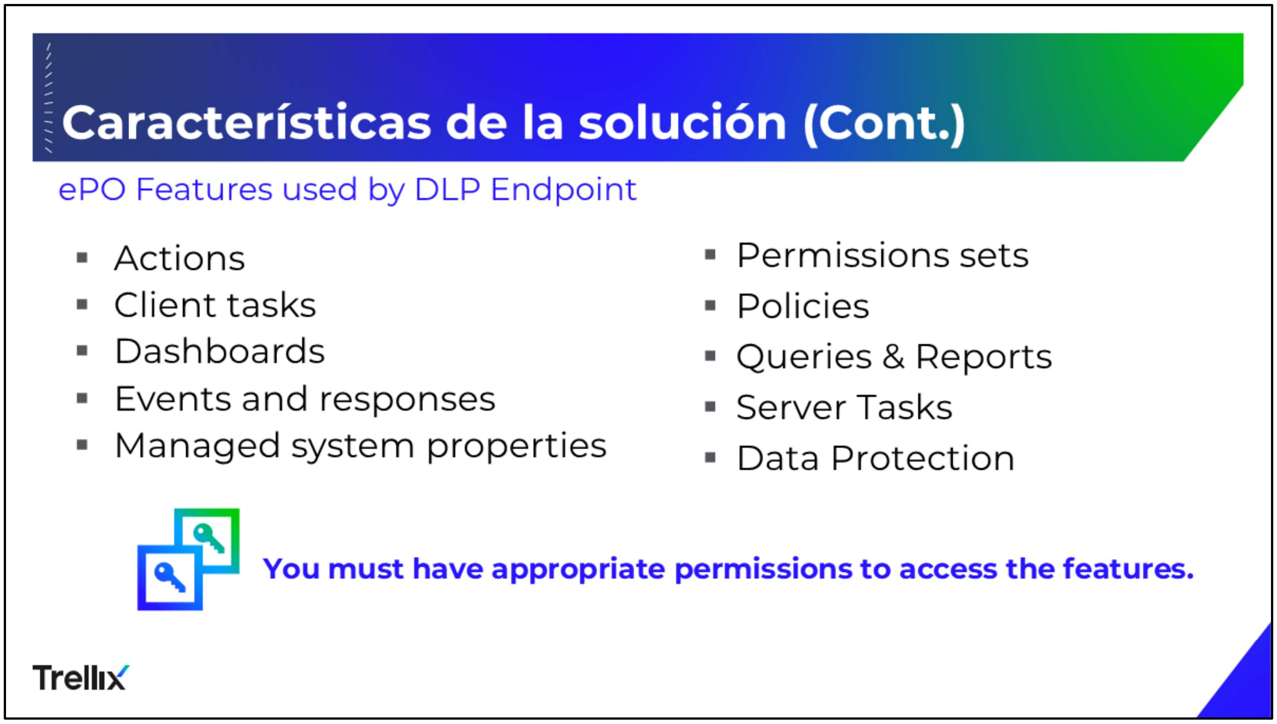
Trellix

The features are:

- DLP Endpoint includes all Device Control features such as controls, protects or blocks removable media.
- Classification engine applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied.
- Protection rules apply the classification criteria and other definitions to protect the sensitive content.
- Protects against data loss from Clipboard software, Cloud applications, Email (including email sent to mobile devices), Network shares, Printers, Screenshots, Specified web applications and browsers, Web posts, Removable storage, and Local file system files.

Note: Clipboard, email, printers, screenshots, specified apps, and web posts protection are not currently supported on macOS.

The DLP Endpoint discovery crawler runs on the local endpoint, searching local file system and email storage files and applying policies to protect sensitive content.



Características de la solución (Cont.)

ePO Features used by DLP Endpoint

- Actions
- Client tasks
- Dashboards
- Events and responses
- Managed system properties
- Permissions sets
- Policies
- Queries & Reports
- Server Tasks
- Data Protection

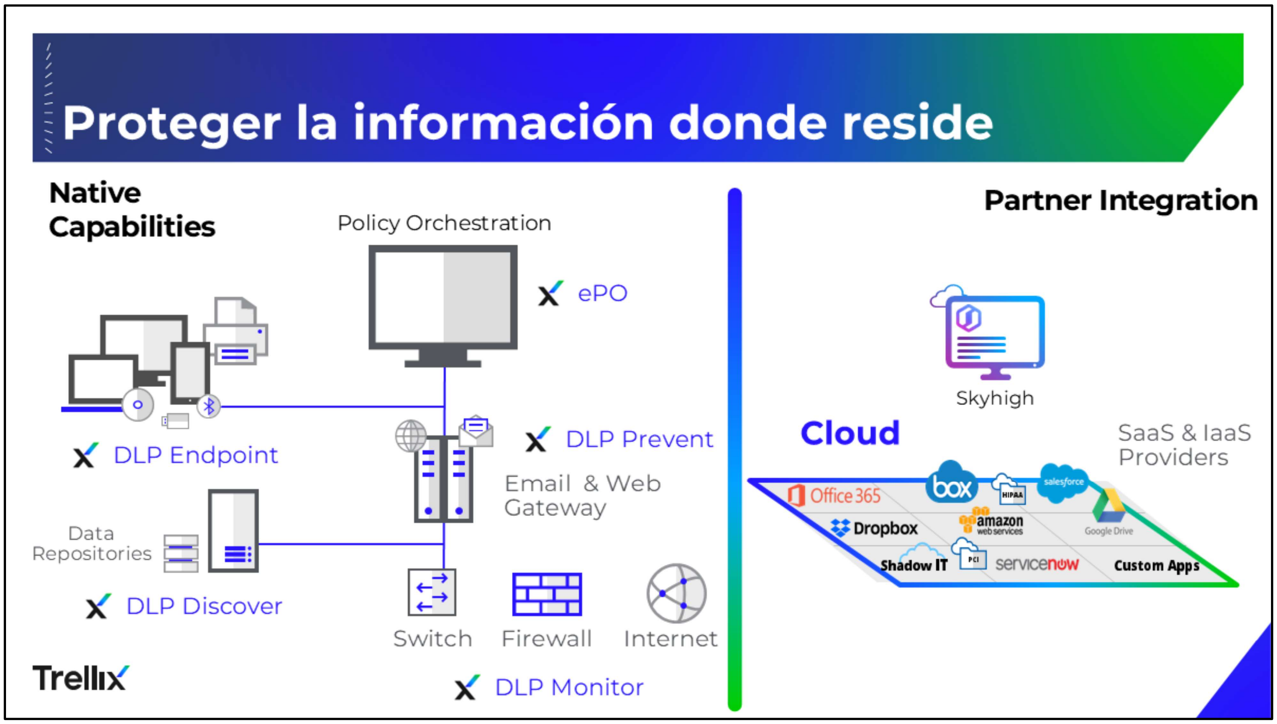
You must have appropriate permissions to access the features.

Trellix

DLP Endpoint uses the following ePO features:

Actions: Actions that you can perform from the System Tree or use to customize automatic responses.
Client tasks (DLP Endpoint only): Client tasks that you can use to automate management and maintenance on client systems.
Dashboards: Dashboards and monitors that you can use to keep watch on your environment.
Events and responses: Events for which you can configure automatic responses and event groups and event types that you can use to customize automatic responses.
Managed system properties: Properties that you can review in the System Tree or use to customize queries.
Permissions sets: Available in all existing permission sets-**Data Loss Prevention, DLP Appliance Management Policy**, and **DLP Help Desk Actions.**
Policies: DLP Policy, **Windows Client Configuration**, and **Mac OS X Client Configuration** for DLP Endpoint, and **Server Configuration** for DLP Discover and DLP appliance policy categories in the **Data Loss Prevention <version>** product group.
Queries and reports: Default queries that you can use to run reports. Custom property groups based on managed system properties that you can use to build your own queries and reports.
Server tasks: Server tasks for DLP Endpoint include DLP Incident Manager and DLP Operations. Use the **Roll UP Data** task to roll up DLP incidents, operational events, or endpoint discovery data from selected ePO servers

to produce a single report.
Data Protection: Used to configure, manage, and monitor DLP.



Proteger la información donde reside

Native Capabilities

Policy Orchestration

ePO

DLP Endpoint

DLP Prevent

Email & Web Gateway

Data Repositories

DLP Discover

Switch

Firewall

Internet

DLP Monitor

Trellix

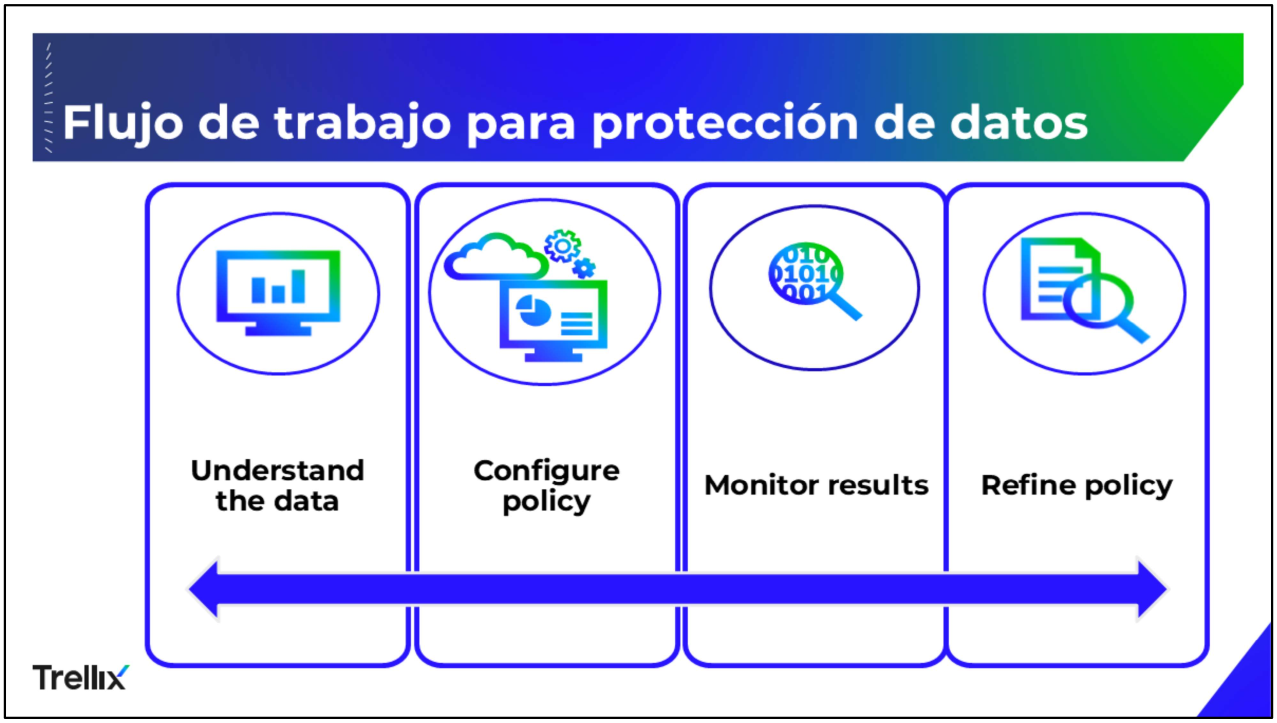
Partner Integration

Skyhigh

Cloud

SaaS & IaaS Providers

Consider all the data loss vectors from endpoint to network and to cloud.



Flujo de trabajo para protección de datos

Understand the data

Configure policy

Monitor results

Refine policy

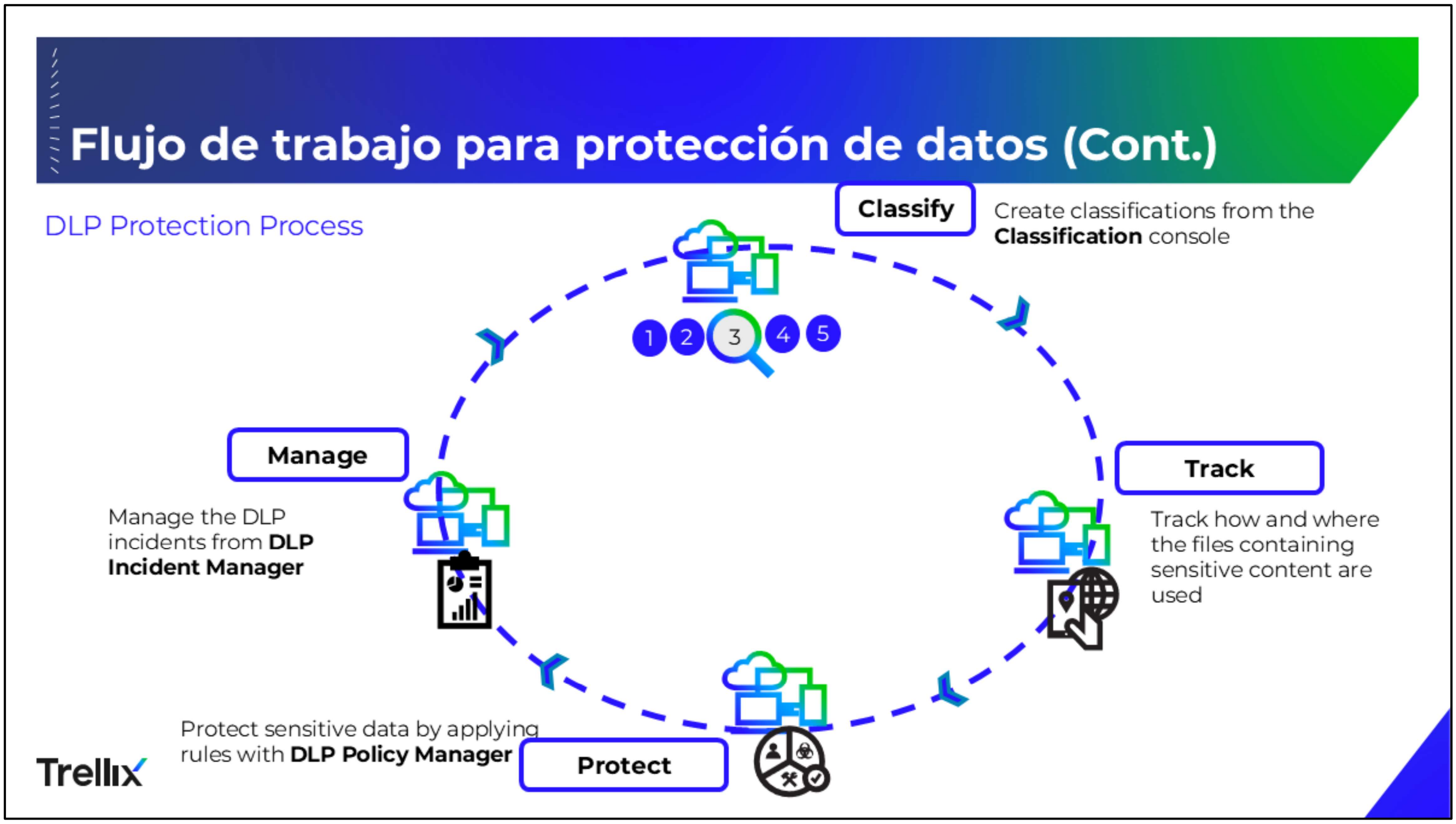
Use the following workflow as general guidance for setting up and working with your DLP products in ePO.

- **Understand the data:** Detect and identify what data is on your network.
  1. Use DLP to passively monitor the data and user actions on the network. You can use predefined rules or create a basic policy.
  2. Review incidents and analyze scan results to see potential policy violations. Use this information to begin creating an effective policy.

- **Configure policy:** Use rules to react to violations to protect data.
  1. Classify and define sensitive data by configuring classifications and definitions.
  2. Track sensitive data and files with content fingerprinting and registered documents.
  3. Protect data with scans and rules. Configure the action to take when sensitive data is discovered, accessed, or transmitted.

- **Monitor results:** Monitor incidents and create reports.
  1. Review incidents for false positives and genuine policy violations.
  2. Group related incidents into cases, which can be escalated to other departments, such as legal or Human Resources.

- **Refine policy:** Fine-tune your policy as needed. Continue monitoring incidents and scan results, adjusting the policy based on the types of violations and false positives you find.



Flujo de trabajo para protección de datos (Cont.)

DLP Protection Process

Classify

Create classifications from the **Classification** console

Track

Track how and where the files containing sensitive content are used

Protect

Protect sensitive data by applying rules with **DLP Policy Manager**

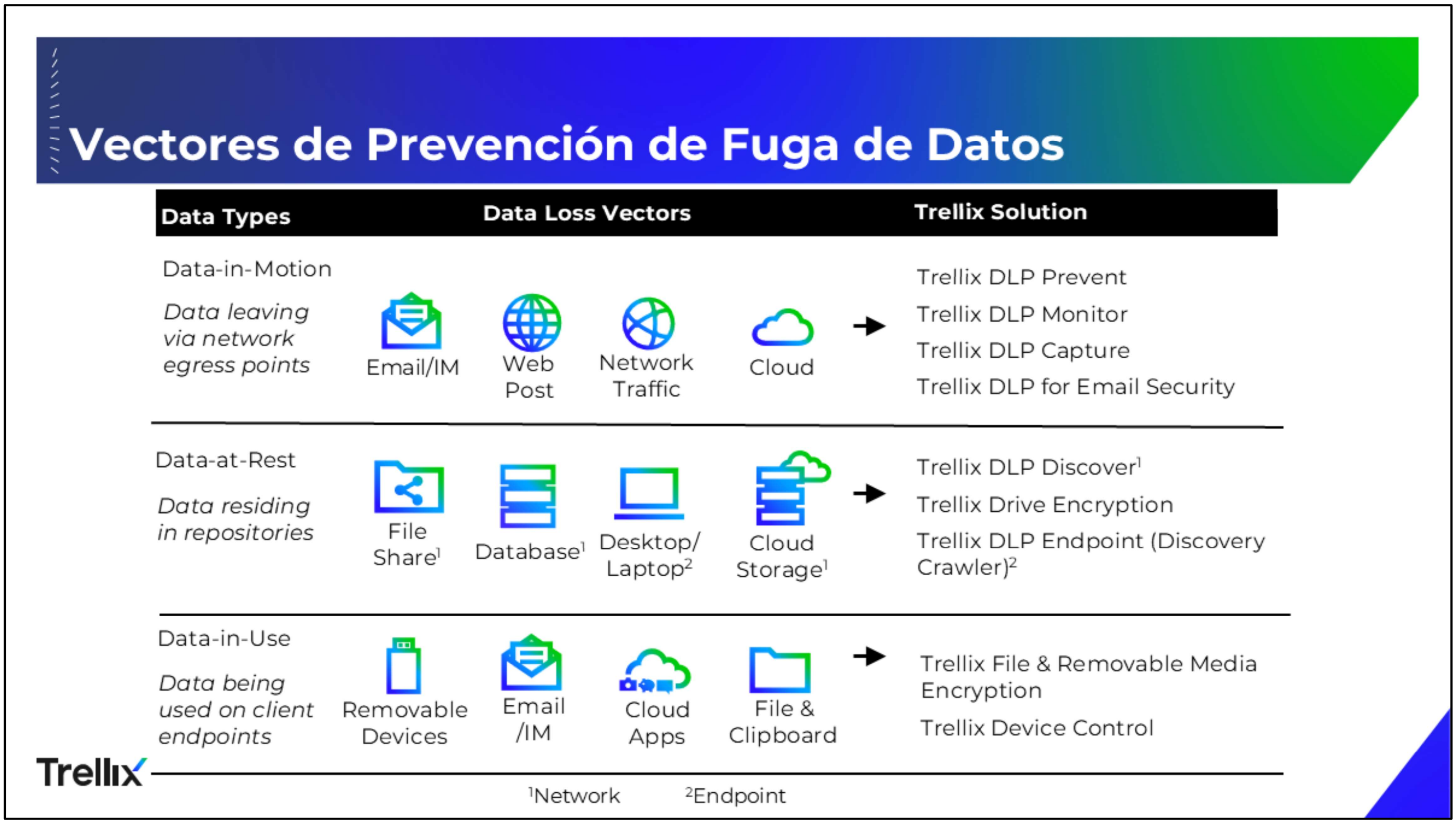
Manage

Manage the DLP incidents from **DLP Incident Manager**

Use **DLP** to monitor the data and user actions on the network. You can use predefined rules or create a basic policy.

The image depicts the ***DLP protection workflow***:

1. Create classifications from the **Classification** console. Classify and define sensitive data by configuring classifications and definitions.
2. Track how and where the files containing sensitive content are used with tags or registered documents.
3. Protect sensitive data by applying rules with **DLP Policy Manager**. Protect data with scans and rules. Configure the action to take when sensitive data is discovered, accessed, or transmitted.
4. Manage the DLP incidents from **DLP Incident Manager**. Review incidents and analyze scan results to see potential policy violations. Use this information to begin creating an effective policy. Group and work with incidents, which can be escalated to other departments, such as legal or Human Resources. You can also create reports with dashboards and queries.



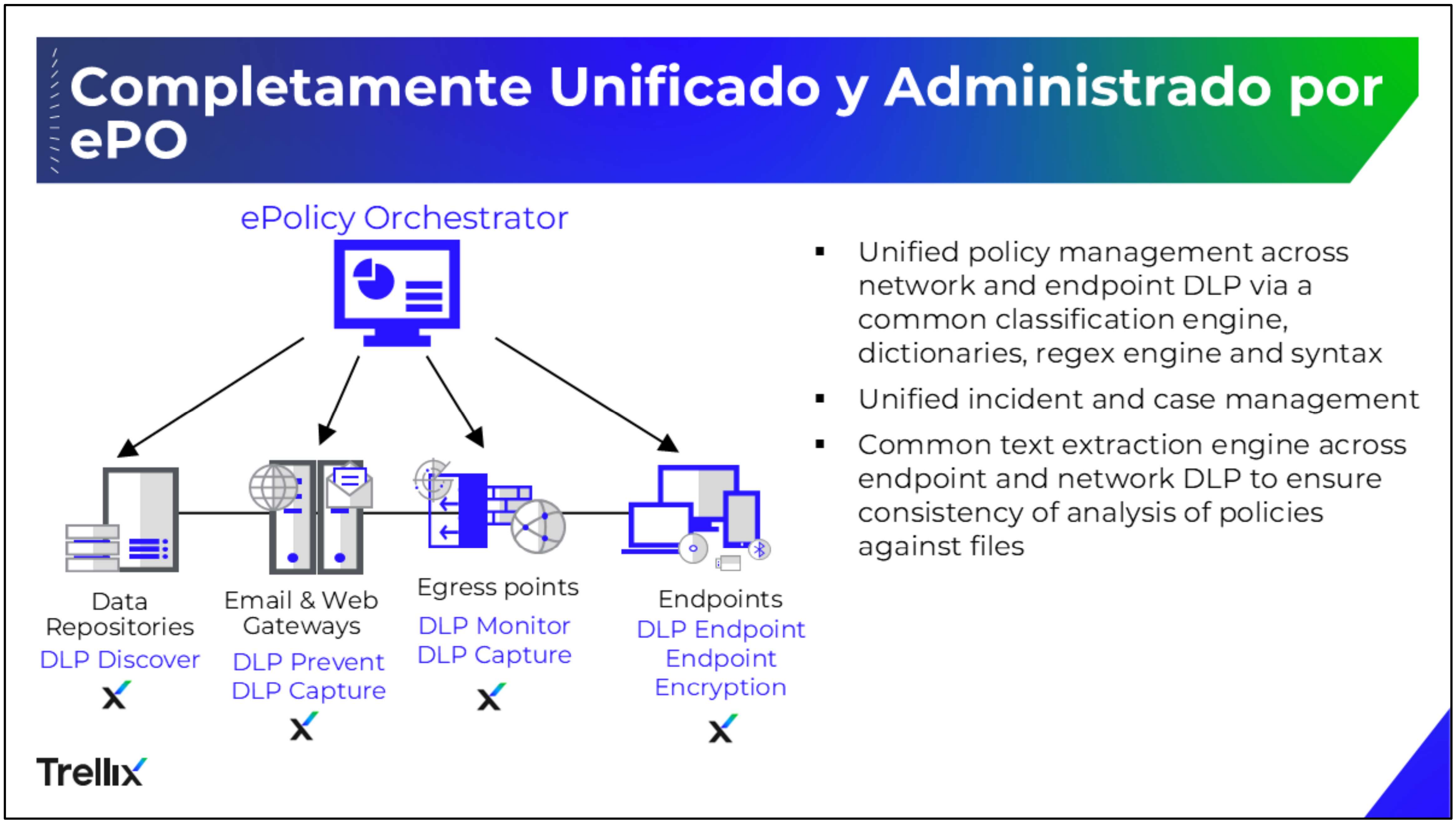
Vectores de Prevención de Fuga de Datos

Data Types	Data Loss Vectors				Trellix Solution
Data-in-Motion *Data leaving via network egress points*	Email/IM	Web Post	Network Traffic	Cloud	→ Trellix DLP Prevent Trellix DLP Monitor Trellix DLP Capture Trellix DLP for Email Security
Data-at-Rest *Data residing in repositories*	File Share[1]	Database[1]	Desktop/ Laptop[2]	Cloud Storage[1]	→ Trellix DLP Discover[1] Trellix Drive Encryption Trellix DLP Endpoint (Discovery Crawler)[2]
Data-in-Use *Data being used on client endpoints*	Removable Devices	Email /IM	Cloud Apps	File & Clipboard	→ Trellix File & Removable Media Encryption Trellix Device Control

[1]Network [2]Endpoint

- Sensitive data can live anywhere in your organization. Trellix Data Loss Protection (DLP) is a portfolio of products that work alone are together to protect your data.
- The data protection industry categorizes data into three data loss vectors: Data-in-Motion, Data-at-Rest, and Data-in-Use. The figure shows how Trellix DLP maps to these categories.
- Trellix DLP Monitor and Trellix DLP Prevent are intended for Data-in-Motion. Data-in-Motion is the data that leaves your organization via network egress points such email, instant messaging (IM) and web posting. Trellix DLP Monitor gathers, tracks, and reports on live data across your entire network, providing continuous data protection. Trellix DLP Prevent interacts with email traffic, generates incidents, and records the incidents in Trellix ePO for subsequent case review.
- Trellix DLP Discover targets Data-at-Rest. Data-at-Rest is the important data that sits in data repositories such as database, Servers, cloud and file shares. DLP Discover scans file repositories to identify and protect sensitive data. Trellix DLP Endpoint addresses data-at-rest at the endpoint with its discovery crawler.
- Data-in-Use talks about the data that lives on employee machines, such as laptops and desktops. Data can leak via USBs, printing or screen captures, and cloud applications. Trellix Device Control monitors and controls the use of removable media on endpoints. Trellix DLP Endpoint (DLPe) inspects and controls content and user actions on endpoints. Skyhigh Security Cloud

enforces DLP policies on data in the cloud, in sync with your endpoint DLP.



Completamente Unificado y Administrado por ePO

ePolicy Orchestrator

Data Repositories

DLP Discover

Email & Web Gateways

DLP Prevent

DLP Capture

Egress points

DLP Monitor

DLP Capture

Endpoints

DLP Endpoint

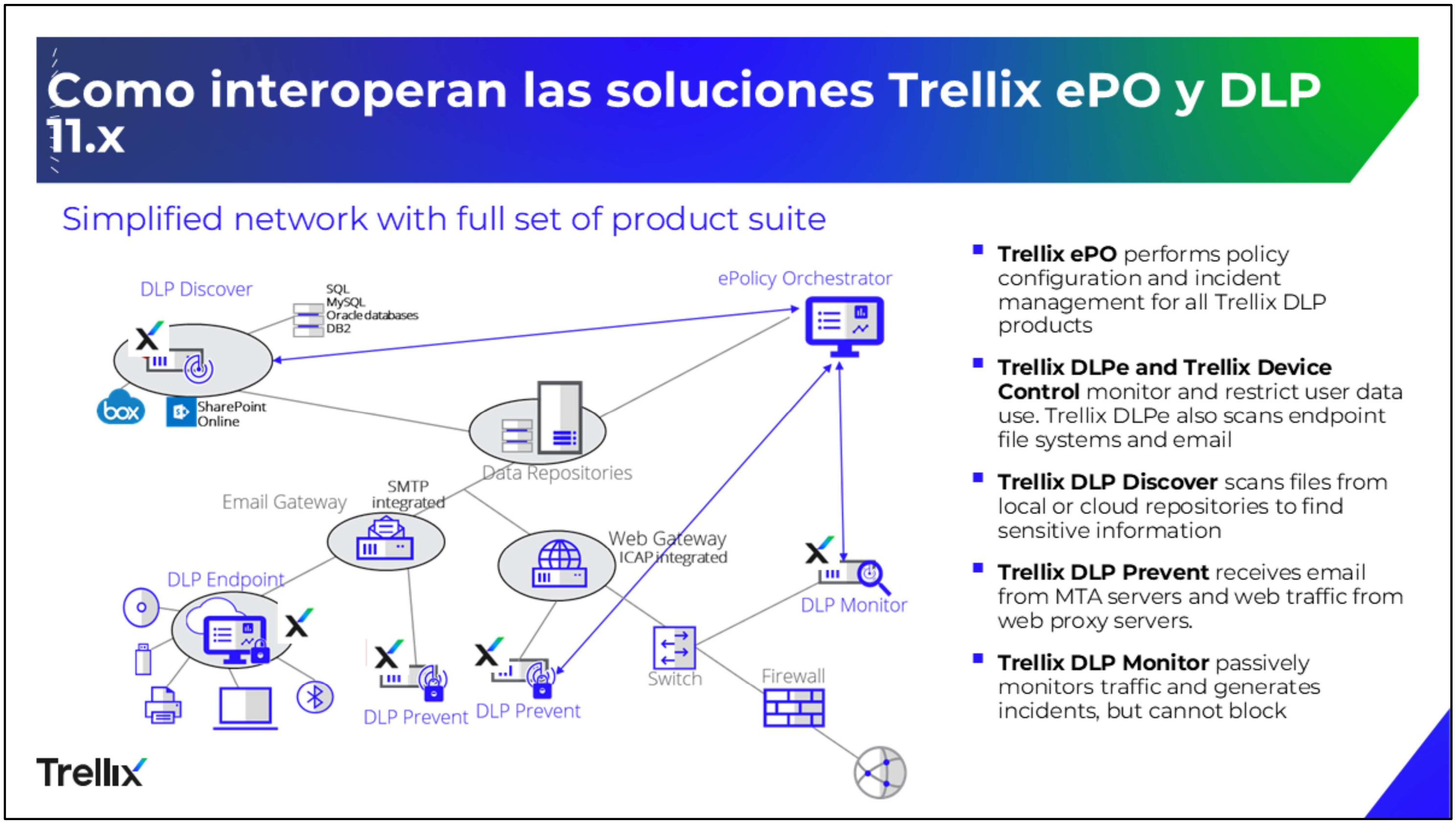
Endpoint Encryption

- Unified policy management across network and endpoint DLP via a common classification engine, dictionaries, regex engine and syntax
- Unified incident and case management
- Common text extraction engine across endpoint and network DLP to ensure consistency of analysis of policies against files

Trellix

ePolicy Orchestrator® (ePO™) provides unified policy management across network and endpoint Data Loss Prevention (DLP) products via a common classification engine, dictionaries, regex engine, and syntax.

ePO also provides unified incident and case management and a common text extraction engine across endpoint and network DLP products to ensure consistency of analysis of policies against files.



Como interoperan las soluciones Trellix ePO y DLP 11.x

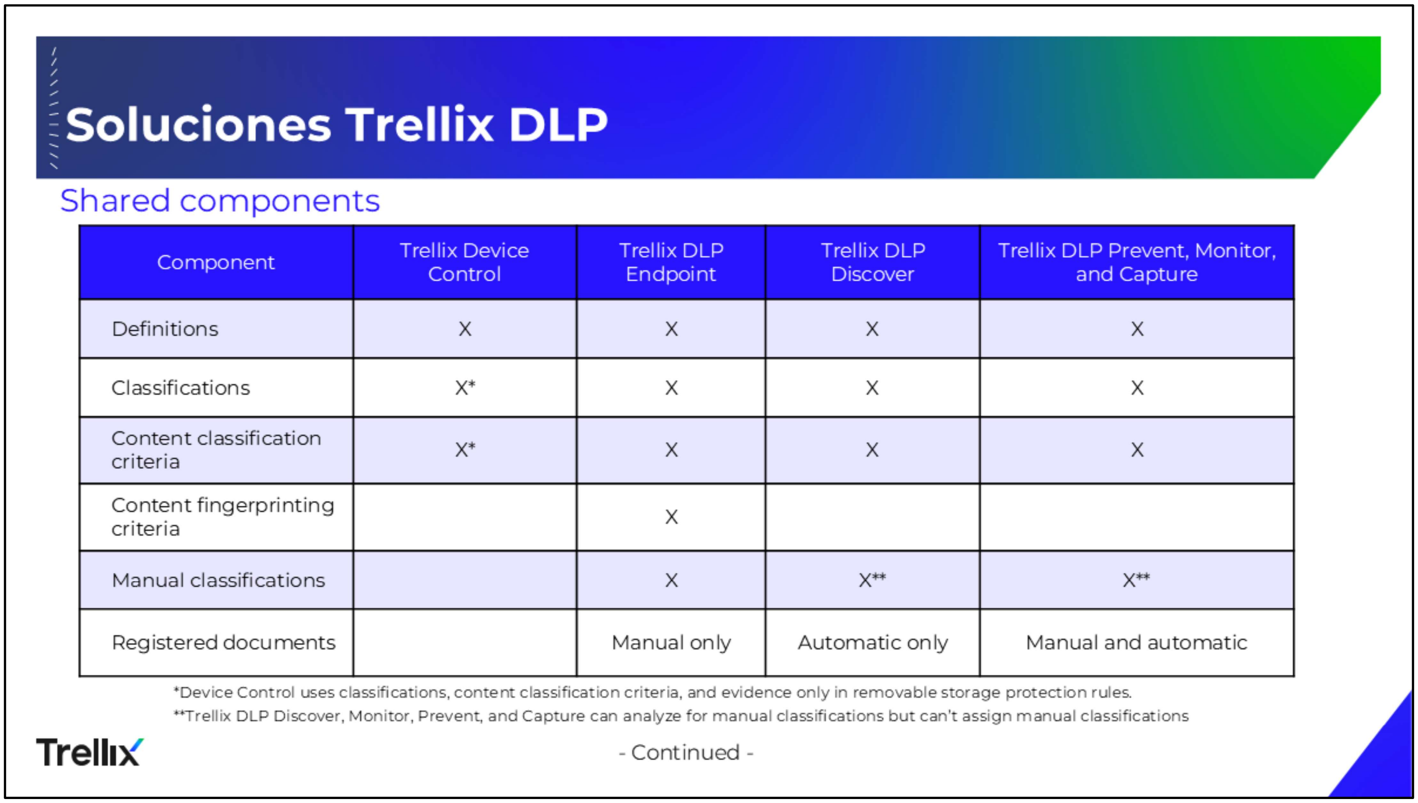
Simplified network with full set of product suite

- **Trellix ePO** performs policy configuration and incident management for all Trellix DLP products
- **Trellix DLPe and Trellix Device Control** monitor and restrict user data use. Trellix DLPe also scans endpoint file systems and email
- **Trellix DLP Discover** scans files from local or cloud repositories to find sensitive information
- **Trellix DLP Prevent** receives email from MTA servers and web traffic from web proxy servers.
- **Trellix DLP Monitor** passively monitors traffic and generates incidents, but cannot block

Installing all DLP 11.10X products allows you to use the full feature set of the product suite. This figure shows a simplified network where all Trellix DLP products and Trellix ePO are deployed.

1. **Trellix ePO** handles policy configuration and incident management for all Trellix DLP products. The data vector does not apply.
2. **Trellix DLPe and Trellix Device Control** monitor and restrict users' data use. Trellix DLPe also scans endpoint file systems and email. The applicable data vectors are Data in Use and Data at Rest).
3. **Trellix DLP Discover** scans files from local or cloud repositories to find sensitive information. The applicable data vector is Data at Rest).
4. **Trellix DLP Prevent** receives email from MTA servers. It analyzes the messages, adds appropriate headers based on configured policy, and sends the emails to a single MTA server, also known as the Smart Host. Trellix DLP Prevent also receives web traffic from web proxy servers. It analyzes the web traffic, determines if the traffic should be allowed or blocked, and sends the traffic back to the appropriate web proxy server.
5. **Trellix DLP Monitor** passively monitors traffic and generates incidents but cannot block.

Note: DLP Capture is a feature which can be enabled on a DLP Prevent or Monitor appliance and therefore sits in the same architecture locations as those appliances.



Soluciones Trellix DLP

Shared components

Component	Trellix Device Control	Trellix DLP Endpoint	Trellix DLP Discover	Trellix DLP Prevent, Monitor, and Capture
Definitions	X	X	X	X
Classifications	X*	X	X	X
Content classification criteria	X*	X	X	X
Content fingerprinting criteria		X		
Manual classifications		X	X**	X**
Registered documents		Manual only	Automatic only	Manual and automatic

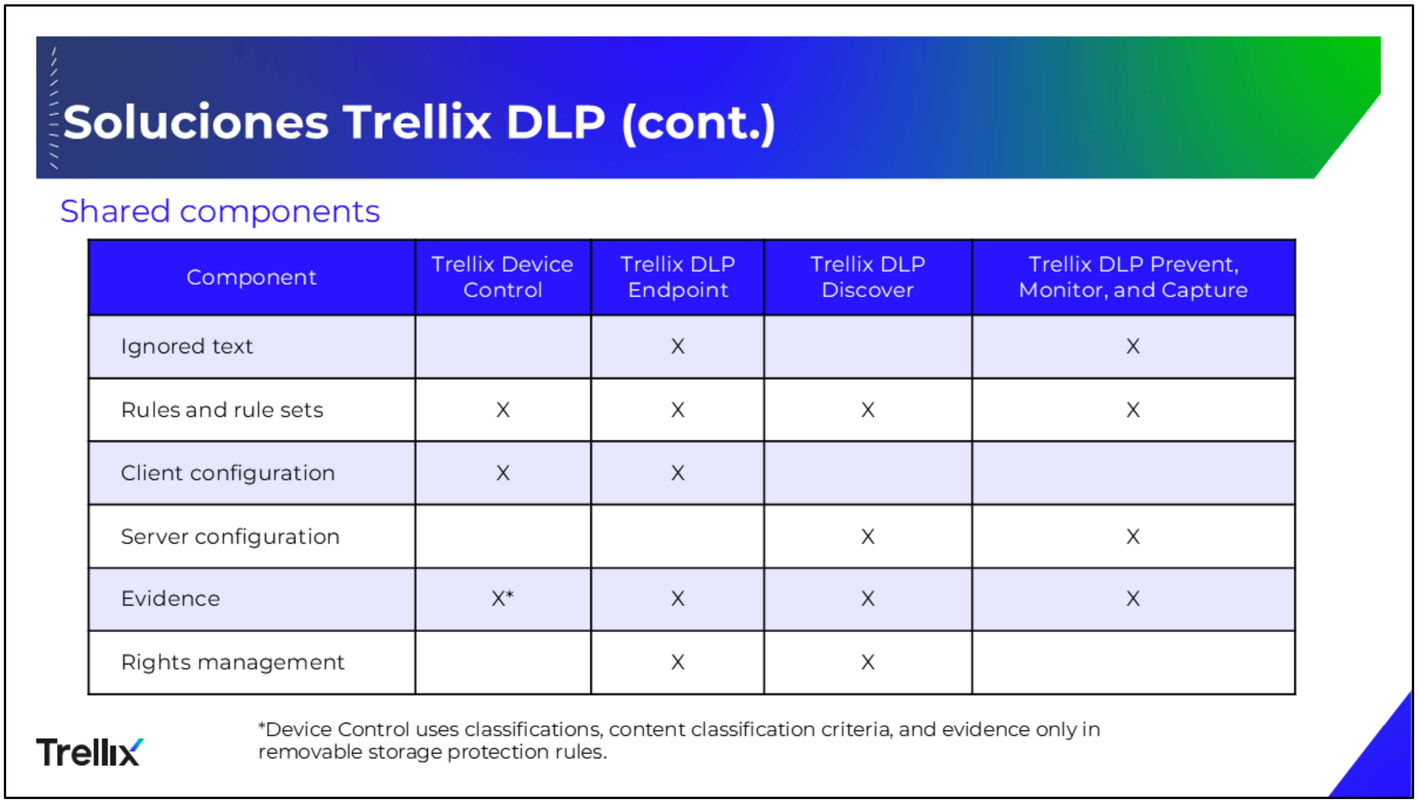
*Device Control uses classifications, content classification criteria, and evidence only in removable storage protection rules.

**Trellix DLP Discover, Monitor, Prevent, and Capture can analyze for manual classifications but can't assign manual classifications

- Continued -

The table shows components shared by all the Trellix DLP products.

Continued on the next page.

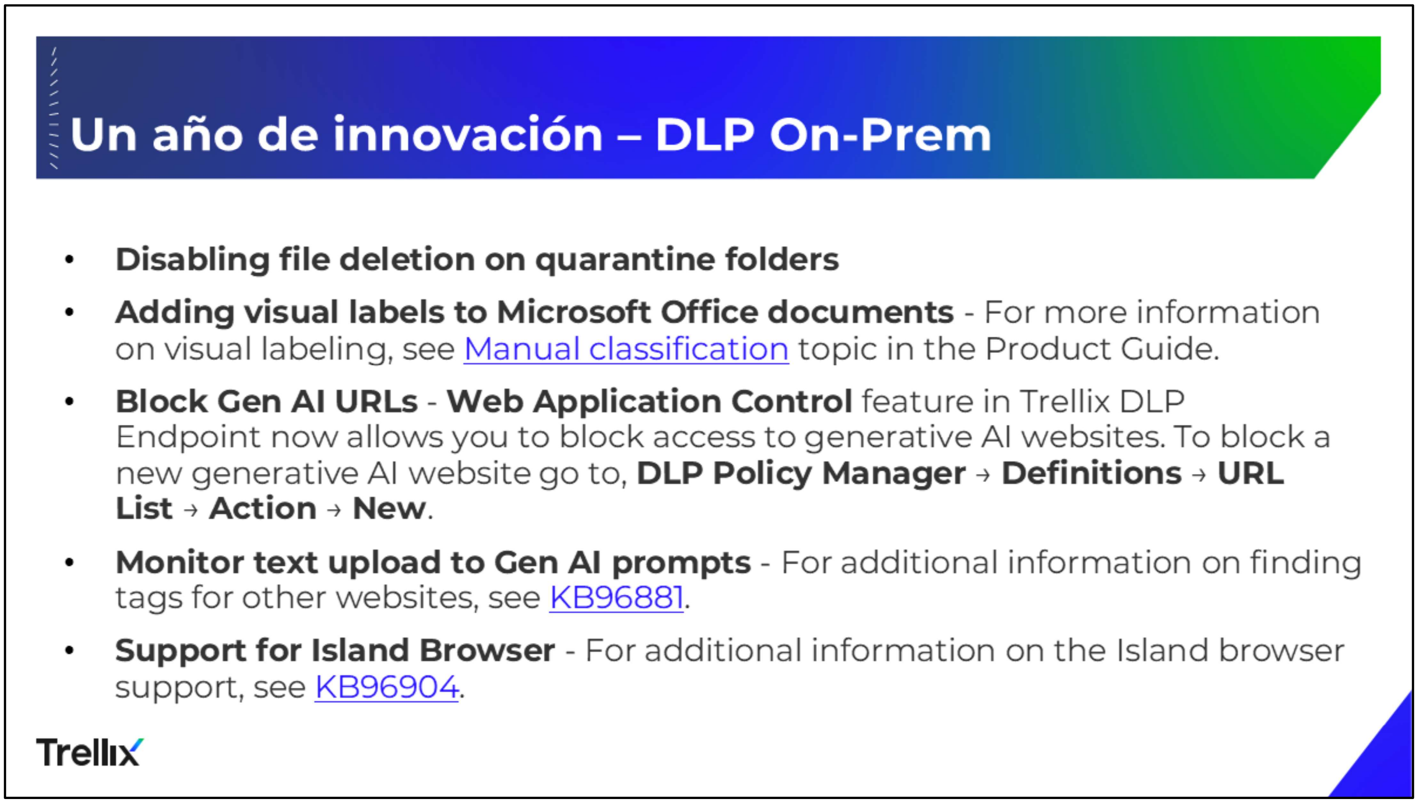


Soluciones Trellix DLP (cont.)

Shared components

Component	Trellix Device Control	Trellix DLP Endpoint	Trellix DLP Discover	Trellix DLP Prevent, Monitor, and Capture
Ignored text		X		X
Rules and rule sets	X	X	X	X
Client configuration	X	X		
Server configuration			X	X
Evidence	X*	X	X	X
Rights management		X	X	

*Device Control uses classifications, content classification criteria, and evidence only in removable storage protection rules.

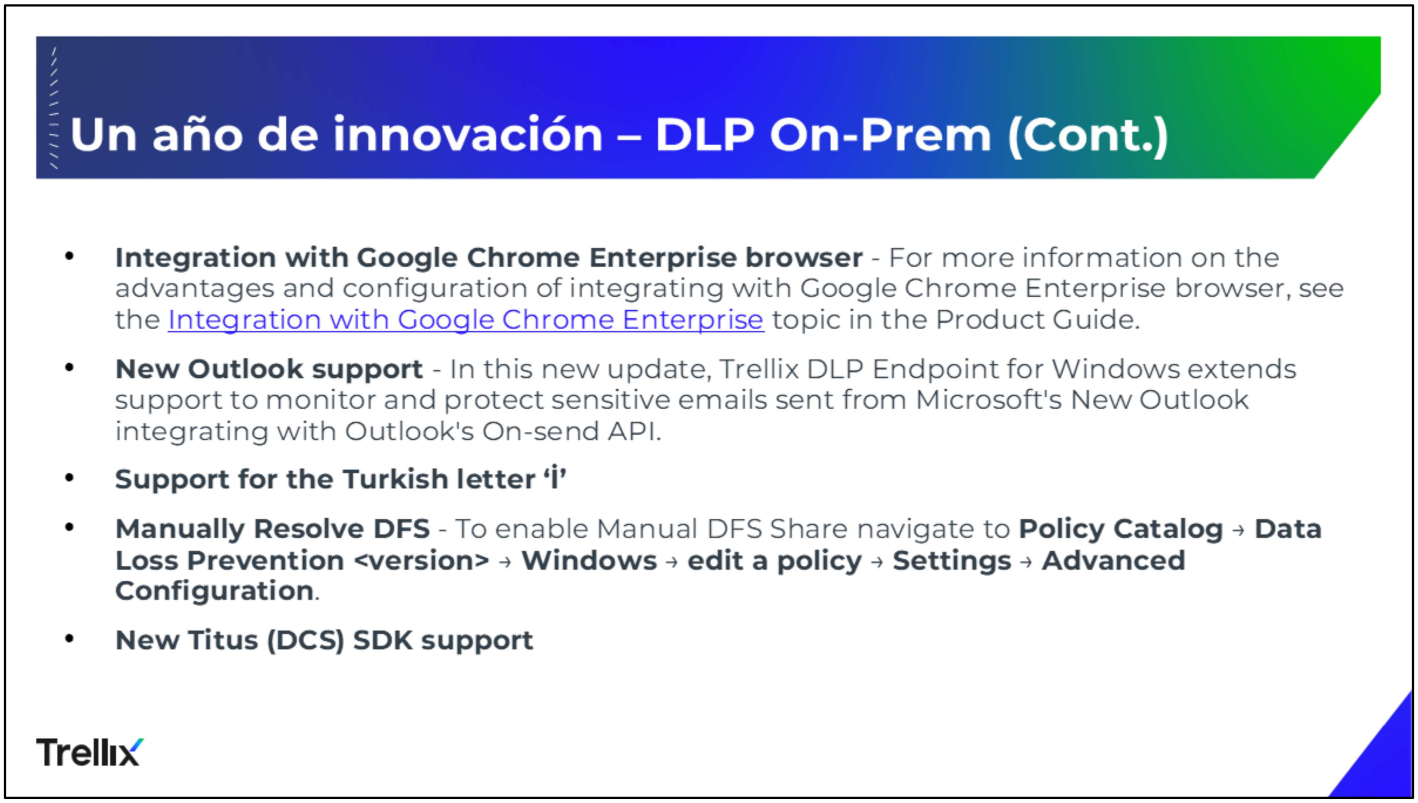


Un año de innovación – DLP On-Prem

- **Disabling file deletion on quarantine folders**
- **Adding visual labels to Microsoft Office documents** - For more information on visual labeling, see Manual classification topic in the Product Guide.
- **Block Gen AI URLs** - **Web Application Control** feature in Trellix DLP Endpoint now allows you to block access to generative AI websites. To block a new generative AI website go to, **DLP Policy Manager** → **Definitions** → **URL List** → **Action** → **New**.
- **Monitor text upload to Gen AI prompts** - For additional information on finding tags for other websites, see KB96881.
- **Support for Island Browser** - For additional information on the Island browser support, see KB96904.

- **Disabling file deletion on quarantine folders** - Trellix Data Loss Prevention extension is now enhanced with new functionality to prevent the automatic deletion of quarantine files based on time limits. This feature allows you to avoid the deletion of quarantine files in quarantine folders and achieve the goal of "never deleting the quarantine files". To prevent deletion of quarantine files go to, **Policy Catalog** → **Data Loss Prevention** → **Windows Client Configuration** → **Quarantine** and set the value of **Quarantine duration (Days)** to "0".
- **Adding visual labels to Microsoft Office documents** - Visual labeling is a document labeling solution for Microsoft Office documents (Word, Excel, and PowerPoint) that forces users to manually select the classification before saving a document. You can use this method to display visual labels in the header, footer, and watermark of the document as supported by Microsoft Office applications to identify its sensitivity and label the document without the use of third-party tools. For more information on visual labeling, see Manual classification topic in the Product Guide.
- **Block Gen AI URLs** - **Web Application Control** feature in Trellix DLP Endpoint now allows you to block access to generative AI websites. To block a new generative AI website go to, **DLP Policy Manager** → **Definitions** → **URL List** → **Action** → **New**.
- **Monitor text upload to Gen AI prompts** - In the web protection page, you can now add web URL tags in order to monitor text uploads to the generative AI website. As a result, corporate devices can be monitored in order to avoid sensitive data leak. For additional information on finding tags for other websites, see KB96881.

- **Support for Island Browser** - This beta release feature for Island browser supports the Web protection rules, Printer protection rules, Clipboard protection rules, and screen capture protection rules that monitor or protect the activities in Island browser. For additional information on the Island browser support, see KB96904.



Un año de innovación – DLP On-Prem (Cont.)

- **Integration with Google Chrome Enterprise browser** - For more information on the advantages and configuration of integrating with Google Chrome Enterprise browser, see the [Integration with Google Chrome Enterprise]() topic in the Product Guide.
- **New Outlook support** - In this new update, Trellix DLP Endpoint for Windows extends support to monitor and protect sensitive emails sent from Microsoft's New Outlook integrating with Outlook's On-send API.
- **Support for the Turkish letter 'İ'**
- **Manually Resolve DFS** - To enable Manual DFS Share navigate to **Policy Catalog** → **Data Loss Prevention <version>** → **Windows** → **edit a policy** → **Settings** → **Advanced Configuration**.
- **New Titus (DCS) SDK support**

Trellix

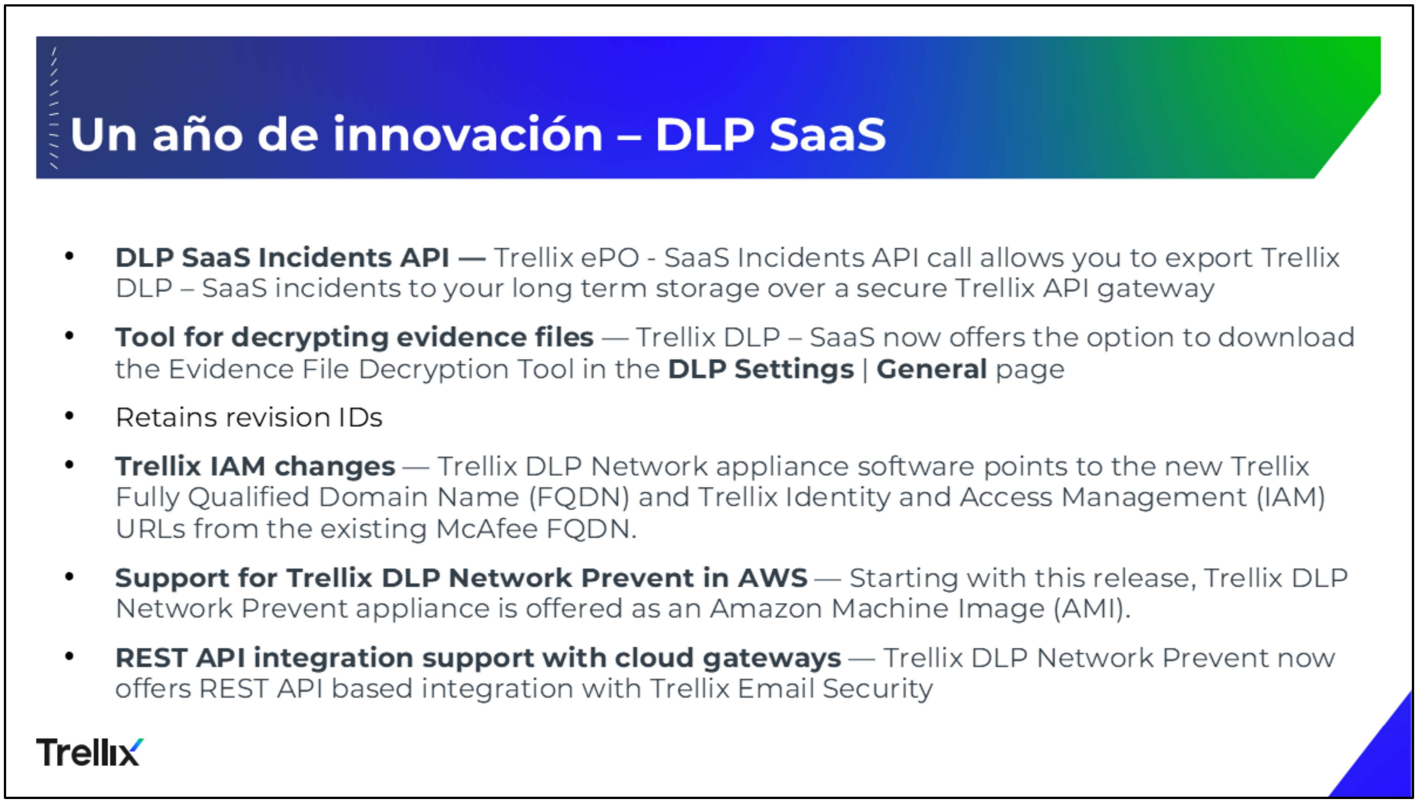
- **Integration with Google Chrome Enterprise browser** - Trellix DLP Endpoint for Windows can now be seamlessly integrated with Chrome Enterprise using the Content Analysis SDK in Chrome. This improves performance, security and enhanced browsing experience. For more information on the advantages and configuration of integrating with Google Chrome Enterprise browser, see the [Integration with Google Chrome Enterprise]() topic in the Product Guide.
- **New Outlook support** - In this new update, Trellix DLP Endpoint for Windows extends support to monitor and protect sensitive emails sent from Microsoft's New Outlook integrating with Outlook's On-send API.
- **Support for the Turkish letter 'İ'** - Trellix DLP Endpoint for Windows now supports Turkish characters with case insensitivity for dictionary and keyword. For example, when a classification is created using a keyword containing the uppercase letter "İ", Trellix DLP converts it to the lowercase letter "i" allowing the rule to trigger.
- **Note**
- Trellix DLP Endpoint can not convert to lowercase Turkish letter "ı" Ascii character code (305). However, you can create an entry in **Dictionary** tab for both "ı" Ascii character code (305) and "i" Ascii character code (105) or you can create an advance pattern to detect all "iıİ".
- **Manually Resolve DFS** - Using this option, you can manually resolve network share paths of all the child nodes of DFS shares and enter them individually in the network definitions. Alternatively, if you uncheck this option, Trellix DLP Endpoint resolves all child nodes' share paths of the DFS share paths mentioned in the network definition. To enable Manual DFS

Share navigate to **Policy Catalog** → **Data Loss Prevention <version>** → **Windows** → **edit a policy** → **Settings** → **Advanced Configuration**.

- **New Titus (DCS) SDK support** - Trellix DLP Endpoint for Windows now includes support for Fortra Data Classification Suite (DCS) SDK version 5.1.123, formerly known as Titus Classification SDK. This update enhances security and seamless integration capabilities by:
- Enabling Control-flow Enforcement Technology (CET) and Hardware-enforced Stack Protection (HSP).
- Ensuring integration is independent of any version of the Fortra Data Classification Suite (DCS) for Windows clients, formerly known as Titus Classification Client for windows.
- With this release, Trellix DLP Endpoint for Windows no longer supports previous versions of the Titus Client or SDK. We recommend you upgrade to the latest Titus Client and SDK versions to ensure continued compatibility and support.

Note

As a prerequisite, you must download and install Microsoft .NET 6.0.



Un año de innovación – DLP SaaS

- **DLP SaaS Incidents API —** Trellix ePO - SaaS Incidents API call allows you to export Trellix DLP – SaaS incidents to your long term storage over a secure Trellix API gateway
- **Tool for decrypting evidence files** — Trellix DLP – SaaS now offers the option to download the Evidence File Decryption Tool in the **DLP Settings** | **General** page
- Retains revision IDs
- **Trellix IAM changes** — Trellix DLP Network appliance software points to the new Trellix Fully Qualified Domain Name (FQDN) and Trellix Identity and Access Management (IAM) URLs from the existing McAfee FQDN.
- **Support for Trellix DLP Network Prevent in AWS** — Starting with this release, Trellix DLP Network Prevent appliance is offered as an Amazon Machine Image (AMI).
- **REST API integration support with cloud gateways** — Trellix DLP Network Prevent now offers REST API based integration with Trellix Email Security

Trellix

DLP SaaS Incidents API — Trellix ePO - SaaS Incidents API call allows you to export Trellix DLP – SaaS incidents to your long term storage over a secure Trellix API gateway. These APIs:

- Conform to JSON API standards that offers a secure interface.
- Provide visibility of DLP incidents in your existing third-party dashboard, reporting, or incident management tools.
- Enrich your threat event data from other sources with Trellix DLP – SaaS Indicators of Compromise (IoC).
- Help build automated workflows for case management.
- Provide long term retention of Trellix DLP – SaaS incidents outside of Trellix database.

Important

The existing DLP Events API (/epo/v2/events) will be deprecated by the end of 2024, and we recommend that you migrate to the new API (DLP SaaS Incidents API) before the end of Q3 2024. The DLP SaaS Incidents API provides these additional features:

- Increased retention period
- Improved filter capabilities, utilizing JSON:API
- Improved response body and additional attributes

For information about DLP SaaS Incident APIs, see DLP SaaS Incident API call to get incidents and for information about Trellix APIs, see Understanding Trellix API.

Tool for decrypting evidence files — Trellix DLP – SaaS now offers the option to download the Evidence File Decryption Tool in the **DLP Settings** | **General** page. The Evidence Decryption Tool is an offline command-line executable binary file that provides you the ability to decrypt evidence files independently. As this tool is specific to customer decryption configurations, it is downloaded as a password-protected zip file. Therefore, Trellix recommends that the tool be secured. For more information about the Evidence Decryption Tool, see Download Evidence File Decryption Tool.

Important

The Evidence File Decryption Tool is only available with the Trellix API Gateway license subscriptions.

Retains revision IDs - Policy revision IDs are now retained during a policy migration from Trellix DLP on-premises to Trellix DLP – SaaS.

Trellix IAM changes — Trellix DLP Network appliance software points to the new Trellix Fully Qualified Domain Name (FQDN) and Trellix Identity and Access Management (IAM) URLs from the existing McAfee FQDN. To ensure uninterrupted service to IAM, update your firewall settings to allow the https://iam.cloud.trellix.com URL. The https://iam.mcafee-cloud.com is now changed to https://iam.cloud.trellix.com. To migrate to new Trellix IAM domains, upgrade to Trellix DLP Network Appliances version 11.10.700. If you do not intend to upgrade to 11.10.700, see article 000013552 to migrate to the Trellix domain.

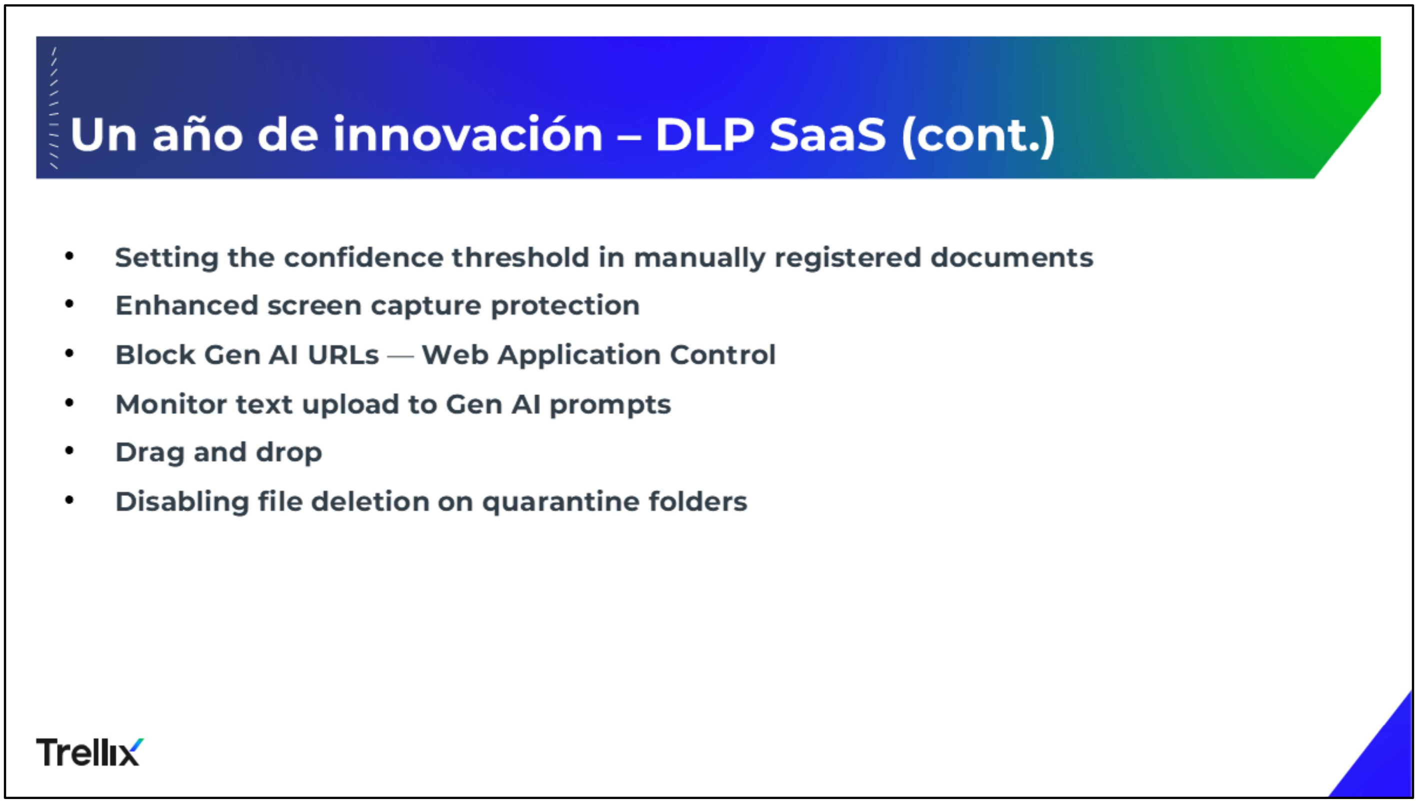
Support for Trellix DLP Network Prevent in AWS — Starting with this release, Trellix DLP Network Prevent appliance is offered as an Amazon Machine Image (AMI). This helps you deploy the appliance seamlessly on AWS EC2 instance, which can be integrated with cloud web or email gateways.

For information about deploying and installing the Trellix DLP Network Prevent - SaaS appliance in the AWS environment, see Deploy and install the Trellix DLP Network Prevent appliance in AWS using the .iso file and Deploy and install the Trellix DLP Network Prevent appliance using the Amazon Machine Image (AMI).

REST API integration support with cloud gateways — Trellix DLP Network Prevent now offers REST API based integration with Trellix Email Security - Cloud to scan outbound emails and enable Trellix Email Security - Cloud to take action based on the defined Trellix DLP policies. This API integration is also supported with other third party cloud gateways integration.

This provides seamless native integration with Trellix Email Security - Cloud and other cloud gateways without requiring to backhaul the traffic to on-prem appliances for inspection.

For more information, see Trellix DLP REST API integration with cloud gateways.



Un año de innovación – DLP SaaS (cont.)

- Setting the confidence threshold in manually registered documents
- Enhanced screen capture protection
- Block Gen AI URLs — Web Application Control
- Monitor text upload to Gen AI prompts
- Drag and drop
- Disabling file deletion on quarantine folders

Trellix

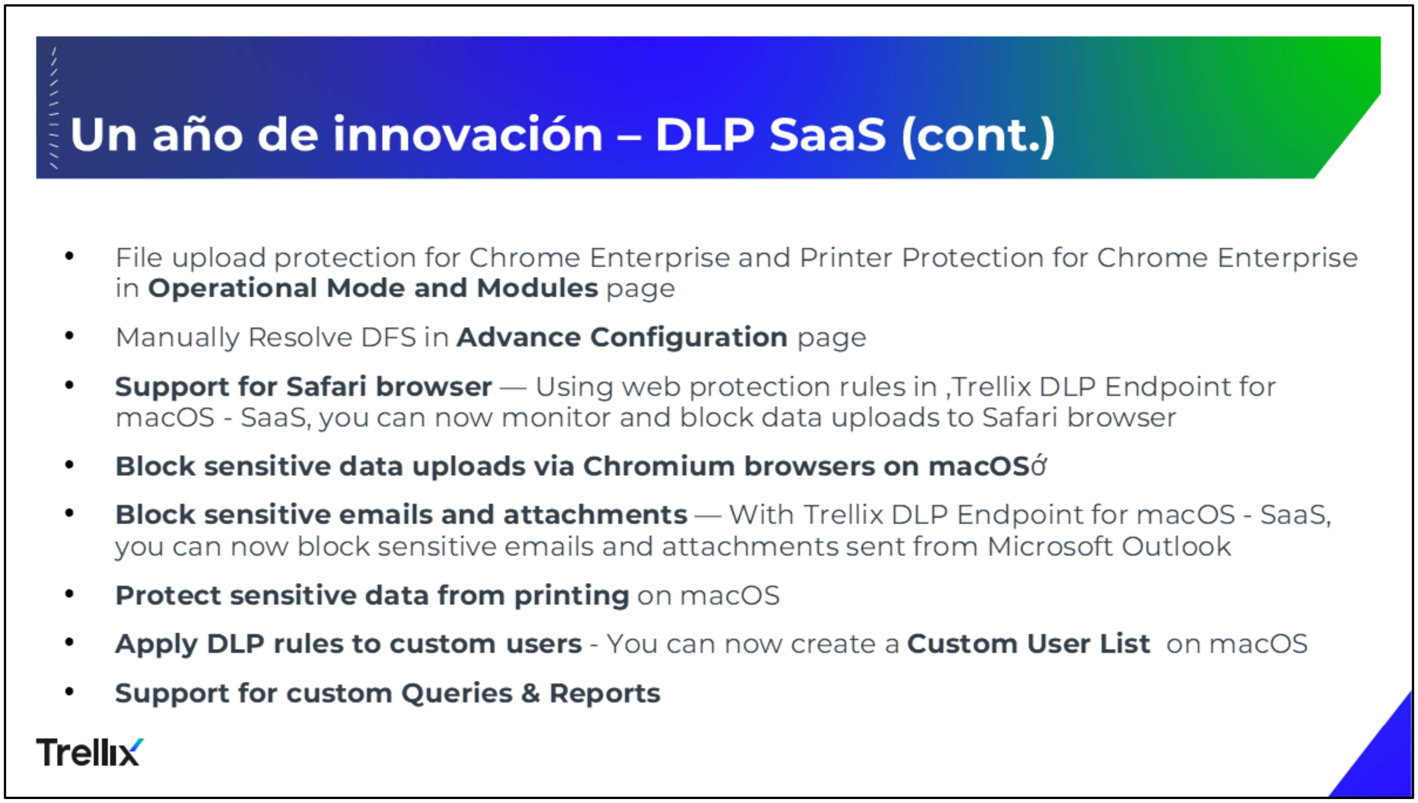
Trellix DLP Endpoint for Windows 11.10.200 or later supports the following features:

- **Setting the confidence threshold in manually registered documents** — Trellix Data Loss Prevention Discover and Trellix DLP – SaaS Network Appliances allow you to configure the number of fingerprints that must be matched in a manually fingerprinted document to trigger a violation. This helps in increasing the detection confidence as it minimizes false positives by triggering more accurate detections and reduces the analysis time. An incident is triggered when the number of matches is equal to or higher than the set confidence threshold. You can set the Confidence Threshold percentage between 10 to 100 percent. For example, if a fingerprinted document generates 100 signatures, and if you select 10%, then 10 signatures are matched at random in the scanned document. To set the threshold percentage go to, **Classification** → **Registered Documents** → **Manual Registration** → **Confidence Threshold**.
- **Enhanced screen capture protection** — Screen capture actions performed using Universal Windows Platform apps, such as Snip & Sketch are now protected by Trellix DLP Endpoint for Windows - SaaS.

Note

In Microsoft Windows 11, Trellix DLP Endpoint for Windows - SaaS only supports data protection with the snip option. However, it does not provide data protection if the screen is recorded.

- **Block Gen AI URLs** — **Web Application Control** feature in Trellix DLP Endpoint for Windows - SaaS now allows you to block access to generative AI websites.
- To block a new generative AI website go to **DLP Policy Manager** → **Definitions** → **URL List** → **Action** → **New**.
- **Monitor text upload to Gen AI prompts** — In the **Web Protection** page, you can now add web URL tags in order to monitor text uploads to the generative AI website. As a result, corporate devices can be monitored in order to avoid sensitive data leaks. For additional information on finding tags for other websites, see article 000012846.
- **Drag and drop** — This release provides an option in the **Web Protection** page to optionally disable drag and drop of attachments from Microsoft Outlook into supported Chromium browsers.
- **Disabling file deletion on quarantine folders** — Trellix DLP – SaaS extension is now enhanced with new functionality to prevent the automatic deletion of quarantine files based on time limits. This feature allows you to avoid the deletion of quarantine files in quarantine folders and achieve the goal of "never deleting the quarantine files".
- To prevent deletion of quarantine files go to **Policy Catalog** → **Data Loss Prevention** → **Windows Client Configuration** → **Quarantine** and set the value of **Quarantine duration (Days)** to "0".



Un año de innovación – DLP SaaS (cont.)

- File upload protection for Chrome Enterprise and Printer Protection for Chrome Enterprise in **Operational Mode and Modules** page
- Manually Resolve DFS in **Advance Configuration** page
- **Support for Safari browser** — Using web protection rules in ,Trellix DLP Endpoint for macOS - SaaS, you can now monitor and block data uploads to Safari browser
- **Block sensitive data uploads via Chromium browsers on macOS**ớ
- **Block sensitive emails and attachments** — With Trellix DLP Endpoint for macOS - SaaS, you can now block sensitive emails and attachments sent from Microsoft Outlook
- **Protect sensitive data from printing** on macOS
- **Apply DLP rules to custom users** - You can now create a **Custom User List** on macOS
- **Support for custom Queries & Reports**

Trellix DLP Endpoint for Windows 11.11.0 or later supports the following features:
The user interface in Trellix DLP – SaaS 2408 version shows the following features that will be available for use in the next release of Trellix DLP Endpoint for Windows - SaaS:

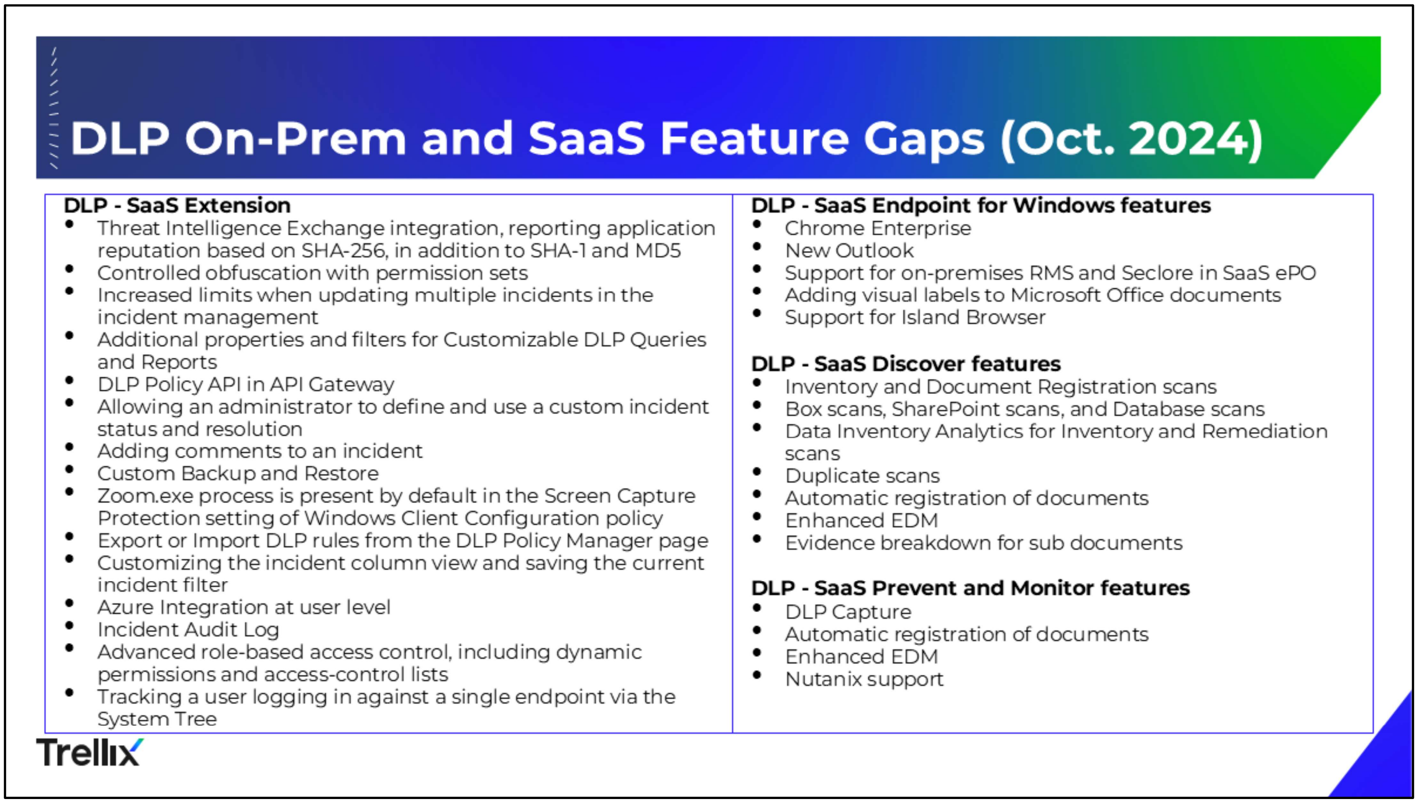
- File upload protection for Chrome Enterprise and Printer Protection for Chrome Enterprise in **Operational Mode and Modules** page.
- Manually Resolve DFS in **Advance Configuration** page.
- Citrix Studio configuration in **Device Control** page.

Trellix DLP Endpoint for macOS 11.10.100 and above supports the following features:

- **Support for Safari browser** — Using web protection rules in ,Trellix DLP Endpoint for macOS - SaaS, you can now monitor and block data uploads to Safari browser.
- **Block sensitive data uploads via Chromium browsers** — Using web protection rules in Trellix DLP Endpoint for macOS - SaaS, you can now block data uploads to Google Chrome and Microsoft Edge browsers.
- For more information about how to deploy Trellix DLP web protection extension on browsers using mobile config, see article 000013383.
- **Block sensitive emails and attachments** — With Trellix DLP Endpoint for macOS - SaaS, you can now block sensitive emails and attachments sent from Microsoft Outlook.
- **Protect sensitive data from printing** - By using printer protection rules, you can now monitor and block confidential documents from being printed on both local and network printers. For more information on Privacy Preferences Policy Control for printer protection, see KB91109.
- **Apply DLP rules to custom users** - You can now create a **Custom User List** in **DLP Policy Manager** → **Definitions** page. Using the **Policy Catalog** → **DLP Rule Set**, you can now apply **Data Protection** and **Device Control** rules to local users by selecting **belongs to one of the Custom User List** in the **Conditions** → **and End-User** field.
- **Note**
- **belongs to one of the Custom User List** option is not available for email protection rules.

Trellix DLP – SaaS extension supports the following features:

- **Support for custom Queries & Reports** — Create custom queries and generate reports for the following types of events:
- DLP Computer Policies
- DLP Computer Properties
- DLP Discover Scans
- DLP Endpoint Installed version summary
- DLP Operational Events



DLP On-Prem and SaaS Feature Gaps (Oct. 2024)

DLP - SaaS Extension

- Threat Intelligence Exchange integration, reporting application reputation based on SHA-256, in addition to SHA-1 and MD5
- Controlled obfuscation with permission sets
- Increased limits when updating multiple incidents in the incident management
- Additional properties and filters for Customizable DLP Queries and Reports
- DLP Policy API in API Gateway
- Allowing an administrator to define and use a custom incident status and resolution
- Adding comments to an incident
- Custom Backup and Restore
- Zoom.exe process is present by default in the Screen Capture Protection setting of Windows Client Configuration policy
- Export or Import DLP rules from the DLP Policy Manager page
- Customizing the incident column view and saving the current incident filter
- Azure Integration at user level
- Incident Audit Log
- Advanced role-based access control, including dynamic permissions and access-control lists
- Tracking a user logging in against a single endpoint via the System Tree

DLP - SaaS Endpoint for Windows features

- Chrome Enterprise
- New Outlook
- Support for on-premises RMS and Seclore in SaaS ePO
- Adding visual labels to Microsoft Office documents
- Support for Island Browser

DLP - SaaS Discover features

- Inventory and Document Registration scans
- Box scans, SharePoint scans, and Database scans
- Data Inventory Analytics for Inventory and Remediation scans
- Duplicate scans
- Automatic registration of documents
- Enhanced EDM
- Evidence breakdown for sub documents

DLP - SaaS Prevent and Monitor features

- DLP Capture
- Automatic registration of documents
- Enhanced EDM
- Nutanix support

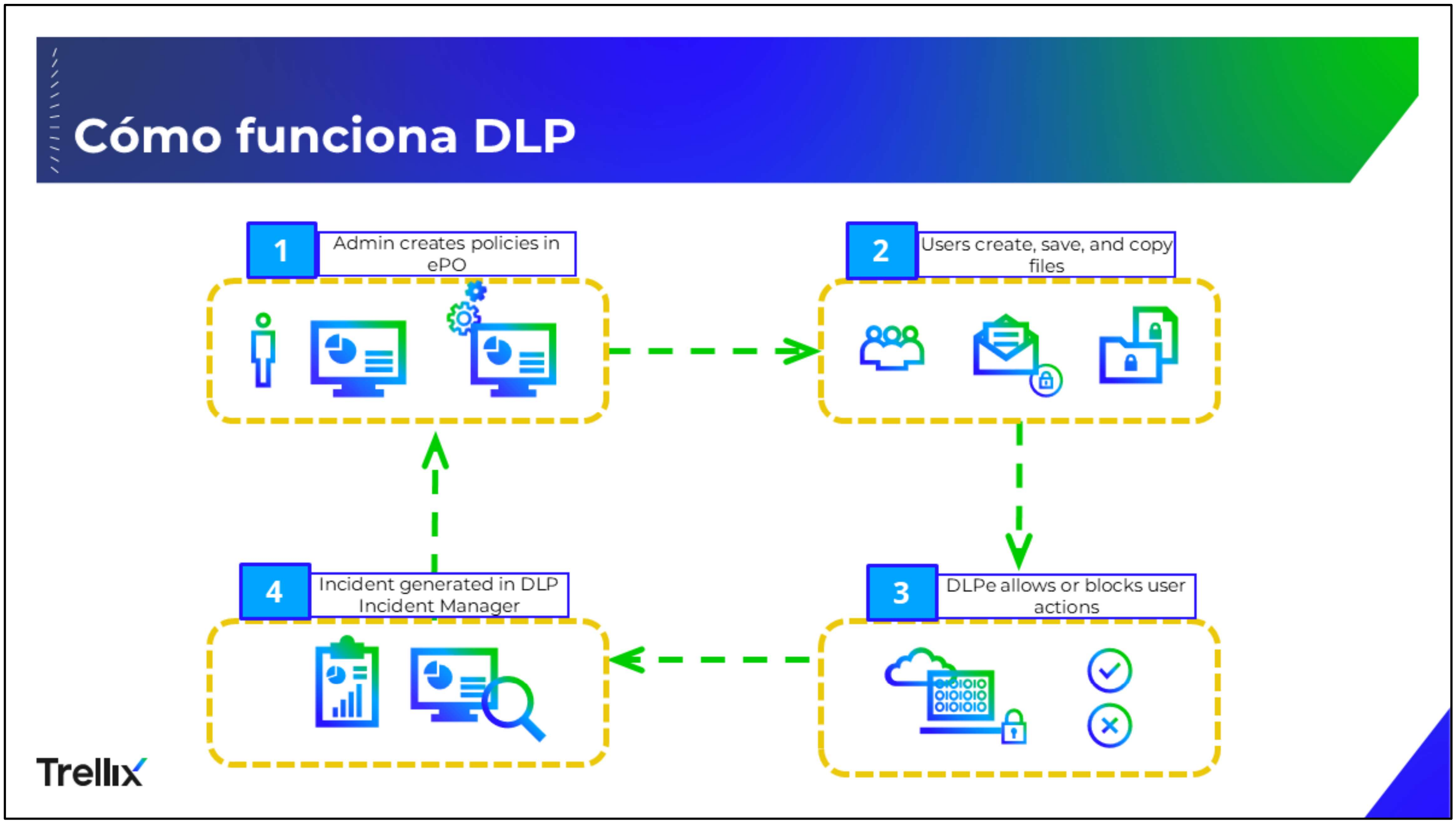
Trellix

- For up to date information visit https://thrive.trellix.com/s/article/KB94965

Trellix

Fundamentos de DLP

Revisar lo básico



Cómo funciona DLP

1 Admin creates policies in ePO

2 Users create, save, and copy files

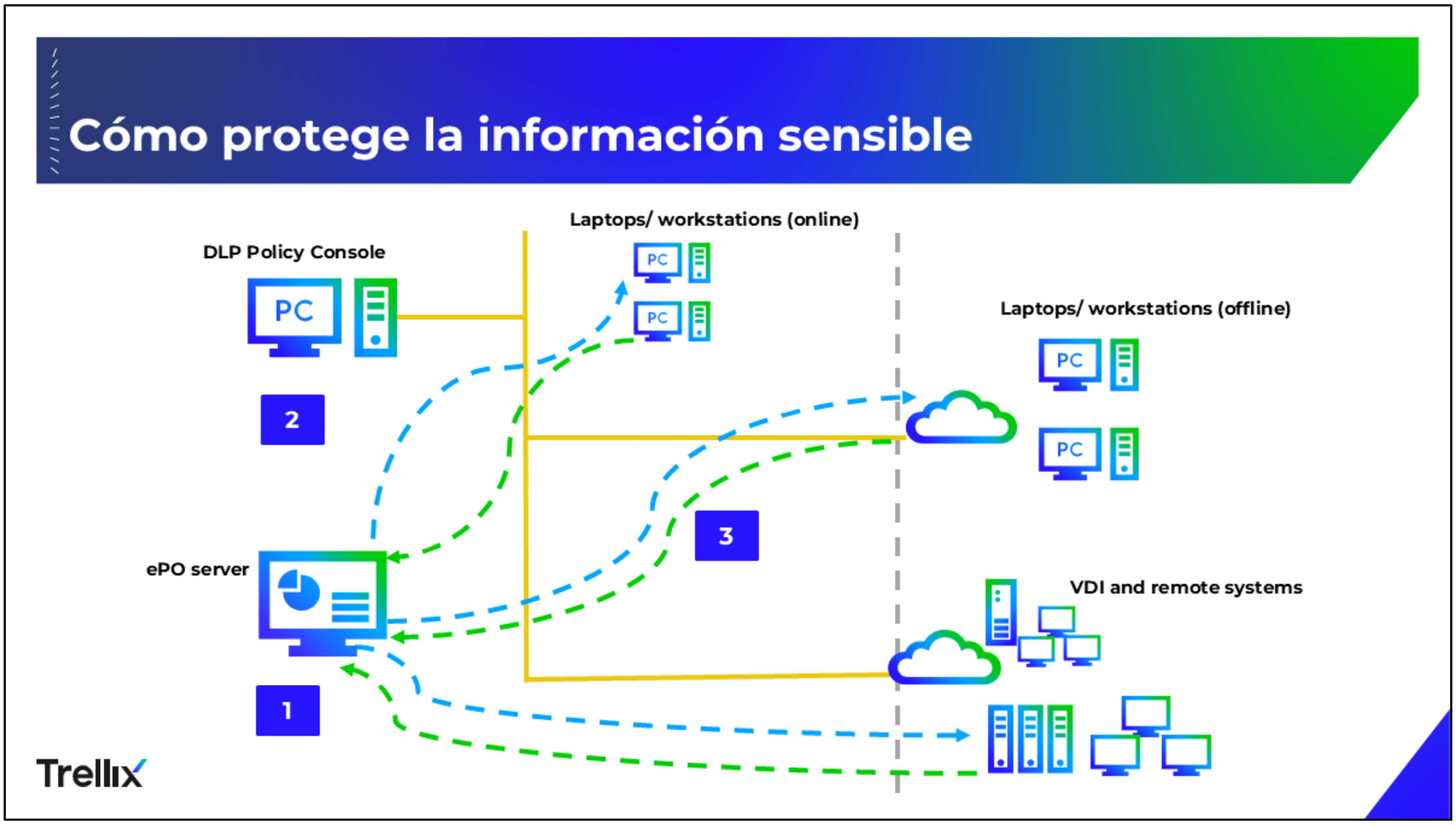
3 DLPe allows or blocks user actions

4 Incident generated in DLP Incident Manager

Trellix

DLP Endpoint identifies sensitive data or user activity, take action on policy violations, and create incidents of violations.

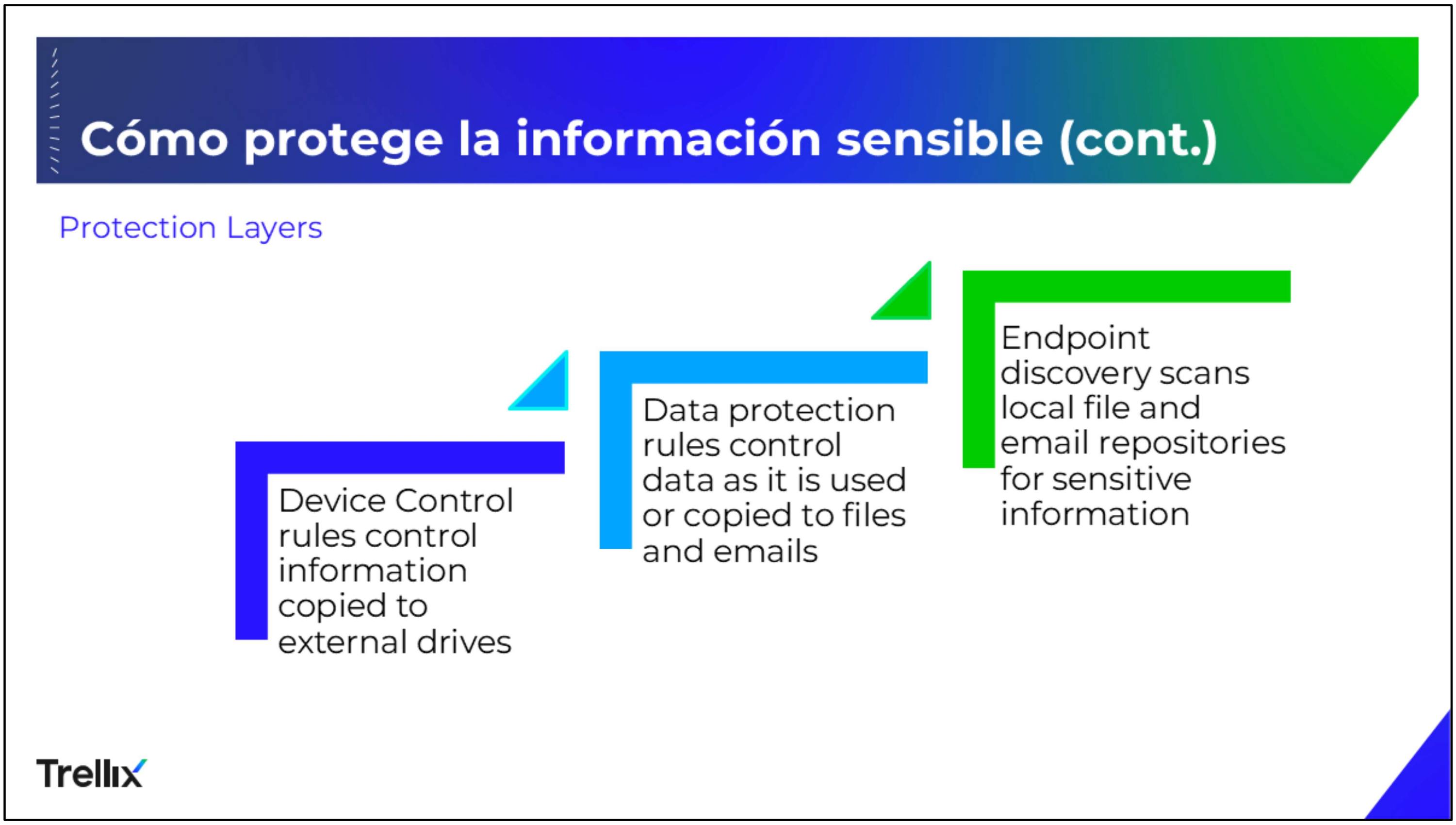
- The diagram shows a simplified network of DLP Endpoint.
  1. Administrators create policies in ePO and deploy them to DLP Endpoint.
  2. Users create, save, and copy files or emails.
  3. DLP Endpoint client applies policies and either blocks or allows user actions.
  4. Applying the policies creates incidents that are sent to **DLP Incident Manager** in ePO for reporting and analysis.



Cómo protege la información sensible

Device Control controls sensitive content copied to removable devices. DLP Endpoint also inspects enterprise users' actions on sensitive content when emailing, using cloud applications, and posting to websites or network shares. The DLP Endpoint client software is deployed as a Trellix Agent plug-in, and enforces the policies defined in the DLP policy. It audits user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data and generates *events* recorded by the ePO Event Parser. Events generated by the DLP Endpoint client software are sent to the ePO Event Parser and recorded in tables in the ePO database. Events are stored in the database for further analysis and used by other system components.

1. Create policies consisting of definitions, classifications, and rule sets (groups of Device Control, Data Protection, and Discovery rules) in the DLP Policy Manager and Classification consoles in ePO.
2. Deploy the policies to the endpoints.
3. Collect incidents from the endpoints for monitoring and reporting.



Cómo protege la información sensible (cont.)

Protection Layers

Device Control rules control information copied to external drives

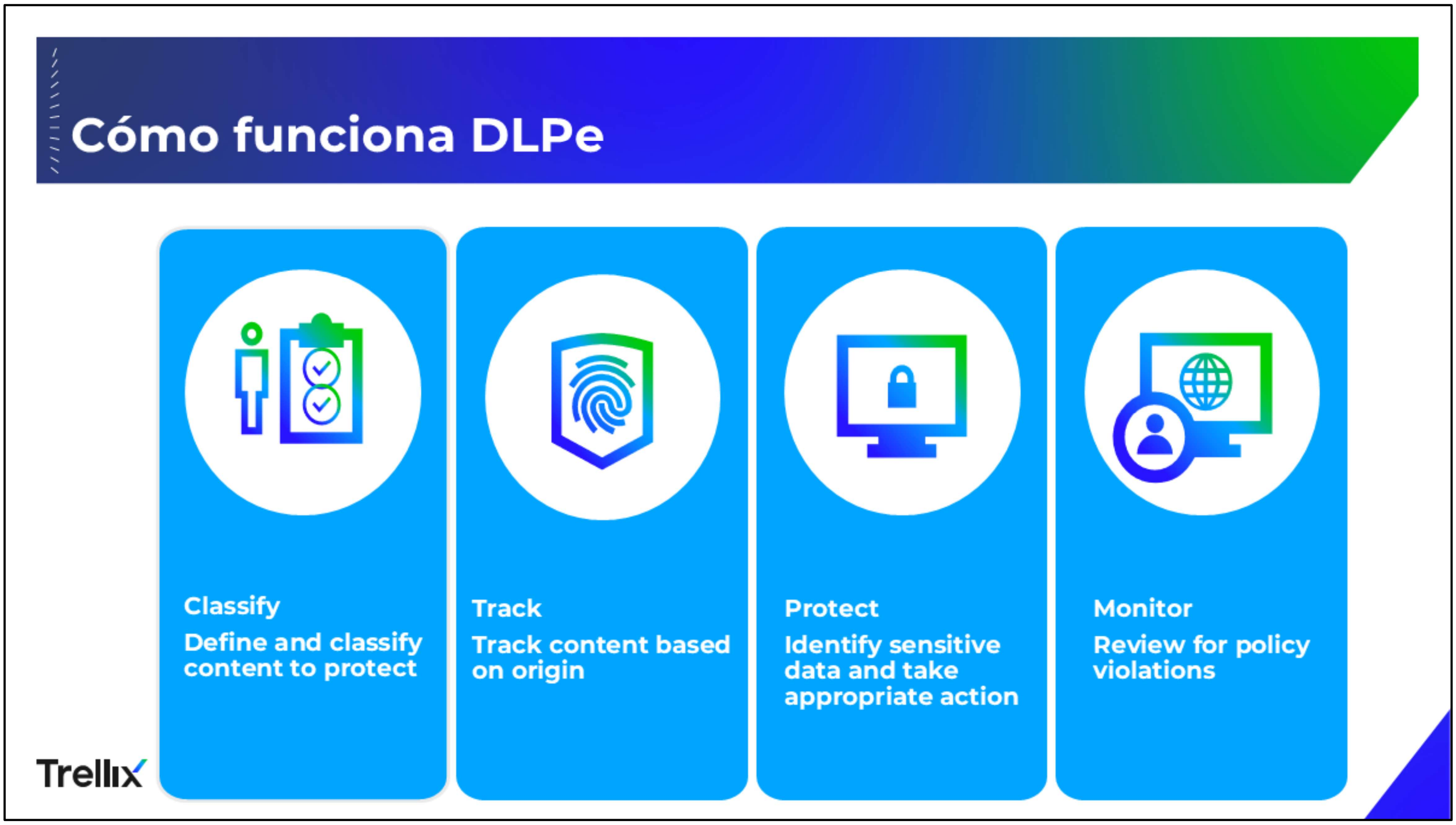
Data protection rules control data as it is used or copied to files and emails

Endpoint discovery scans local file and email repositories for sensitive information

DLP Endpoint client software is deployed as the Trellix Agent plug-in, and enforces the policies defined in the DLP Endpoint policy. It audits user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data and generates events recorded by the ePO Event Parser. Events are stored in a cloud container for further analysis and used by other system components.

DLP Endpoint for Windows safeguards sensitive enterprise information using three layers of protection:

1. Device Control rules control information copied to external drives.
2. Data protection rules control data as it is used or copied to files and emails.
3. Endpoint discovery scans local file and email repositories for sensitive information.



Cómo funciona DLPe

Classify

Define and classify content to protect

Track

Track content based on origin

Protect

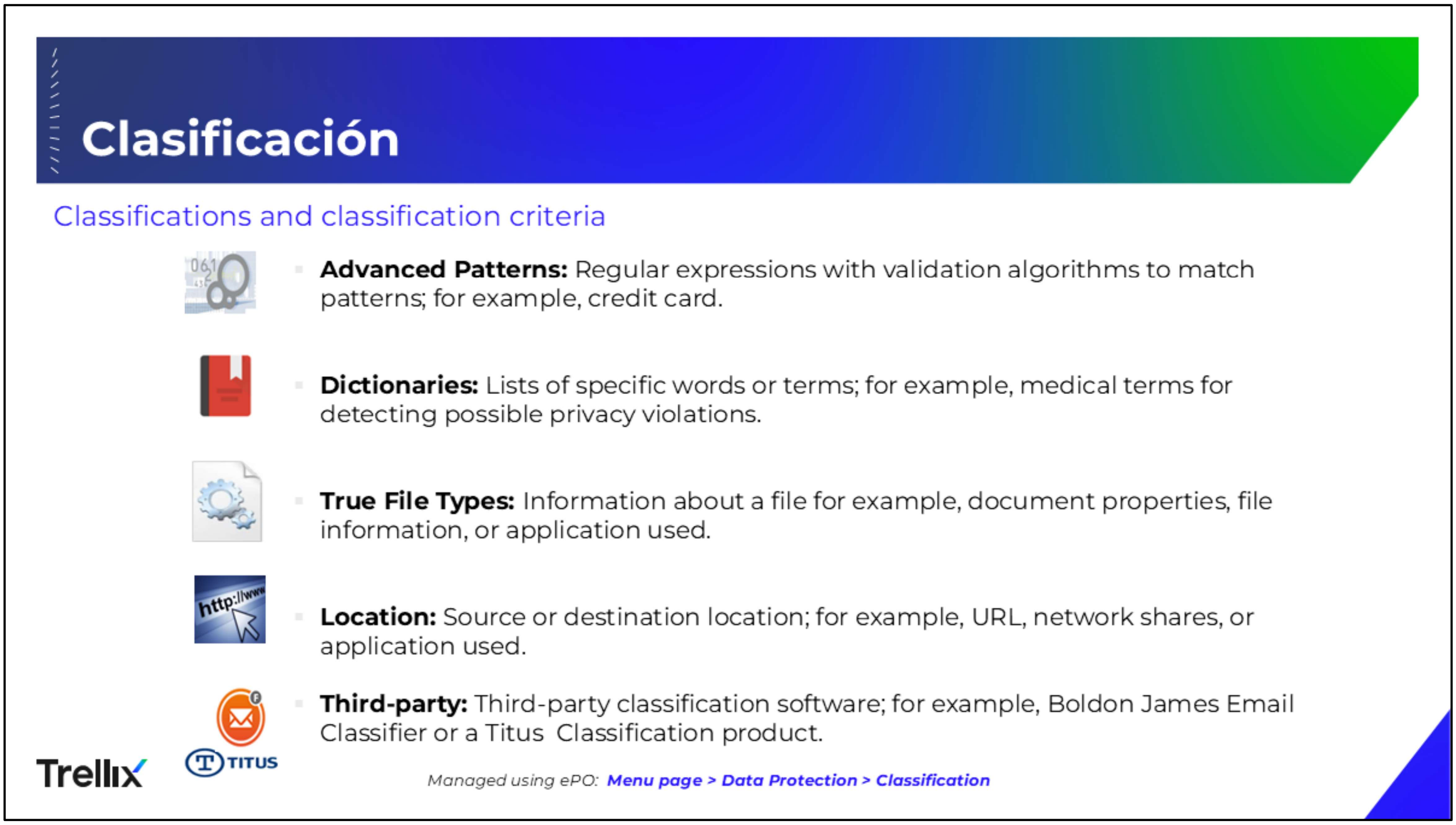
Identify sensitive data and take appropriate action

Monitor

Review for policy violations

Trellix

DLPe safeguards sensitive content using a comprehensive protection process: **Classify, Track, Protect, and Monitor.** Each process is discussed in more detail in the following sections.



Clasificación

Classifications and classification criteria

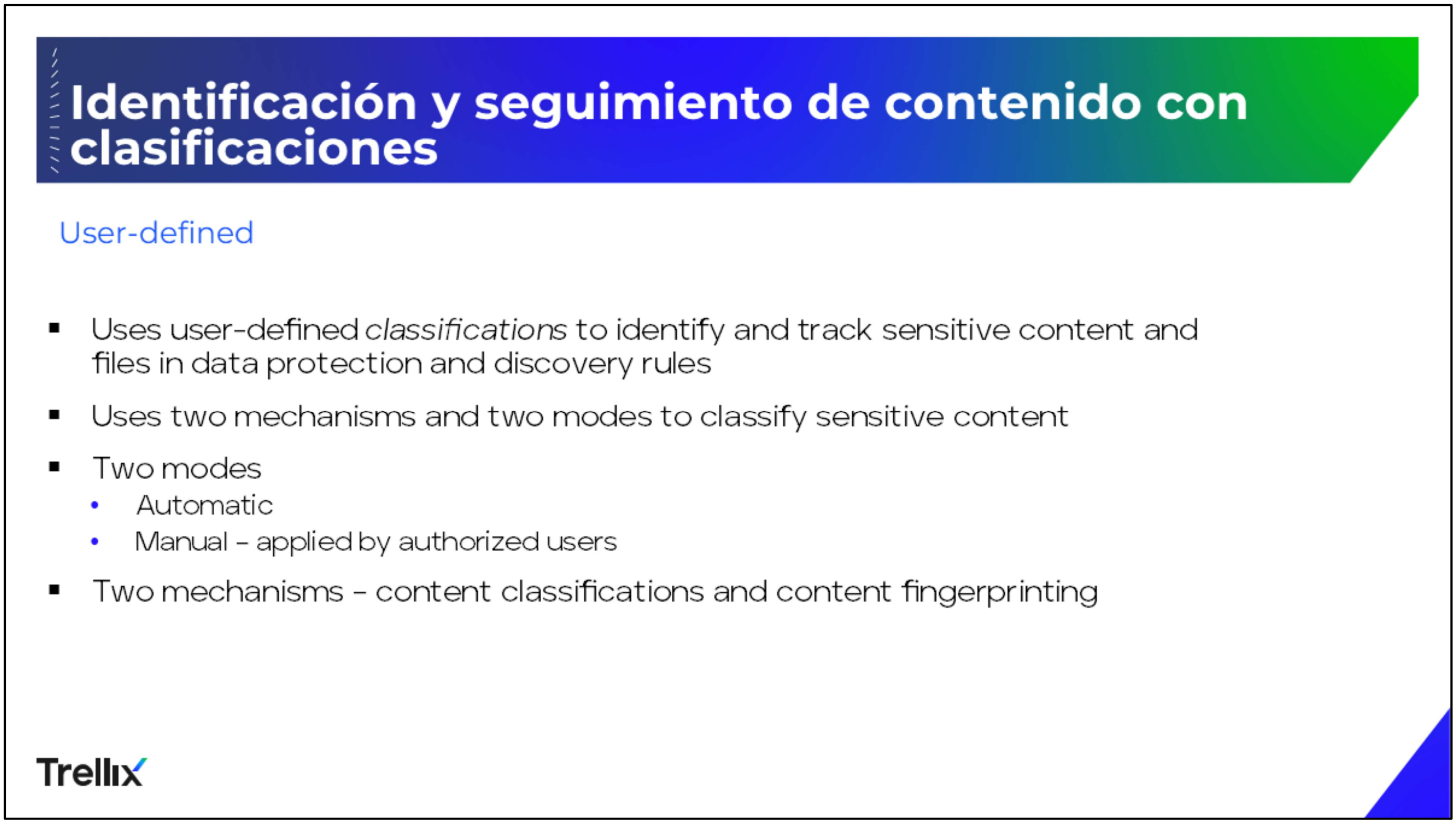
- **Advanced Patterns:** Regular expressions with validation algorithms to match patterns; for example, credit card.
- **Dictionaries:** Lists of specific words or terms; for example, medical terms for detecting possible privacy violations.
- **True File Types:** Information about a file for example, document properties, file information, or application used.
- **Location:** Source or destination location; for example, URL, network shares, or application used.
- **Third-party:** Third-party classification software; for example, Boldon James Email Classifier or a Titus Classification product.

Managed using ePO: ***Menu page > Data Protection > Classification***

Trellix

To protect sensitive content, start by defining and classifying sensitive information to be protected. Content is classified by defining classifications and classification criteria.

Classification criteria defines the conditions on how data is classified.



Identificación y seguimiento de contenido con clasificaciones

User-defined

- Uses user-defined *classifications* to identify and track sensitive content and files in data protection and discovery rules
- Uses two mechanisms and two modes to classify sensitive content
- Two modes
  - Automatic
  - Manual – applied by authorized users
- Two mechanisms – content classifications and content fingerprinting

Trellix

Identifying and tracking content with classifications

Trellix DLP uses user-defined *classifications* to identify and track sensitive content and files in data protection and discovery rules.

Trellix DLP uses two mechanisms and two modes to classify sensitive content.

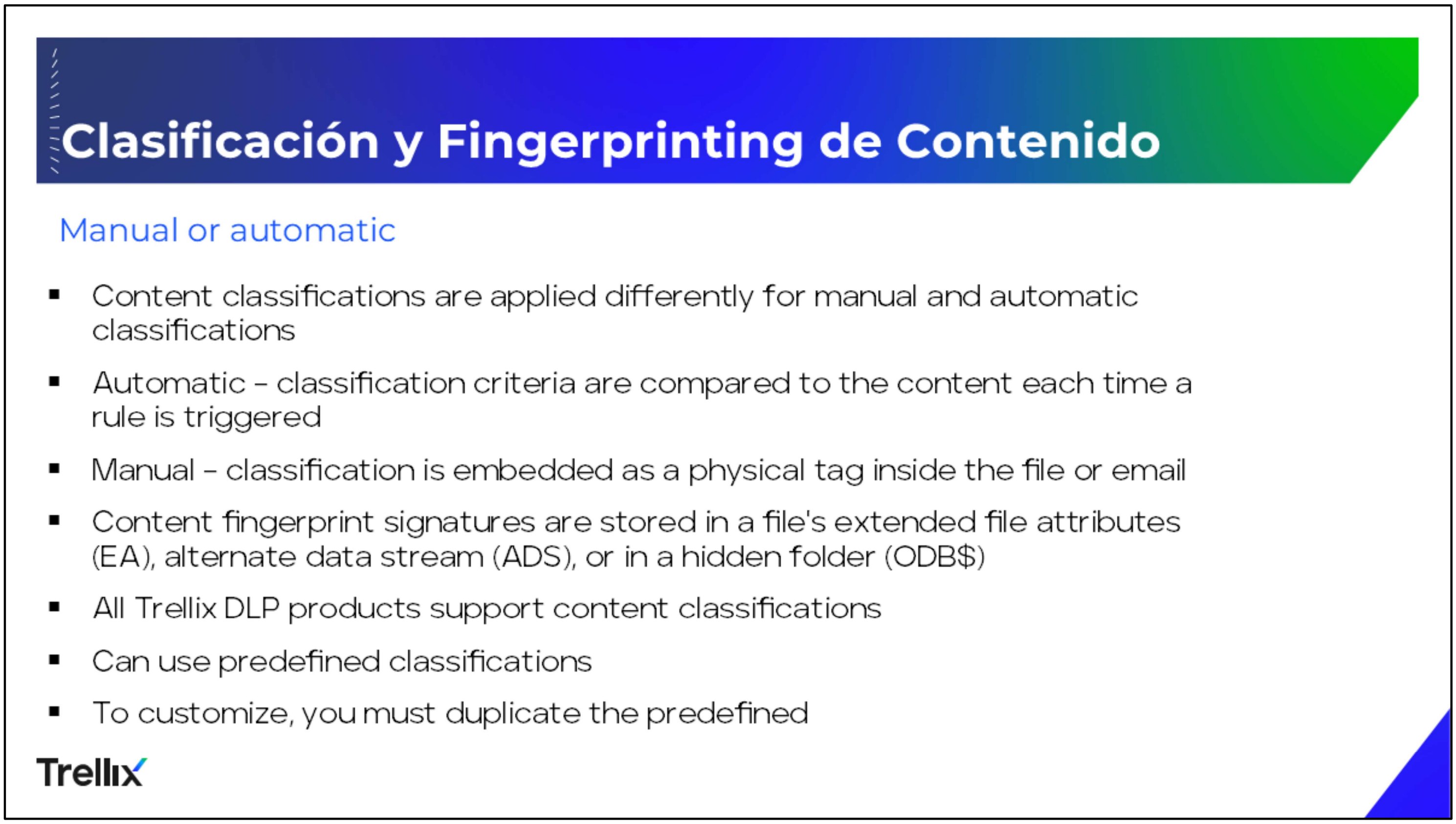
The two modes are automatic and manual classification.

- Automatic classifications are defined in Trellix DLP and distributed by Trellix ePO - On-prem in the deployed policies. They can then be applied to content with data protection rules or discovery rules.
- Manual classifications are applied by authorized users to files and emails on their computers. The manual classification dialog is supported on Trellix DLP Endpoint for Windows and Trellix DLP Endpoint for Mac.

NOTE: Trellix DLP Prevent and Trellix DLP Monitor can enforce data protection rules based on manual classifications, but cannot set or view them.

The two mechanisms are content classifications and content fingerprinting.

NOTE: Trellix DLP Endpoint only supports content classifications.



Clasificación y Fingerprinting de Contenido

Manual or automatic

- Content classifications are applied differently for manual and automatic classifications
- Automatic – classification criteria are compared to the content each time a rule is triggered
- Manual – classification is embedded as a physical tag inside the file or email
- Content fingerprint signatures are stored in a file's extended file attributes (EA), alternate data stream (ADS), or in a hidden folder (ODB$)
- All Trellix DLP products support content classifications
- Can use predefined classifications
- To customize, you must duplicate the predefined

Trellix

Content classifications are applied differently for manual and automatic classifications

- For automatic classification, the classification criteria are compared to the content each time a rule is triggered.
- For manual classification, the classification is embedded as a physical tag inside the file or email.
- Content fingerprint signatures are stored in a file's extended file attributes (EA), alternate data stream (ADS), or in a hidden folder (ODB$).
- All Trellix DLP products support content classifications, that is, can apply them by assigning them to data protection or discovery rules.
- On deployment, Trellix DLP displays many predefined classifications. Predefined classifications include, amongst others, classifications for personal data specific to different European Union countries, that can be used for detection accuracy, specifically when scanning for personal data for European Union Citizens.
- You can use predefined classifications as is in protection rules, but if you want to customize a classification you must duplicate it first. The classifications reduce false positives.

Fingerprinting Criteria provides another method for classifying content. It is primarily used when a pattern is not readily available.

The types of fingerprinting are:

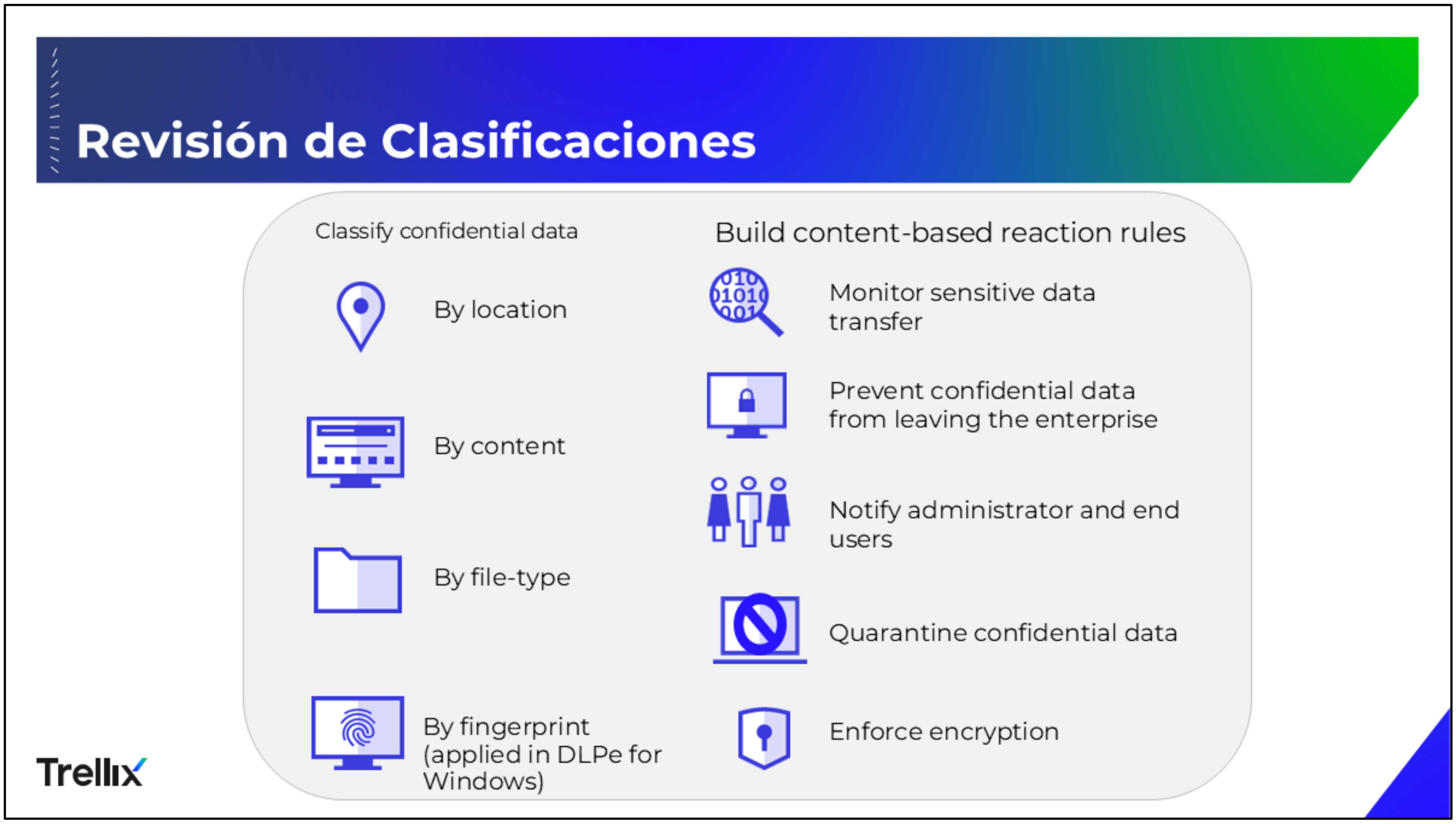
- **Application-based Fingerprinting:** Use application-based fingerprinting to physically fingerprint files created by a specific application.
- **Box-based Fingerprinting:** Add box content fingerprinting criteria
- **Location-based Fingerprinting:** Use location-based fingerprinting to assign physically fingerprinted files opened (or downloaded) from a specified network shares (UNC).
- **SharePoint-based Fingerprinting:** Define and add SharePoint content fingerprinting criteria
- **Web Application-based Fingerprinting:** Use web application-based fingerprinting to physically fingerprint to files opened (or downloaded) from a specified web addresses (URL). Fingerprinting criteria are stored in a file's extended file attributes (EA) or alternate data streams (ADS) and are applied to a file when the file is saved. If a user copies or moves fingerprinted content to another file, the fingerprinting criteria are applied to that file. If the fingerprinted content is removed from the file, the fingerprinting criteria are also removed.

  Note: DLP Endpoint applies fingerprinting criteria to files after a policy is applied regardless of whether the classification is used in a protection rule or not.

  Content fingerprinting is a content tracking technique unique to the DLPe product. The administrator creates a set of content fingerprinting criteria that define either the file location or the application used to access the file, and the classification to place on the files. The DLPe client tracks any file that is opened from the locations, or by the applications, defined in the content fingerprinting criteria and creates fingerprint signatures of these files in real time when the files are accessed. It then uses these signatures to track the files or fragments of the files. Content fingerprinting criteria can be defined by application, UNC path (location), or URL (web application).

Persistent fingerprinting maintains fingerprints as content travels from one computer to another inside the organization provided that the endpoint client is installed. Content fingerprint signatures are stored in a file's extended file attributes (EA) or alternate data streams (ADS). When such files are accessed, DLP Endpoint software tracks data transformations and maintains the classification of the sensitive content persistently, regardless of how it is being used. For example, if a user opens a fingerprinted Word document, copies a few paragraphs of it into a text file, and attaches the text file to an email message, the outgoing message has the same signatures as the original document.

When uploading fingerprinted content to file servers, two different strategies are used to preserve fingerprints for NTFS and non-NTFS servers.
Note: The DLPe client must be installed on both the sending and receiving computers to prevent the file from leaving the organization, as shown in the figures on the following slides. Fingerprints are lost when an encrypted file is opened and then saved again. Fingerprints are not preserved for files that are extracted from fingerprinted, password protected, compressed folders.



Revisión de Clasificaciones

Classify confidential data

- By location
- By content
- By file-type
- By fingerprint (applied in DLPe for Windows)

Build content-based reaction rules

- Monitor sensitive data transfer
- Prevent confidential data from leaving the enterprise
- Notify administrator and end users
- Quarantine confidential data
- Enforce encryption

The Classification module stores content classification and fingerprinting criteria, and the definitions used to configure them. Some key features are:

Confidential data classification:

- Classify by location (file server, shared drives, etc.).
- Classify by content characteristics (keywords, advanced pattern, even setting of thresholds; for example, if more than five credit card numbers in an email.
- Classify by file-type, specifically if a specific application generated data; for example, Systems, Applications and Products (SAP) BusinessObjects.
- Classify by fingerprint (unique digital signature, hash) – Applied in Data Loss Prevention Endpoint for Windows.

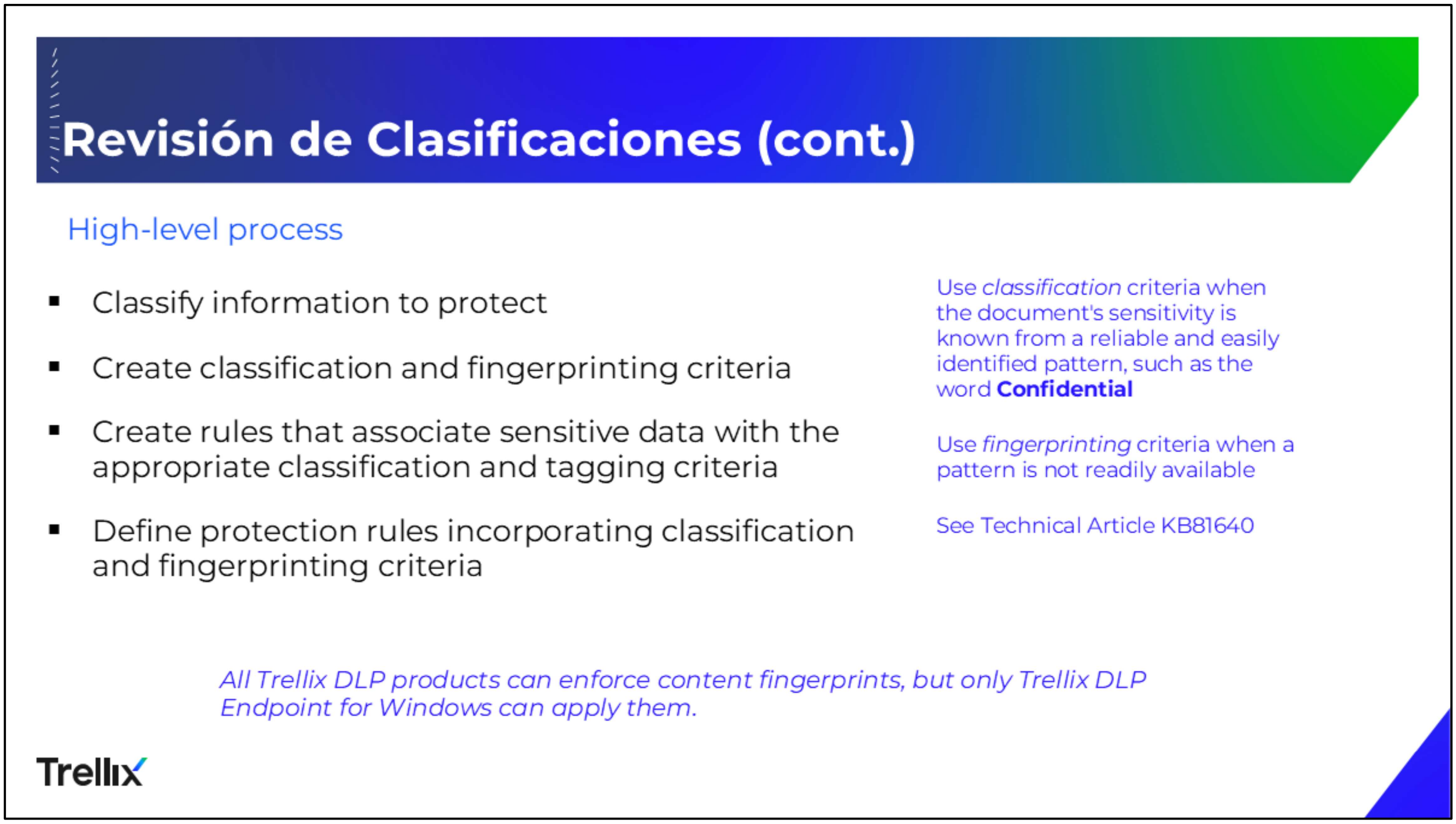
Content-based, reaction rules:

- Monitor sensitive data transfer.
- Prevent confidential data from leaving the enterprise.
- Notify administrator and end users.
- Quarantine confidential data.
- Enforce encryption (send to encryption service).

Data loss prevention visibility:

- Provide forensic logs and collect events and incidents for monitoring and analysis.
- Provide real-time end user alerts for education and training.

- Allow bypass and policy exceptions.



Revisión de Clasificaciones (cont.)

High-level process

- Classify information to protect
- Create classification and fingerprinting criteria
- Create rules that associate sensitive data with the appropriate classification and tagging criteria
- Define protection rules incorporating classification and fingerprinting criteria

Use *classification* criteria when the document's sensitivity is known from a reliable and easily identified pattern, such as the word **Confidential**

Use *fingerprinting* criteria when a pattern is not readily available

See Technical Article KB81640

All Trellix DLP products can enforce content fingerprints, but only Trellix DLP Endpoint for Windows can apply them.

Trellix DLP gives you several ways to classify sensitive content. A high level process for classifying content is:

- Classify information to protect.
- Create classification and fingerprinting criteria.
- Create rules that associate sensitive data with the appropriate classification and fingerprinting criteria.
- Define protection rules incorporating classification and fingerprinting criteria that block, monitor, or encrypt the sensitive data when users send it to portable devices or specified network locations.

Classification Versus Fingerprinting Criteria

Classification criteria is recommended in use cases where the nature of the document's sensitivity can be known from a reliable and easily identified pattern, such as the word **confidential**.

In cases where such a pattern is not readily available, content can be protected with fingerprinting. For more information, see Technical Article KB81640.

Keep in mind that all Trellix DLP products can enforce content fingerprints, but only Trellix DLP Endpoint for Windows can apply them.

There are two mechanisms for DLP Endpoint to detect sensitive content:

- Tagging
- Content Classification

Technical Support recommends that you use **Content Classification** in use cases where the nature of the document's sensitivity can be known from a reliable and easily identified pattern, such as the word "confidential." In cases where such a pattern isn't readily available, content can be protected with **Tagging**. For more information, see the *Product Guide*.

Continued on the next page

If a **Protection Rule** triggers unexpectedly on a document, it's possible to determine if the document is tagged by inspecting the **Manual Tagging** mechanism. For more information, see the *Product Guide*. If a document has been confirmed as being tagged, there are five possible ways in which the document is tagged: Application-based tagging rules apply tags generically in one of two ways. It applies tags based on the application or applications that create a file, as specified in application definitions, or based on the file type or file extension. You can also add text patterns and dictionaries to further restrict how the tags are applied.

- Location-based tagging rules apply tags based on the location of the source file. For example, a file being copied locally from a share on a network server. You can add text patterns and dictionaries as well to further restrict how the tags are applied.
- Tags can be applied manually via Manual Tagging.
- Tags can be applied during the Discover Process.
- Tags propagate via the DLPE software. This software tracks data transformations and maintains the classification of the sensitive content persistently, regardless of how it's being used. For example, if an application reads a tagged document and then later saves a file elsewhere with a few paragraphs of the same content.

Often, a process of elimination can be used to determine which method was used to tag the document. For example, if there are no **Discovery Scans** configured, the document wasn't tagged via the **Discover Scan** method.

If a tag appears on too many documents, it can be reset in ePO through the DLP Policy. Go to **Definitions / Tags** and **Categories** and right-click the individual tag. This action resets the unique identifier used. After the policy change is enforced on the client computer, the tag isn't applied to any documents until one of the above mechanisms occurs.

Unless something else is changed in the policy, it's likely that whatever behavior led to the initial tagging can happen again. So, make sure that the users with the Manual Tagging capability are aware not to tag documents that aren't intended to be protected. Also, any copy from a location specified in a **Location Based Tagging Rule** by a user with **read** permission to that location results in the destination document being tagged. To make sure that any possible Tagging vector is fine-tuned, double-check the **Application Definitions** and the **Discover Scan** settings.

The following is an example of how a new or recently reset tag can spread in an environment:

A Location-Based tagging rule is used. An application on a host with DLP Endpoint, without alerting the user, automatically reads a file from a location, such as a desktop.ini file or any configuration file. It then saves a new file with a part of the sensitive content into a new share folder. Now, a second user that doesn't have the rights to the first location can use an application that reads a file from the second share. The tag is propagated when a file with the same content is saved.

- To find out in more detail how a new or recently reset tag is multiplying in an environment, use the **Log All Messages** option. Use this option on all users that have Manual Tagging rights to read from a share specified in a **Location Based tagging rule, use any applications** in an **Application Based Tagging Rule**. Or, use the option on all users whose computers are configured for a Discover Scan. This setting is available under **Events and Logging** in the Agent Configuration of DLP Policy in ePO.
  The following sample log shows how to determine when files are tagged:

  Note: The logfile name is **HDLP_Agent_(DD.MM.YYYY)(X-XX-XX).log** and is located under **c:\Program Data\McAfee\DLP\temp\logs\session##**In the following example, the file named **notepadtext.txt** is read by Process ID 2644:
- 18:5:44:388 [2584] [ODEBUG] [File Tracker] [RunningProcessInfo::addFileInfo] Adding the file(**notepadtest.txt**) to **process (2644)**
  18:5:44:388 [2584] [ODEBUG] [File Tracker] [FileContentAccessedEvent::startProcessEvent] FAcc.FF#000183 start event handler file : **\\grepo5\grshare\notepadtest.txt**
- In the following example, a process with PID 2644 saves a file that is then tagged by the DLP Endpoint:
- 18:5:44:388 [2584] [ODEBUG] [File Handler] [FileFilterHandler::onOpen] File open for **PID(2644)** write **c:\users\administrator\desktop\notepadtest.txt**...
- Continued on the next page.

Definiciones

Duplicate built-in definitions or create custom ones

Data:

- File Extension

Notification:

- User Notification

Other:

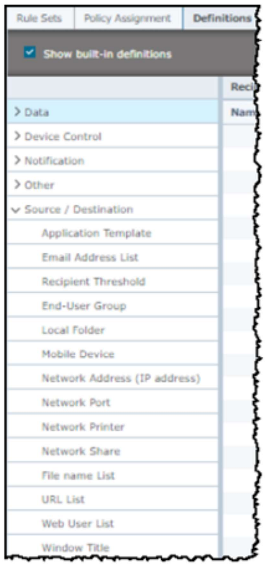
- Discussed in Trellix DLP Discover module

Source / Destination:

- Application Template (only supported by DLPe)
- Email Address List
- Recipient Threshold (only supported by DLPe)
- End-User Group (only supported by DLPe)
- Local Folder (Only supported by DLPe)
- Mobile Device (Only supported by NDLP)
- Network Address (IP address)
- Network Port
- Network Printer
- Network Share (only supported by DLPe)
- File name list
- URL List
- Web User List
- Windows Title

Repositories:

- Used only for NDLP



Trellix

Data Protection > DLP Policy Manager > Definitions

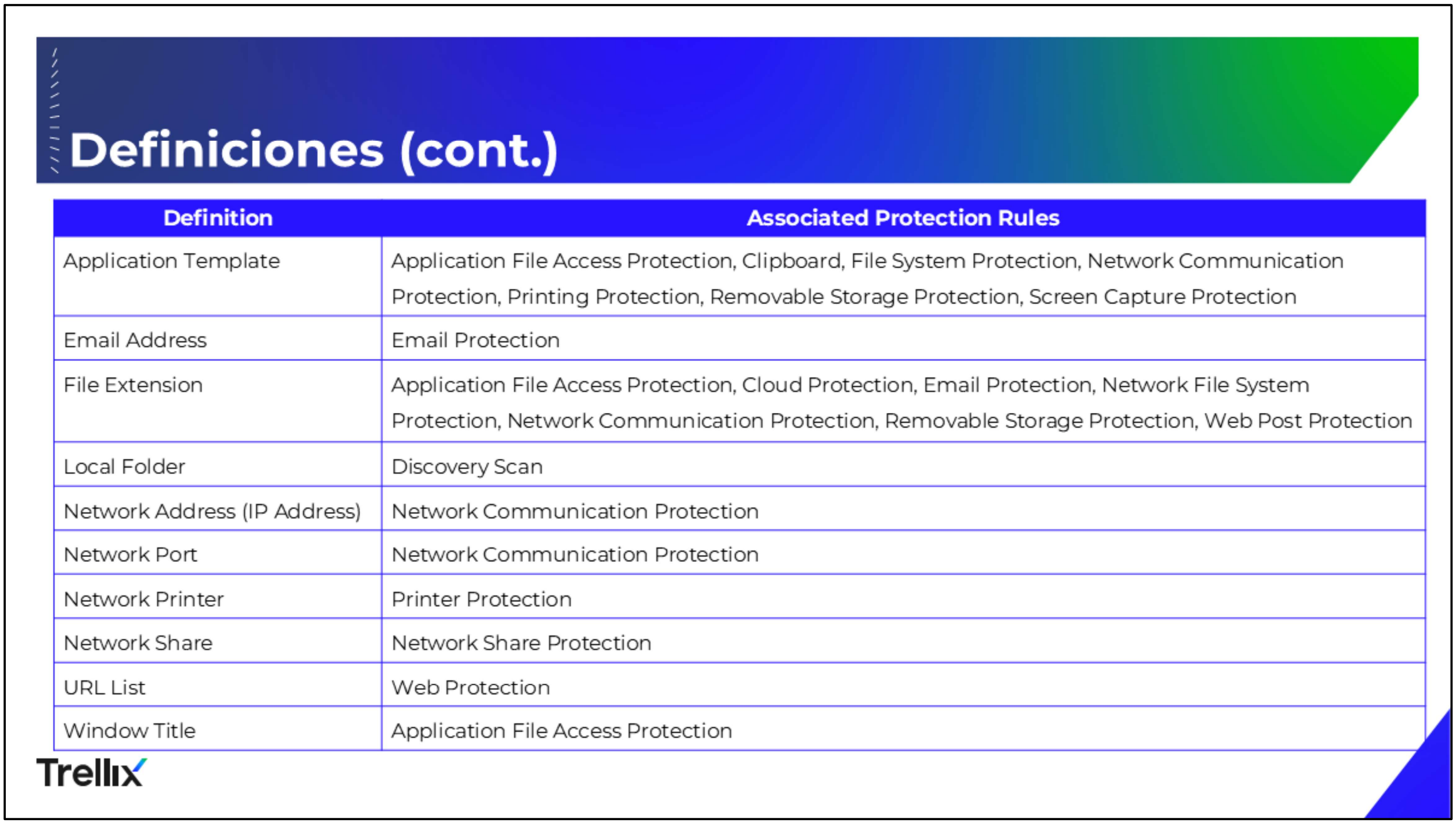
As discussed earlier in the course, a first step is to identify the definitions needed for your content protection rules Definitions typically used for content protection are listed below. Many of these definitions have built-in examples, which you can duplicate and edit. You can also create custom ones. In this section, we will discuss definitions used for data protection rules.

Data:

- File Extension

Source / Destination:

- Application Template
- Email Address
- Local Folder
- Mobile Device
- Network Address (IP address)
- Network Port
- Network Printer
- Network Share
- File name List
- URL List
- Window Title



Definiciones (cont.)

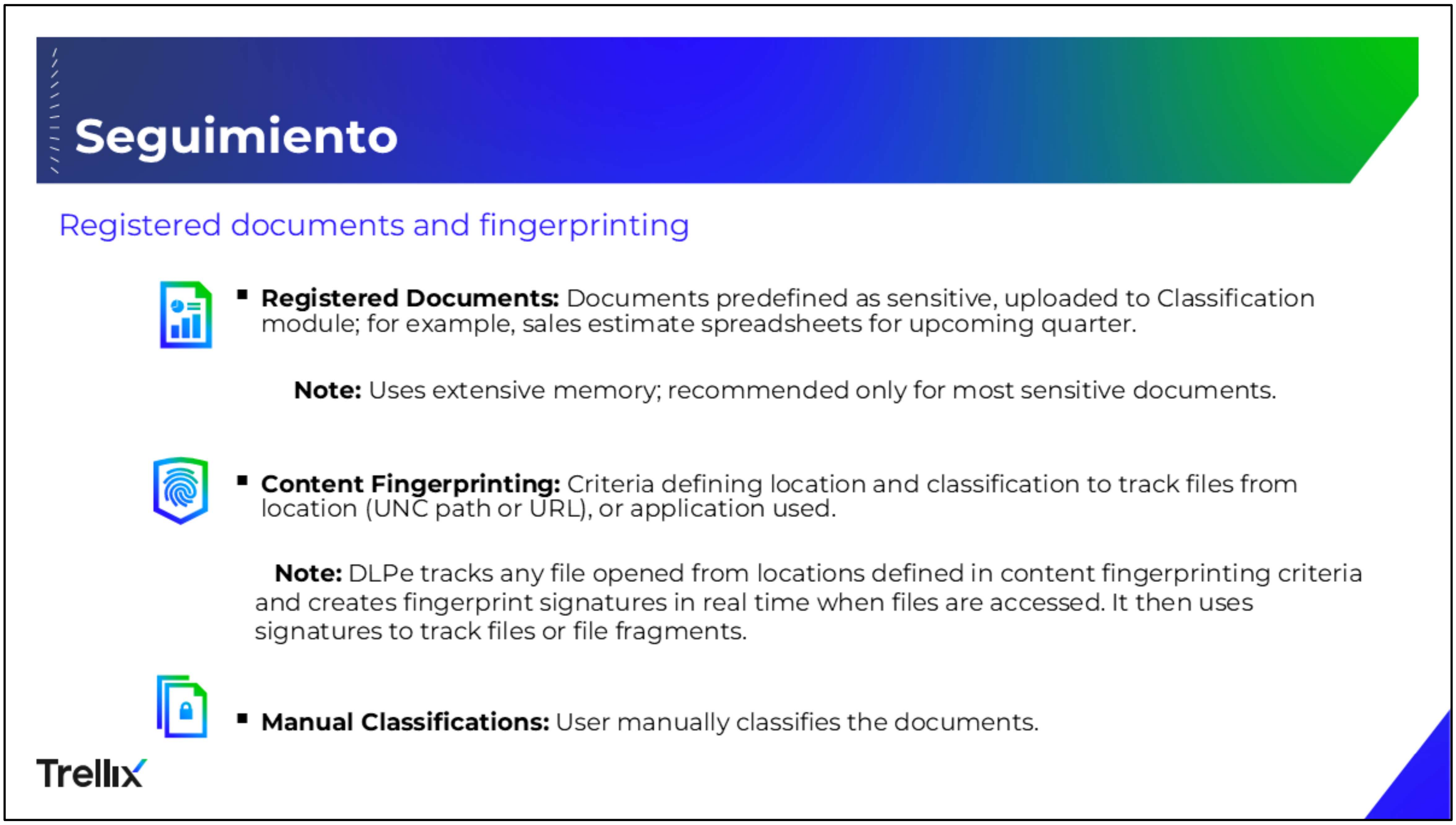
Definition	Associated Protection Rules
Application Template	Application File Access Protection, Clipboard, File System Protection, Network Communication Protection, Printing Protection, Removable Storage Protection, Screen Capture Protection
Email Address	Email Protection
File Extension	Application File Access Protection, Cloud Protection, Email Protection, Network File System Protection, Network Communication Protection, Removable Storage Protection, Web Post Protection
Local Folder	Discovery Scan
Network Address (IP Address)	Network Communication Protection
Network Port	Network Communication Protection
Network Printer	Printer Protection
Network Share	Network Share Protection
URL List	Web Protection
Window Title	Application File Access Protection

Definitions are used in the creation of data protection, device control, and discovery rules. This figure shows the definitions used with protection rules and their associated rules.
Definitions are the fundamental building blocks used to create rules. You create a definition for each category you want to control. When you modify a definition, the modification is automatically propagated to all rules that use the definition.

Definitions let you customize the system to enforce your enterprise security policy and other requirements, such as compliance issues and privacy laws. Customizing these definitions creates an efficient method of maintaining company policies.

Definitions can be assigned to any new or existing rule. Changes take effect immediately upon redeploying the system policy to the agents.

Definitions are created in a two-step process: first you create the definition (right-click, select **Add New**), then you define it (double-click the newly created definition.) These two steps should always be done together. Leaving a definition empty (undefined) will, in most cases, generate an error when you try to apply the policy to ePO. At the very least, it will generate a warning.



Seguimiento

Registered documents and fingerprinting

- **Registered Documents:** Documents predefined as sensitive, uploaded to Classification module; for example, sales estimate spreadsheets for upcoming quarter.

  Note: Uses extensive memory; recommended only for most sensitive documents.

- **Content Fingerprinting:** Criteria defining location and classification to track files from location (UNC path or URL), or application used.

  Note: DLPe tracks any file opened from locations defined in content fingerprinting criteria and creates fingerprint signatures in real time when files are accessed. It then uses signatures to track files or file fragments.

- **Manual Classifications:** User manually classifies the documents.

Trellix

DLPe tracks content based on its origin using registered documents and fingerprinting criteria. Using these techniques, you can, for example, specify that all files downloaded from the engineering SharePoint site are tracked and classified as Intellectual Property.

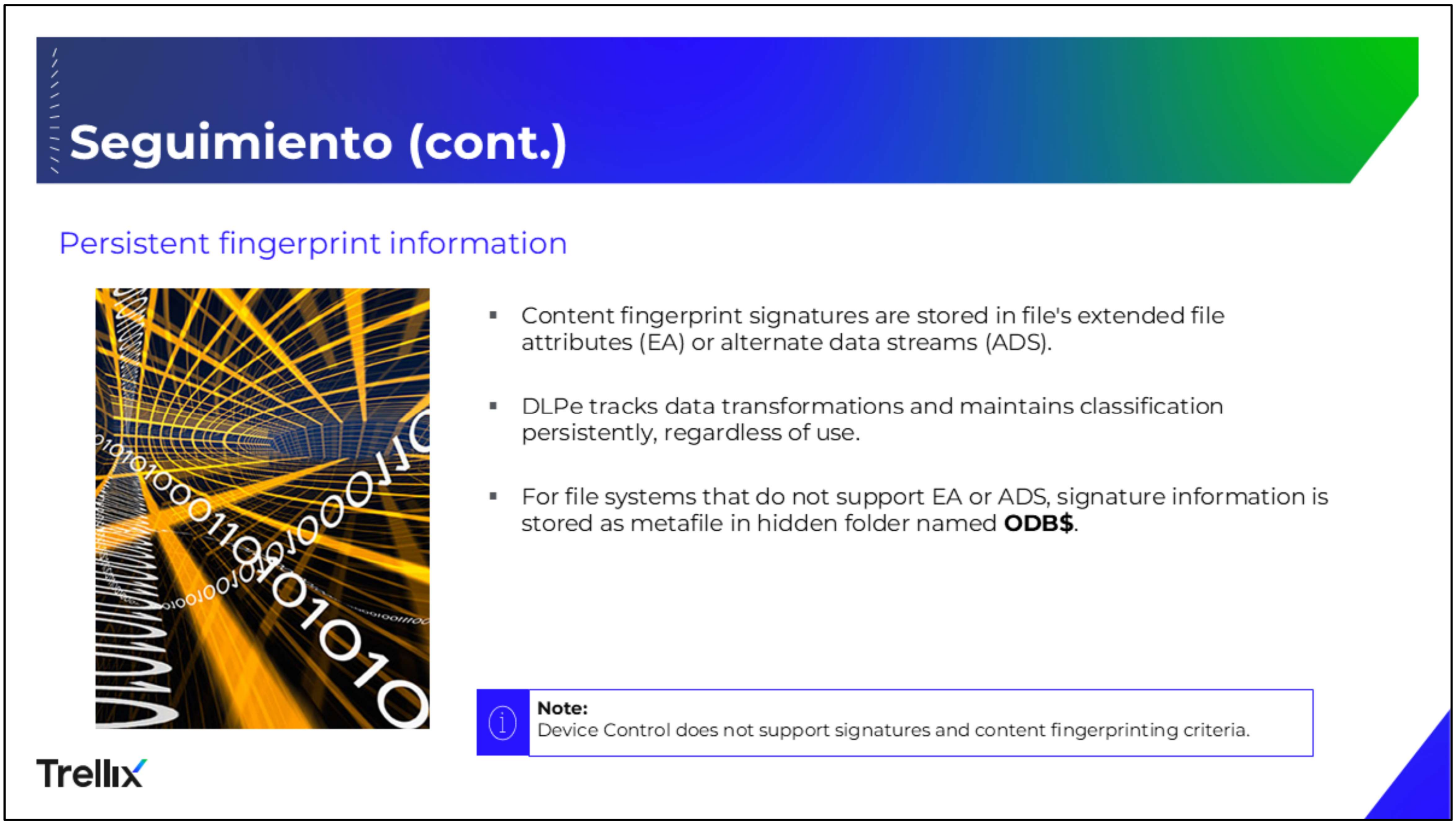
Registered Documents
The registered documents feature is based on pre-scanning all files in specified repositories (such as the engineering SharePoint) and creating signatures of fragments of each file in these repositories. These signatures are then distributed to all managed endpoints. The DLPe client is then able to track any paragraph copied from one of these documents and classify it according to the classification of the registered document signature.

Caution: Registered documents use extensive memory which might affect performance, as each document that the DLP Endpoint client inspects is compared to all registered document signatures to identify its origin. As a best practice, to minimize the number of signatures and the performance implications of this technique, use registered documents to track only the most sensitive documents.

Content Fingerprinting
Content fingerprinting is a content tracking technique unique to the DLPe product. The administrator creates a set of content fingerprinting criteria that define the file location and the classification to place on files from that location. DLPe client tracks any file that is opened from the locations defined in the content fingerprinting criteria and creates fingerprint signatures of these files in real time when the files are accessed. It then uses these signatures to track the files or fragments of the files. Content fingerprinting criteria can be defined by location (UNC path or URL) or the application used to access the file.

Manual Classification
End users can manually apply or remove classifications or content fingerprinting to files. The manual classification feature applies file classification. That is, the classifications applied do not need to be related to content. For example, a user can place a PCI classification on any file. The file does not have to contain credit card numbers. Manual classification is embedded in the file. In Microsoft Office files, the classification is stored as a document property. In other supported files, it is stored as an XMP property.

For email, it is added as markup text.



Seguimiento (cont.)

Persistent fingerprint information

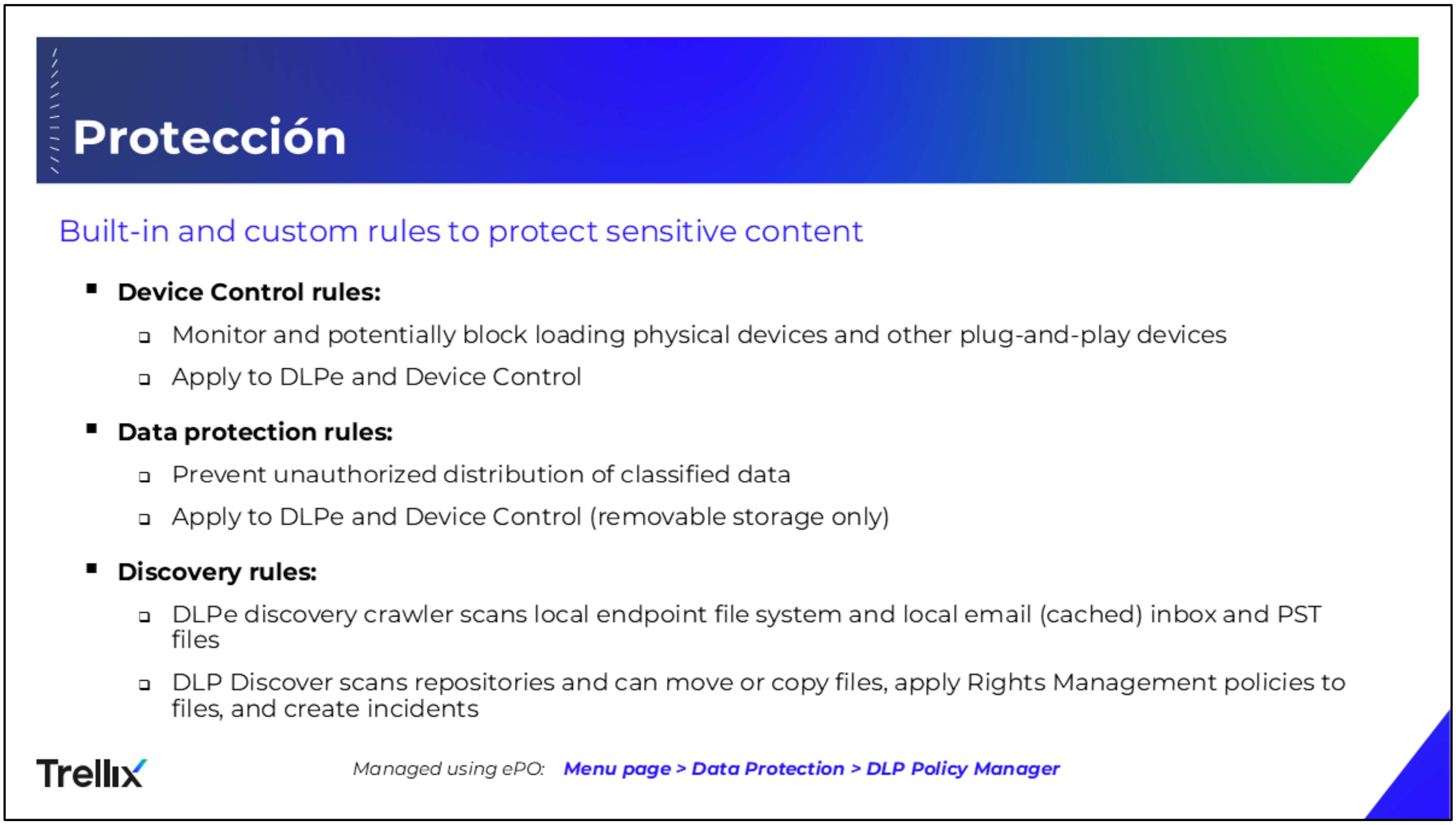
- Content fingerprint signatures are stored in file's extended file attributes (EA) or alternate data streams (ADS).
- DLPe tracks data transformations and maintains classification persistently, regardless of use.
- For file systems that do not support EA or ADS, signature information is stored as metafile in hidden folder named **ODB$**.

Note:
Device Control does not support signatures and content fingerprinting criteria.

Trellix

Content fingerprint signatures are stored in a file's extended File Attributes (EA) or Alternate Data Streams (ADS). When such files are accessed, DLPe tracks data transformations and maintains the classification of the sensitive content persistently, regardless of how it is being used; for example, if a user opens a fingerprinted Word document, copies a few paragraphs of it into a text file, and attaches the text file to an email message, the outgoing message has the same signatures as the original document.

- For file systems that do not support EA or ADS, DLPe stores signature information as a metafile on the disk.
- The metafiles are stored in a hidden folder named ODB$, which the device control creates automatically.
- **Device Control** does not support signatures and content fingerprinting criteria.



Protección

Built-in and custom rules to protect sensitive content

- **Device Control rules:**
  - Monitor and potentially block loading physical devices and other plug-and-play devices
  - Apply to DLPe and Device Control
- **Data protection rules:**
  - Prevent unauthorized distribution of classified data
  - Apply to DLPe and Device Control (removable storage only)
- **Discovery rules:**
  - DLPe discovery crawler scans local endpoint file system and local email (cached) inbox and PST files
  - DLP Discover scans repositories and can move or copy files, apply Rights Management policies to files, and create incidents

Trellix

Managed using ePO: ***Menu page > Data Protection > DLP Policy Manager***

Device Control Rules

- Device Control rules monitor and potentially block the system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug-and-play devices.
- Device Control rules consist of device definitions and reaction specifications and can be assigned to specific end-user groups by filtering the rule with end-user group definitions.

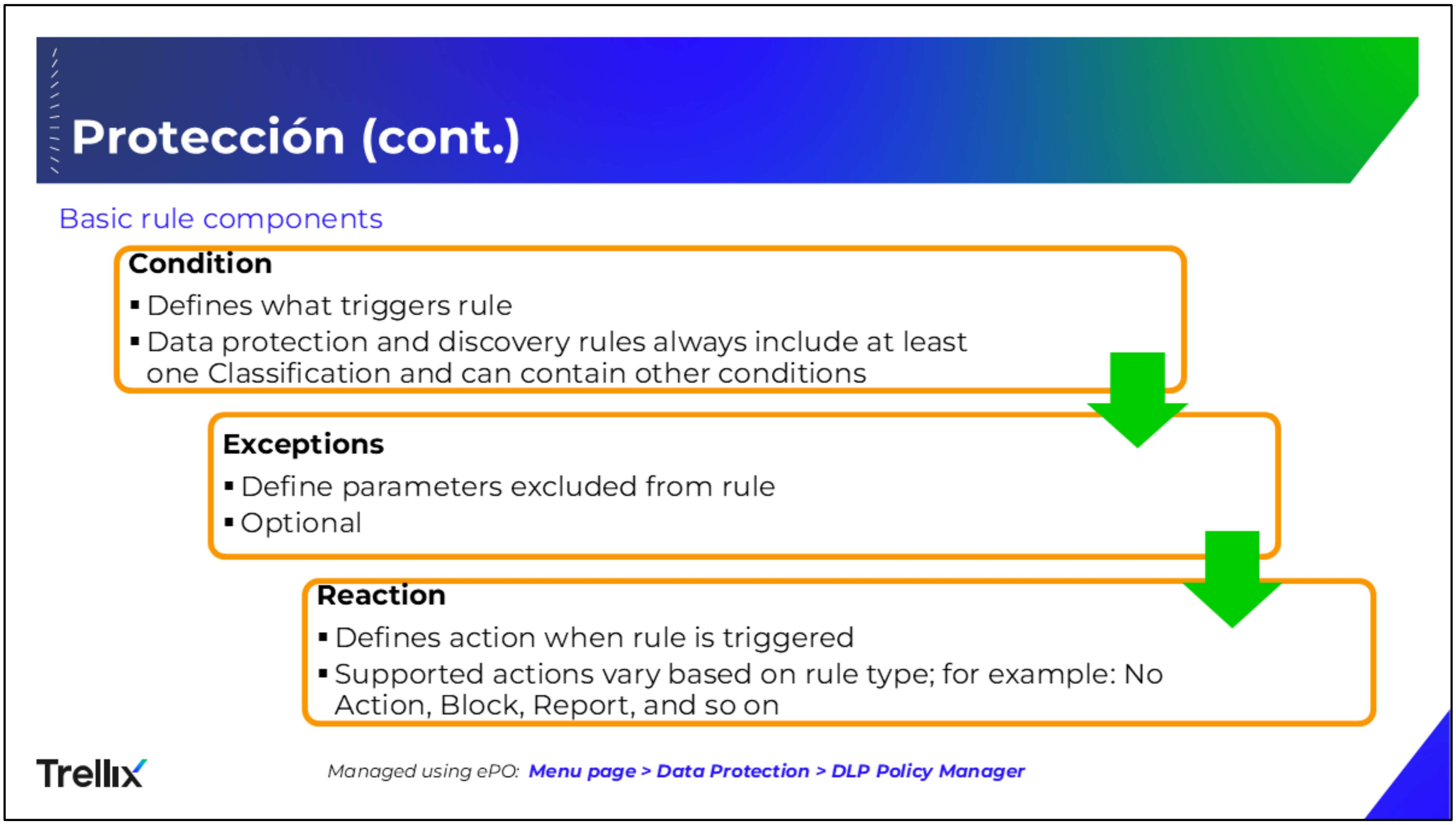
Data Protection Rules

- Data protection rules are used by DLPe and Device Control to prevent unauthorized distribution of classified data.
- When a user tries to copy or attach classified data, DLP intercepts the attempt and uses the data protection rules to determine what action to take. For
- example, DLP Endpoint can halt the attempt and display a dialog to the end user. The user inputs the justification for the attempt, and processing continues.
- Device Control uses only removable storage data protection rules.

Discovery Rules

- DLPe and DLP Discover use discovery rules for file and data scanning. DLPe uses a discovery crawler that runs on managed computers. It scans the local endpoint file system and the local email (cached) inbox and PST files. Local file system and email storage discovery rules define whether the content is to be quarantined, fingerprinted, or encrypted. These rules can also define whether the classified file or email is reported as an incident, and whether to store the file or email as evidence included in the incident. File system scans are not supported on server operating systems.
- DLP Discover scans repositories and can move or copy files, apply Rights

Management policies to files, and create incidents.



Protección (cont.)

Basic rule components

Condition

- Defines what triggers rule
- Data protection and discovery rules always include at least one Classification and can contain other conditions

Exceptions

- Define parameters excluded from rule
- Optional

Reaction

- Defines action when rule is triggered
- Supported actions vary based on rule type; for example: No Action, Block, Report, and so on

Trellix

Managed using ePO: ***Menu page > Data Protection > DLP Policy Manager***

DLPe uses rules to identify sensitive data and take appropriate action. Rules are made up of condition settings, exceptions (optional), and actions.

Condition

- The condition defines what triggers the rule. For data protection and discovery rules, the condition always includes a Classification and can include other conditions. For example, a cloud protection rule contains fields to define the end user and cloud service in addition to the classification. For device control rules, the condition always specifies the end user, and can include other conditions such as the device definition. Device control rules do not include classifications.

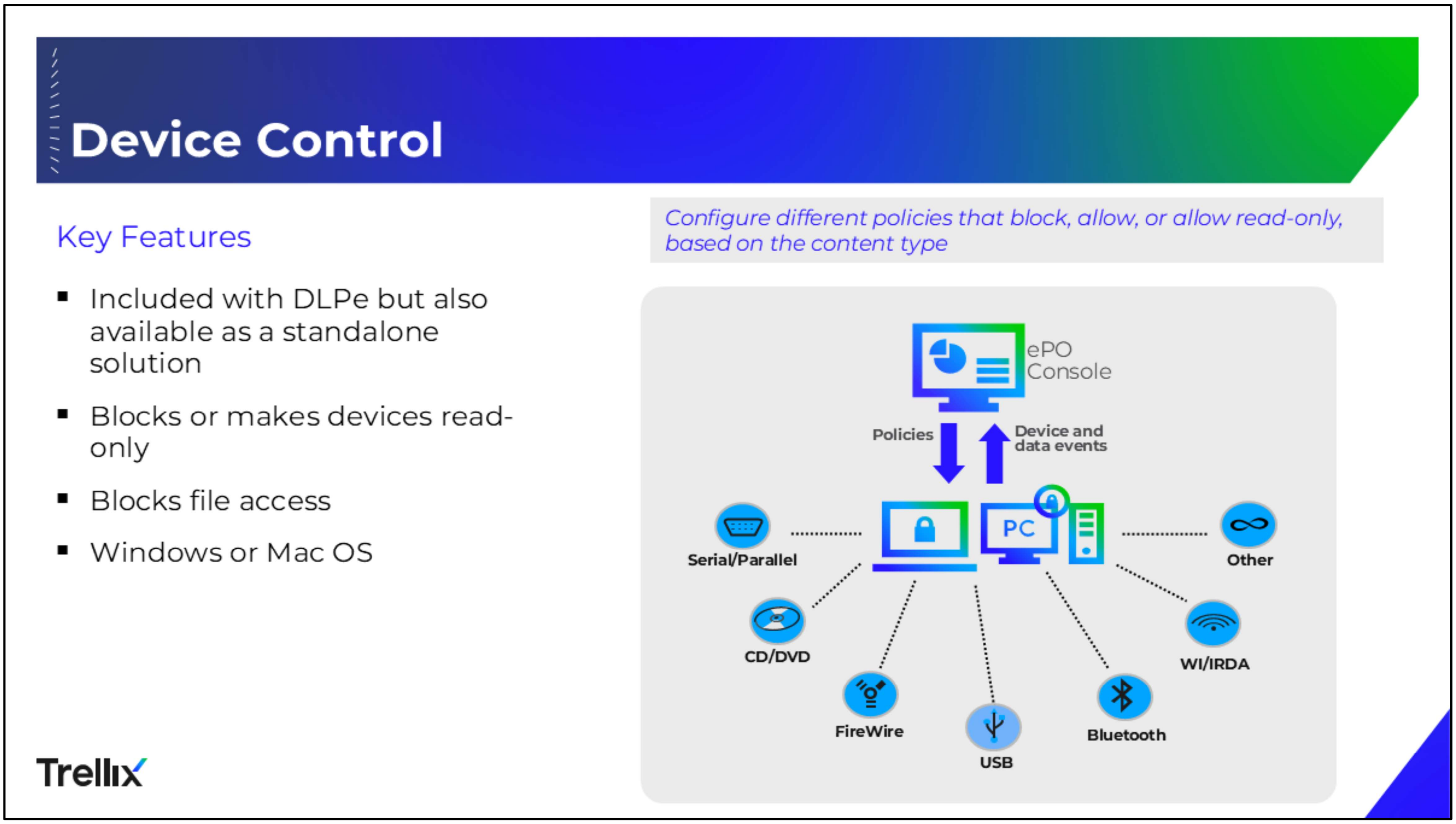
Exceptions

- Exceptions define parameters excluded from the rule. For example, a cloud protection rule can allow specified users and classifications to upload data to the specified cloud services, while blocking those users and classifications defined in the condition section of the rule. Exceptions have a separate setting to enable or disable them, allowing you to turn the exception on or off when testing rules. Creating an exception definition is optional.
- Exception definitions for data protection and discovery rules are similar to condition definitions. The parameters available for exclusion are a subset of the parameters available for defining the condition. For device control rules, the exception is defined by selecting whitelisted definitions from a list. The available whitelisted definitions depend on the type of device rule.

Reaction

- The reaction defines what happens when the rule is triggered. The actions available vary with the type of rule, but the default for all rules is No Action. When selected together with the Report Incident option, you can monitor the frequency of rule violations. This procedure is useful for tuning the rule to the correct level to catch data leaks without creating false positives.
- The reaction also defines whether the rule is applied outside the enterprise and, for

some rules, when connected.



Device Control

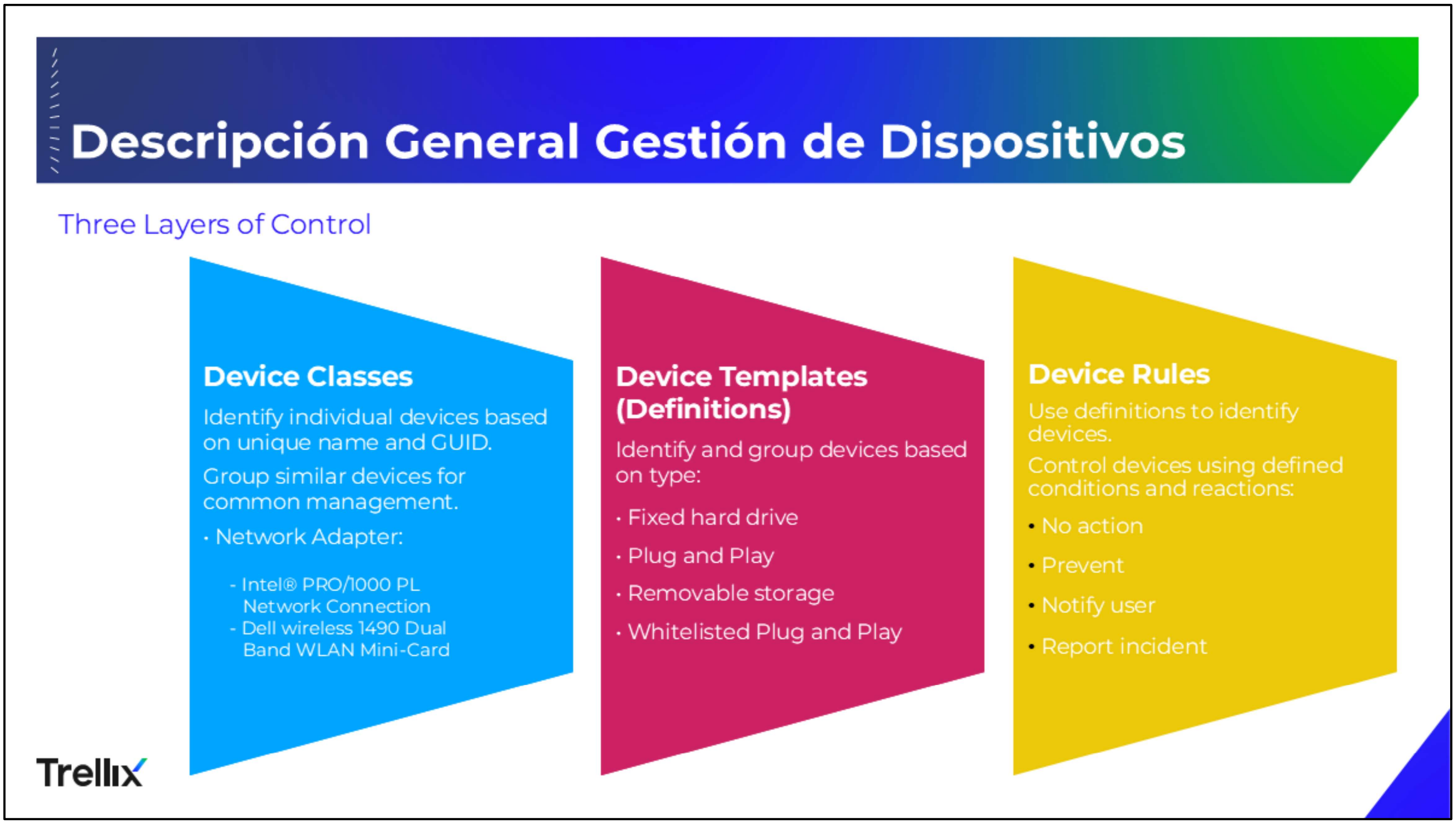
Key Features

- Included with DLPe but also available as a standalone solution
- Blocks or makes devices read-only
- Blocks file access
- Windows or Mac OS

Configure different policies that block, allow, or allow read-only, based on the content type

Trellix

Trellix Device Control is a comprehensive device management solution that helps you protect confidential data from being copied to removable storage devices, such as Universal Serial Bus (USB) drives, media players, compact discs (CDs), digital versatile or video discs (DVDs). It lets you specify and categorize device parameters, such as product identification (ID) number, vendor ID, serial number, device class, and device name. It also lets you configure different policies that block or encrypt data, based on the type of content loaded onto removable devices.



Descripción General Gestión de Dispositivos

Three Layers of Control

Device Classes

Identify individual devices based on unique name and GUID.

Group similar devices for common management.

- Network Adapter:
  - Intel® PRO/1000 PL Network Connection
  - Dell wireless 1490 Dual Band WLAN Mini-Card

Device Templates (Definitions)

Identify and group devices based on type:

- Fixed hard drive
- Plug and Play
- Removable storage
- Whitelisted Plug and Play

Device Rules

Use definitions to identify devices.

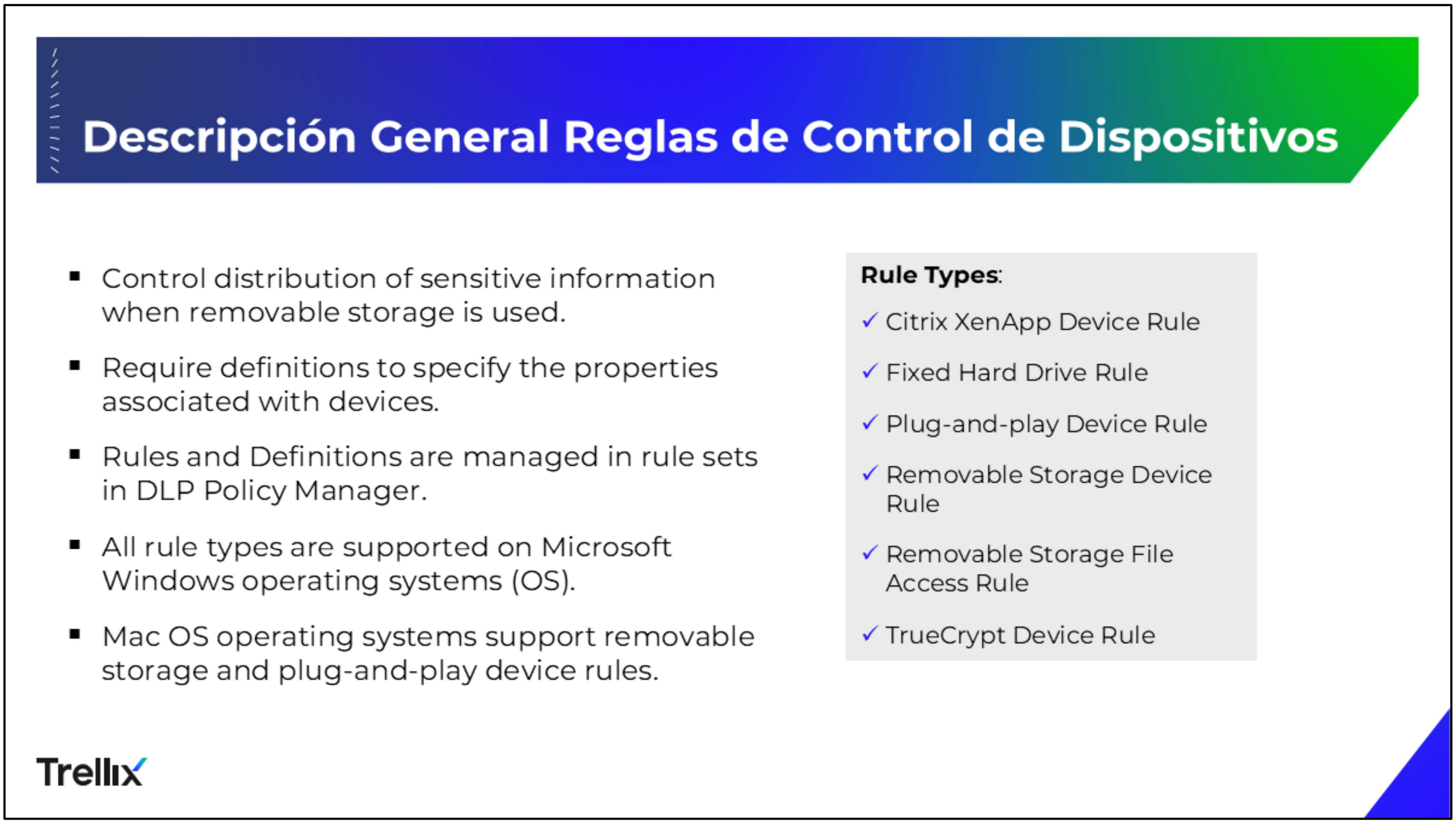
Control devices using defined conditions and reactions:

- No action
- Prevent
- Notify user
- Report incident

Trellix

Trellix Device Control protection is built in three layers:

- **Device classes**: Collection of devices that have similar characteristics and can be managed in a similar manner.
- **Device templates (definitions)**: Identify and group devices according to their common properties.
- **Device Rules**: Control the behavior of devices. Device rules are discussed in more detail in the **Data Protection Rules** module.



Descripción General Reglas de Control de Dispositivos

- Control distribution of sensitive information when removable storage is used.
- Require definitions to specify the properties associated with devices.
- Rules and Definitions are managed in rule sets in DLP Policy Manager.
- All rule types are supported on Microsoft Windows operating systems (OS).
- Mac OS operating systems support removable storage and plug-and-play device rules.

Rule Types:

✓ Citrix XenApp Device Rule

✓ Fixed Hard Drive Rule

✓ Plug-and-play Device Rule

✓ Removable Storage Device Rule

✓ Removable Storage File Access Rule

✓ TrueCrypt Device Rule

Trellix

Device control rules control the distribution of sensitive information when removable storage is used.
All device rule conditions include an End-User and the type of device. Depending on the rule type, other conditions might be available.

The following rule types are supported. All rule types are supported on Microsoft Windows operating systems (OS). For Mac OS operating systems, only removable storage and plug and play device rules are supported.

- Citrix XenApp device
- Fixed hard drive
- Plug and play device
- Removable storage device
- Removable storage file access
- TrueCrypt device

Alert: The list of device classes is managed in the DLP Policy Manager. During day-to-day operation, do not tamper with the device classes list because improper use (such as, blocking the managed computer's hard disk controller) can cause a system or operating system malfunction. New classes of devices, identified by their GUIDs, can be added to the list for use in device rules.

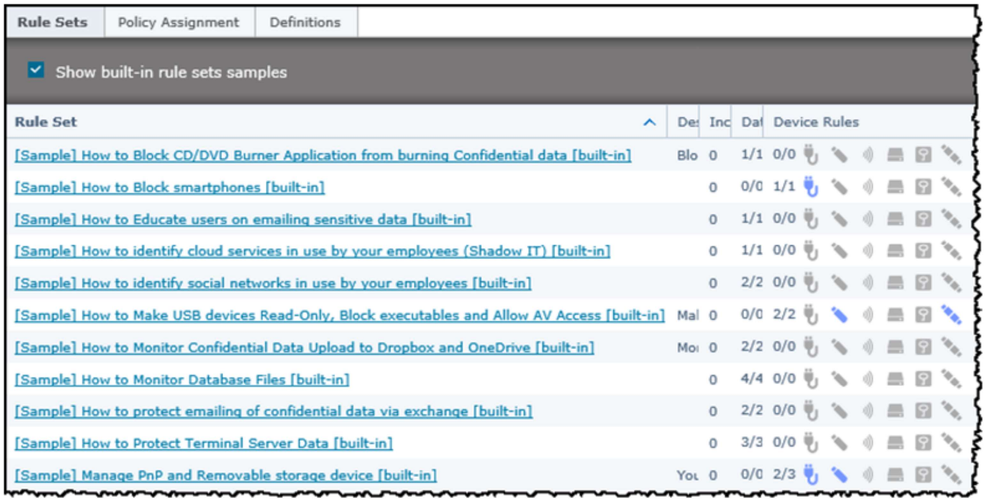
Continued on the next page.

Descripción General Reglas de Control de Dispositivos (cont.)

Menu > Data Protection> DLP Policy Manager > Rule Sets

- Duplicate built-in rule sets/rule or add new ones.

Blue icons in Rules Sets columns indicate built-in rules for the rule set

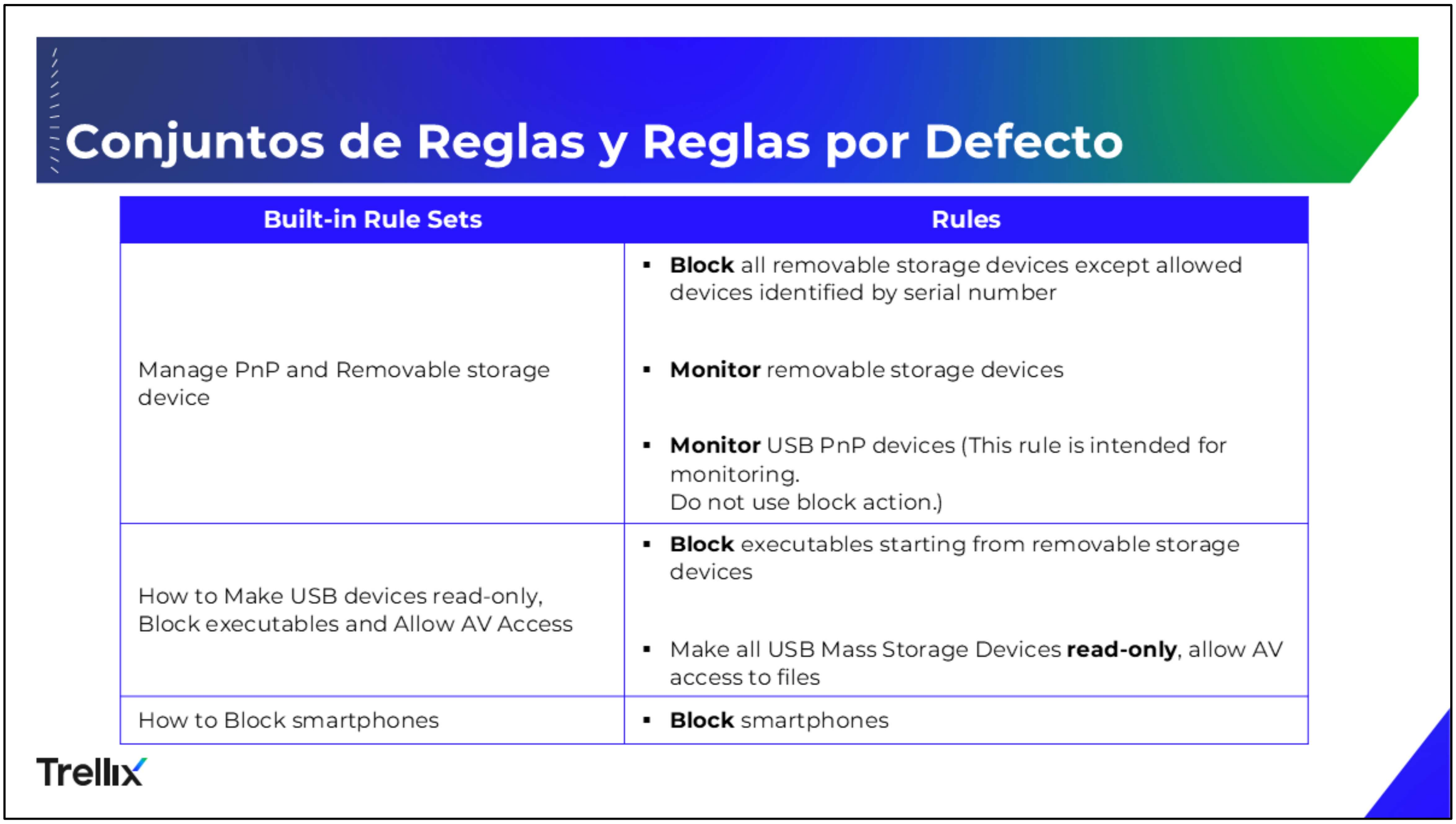


Rule Sets | Policy Assignment | Definitions

☑ Show built-in rule sets samples

Rule Set	De:	Inc	Dat	Device Rules
[Sample] How to Block CD/DVD Burner Application from burning Confidential data [built-in]	Blo	0	1/1	0/0
[Sample] How to Block smartphones [built-in]		0	0/0	1/1
[Sample] How to Educate users on emailing sensitive data [built-in]		0	1/1	0/0
[Sample] How to identify cloud services in use by your employees (Shadow IT) [built-in]		0	1/1	0/0
[Sample] How to identify social networks in use by your employees [built-in]		0	2/2	0/0
[Sample] How to Make USB devices Read-Only, Block executables and Allow AV Access [built-in]	Mal	0	0/0	2/2
[Sample] How to Monitor Confidential Data Upload to Dropbox and OneDrive [built-in]	Mo	0	2/2	0/0
[Sample] How to Monitor Database Files [built-in]		0	4/4	0/0
[Sample] How to protect emailing of confidential data via exchange [built-in]		0	2/2	0/0
[Sample] How to Protect Terminal Server Data [built-in]		0	3/3	0/0
[Sample] Manage PnP and Removable storage device [built-in]	You	0	0/0	2/3

As discussed earlier, rule sets are managed using the DLP Policy Manager (**Menu** > **Data Protection**> **DLP Policy Manager > Rule Sets** tab. Built-in rules and rule sets are read-only. You can only duplicate them.
Custom rule sets are editable; therefore, you can edit, duplicate, and delete them.

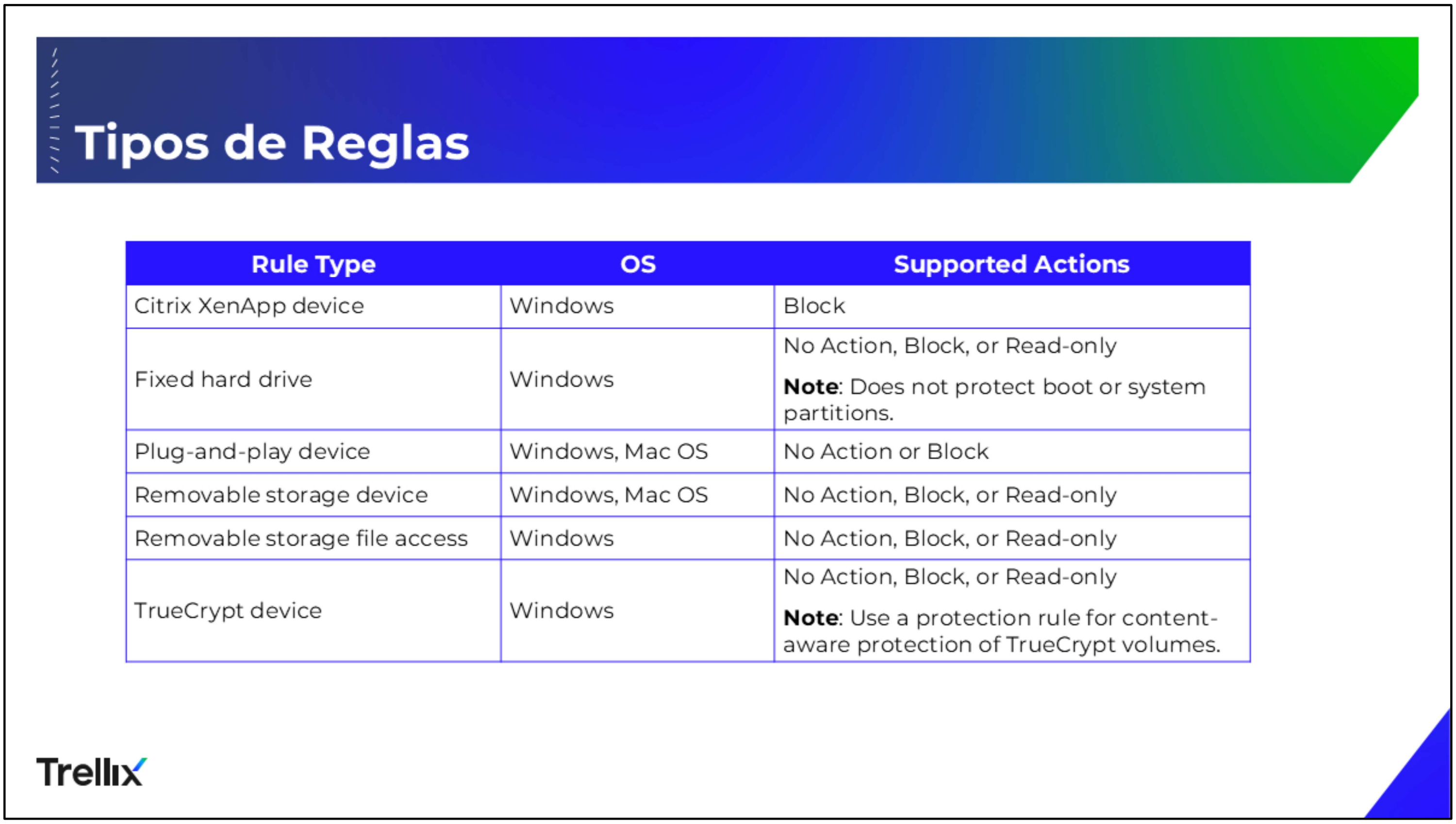


Conjuntos de Reglas y Reglas por Defecto

Built-in Rule Sets	Rules
Manage PnP and Removable storage device	▪ **Block** all removable storage devices except allowed devices identified by serial number ▪ **Monitor** removable storage devices ▪ **Monitor** USB PnP devices (This rule is intended for monitoring. Do not use block action.)
How to Make USB devices read-only, Block executables and Allow AV Access	▪ **Block** executables starting from removable storage devices ▪ Make all USB Mass Storage Devices **read-only**, allow AV access to files
How to Block smartphones	▪ **Block** smartphones

Trellix

The table lists the built-in (sample) rule sets and their associated rules. You can duplicate and use these as starting point or add new ones.



Tipos de Reglas

Rule Type	OS	Supported Actions
Citrix XenApp device	Windows	Block
Fixed hard drive	Windows	No Action, Block, or Read-only **Note**: Does not protect boot or system partitions.
Plug-and-play device	Windows, Mac OS	No Action or Block
Removable storage device	Windows, Mac OS	No Action, Block, or Read-only
Removable storage file access	Windows	No Action, Block, or Read-only
TrueCrypt device	Windows	No Action, Block, or Read-only **Note**: Use a protection rule for content-aware protection of TrueCrypt volumes.

Trellix

Citrix XenApp Device Rule

The Citrix XenApp device rule is used to protect devices mapped to shared Citrix XenApp desktop sessions. The only supported prevent action is Block.

Fixed Hard Drive

The fixed hard drive device rule is used to block, monitor, or force read-only access to fixed hard drives.

Note: This rule type does not protect the boot or system partitions.

Plug and Play Device Rule

The plug and play device is used to block or monitor plug and play devices. This rule is triggered when the hardware device is plugged into the computer.

Note: You can use the plug and play device rule to block USB devices; however, it is recommended to use a removable storage device rule instead. A plug and play device rule can result in blocking the entire USB hub/controller.

Continued on the next page.

Removable Storage Device Rule

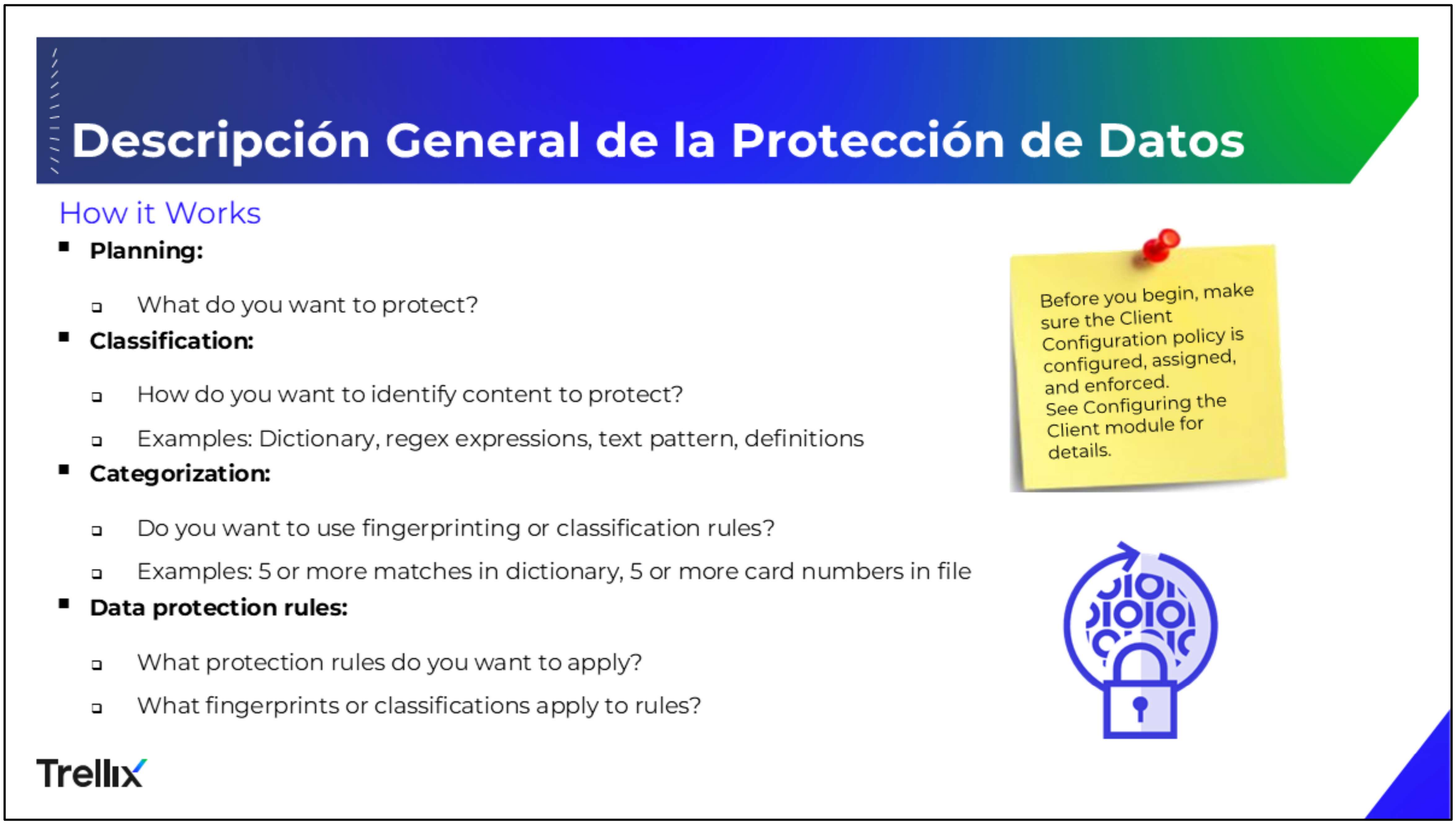
The removable storage device rule allows the device to initialize and register with Windows but prevents file-write operations to the device (if so configured) by defining the device as read-only. With Removable storage device rules, you can monitor hardware devices and prevent them from being loaded by the system, just as you can with Plug and Play Device Rules; however, with the additional read-only mode restriction, you can prevent data from being written to the device.

Removable Storage File Access

- The removable storage file access rules block removable storage media from running specified applications. Whitelisted application definitions provide lists of specific files that are exempt from the blocking rule.

TrueCrypt Device Rules

- The TrueCrypt device rule allows you to block or monitor TrueCrypt virtual encryption devices or set them to read-only.
- **Note**: Use a protection rule for content-aware protection of TrueCrypt volumes. TrueCrypt volumes do not support extended file attributes, so DLPe tags are lost when tagged content is copied to TrueCrypt volumes. Use document properties, file encryption, or file type groups definitions in the classification definition to identify the content.



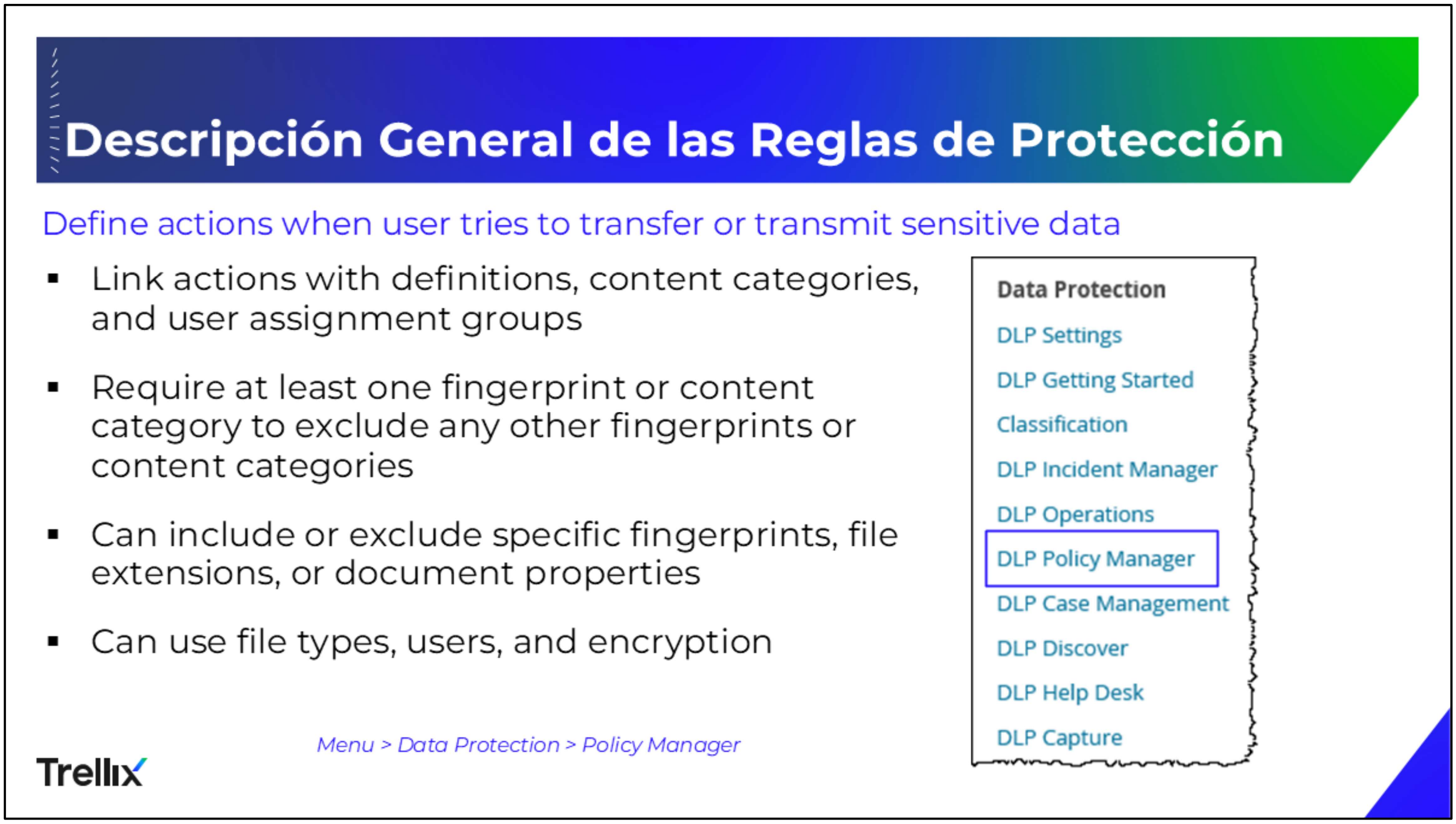
Descripción General de la Protección de Datos

How it Works

- **Planning:**
  - What do you want to protect?
- **Classification:**
  - How do you want to identify content to protect?
  - Examples: Dictionary, regex expressions, text pattern, definitions
- **Categorization:**
  - Do you want to use fingerprinting or classification rules?
  - Examples: 5 or more matches in dictionary, 5 or more card numbers in file
- **Data protection rules:**
  - What protection rules do you want to apply?
  - What fingerprints or classifications apply to rules?

Before you begin, make sure the Client Configuration policy is configured, assigned, and enforced.
See Configuring the Client module for details.

The slide highlights important considerations when planning your data protection strategy. As a reminder, many rules have related settings in the Client Configuration policy. Before you begin, make sure the Client Configuration policy is configured, assigned, and enforced. See Configuring the Client module for details.



Descripción General de las Reglas de Protección

Define actions when user tries to transfer or transmit sensitive data

- Link actions with definitions, content categories, and user assignment groups
- Require at least one fingerprint or content category to exclude any other fingerprints or content categories
- Can include or exclude specific fingerprints, file extensions, or document properties
- Can use file types, users, and encryption

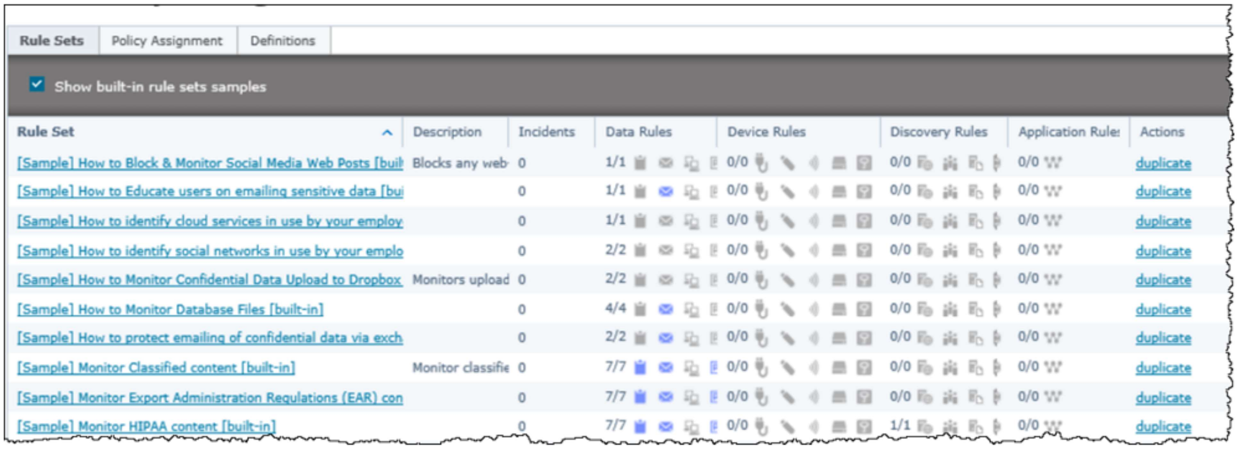
Menu > Data Protection > Policy Manager

- Protection rules control the flow of data by defining the action taken when an attempt is made to transfer or transmit sensitive data. They do this by linking actions with definitions, fingerprints and content categories, and user assignment groups. Protection rules specify the transfer method, named fingerprint(s), and how the system should react to attempts to transfer data. Each event is given a severity level, and options for responding to the event. In some cases, protection rules merely log the event. In other cases, the protection rules may prevent the transfer of data and notify the user of the violation. Protection rules are optionally applied to assignment groups. This allows a rule to apply only to particular user groups.
- You can define protection rules to include or exclude specific fingerprints, file extensions, or document properties. You can also specify file types, users, and encryption (including password protection). Not all options are available for all rules. These options allow creation of rules with considerable granularity.
- **Note**: When excluding fingerprints or content categories in protection rules, the exclude rule works relative to the include rule. You must include at least one fingerprint or content category to exclude any other fingerprints or content categories.

Conjuntos de Reglas

Data Protection > DLP Policy Manager > Rule Sets

Duplicate built-in rule sets/rule or add new

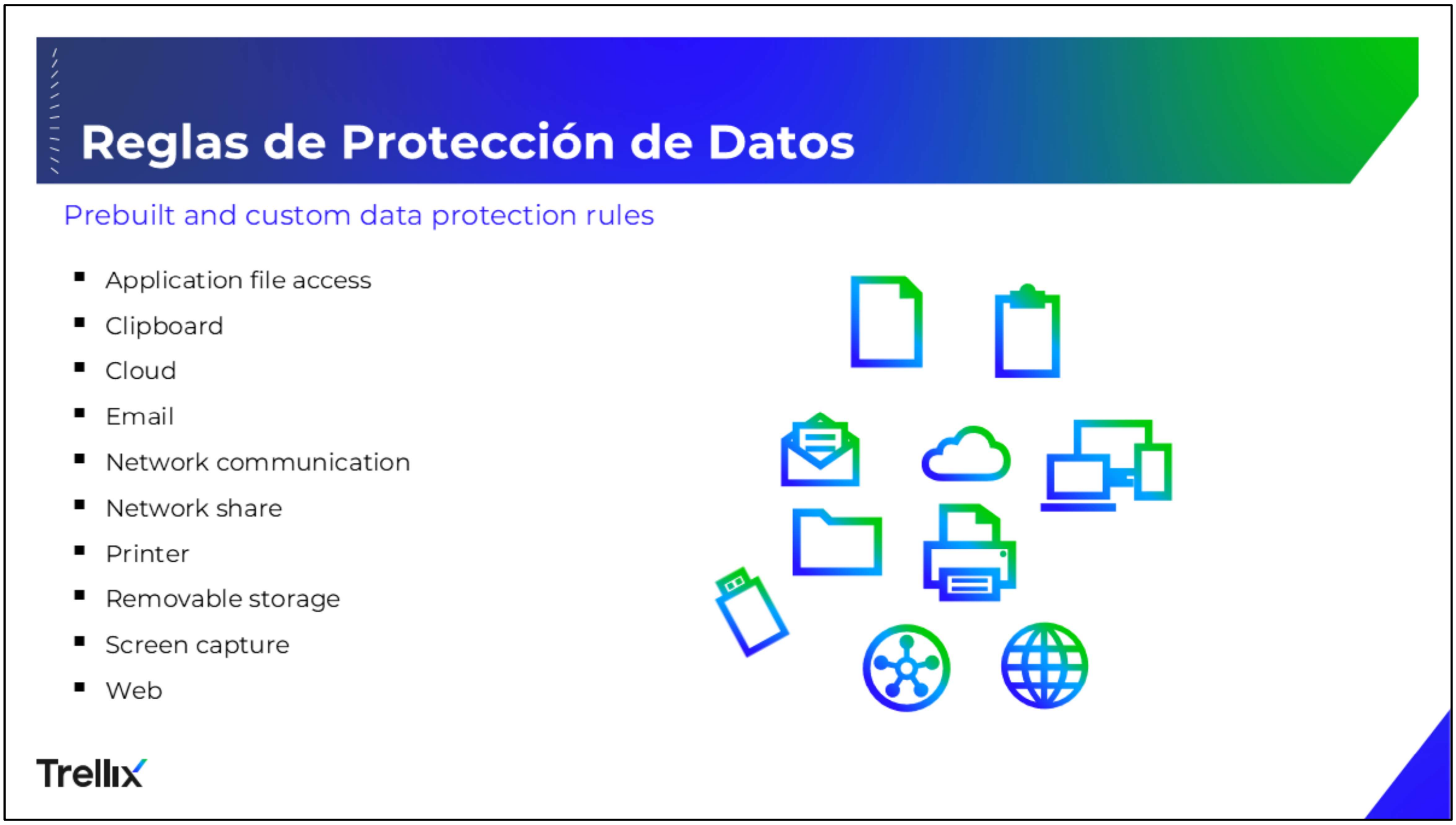


☑ Show built-in rule sets samples

Rule Set	Description	Incidents	Data Rules	Device Rules	Discovery Rules	Application Rule:	Actions
[Sample] How to Block & Monitor Social Media Web Posts [buil	Blocks any web	0	1/1	0/0	0/0	0/0	duplicate
[Sample] How to Educate users on emailing sensitive data [bui		0	1/1	0/0	0/0	0/0	duplicate
[Sample] How to identify cloud services in use by your employ		0	1/1	0/0	0/0	0/0	duplicate
[Sample] How to identify social networks in use by your emplo		0	2/2	0/0	0/0	0/0	duplicate
[Sample] How to Monitor Confidential Data Upload to Dropbox	Monitors upload	0	2/2	0/0	0/0	0/0	duplicate
[Sample] How to Monitor Database Files [built-in]		0	4/4	0/0	0/0	0/0	duplicate
[Sample] How to protect emailing of confidential data via exch		0	2/2	0/0	0/0	0/0	duplicate
[Sample] Monitor Classified content [built-in]	Monitor classifie	0	7/7	0/0	0/0	0/0	duplicate
[Sample] Monitor Export Administration Regulations (EAR) con		0	7/7	0/0	0/0	0/0	duplicate
[Sample] Monitor HIPAA content [built-in]		0	7/7	0/0	1/1	0/0	duplicate

Blue icons in Rules columns indicate built-in rules for the rule set.

Like other rule types, you can duplicate and edit the built-in rules and rule sets or create your own.



Reglas de Protección de Datos

Prebuilt and custom data protection rules

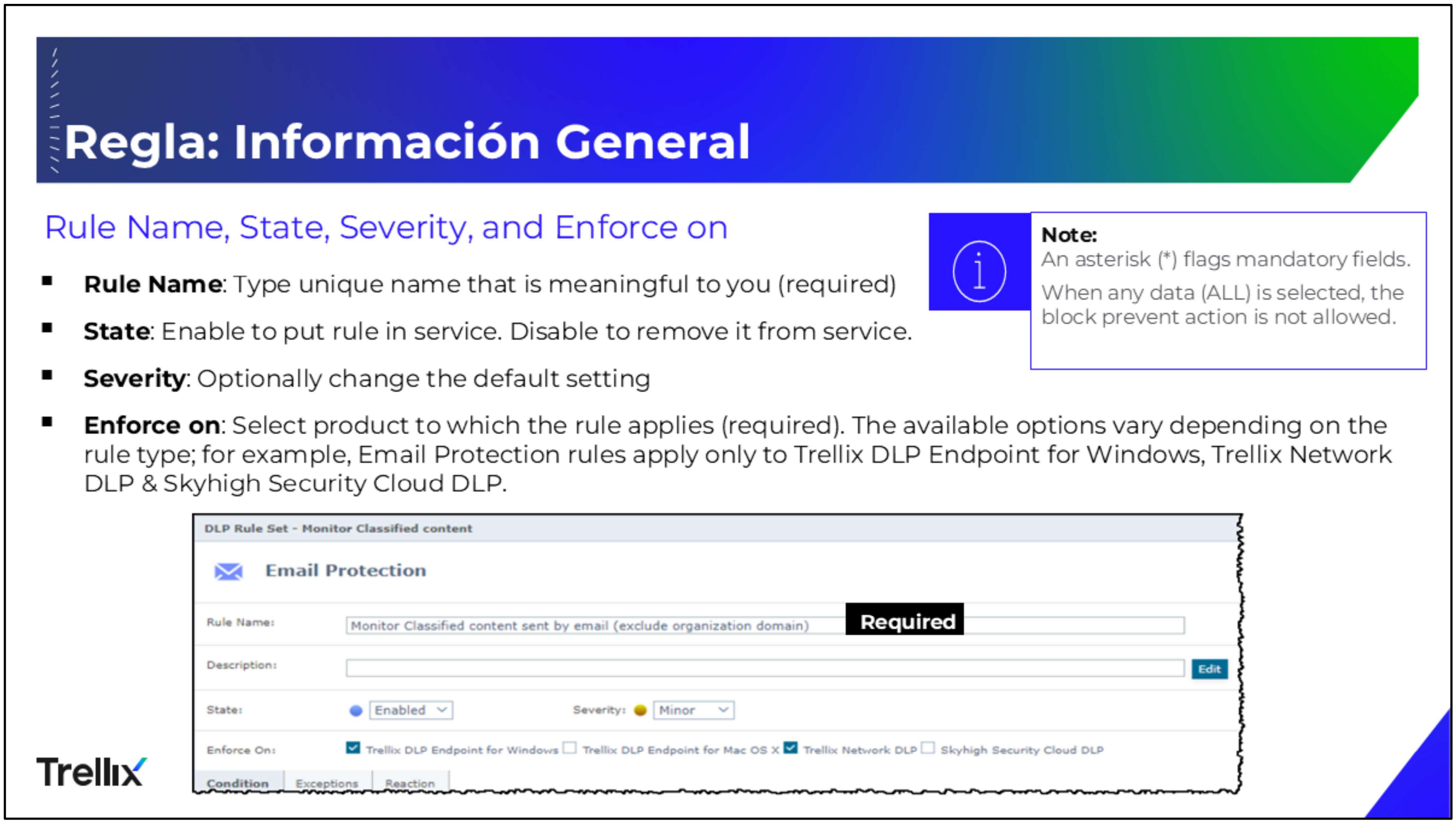
- Application file access
- Clipboard
- Cloud
- Email
- Network communication
- Network share
- Printer
- Removable storage
- Screen capture
- Web

Trellix

Data protection rules monitor and control user content and activity. You can customize the prebuilt data protection rules.

The prebuilt rules are:

- Application file access
- Clipboard
- Cloud
- Email
- Network communication
- Network share
- Printer
- Removable storage
- Screen capture
- Web



Regla: Información General

Rule Name, State, Severity, and Enforce on

- **Rule Name**: Type unique name that is meaningful to you (required)
- **State**: Enable to put rule in service. Disable to remove it from service.
- **Severity**: Optionally change the default setting
- **Enforce on**: Select product to which the rule applies (required). The available options vary depending on the rule type; for example, Email Protection rules apply only to Trellix DLP Endpoint for Windows, Trellix Network DLP & Skyhigh Security Cloud DLP.

Note:
An asterisk (*) flags mandatory fields.
When any data (ALL) is selected, the block prevent action is not allowed.

DLP Rule Set - Monitor Classified content

Email Protection

Rule Name: Monitor Classified content sent by email (exclude organization domain)

Required

Description:

State: ● Enabled

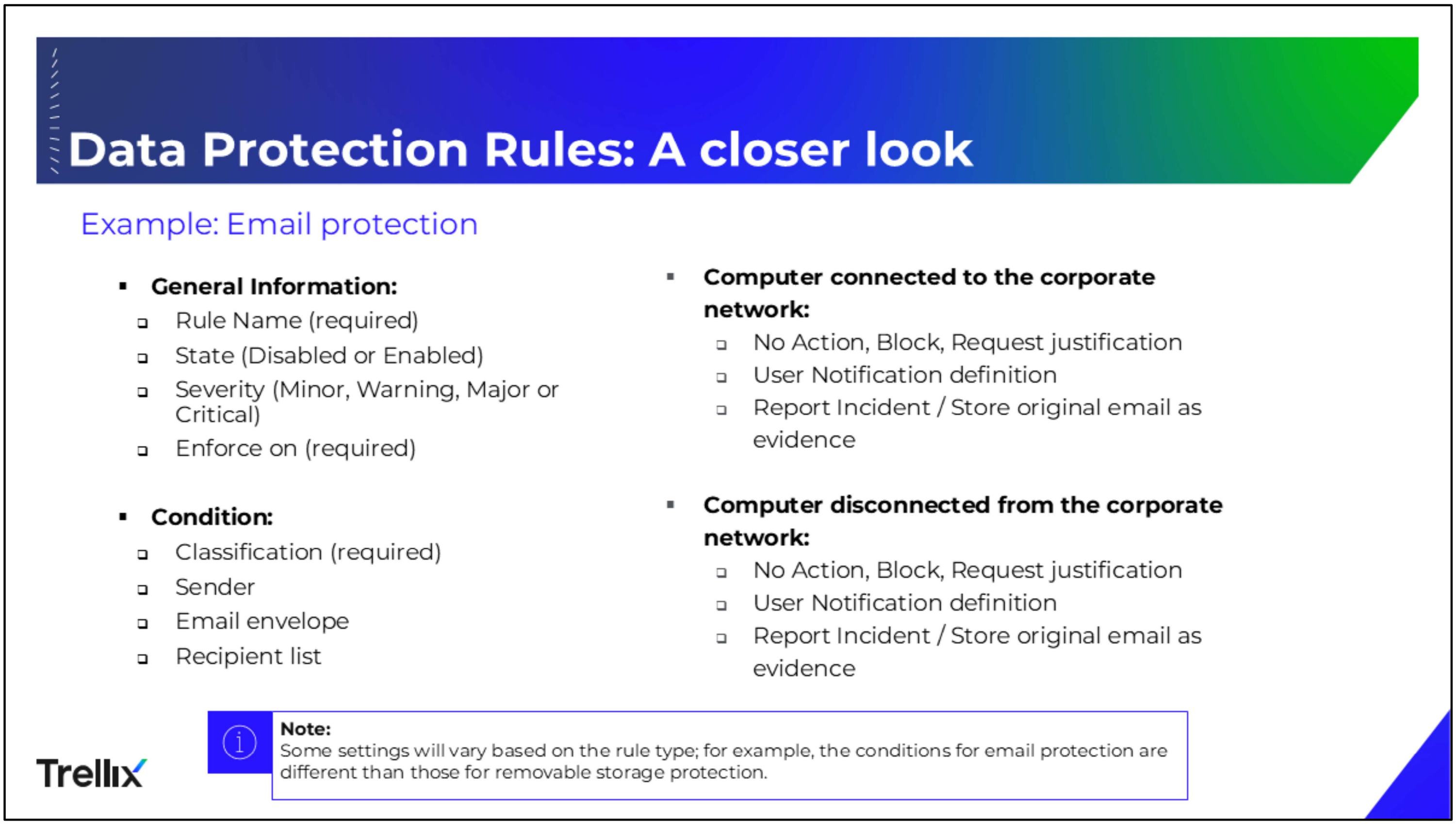
Severity: ● Minor

Enforce On: ☑ Trellix DLP Endpoint for Windows ☐ Trellix DLP Endpoint for Mac OS X ☑ Trellix Network DLP ☐ Skyhigh Security Cloud DLP

General information for configuring rules includes rule name, state, severity, and enforce on.

Like other rule types, basic building blocks for data protection rules are:

- **Condition**: The condition defines what triggers the rule. For data protection and discovery rules, the condition always includes at least one classification. It can include other conditions.
- **Exceptions**: Exceptions define parameters excluded from the rule. For example, a cloud protection rule can allow specified users and classifications to upload data to the specified cloud services, while blocking those users and classifications defined in the condition section of the rule. Exceptions have a separate setting to enable or disable them, allowing you to turn the exception on or off when testing rules. Exceptions are optional.
- **Reaction**: The reaction defines what happens when the rule triggers. The actions available vary with the type of rule, but the default for all rules is No Action. When selected together with the Report Incident option, you can monitor the frequency of rule violations. This procedure is useful for tuning the rule to the correct level to catch data leaks without creating false positives.



Data Protection Rules: A closer look

Example: Email protection

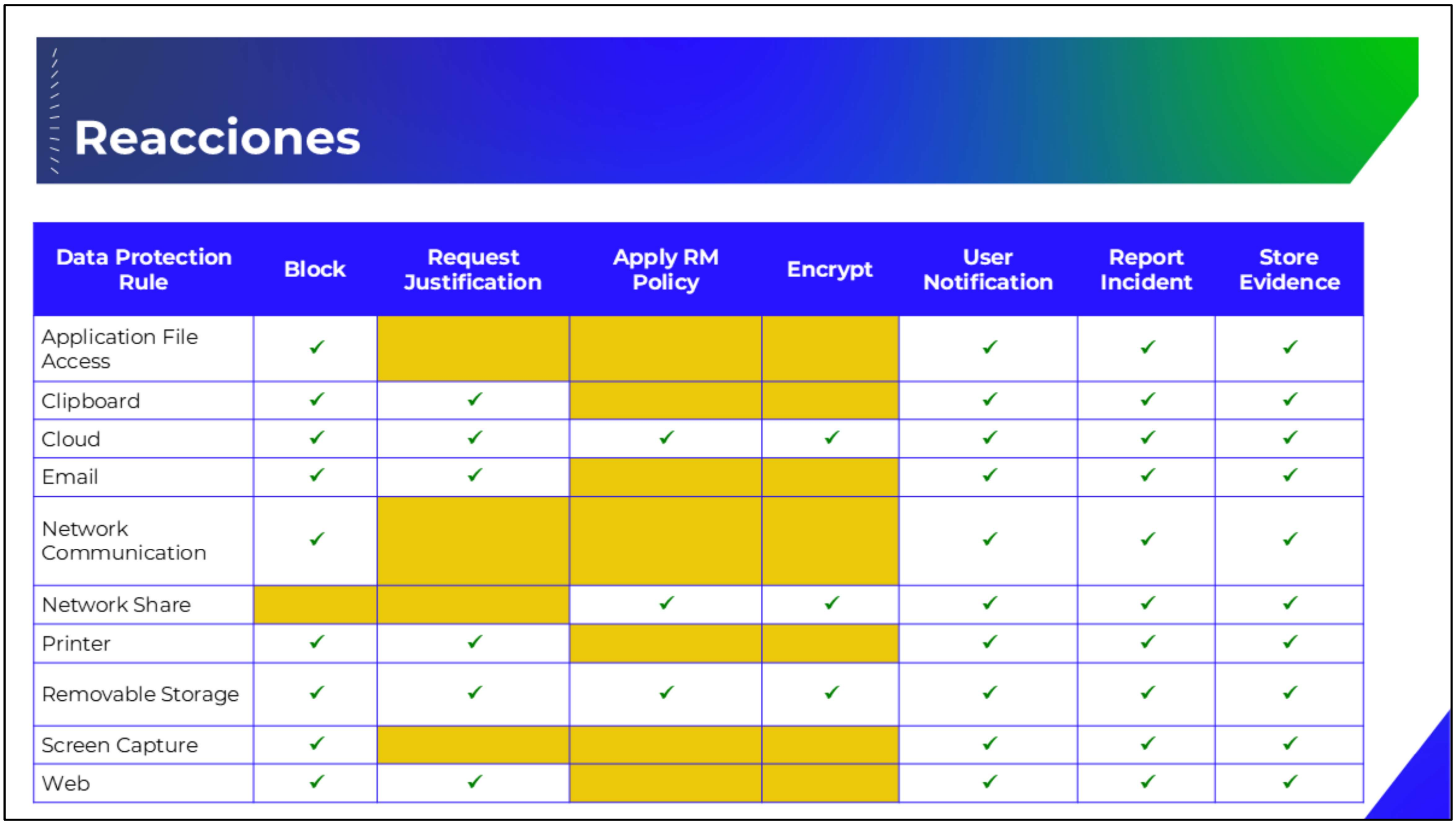
- **General Information:**
  - Rule Name (required)
  - State (Disabled or Enabled)
  - Severity (Minor, Warning, Major or Critical)
  - Enforce on (required)
- **Condition:**
  - Classification (required)
  - Sender
  - Email envelope
  - Recipient list
- **Computer connected to the corporate network:**
  - No Action, Block, Request justification
  - User Notification definition
  - Report Incident / Store original email as evidence
- **Computer disconnected from the corporate network:**
  - No Action, Block, Request justification
  - User Notification definition
  - Report Incident / Store original email as evidence

Note:
Some settings will vary based on the rule type; for example, the conditions for email protection are different than those for removable storage protection.

Trellix

We will now take a closer look at a data protection rule, using email protection as an example. Remember, some settings will vary among rule types.

Email protection rules monitor, or block email sent to specific destinations or users.



Reacciones

Data Protection Rule	Block	Request Justification	Apply RM Policy	Encrypt	User Notification	Report Incident	Store Evidence
Application File Access	✓	🟨	🟨	🟨	✓	✓	✓
Clipboard	✓	✓	🟨	🟨	✓	✓	✓
Cloud	✓	✓	✓	✓	✓	✓	✓
Email	✓	✓	🟨	🟨	✓	✓	✓
Network Communication	✓	🟨	🟨	🟨	✓	✓	✓
Network Share	🟨	🟨	✓	✓	✓	✓	✓
Printer	✓	✓	🟨	🟨	✓	✓	✓
Removable Storage	✓	✓	✓	✓	✓	✓	✓
Screen Capture	✓	🟨	🟨	🟨	✓	✓	✓
Web	✓	✓	🟨	🟨	✓	✓	✓

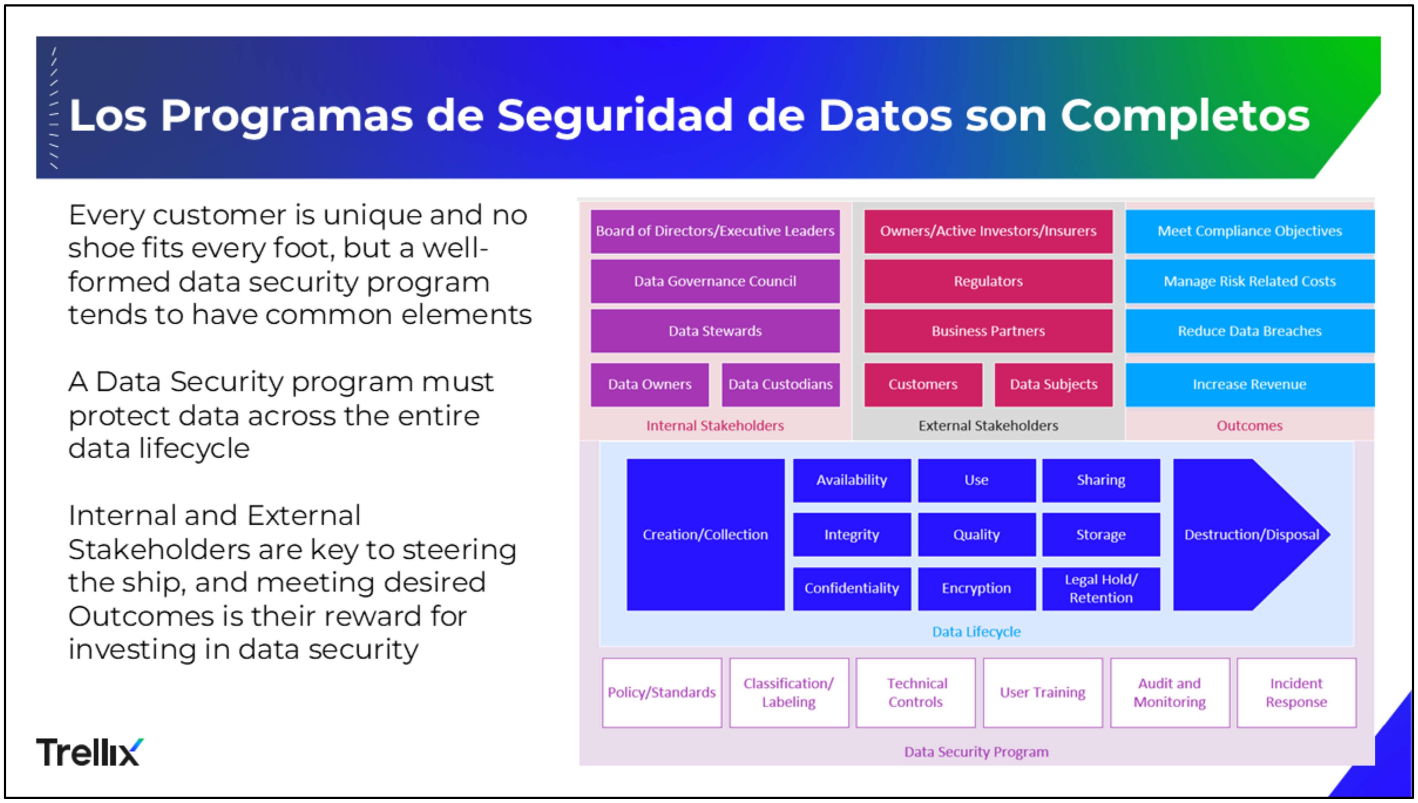
Protection rules define the action taken when an attempt is made to transfer or transmit fingerprinted data.
The table describes the actions available for each protection rule.

On the left you can see all the Protection Rules listed. Across the top lists the actions a Protection Rule can take. Plug and Play device rules, Removable storage device rules, and Discovery rules were covered in earlier lessons and incorporate the use of the remaining actions.

Trellix

Estrategia para el diseño de Políticas y Planificación de una correcta implementación

Manos a la obra



Los Programas de Seguridad de Datos son Completos

Every customer is unique and no shoe fits every foot, but a well-formed data security program tends to have common elements

A Data Security program must protect data across the entire data lifecycle

Internal and External Stakeholders are key to steering the ship, and meeting desired Outcomes is their reward for investing in data security

Board of Directors/Executive Leaders

Data Governance Council

Data Stewards

Data Owners

Data Custodians

Internal Stakeholders

Owners/Active Investors/Insurers

Regulators

Business Partners

Customers

Data Subjects

External Stakeholders

Meet Compliance Objectives

Manage Risk Related Costs

Reduce Data Breaches

Increase Revenue

Outcomes

Creation/Collection

Availability

Use

Sharing

Integrity

Quality

Storage

Confidentiality

Encryption

Legal Hold/ Retention

Destruction/Disposal

Data Lifecycle

Policy/Standards

Classification/ Labeling

Technical Controls

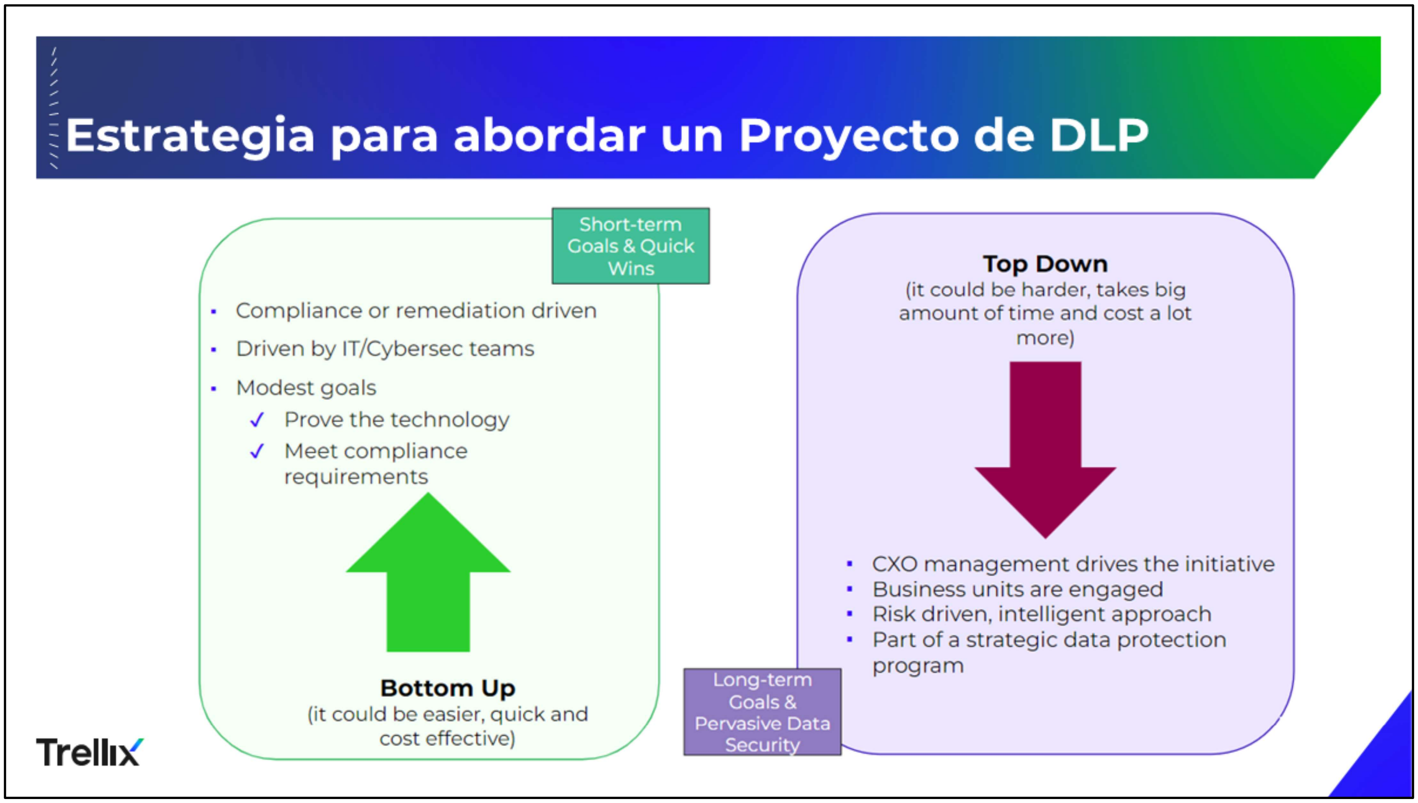
User Training

Audit and Monitoring

Incident Response

Data Security Program

Trellix



Estrategia para abordar un Proyecto de DLP

Short-term Goals & Quick Wins

- Compliance or remediation driven
- Driven by IT/Cybersec teams
- Modest goals
  - ✓ Prove the technology
  - ✓ Meet compliance requirements

Bottom Up
(it could be easier, quick and cost effective)

Top Down
(it could be harder, takes big amount of time and cost a lot more)

- CXO management drives the initiative
- Business units are engaged
- Risk driven, intelligent approach
- Part of a strategic data protection program

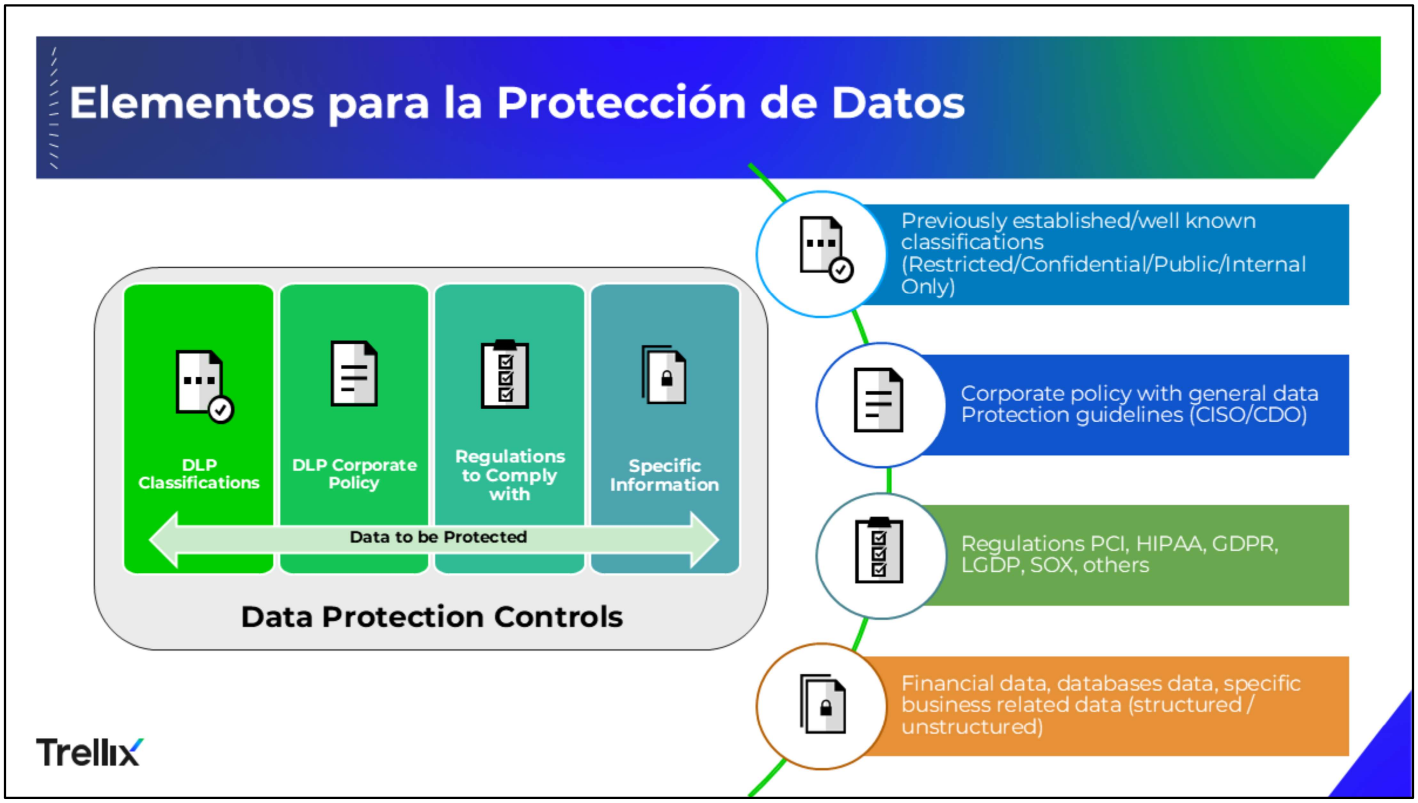
Long-term Goals & Pervasive Data Security

Trellix

Based on the organization strategy, it will be key to define a data protection program strategy aligned with what your organization is trying to accomplish and from where the data protection program is being pushed from.

Both approaches are valid, but one of them delivers the quickest results, quick wins and cost lot less. The Bottom Up approach usually is driven by the IT department or by the Cybersecurity team and it's usually focused on get the essential data classifications and protection controls to protect key business data,and it could involved just a few business units. Very often, there won't be Data Governance, focusing only on key data elements. While this program is easier and quicker to implement, usually will lack of full visibility over the entire organization and lack of government which limit its adoption. Take it as a first approach to full data protection program.

- The Top Down approach is usually drive as an initiative from the C-level that involve the entire organization and the final goal is to have all the necessary elements to protect the data across the organization by implementing a Data Governance through an strategic approach. This program is the best approach to a complete data protection strategy that can be maintained and updated across the time, but it will take far longer than the Bottom Up approach, and it will require far more resources.
- What Trellix Professional Services recommends?. Its all depends on your budget and current needs, if you have no previous experience with Data Protection and you're looking for a short term win that could help you drive a biggest budget-project later, definitely starting with the Bottom Up approach will help you get the support you're looking for.



Elementos para la Protección de Datos

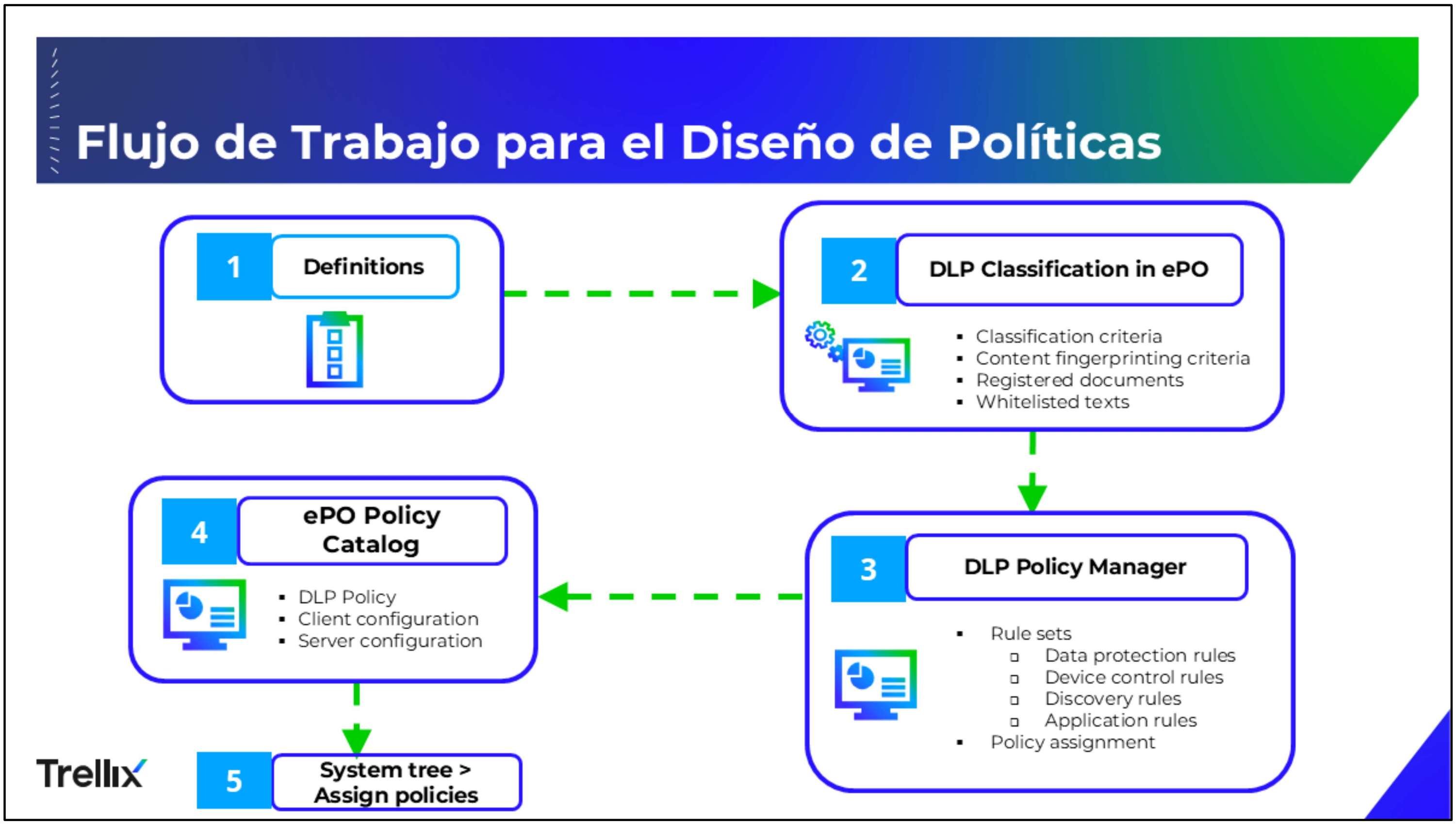
Previously established/well known classifications (Restricted/Confidential/Public/Internal Only)

Corporate policy with general data Protection guidelines (CISO/CDO)

Regulations PCI, HIPAA, GDPR, LGDP, SOX, others

Financial data, databases data, specific business related data (structured / unstructured)

Trellix



Flujo de Trabajo para el Diseño de Políticas

1 Definitions

2 DLP Classification in ePO

- Classification criteria
- Content fingerprinting criteria
- Registered documents
- Whitelisted texts

3 DLP Policy Manager

- Rule sets
  - Data protection rules
  - Device control rules
  - Discovery rules
  - Application rules
- Policy assignment

4 ePO Policy Catalog

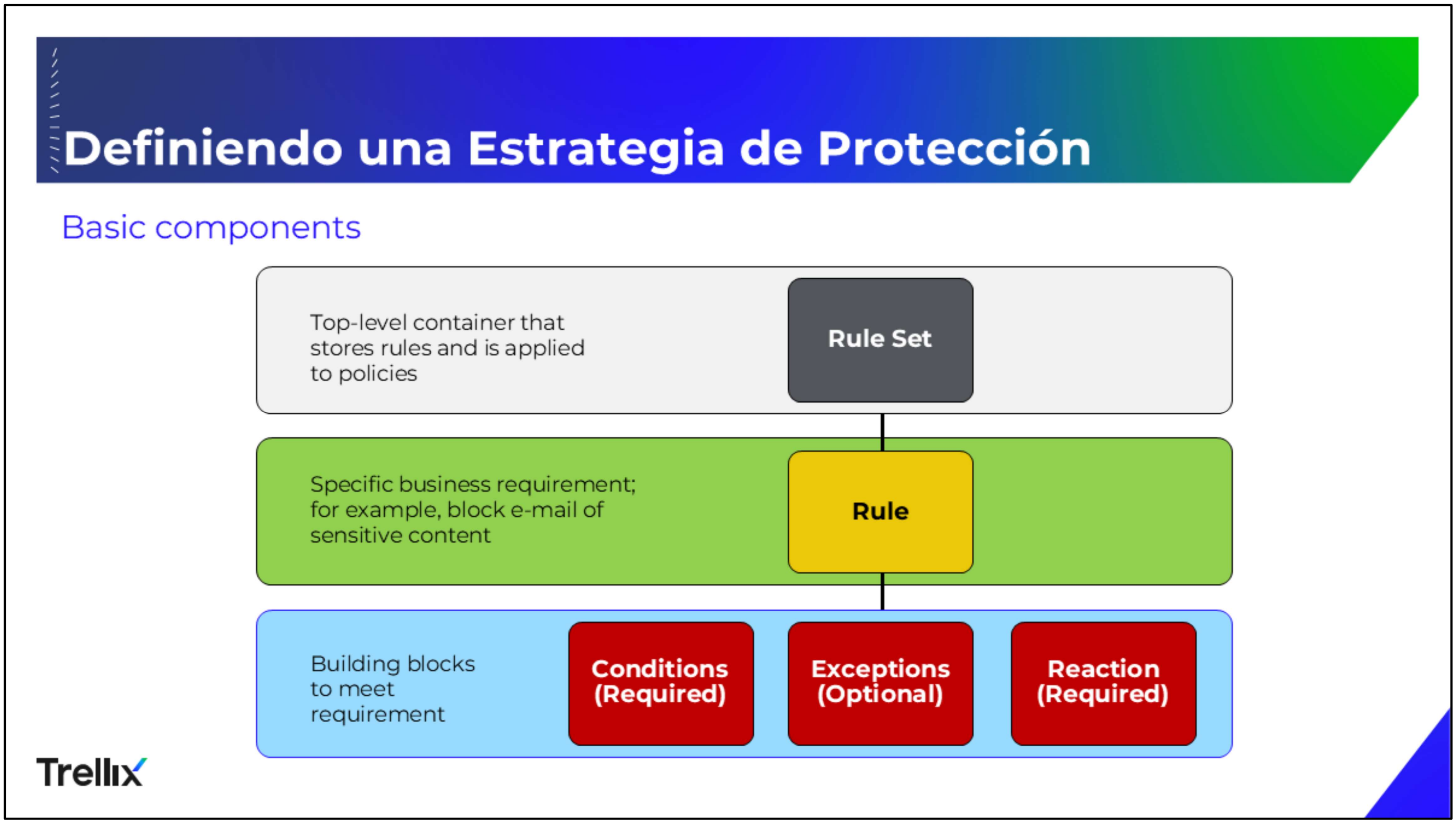
- DLP Policy
- Client configuration
- Server configuration

5 System tree > Assign policies

Trellix

A **Policy** consists of rules, grouped into rule sets. Rules use classifications and definitions to specify what DLP detects. Rule reactions determine the action to take when data matches the rule.
Use the following workflow for creating policies.

1. Create classifications and definitions.
2. Create data protection, device, or discovery rules. All rules require either classifications or definitions in the rule.
3. Assign rule sets to DLP policies.
4. Create scan definitions.
5. Assign policies to system.



Definiendo una Estrategia de Protección

Basic components

Top-level container that stores rules and is applied to policies

Rule Set

Specific business requirement; for example, block e-mail of sensitive content

Rule

Building blocks to meet requirement

Conditions (Required)

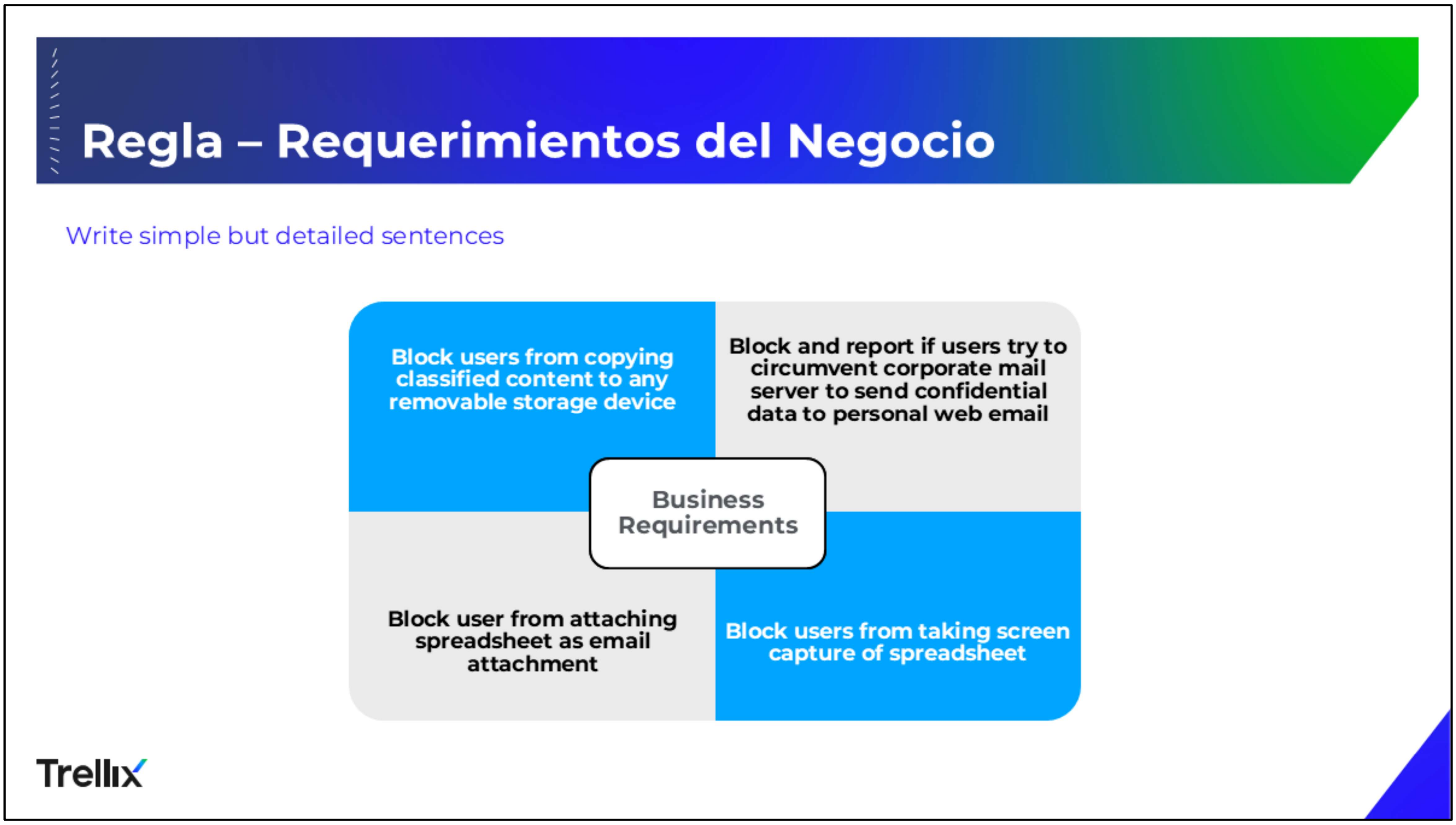
Exceptions (Optional)

Reaction (Required)

When planning a protection strategy, it is important to understand the basic components of rule sets and rules and how these components interwork.

The Rule Set is a high-level container that stores one of more rules. It is applied to policies.
Each rules maps to a specific business requirement; for example, block users from copying sensitive content to a removable storage device.

Finally, each rule consists of basic building blocks that define how to meet the requirements. You must define Conditions and Reactions. You can also optionally define Exceptions.



Regla – Requerimientos del Negocio

Write simple but detailed sentences

Block users from copying classified content to any removable storage device

Block and report if users try to circumvent corporate mail server to send confidential data to personal web email

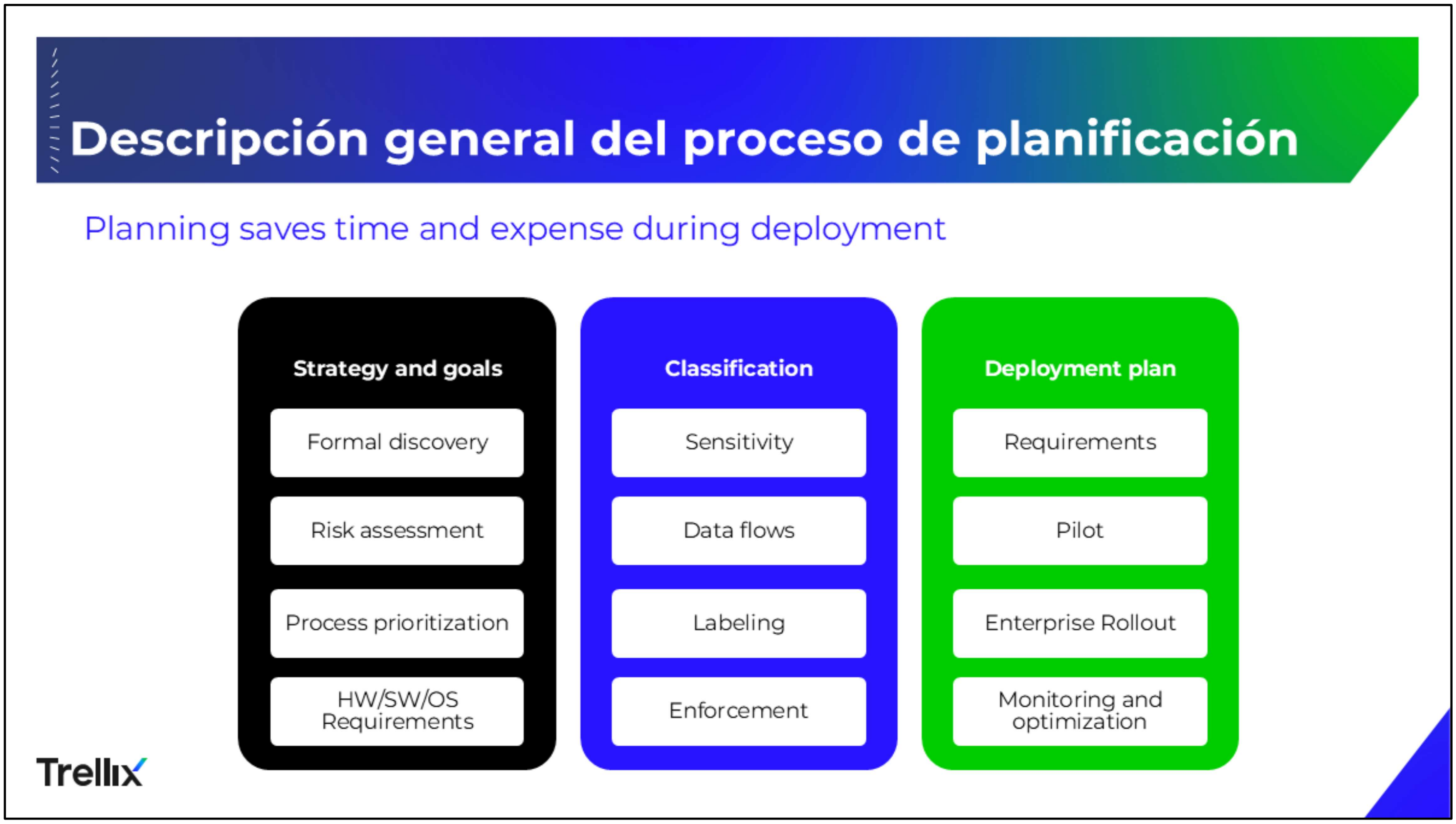
Business Requirements

Block user from attaching spreadsheet as email attachment

Block users from taking screen capture of spreadsheet

A critical part of your data protection strategy is to define each business requirement. Describe the business requirement in simple but detailed sentences; for example:

- Block users from copying classified content to any removable storage device and apply to ALL authorized removable media users but exclude SSN authorized users
- Block and report if users try to circumvent corporate mail server to send confidential data to a personal web email address.
- Block users from taking screen capture of a spreadsheet.
- Block user from attaching a spreadsheet document as an email attachment.



Descripción general del proceso de planificación

Planning saves time and expense during deployment

Strategy and goals

- Formal discovery
- Risk assessment
- Process prioritization
- HW/SW/OS Requirements

Classification

- Sensitivity
- Data flows
- Labeling
- Enforcement

Deployment plan

- Requirements
- Pilot
- Enterprise Rollout
- Monitoring and optimization

We will first review the importance of planning your deployment, as well as recommended planning phases. Time invested in planning saves time and expense during deployment. We will take a closer look at each phase in the subsequent sections.

Program strategy and goals
The first phase of the data security program is to define the program strategy and goals. This process normally entails formal discovery and risk assessment to identify and prioritize process and control gaps. Time invested in this phase saves time and expense during deployment, increasing the likelihood of success.

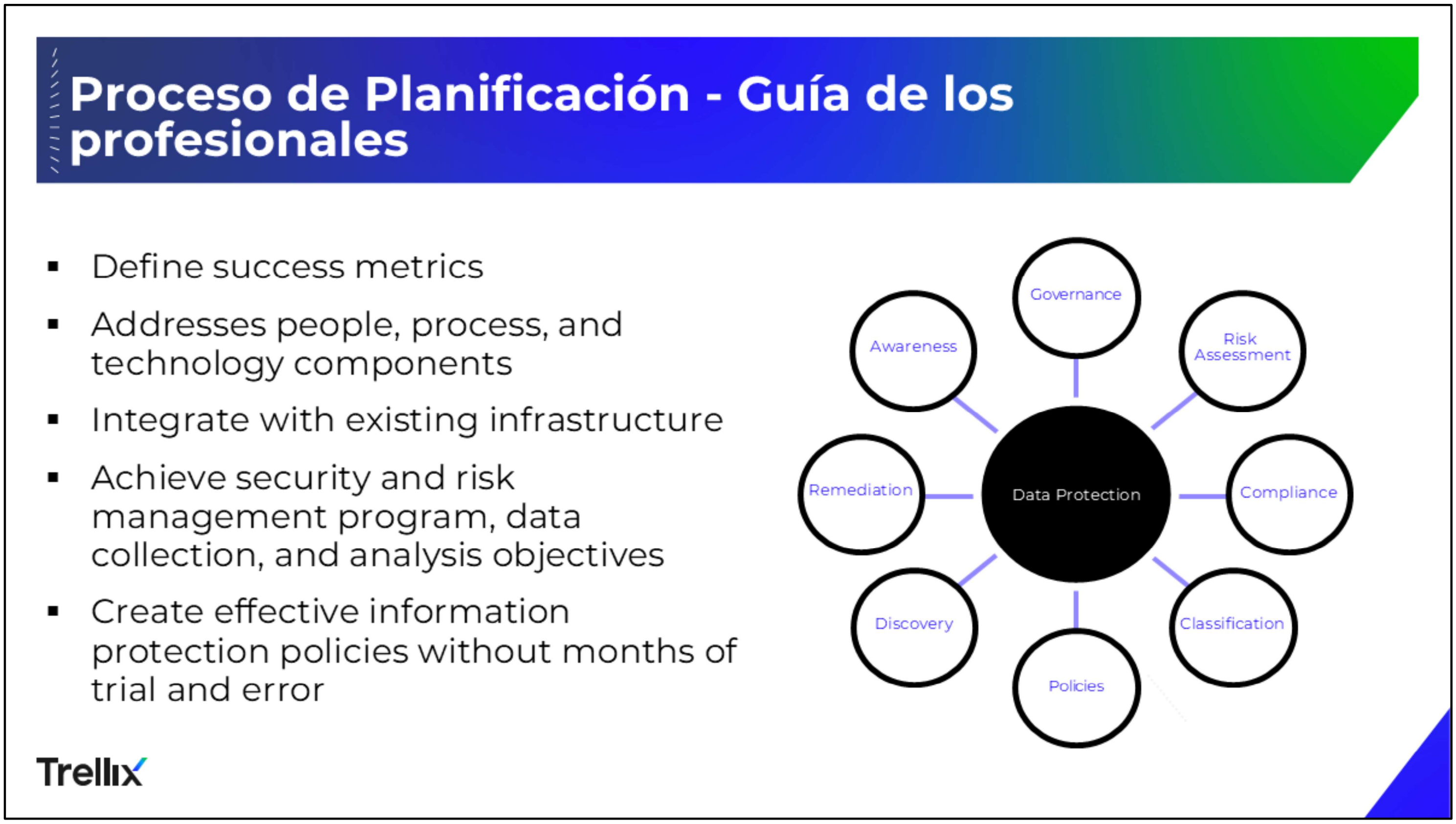
Data classification and policy architecture
Accurate data classifications and useful policies form the core of an effective data security program. This process is best implemented when this phase is broken into several steps:

- Establish data sensitivity classifications by identifying the necessary classification levels and associated definitions.
- Document data flows to create a catalog of the types and sources of data that will use the labels; consider the application sources, locations, and content types.
- Apply labels to the data and enforce the data classification program with a strong DLP solution.

Deployment plan
After defining procedures and controls in the strategy and planning phases, move forward with measures to ensure these processes are adhered to and enforced throughout the organization. Some key considerations are:

- Identify solution requirements and ensure applications compatibility.
- Plan the pilot, including how to validate its success.
- After the deployment, plan its formal rollout in the Enterprise environment.

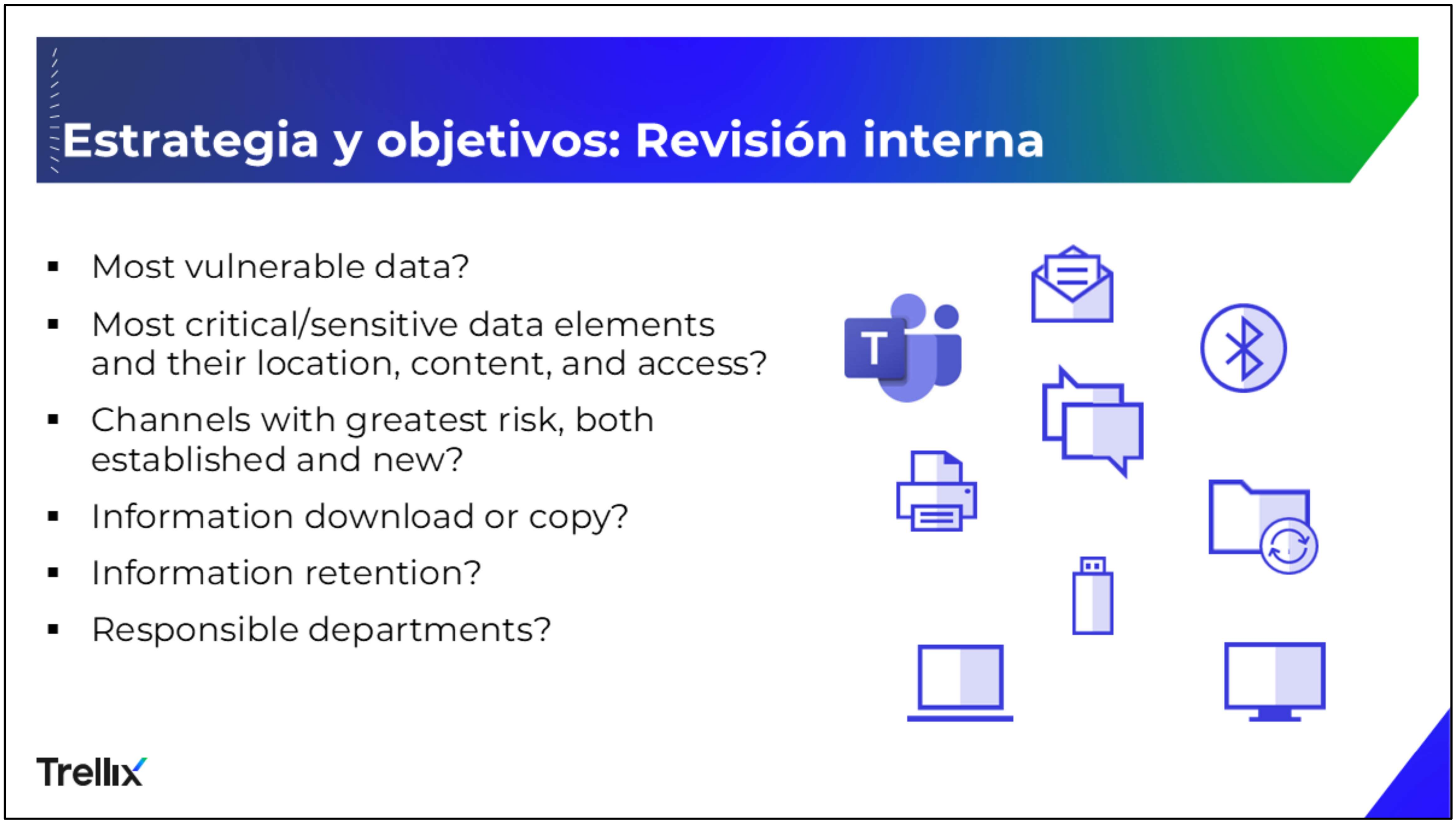
- In addition, plan measures for monitoring and optimizing the solution.



Proceso de Planificación - Guía de los profesionales

- Define success metrics
- Addresses people, process, and technology components
- Integrate with existing infrastructure
- Achieve security and risk management program, data collection, and analysis objectives
- Create effective information protection policies without months of trial and error

Another method of looking at the importance of having a solid deployment plan can been conducted in the Hub and Spoke model represented here.

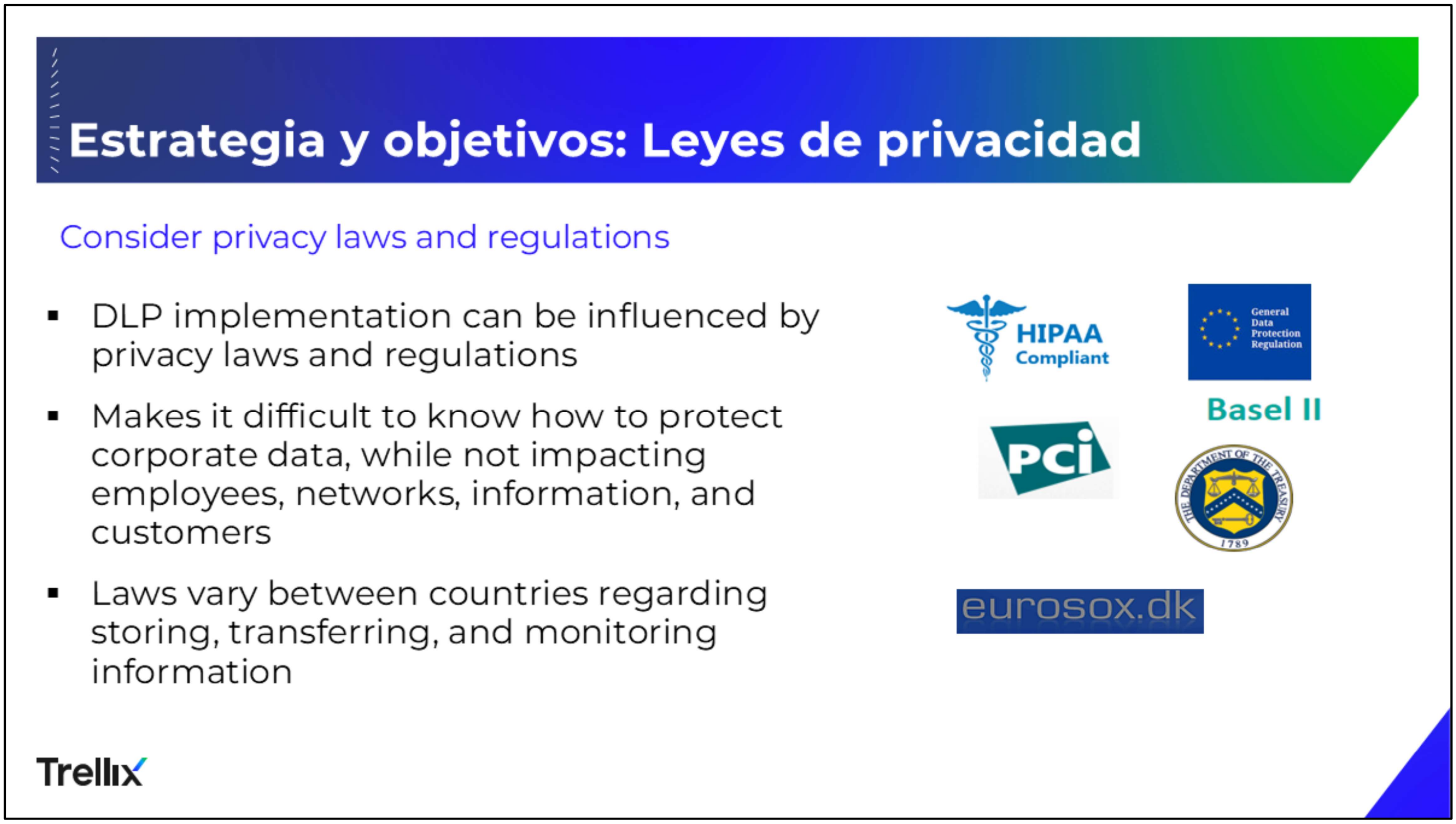


Estrategia y objetivos: Revisión interna

- Most vulnerable data?
- Most critical/sensitive data elements and their location, content, and access?
- Channels with greatest risk, both established and new?
- Information download or copy?
- Information retention?
- Responsible departments?

An internal assessment includes a broad assessment of internal data security controls (such as database access) to identify sources of data leaks that might indicate insecure internal processes. Some questions to ask are:

- What are your most vulnerable data elements in your organization, how are they currently accessed, and which departments within your organization are responsible for those data elements?
- What are your most critical/sensitive data elements and their location, content, and access?
- Do you know which channels pose the greatest risk of data loss? This includes established channels, such as email, removable storage, web access, printing. It also includes newer channels, such as instant messaging, Wi-Fi, and Bluetooth.
- Do you allow users to download or copy any of the above types of information to desktops, laptops, or servers?
- Do you allow users to retain any of the above information on desktops, laptops, or servers? If so, what applications or tools are used?
- What departments within your organization that handles the above information? If so, what applications or tools are used?



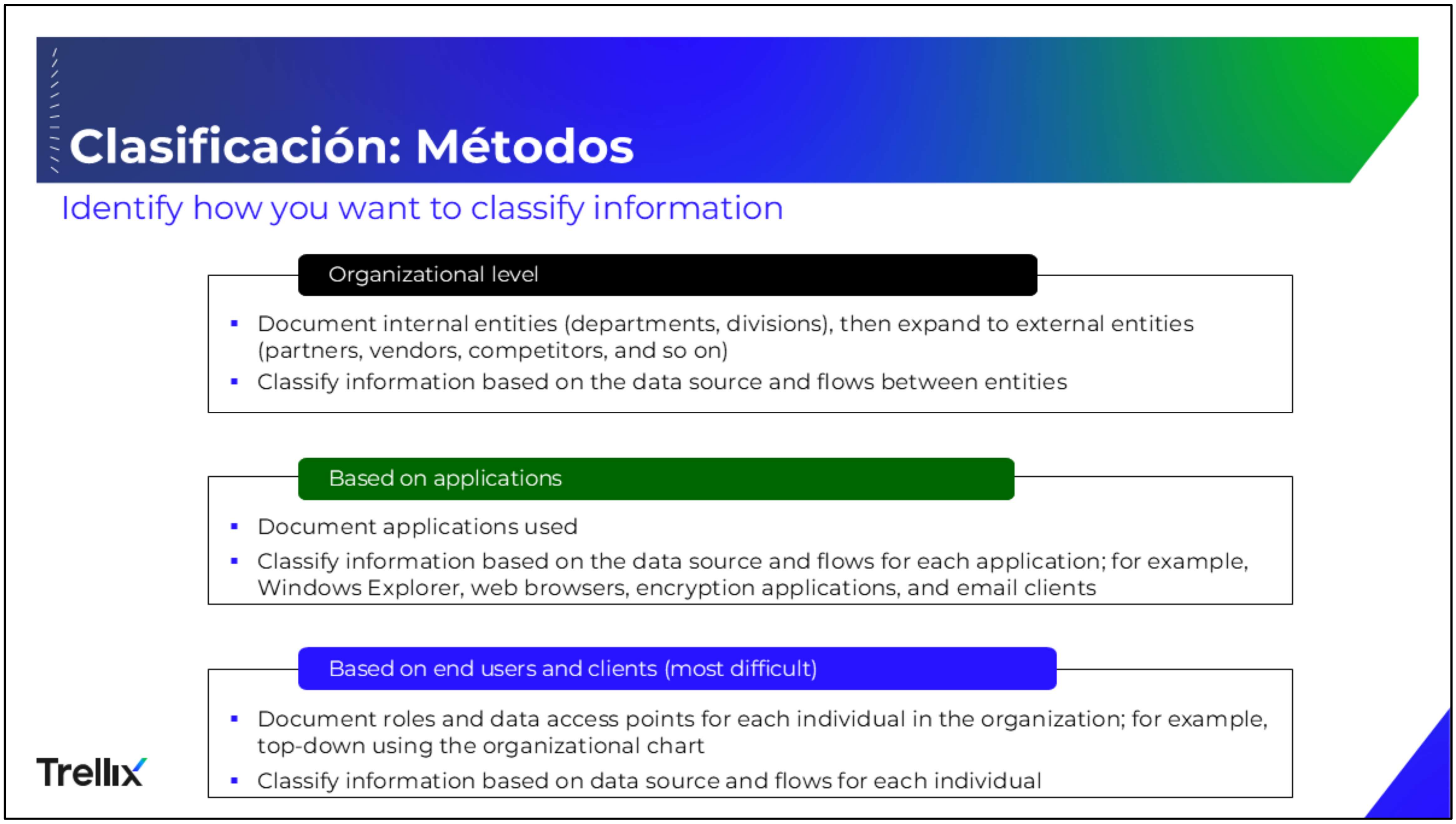
Estrategia y objetivos: Leyes de privacidad

Consider privacy laws and regulations

- DLP implementation can be influenced by privacy laws and regulations
- Makes it difficult to know how to protect corporate data, while not impacting employees, networks, information, and customers
- Laws vary between countries regarding storing, transferring, and monitoring information

HIPAA Compliant
General Data Protection Regulation
Basel II
PCi
THE DEPARTMENT OF THE TREASURY 1789
eurosox.dk
Trellix

When deciding how to implement a DLP solution, consider for a moment how this may be affected by privacy laws in your region. The variety of privacy laws and regulations makes it difficult for companies to know what they can and must do to protect themselves, their employees, their networks, confidential information, and customers. For example, a company’s ability to process, store, transfer, and monitor their employees’ use of confidential information may vary greatly depending upon where the data comes from and where it will be sent. Different countries apply different standards for the collection, processing, and transfer of personal data. As a result, it has become essential for companies operating internationally to understand relevant laws for each jurisdiction in which they operate.



Clasificación: Métodos

Identify how you want to classify information

Organizational level

- Document internal entities (departments, divisions), then expand to external entities (partners, vendors, competitors, and so on)
- Classify information based on the data source and flows between entities

Based on applications

- Document applications used
- Classify information based on the data source and flows for each application; for example, Windows Explorer, web browsers, encryption applications, and email clients

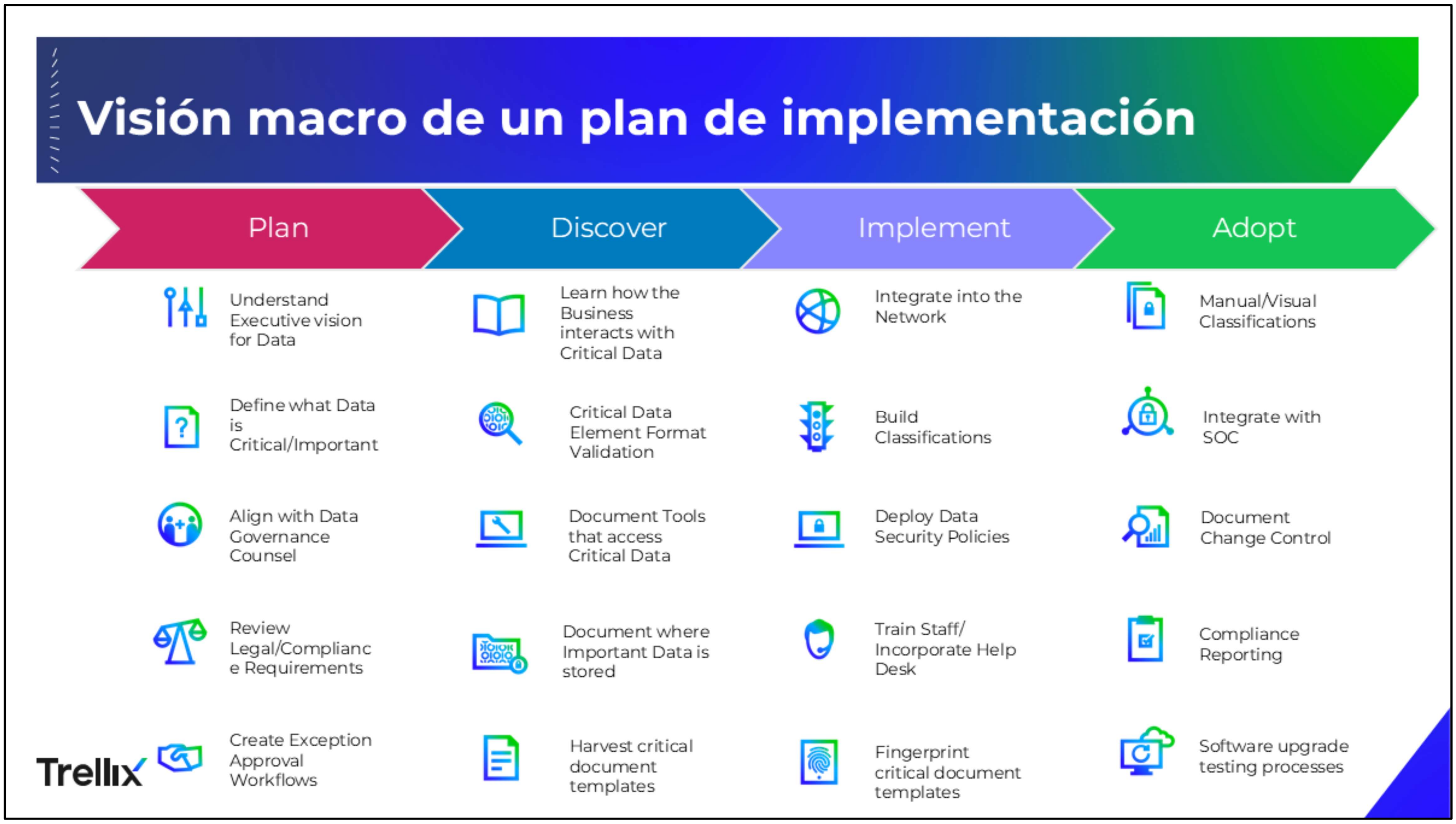
Based on end users and clients (most difficult)

- Document roles and data access points for each individual in the organization; for example, top-down using the organizational chart
- Classify information based on data source and flows for each individual

Trellix

Identify how you want to classify data. Some ways are:

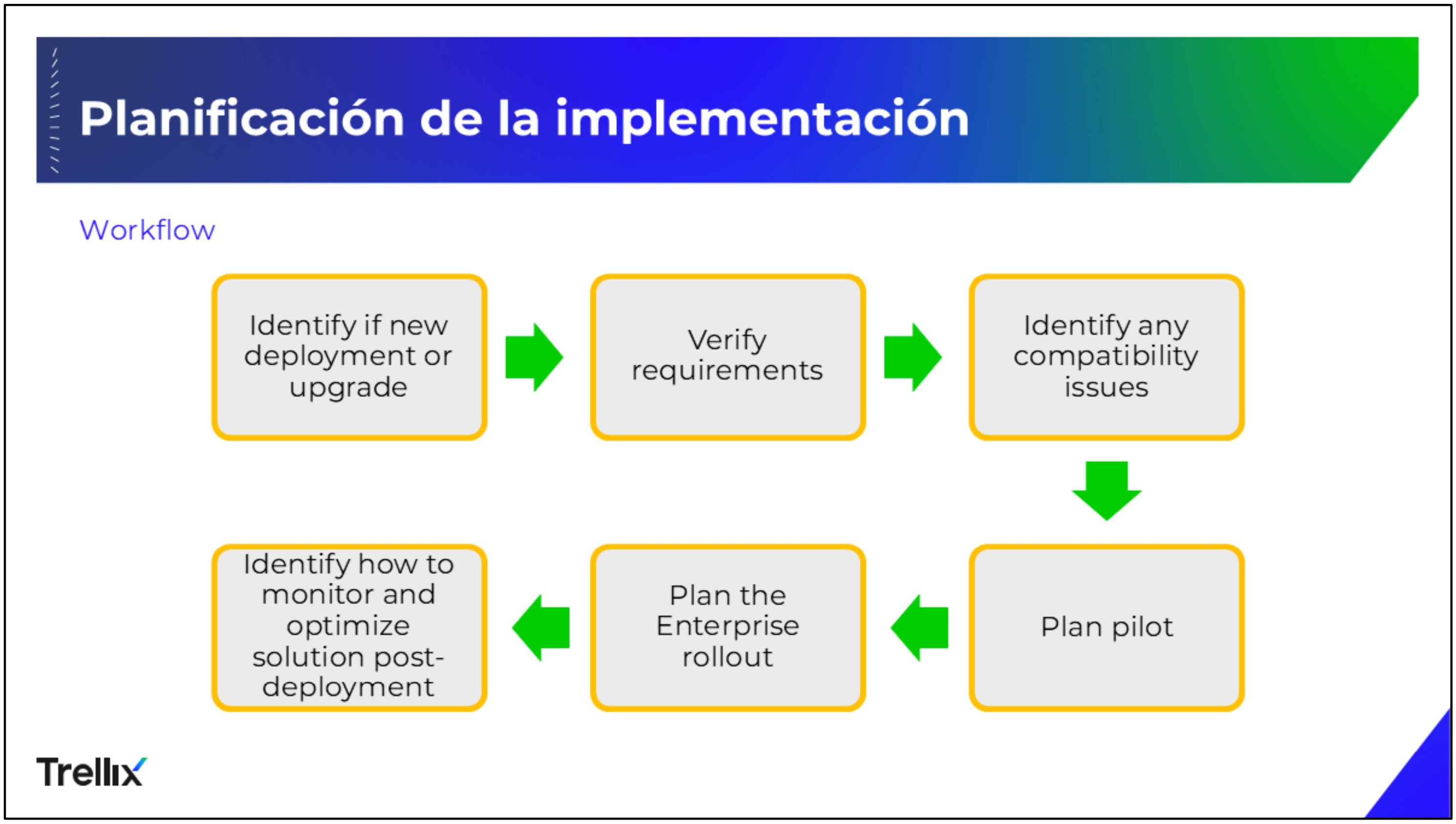
- **At the organizational level**: Document the various entities within the Enterprise; for example, departments and divisions. Expand this list to identify external entities, such as partners, vendors, and even competitors. Classify information, based on data flows between internal and external entities.
- **Based on applications**: Build a comprehensive list of applications (software, programs, and so on) that the organization uses. Using this list, identify and classify information based on source and flows of each application. Some examples include Windows Explorer, web browsers, encryption applications, and email clients.
- **Based on end users and clients**: Begin with the Enterprise's pre-existing structure, the organizational chart. This top-down approach moves from the head of the organization down the chart, identifying the data access points for each individual. After identifying the data points, classify the information.



Visión macro de un plan de implementación

Plan	Discover	Implement	Adopt
Understand Executive vision for Data	Learn how the Business interacts with Critical Data	Integrate into the Network	Manual/Visual Classifications
Define what Data is Critical/Important	Critical Data Element Format Validation	Build Classifications	Integrate with SOC
Align with Data Governance Counsel	Document Tools that access Critical Data	Deploy Data Security Policies	Document Change Control
Review Legal/Complianc e Requirements	Document where Important Data is stored	Train Staff/ Incorporate Help Desk	Compliance Reporting
Create Exception Approval Workflows	Harvest critical document templates	Fingerprint critical document templates	Software upgrade testing processes

Trellix



Planificación de la implementación

Workflow

Identify if new deployment or upgrade

Verify requirements

Identify any compatibility issues

Plan pilot

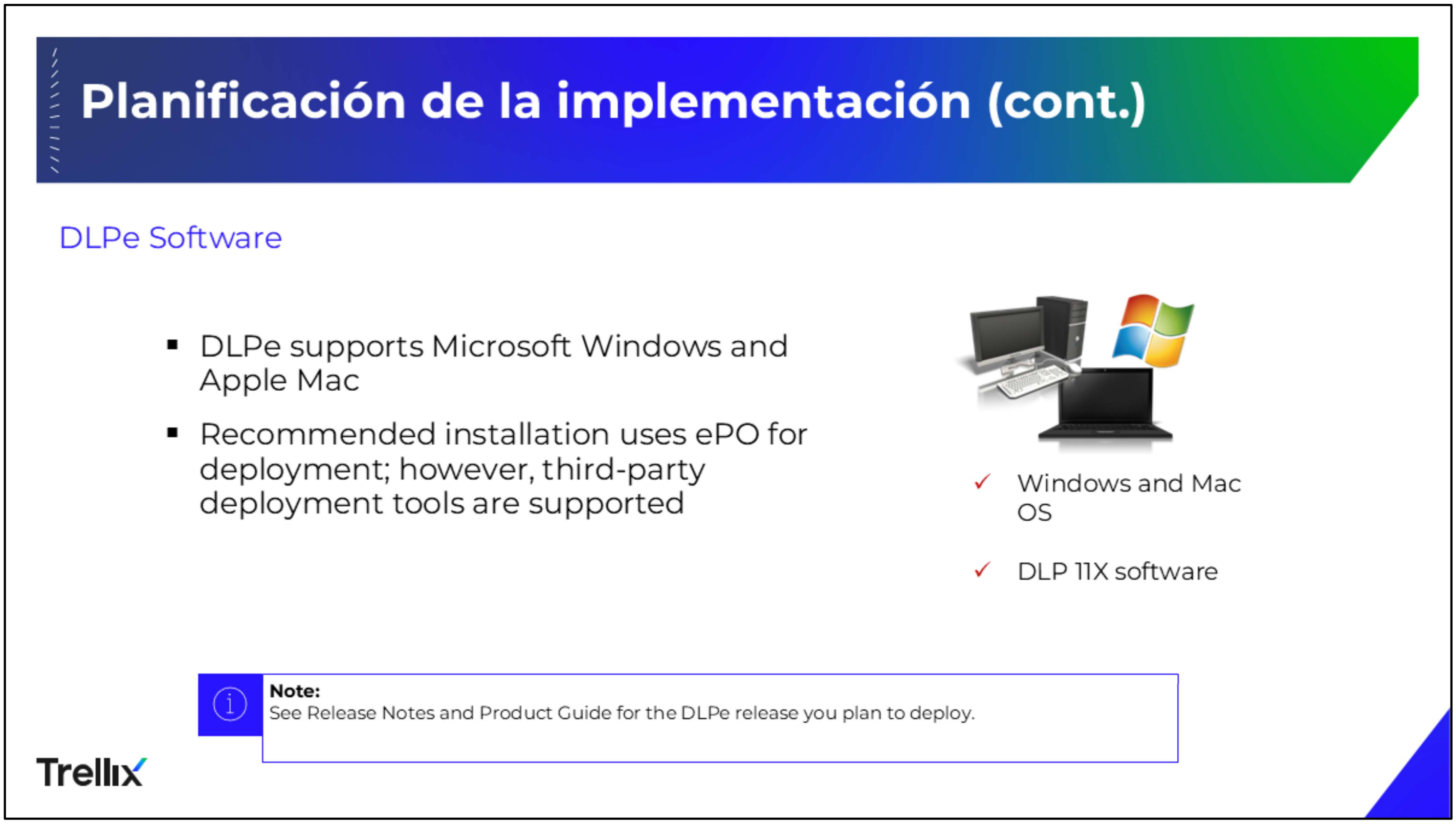
Plan the Enterprise rollout

Identify how to monitor and optimize solution post-deployment

Trellix

After defining procedures and controls in the strategy and planning phases, a data security program must move forward with measures to ensure these processes are adhered to and enforced throughout the organization. A typical DLPe deployment follows this sequence:

- Identify the deployment type, as this impacts the requirements.
- Verify solution requirements are met, including applications compatibility.
- Plan the pilot, including test systems, hosts, users, and rule sets.
- Plan the rollout to the Enterprise, including how to measure its success.
- Identify how to monitor the solution, as well as way to optimize it.



Planificación de la implementación (cont.)

DLPe Software

- DLPe supports Microsoft Windows and Apple Mac
- Recommended installation uses ePO for deployment; however, third-party deployment tools are supported

✓ Windows and Mac OS

✓ DLP 11X software

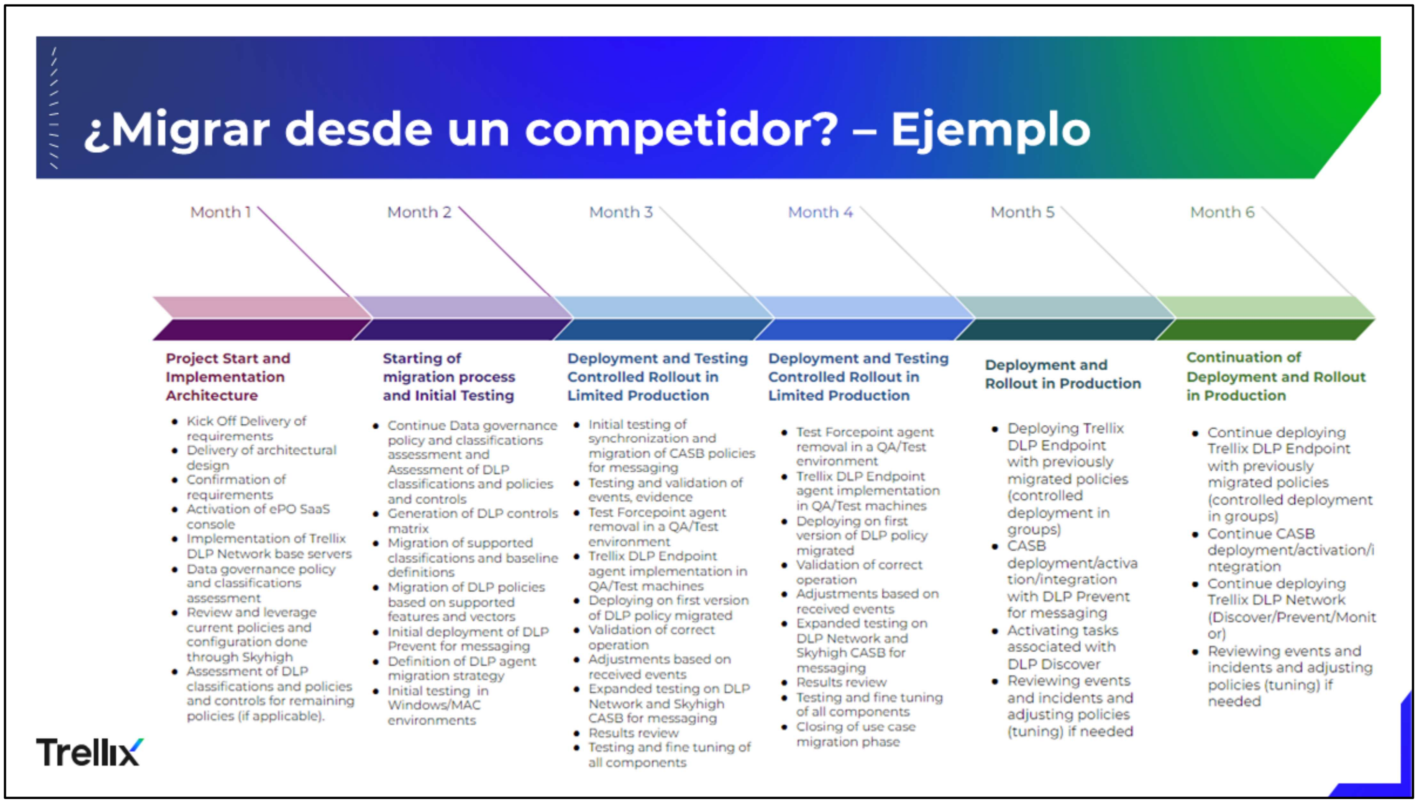
Note:
See Release Notes and Product Guide for the DLPe release you plan to deploy.

Trellix

The **DLPe Client** is available in two versions, one for Microsoft Windows and one for Apple Mac computers. The recommended installation of the client software uses the ePO infrastructure for deployment to the endpoint computers.

You can also deploy DLPe client software to your network using third-party enterprise software deployment tools.

For more information, see the DLPe Product Guide and the release notes for the DLPe release you plan to deploy.



¿Migrar desde un competidor? – Ejemplo

Month 1

Project Start and Implementation Architecture

- Kick Off Delivery of requirements
- Delivery of architectural design
- Confirmation of requirements
- Activation of ePO SaaS console
- Implementation of Trellix DLP Network base servers
- Data governance policy and classifications assessment
- Review and leverage current policies and configuration done through Skyhigh
- Assessment of DLP classifications and policies and controls for remaining policies (if applicable).

Month 2

Starting of migration process and Initial Testing

- Continue Data governance policy and classifications assessment and Assessment of DLP classifications and policies and controls
- Generation of DLP controls matrix
- Migration of supported classifications and baseline definitions
- Migration of DLP policies based on supported features and vectors
- Initial deployment of DLP Prevent for messaging
- Definition of DLP agent migration strategy
- Initial testing in Windows/MAC environments

Month 3

Deployment and Testing Controlled Rollout in Limited Production

- Initial testing of synchronization and migration of CASB policies for messaging
- Testing and validation of events, evidence
- Test Forcepoint agent removal in a QA/Test environment
- Trellix DLP Endpoint agent implementation in QA/Test machines
- Deploying on first version of DLP policy migrated
- Validation of correct operation
- Adjustments based on received events
- Expanded testing on DLP Network and Skyhigh CASB for messaging
- Results review
- Testing and fine tuning of all components

Month 4

Deployment and Testing Controlled Rollout in Limited Production

- Test Forcepoint agent removal in a QA/Test environment
- Trellix DLP Endpoint agent implementation in QA/Test machines
- Deploying on first version of DLP policy migrated
- Validation of correct operation
- Adjustments based on received events
- Expanded testing on DLP Network and Skyhigh CASB for messaging
- Results review
- Testing and fine tuning of all components
- Closing of use case migration phase

Month 5

Deployment and Rollout in Production

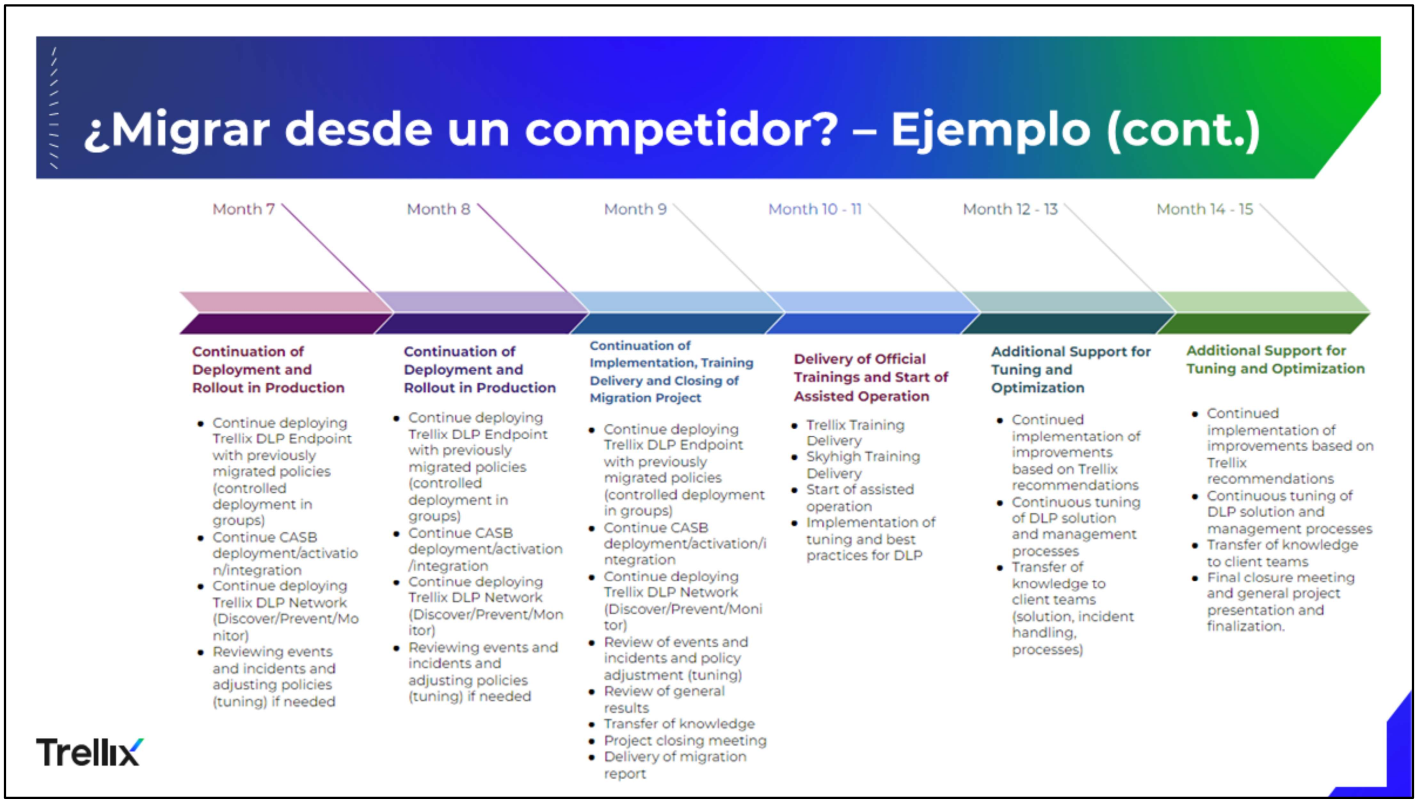
- Deploying Trellix DLP Endpoint with previously migrated policies (controlled deployment in groups)
- CASB deployment/activation/integration with DLP Prevent for messaging
- Activating tasks associated with DLP Discover
- Reviewing events and incidents and adjusting policies (tuning) if needed

Month 6

Continuation of Deployment and Rollout in Production

- Continue deploying Trellix DLP Endpoint with previously migrated policies (controlled deployment in groups)
- Continue CASB deployment/activation/integration
- Continue deploying Trellix DLP Network (Discover/Prevent/Monitor)
- Reviewing events and incidents and adjusting policies (tuning) if needed

Trellix



¿Migrar desde un competidor? – Ejemplo (cont.)

Month 7

Continuation of Deployment and Rollout in Production

- Continue deploying Trellix DLP Endpoint with previously migrated policies (controlled deployment in groups)
- Continue CASB deployment/activation/integration
- Continue deploying Trellix DLP Network (Discover/Prevent/Monitor)
- Reviewing events and incidents and adjusting policies (tuning) if needed

Month 8

Continuation of Deployment and Rollout in Production

- Continue deploying Trellix DLP Endpoint with previously migrated policies (controlled deployment in groups)
- Continue CASB deployment/activation/integration
- Continue deploying Trellix DLP Network (Discover/Prevent/Monitor)
- Reviewing events and incidents and adjusting policies (tuning) if needed

Month 9

Continuation of Implementation, Training Delivery and Closing of Migration Project

- Continue deploying Trellix DLP Endpoint with previously migrated policies (controlled deployment in groups)
- Continue CASB deployment/activation/integration
- Continue deploying Trellix DLP Network (Discover/Prevent/Monitor)
- Review of events and incidents and policy adjustment (tuning)
- Review of general results
- Transfer of knowledge
- Project closing meeting
- Delivery of migration report

Month 10 - 11

Delivery of Official Trainings and Start of Assisted Operation

- Trellix Training Delivery
- Skyhigh Training Delivery
- Start of assisted operation
- Implementation of tuning and best practices for DLP

Month 12 - 13

Additional Support for Tuning and Optimization

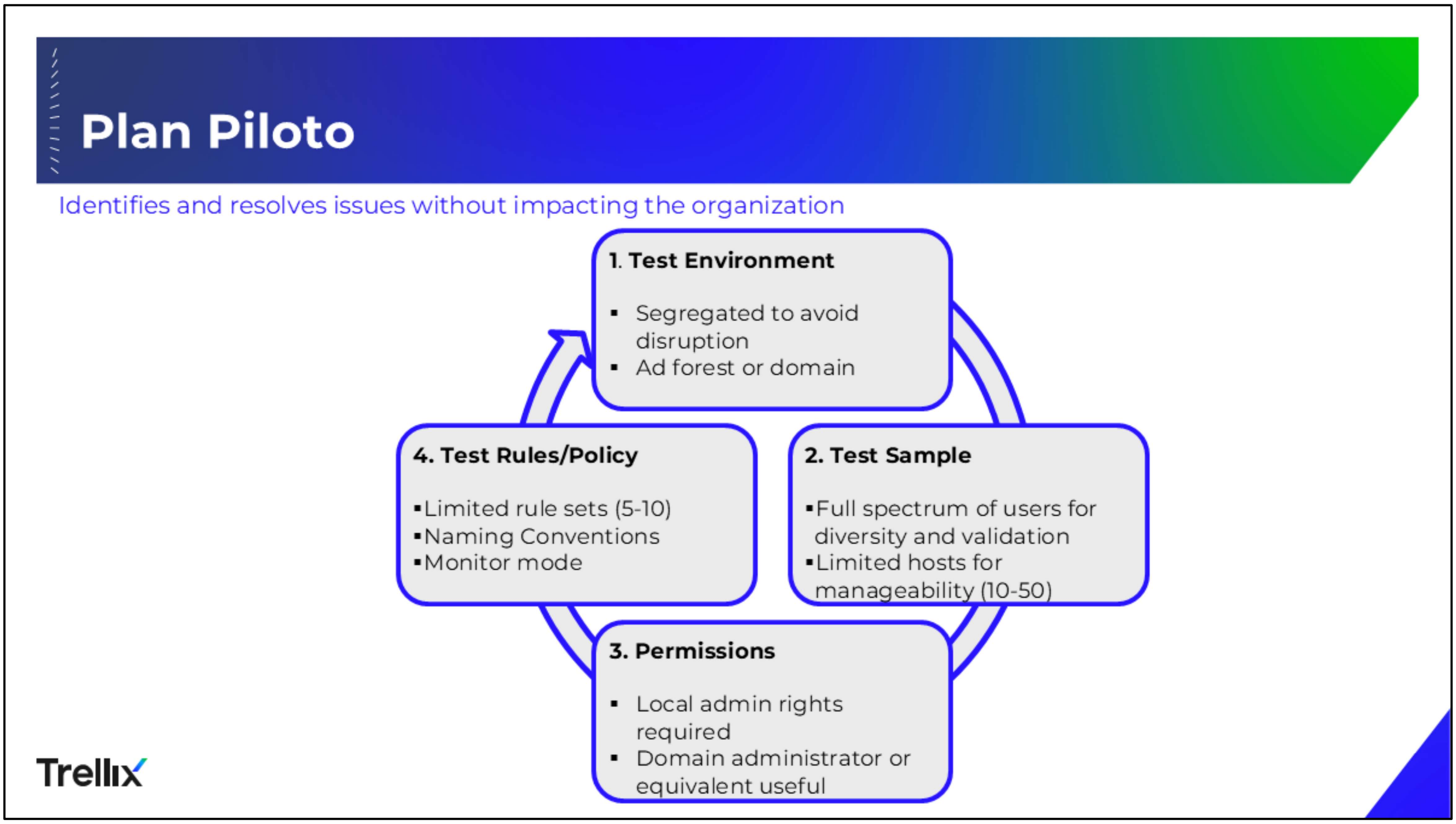
- Continued implementation of improvements based on Trellix recommendations
- Continuous tuning of DLP solution and management processes
- Transfer of knowledge to client teams (solution, incident handling, processes)

Month 14 - 15

Additional Support for Tuning and Optimization

- Continued implementation of improvements based on Trellix recommendations
- Continuous tuning of DLP solution and management processes
- Transfer of knowledge to client teams
- Final closure meeting and general project presentation and finalization.

Trellix



Plan Piloto

Identifies and resolves issues without impacting the organization

1. Test Environment

- Segregated to avoid disruption
- Ad forest or domain

2. Test Sample

▪Full spectrum of users for diversity and validation
▪Limited hosts for manageability (10-50)

3. Permissions

- Local admin rights required
- Domain administrator or equivalent useful

4. Test Rules/Policy

▪Limited rule sets (5-10)
▪Naming Conventions
▪Monitor mode

Trellix

It is crucial to pilot the deployment before rollout to the enterprise. This allows you to identify and resolve any issues without impacting the organization.
Note: Many administrators can perform these steps themselves. If you prefer, partners and service professionals can assist you. These experts contributed heavily to this guide. They follow a similar process, as it reliably activates the risk mitigation most businesses need.

Stress the importance of a controlled Host IPS deployment in a test network. This lets you resolve any potential issues without impacting enterprise service.

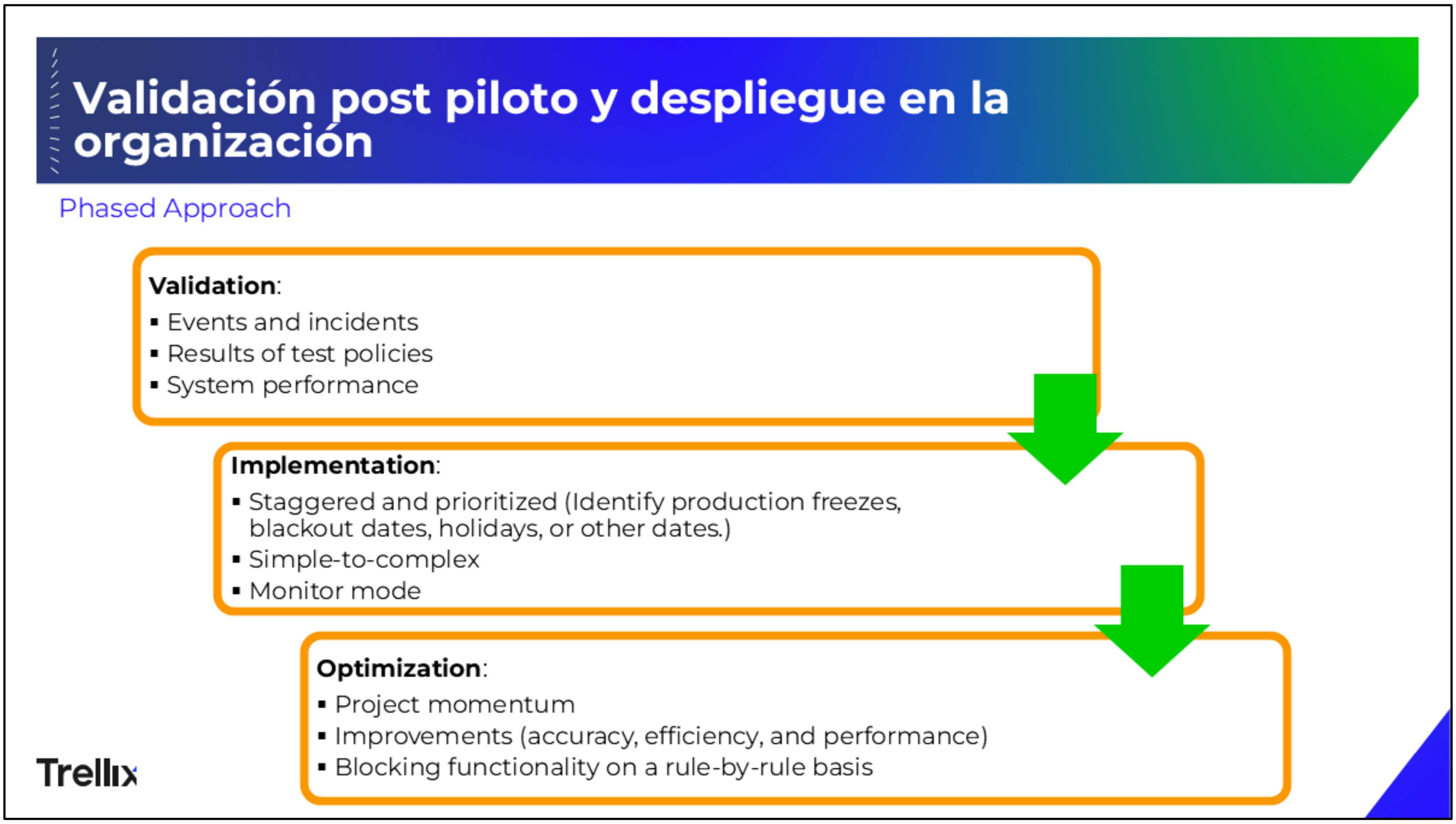
1. **Test Environment:** Identify the test systems to use and segregate them in a test environment. The test environment should have its own Active Directory forest or domain. You can reuse users and groups from an existing Active Directory deployment; however, a separate network helps avoid user disruption.
2. **Test Sample Set:** Make sure the test sample set includes a full spectrum of users. Diversity ensures accurate policy construction and validation. Limit the number of hosts. Between 10 to 50 hosts is an adequate enough sample to provide adequate information for the monitor phase but also small enough to remain manageable at this early stage in the deployment. Because it might be difficult to determine in advance exactly what your unique needs are, we recommend initial deployment to a sample group of 15 to 20 users for a trial period of about a month. During this trial no data is classified, and a policy is created to monitor, not block, transactions. The monitoring data helps the security officers make good decisions about where and how to classify corporate data. The policies created from this information should be tested on a larger test group (or, for very large companies, on a series of successively larger groups) before being deployed to the entire enterprise.

Continued on the next page.

Pilot plan (continued)

3. **Permissions**
   - Local administrator rights are required on each client to install the DLPe Agent. It is best to install the agent as a domain user who is a local administrator on the client system. The local administrator rights can later be revoked. Domain administrator or equivalent rights are useful to facilitate troubleshooting and allow easy joins and removals of clients to and from the domain.
4. **Test Rules/Policy**
   - The initial rule set translates your Enterprise's data security policy, with its organization-specific data classification components. Begin with 5 to 10 rules during this phase of the deployment. Refine these rules before expanding the rule set further. Concentrate on labeling (tagging) rules, rather than over-engineering reaction rules in this initial, learning phase. Some guidelines are:

- Identify the most common and important data security breach points within the organization.
- Plan naming conventions for your rules and associated components is to ensure consistency and to proactively help with troubleshooting.
- Begin with the easiest data security breach points to protect against, such as removable devices or emails being sent to external domains.
- Implement reaction rules in monitor mode to avoid user disruption.



Validación post piloto y despliegue en la organización

Phased Approach

Validation:
- Events and incidents
- Results of test policies
- System performance

Implementation:
- Staggered and prioritized (Identify production freezes, blackout dates, holidays, or other dates.)
- Simple-to-complex
- Monitor mode

Optimization:
- Project momentum
- Improvements (accuracy, efficiency, and performance)
- Blocking functionality on a rule-by-rule basis

Trellix

After the pilot is complete, the solution is rolled out throughout the Enterprise environment. Like the pilot, this is a phased approach. Some key planning considerations are discussed below.

Validation

- During this phase, ensure the solution is operating as planned; for example, ensure test polices are generating the expected results. Some guidelines are:
- Monitor incidents and events and identify anomalies.
- Look for areas where rules or policies require change or can be refined.
- Monitor the performance of the system components; for example, an over-utilized Microsoft SQL Server can negatively impact the performance in the enterprise environment.

Implementation

After monitoring the pilot and refining the deployment, an enterprise DLPe agent rollout begins. Depending on the size of the organization, the deployment pace may vary. Some guidelines are:

- Build a staggered deployment schedule. Prioritization helps ensure a smooth rollout.
- Be sure to document any production freezes, blackout dates, holidays, or other dates that will impact the delivery of services.
- Balance urgency with complexity. Allow simplicity (least complex) to prevail, even if it results in delaying an urgent group. This enables you to address any issues without disrupting critical systems.
- Roll out policies in a controlled manner throughout the Enterprise. Again, stagger the rollout.
- Make sure rules remain in monitor mode.

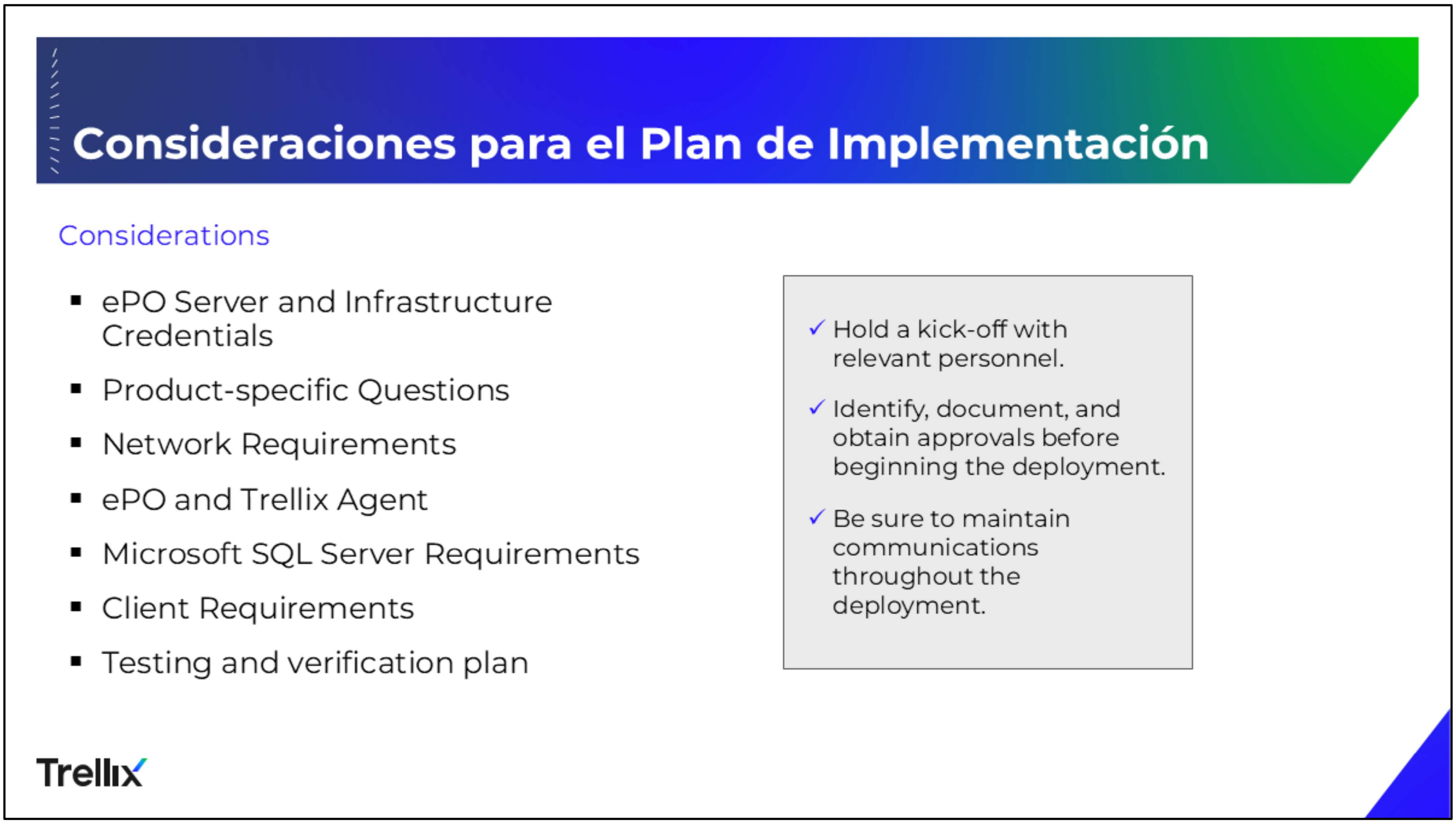
Continued on the next page.

Post pilot validation and enterprise rollout (continued)

Optimize

The last phase is to optimize the deployment. During this phase, focus on project momentum and identify ways to improve accuracy, efficiency, and performance. Some guidelines are:

- Monitor policies regularly to ensure they accurately match the organization’s data security program.
- Refine rules and policies to reduce false positives and noise.
- Remove rules and polices that are no longer required.
- After rules are sufficiently fine-tuned, implement blocking functionality on a rule-by-rule basis.



Consideraciones para el Plan de Implementación

Considerations

- ePO Server and Infrastructure Credentials
- Product-specific Questions
- Network Requirements
- ePO and Trellix Agent
- Microsoft SQL Server Requirements
- Client Requirements
- Testing and verification plan

✓ Hold a kick-off with relevant personnel.

✓ Identify, document, and obtain approvals before beginning the deployment.

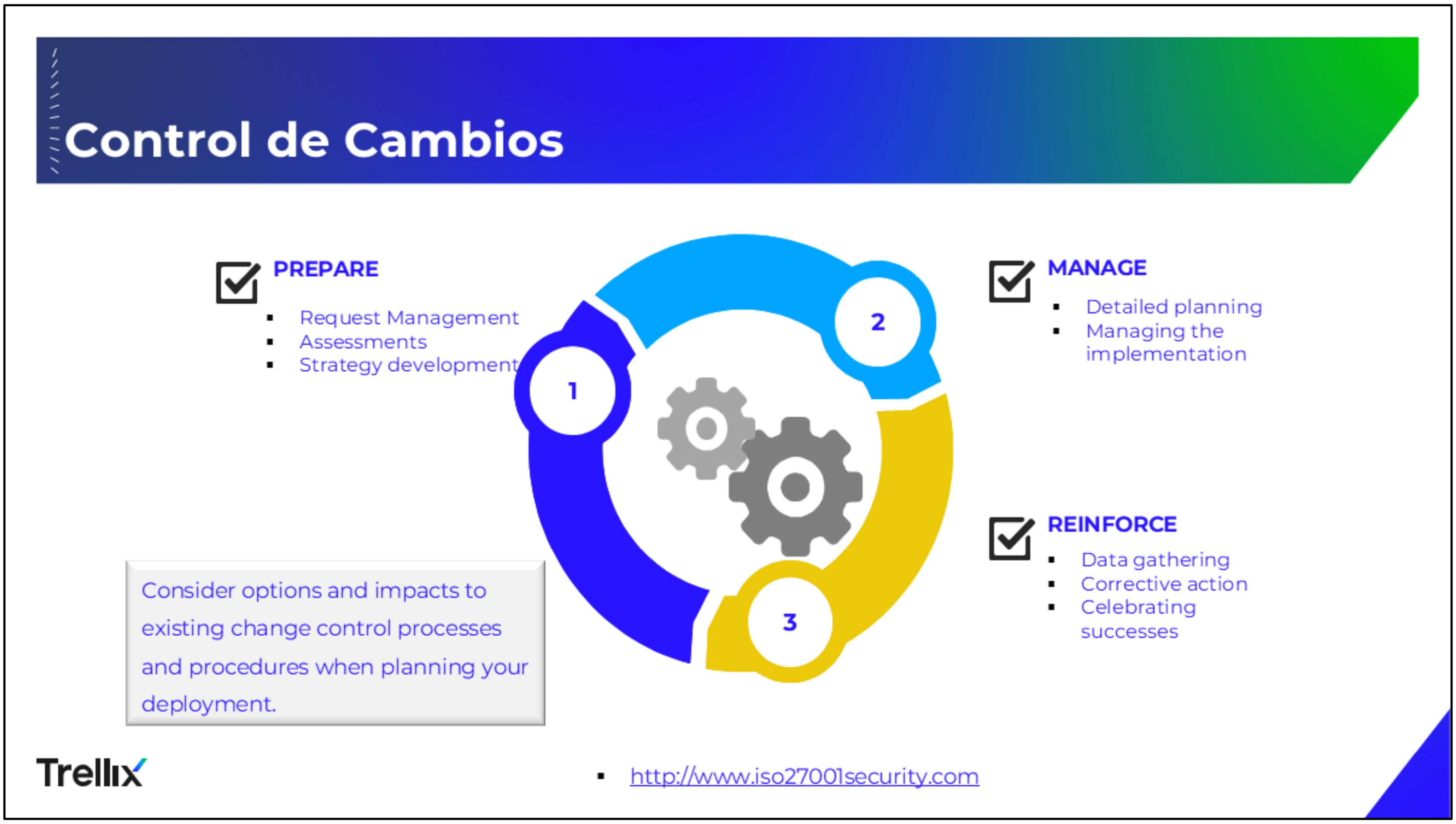
✓ Be sure to maintain communications throughout the deployment.

Trellix

Develop testing and verification plan. Do you have a test environment? Have you identified the test and verification procedures and metrics.

Change control processes ensure that changes proposed to your environment's information resources are reviewed, authorized, tested, implemented and released in a controlled manner. Processes and relevant procedures depend on your company's requirements; however, some recommended phases are:

- Preparing for change: Initial planning and development of change management strategy.
- Managing change: Implementing plan and adding any detail identified.
- Reinforcing change: Data gathering and taking any corrective actions.



Control de Cambios

☑ **PREPARE**

- Request Management
- Assessments
- Strategy development

☑ **MANAGE**

- Detailed planning
- Managing the implementation

☑ **REINFORCE**

- Data gathering
- Corrective action
- Celebrating successes

Consider options and impacts to existing change control processes and procedures when planning your deployment.

Trellix

- http://www.iso27001security.com

As a follow-up to our implementation checklist discussion, a fundamental consideration during any of those steps involves change control, and that each change is closely monitored. Change control processes ensure that changes proposed to your environment's information resources are reviewed, authorized, tested, implemented and released in a controlled manner. This process and relevant procedures are dependent on your company's requirements. However, for purposes of this discussion, a change control process should include the following phases:

- Preparing for change: Request management, assessment, and strategy development
- Managing change: Detailed planning and change management implementation
- Reinforcing change: Data gathering, corrective action and celebrate successes

Prepare:

Request management: This includes identifying potential changes, often in the form of requests, approving, deferring or denying the change requests and determining the priority.

Assessments: When assessing the change, you should define the requirements, determine interdependencies and compliance checks, and assess any other impacts this change will have.

Strategy development: In this step, you should develop an overall strategy for deployment including testing and evaluating user acceptance.

Manage:

Detailed planning: With detailed planning, you should fine-tune your strategy, including a back-out plan. Managing the implementation: Manage all aspects of the change including testing, evaluating user acceptance, and documentation.

Continued on the next page.

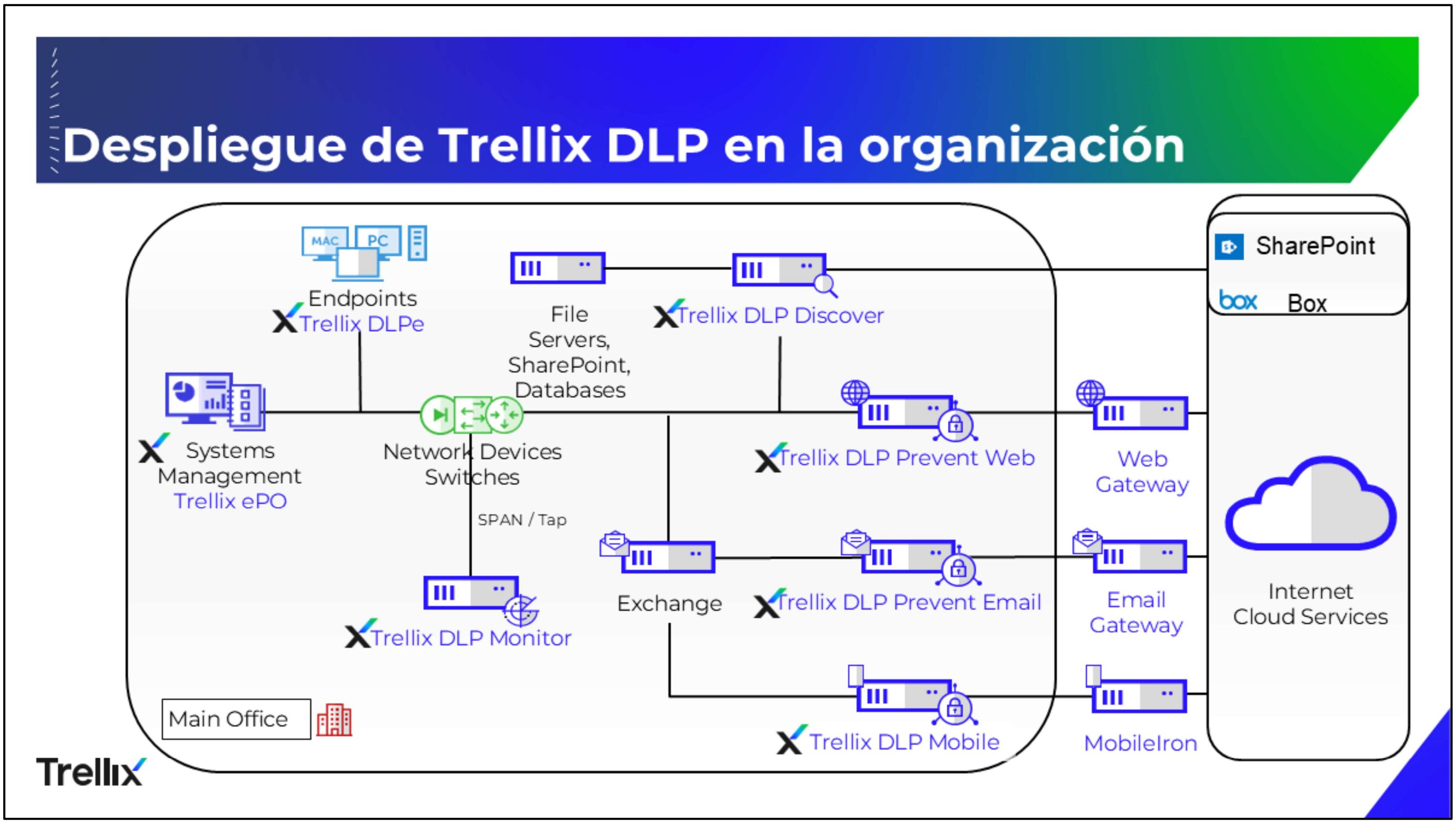
Change Control (continued)

Reinforce:

- Data gathering: After the change has been implemented, gather data to determine its effectiveness. This may trigger another change to improve upon this change or to remove the modifications, although the desired outcome is that the change is behaving as expected and has met its intended goal.
- Corrective action: If the change has not met its intended goal, determine what steps should be done. This may mean better documentation and training, a new change, or backing out the modifications.
- Celebrate successes: It is important to celebrate successes, acknowledging a job well done. While learning from mistakes is often emphasized with lessons learned, it is also important to celebrate what went right in order to continue to replicate

those actions.

Consideraciones para la Implementación de la plataforma Trellix DLP



Despliegue de Trellix DLP en la organización

Endpoints
Trellix DLPe

File Servers, SharePoint, Databases

Trellix DLP Discover

SharePoint

Box

Systems Management
Trellix ePO

Network Devices Switches

SPAN / Tap

Trellix DLP Prevent Web

Web Gateway

Trellix DLP Monitor

Exchange

Trellix DLP Prevent Email

Email Gateway

Internet Cloud Services

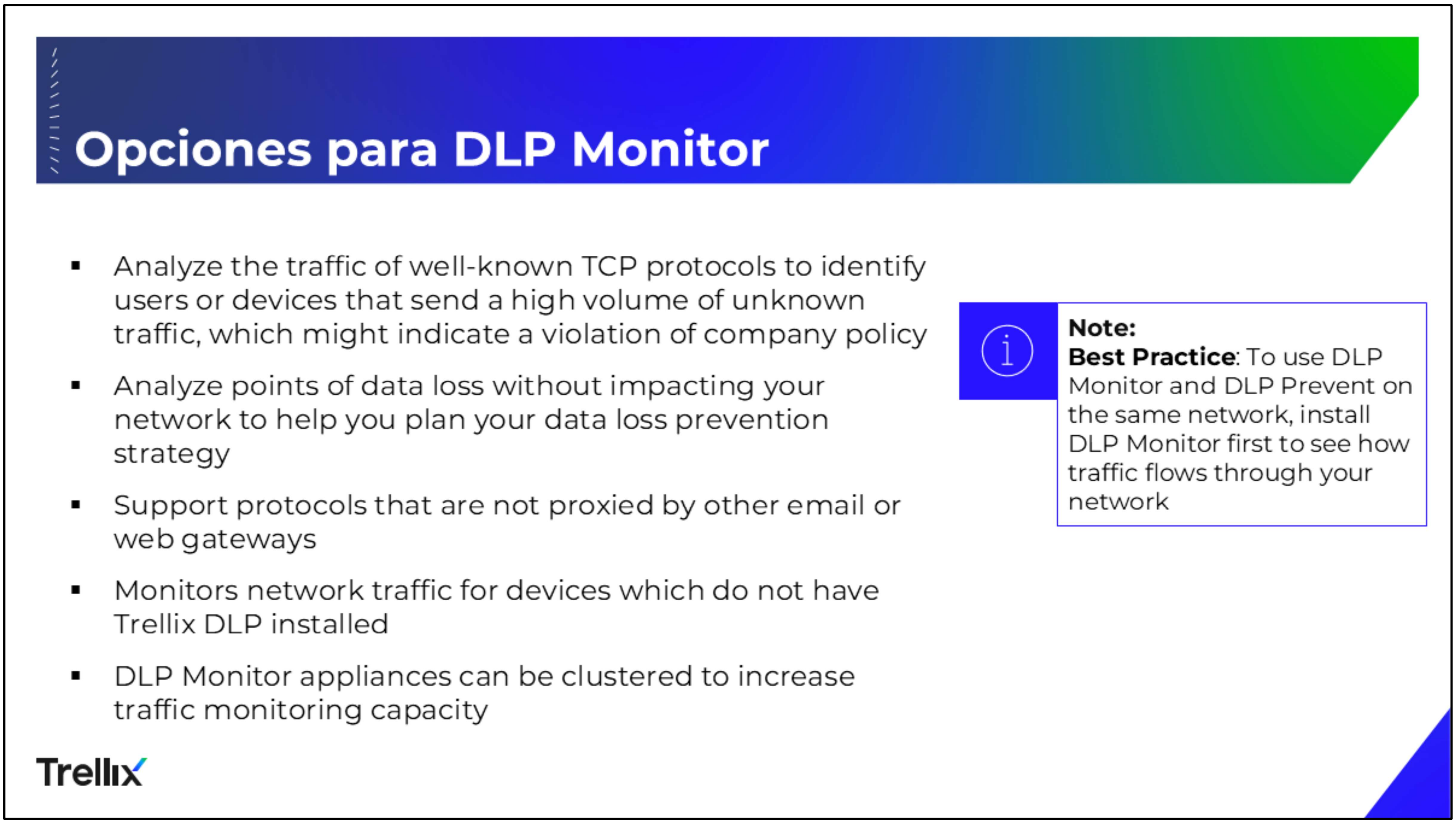
Main Office

Trellix DLP Mobile

MobileIron

Trellix

The slide shows a Trellix DLP deployment in a network.



Opciones para DLP Monitor

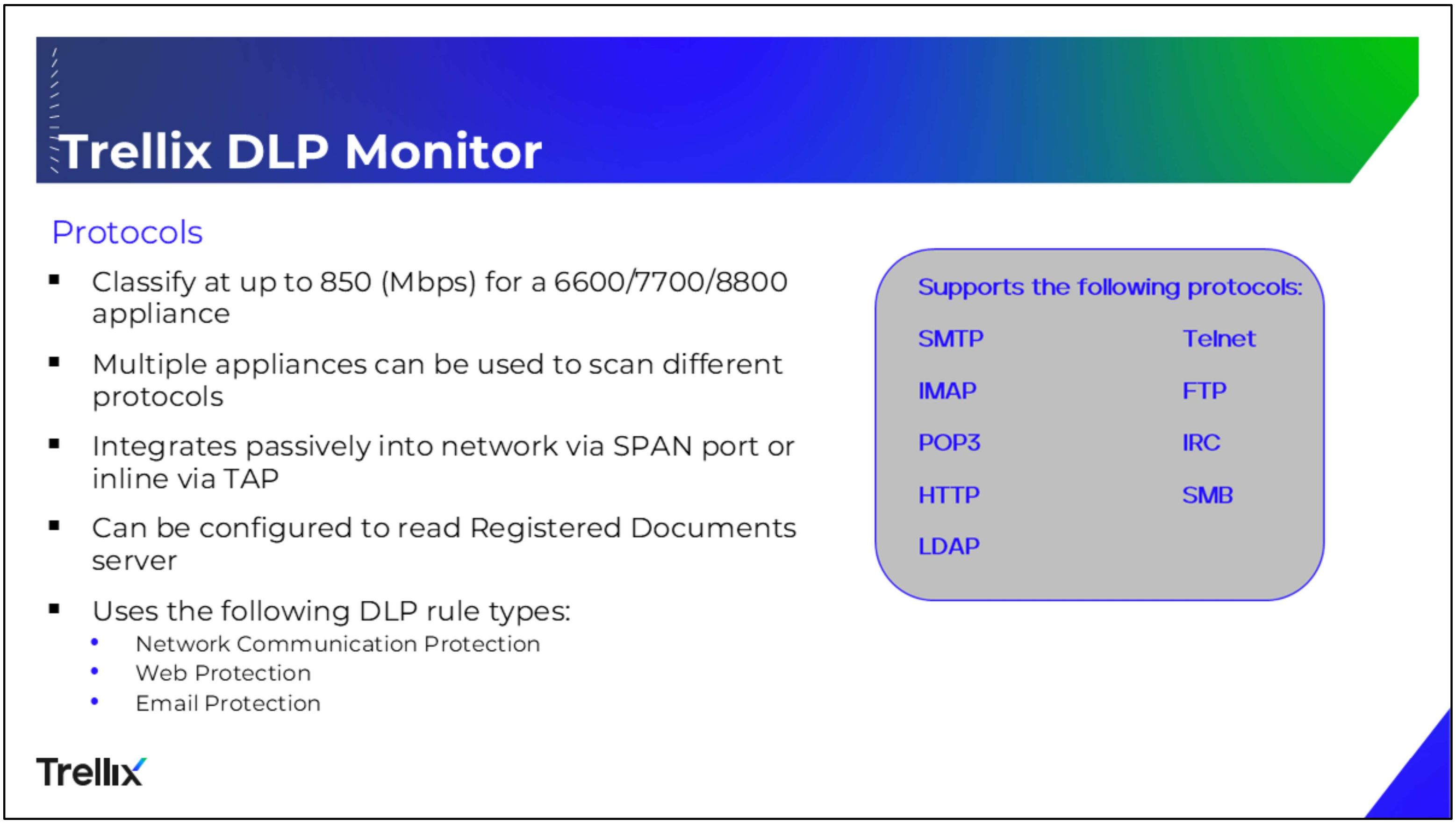
- Analyze the traffic of well-known TCP protocols to identify users or devices that send a high volume of unknown traffic, which might indicate a violation of company policy
- Analyze points of data loss without impacting your network to help you plan your data loss prevention strategy
- Support protocols that are not proxied by other email or web gateways
- Monitors network traffic for devices which do not have Trellix DLP installed
- DLP Monitor appliances can be clustered to increase traffic monitoring capacity

Note:
Best Practice: To use DLP Monitor and DLP Prevent on the same network, install DLP Monitor first to see how traffic flows through your network

Trellix

High-level steps form Trellix DLP Monitor implementation:

1. Connect the appliance to your network.
2. Install Trellix DLP Monitor.
3. Enable relevant predefined policies and rules.
4. Create additional rules and policies.
5. Review incidents generated by Trellix DLP Monitor.
6. Tune rules as needed to reduce false positives.



Trellix DLP Monitor

Protocols

- Classify at up to 850 (Mbps) for a 6600/7700/8800 appliance
- Multiple appliances can be used to scan different protocols
- Integrates passively into network via SPAN port or inline via TAP
- Can be configured to read Registered Documents server
- Uses the following DLP rule types:
  - Network Communication Protection
  - Web Protection
  - Email Protection

Supports the following protocols:

- SMTP
- IMAP
- POP3
- HTTP
- LDAP
- Telnet
- FTP
- IRC
- SMB

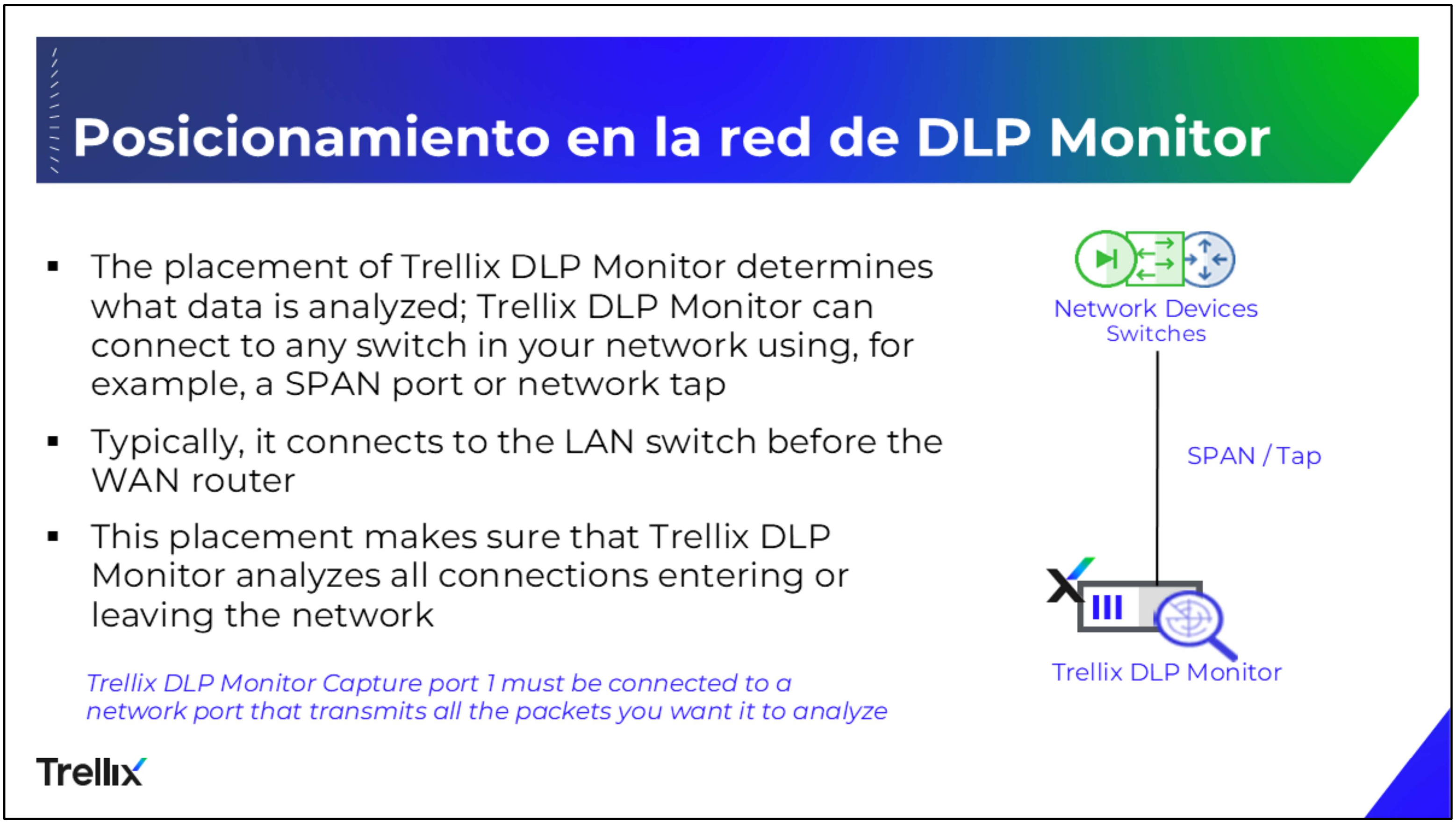
Trellix

Trellix DLP Monitor can be configured to read Registered Document servers. Multiple appliances can be used to scan different protocols. Protocols supported include:

- SMTP
- IMAP
- POP3
- HTTP
- LDAP
- Telnet
- FTP
- IRC
- SMB

Trellix DLP Monitor uses the following DLP rule types:

- Network Communication Protection
- Web Protection
- Email Protection



Posicionamiento en la red de DLP Monitor

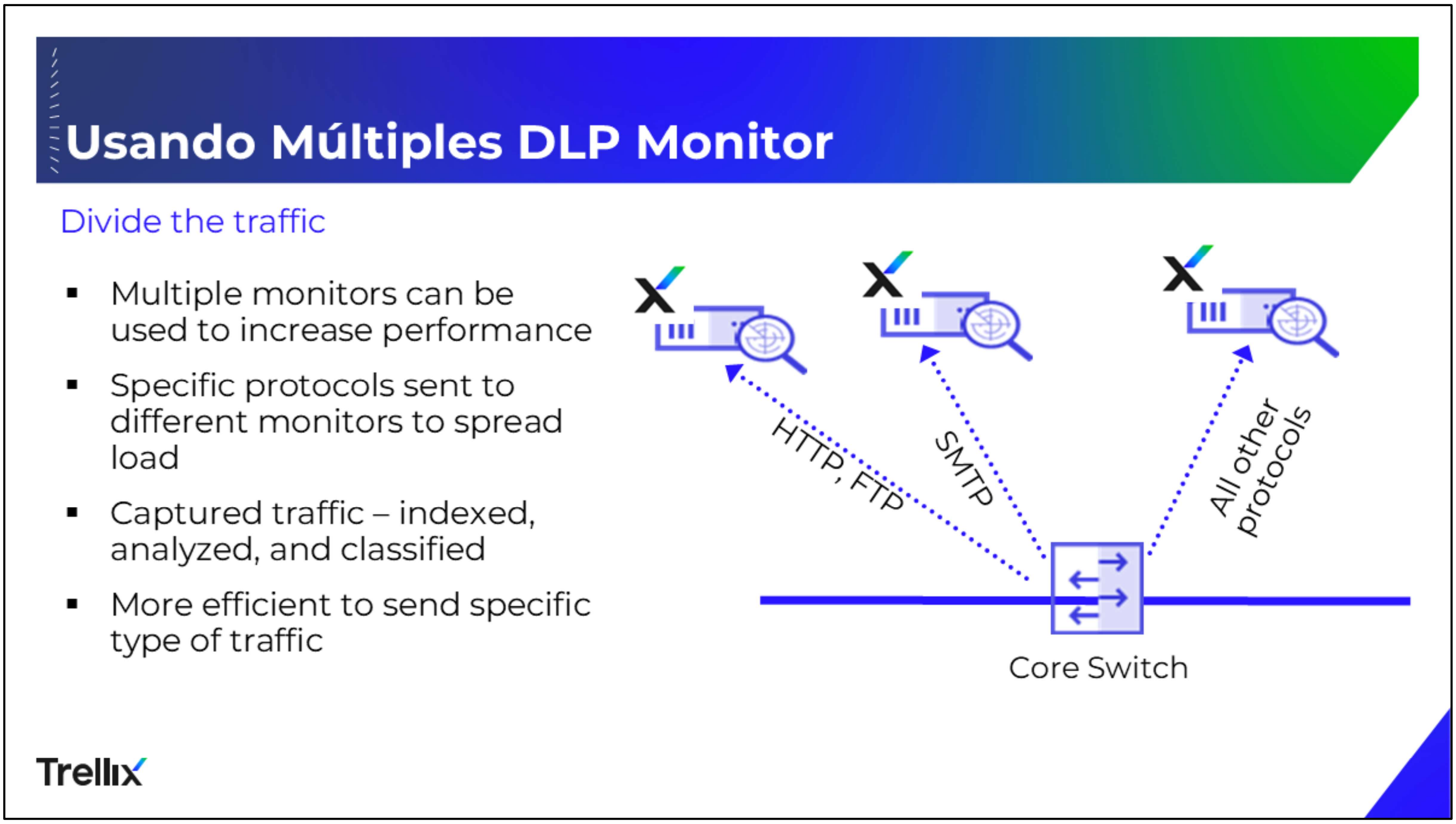
- The placement of Trellix DLP Monitor determines what data is analyzed; Trellix DLP Monitor can connect to any switch in your network using, for example, a SPAN port or network tap
- Typically, it connects to the LAN switch before the WAN router
- This placement makes sure that Trellix DLP Monitor analyzes all connections entering or leaving the network

Trellix DLP Monitor Capture port 1 must be connected to a network port that transmits all the packets you want it to analyze

Trellix

The placement of Trellix DLP Monitor determines what data is analyzed. Trellix DLP Monitor can connect to any switch in your network using, for example, a SPAN port or network tap. Typically, it connects to the LAN switch before the WAN router. This placement makes sure that Trellix DLP Monitor analyzes all connections entering or leaving the network.

Trellix DLP Monitor Capture port 1 must be connected to a network port that transmits all the packets you want it to analyze.



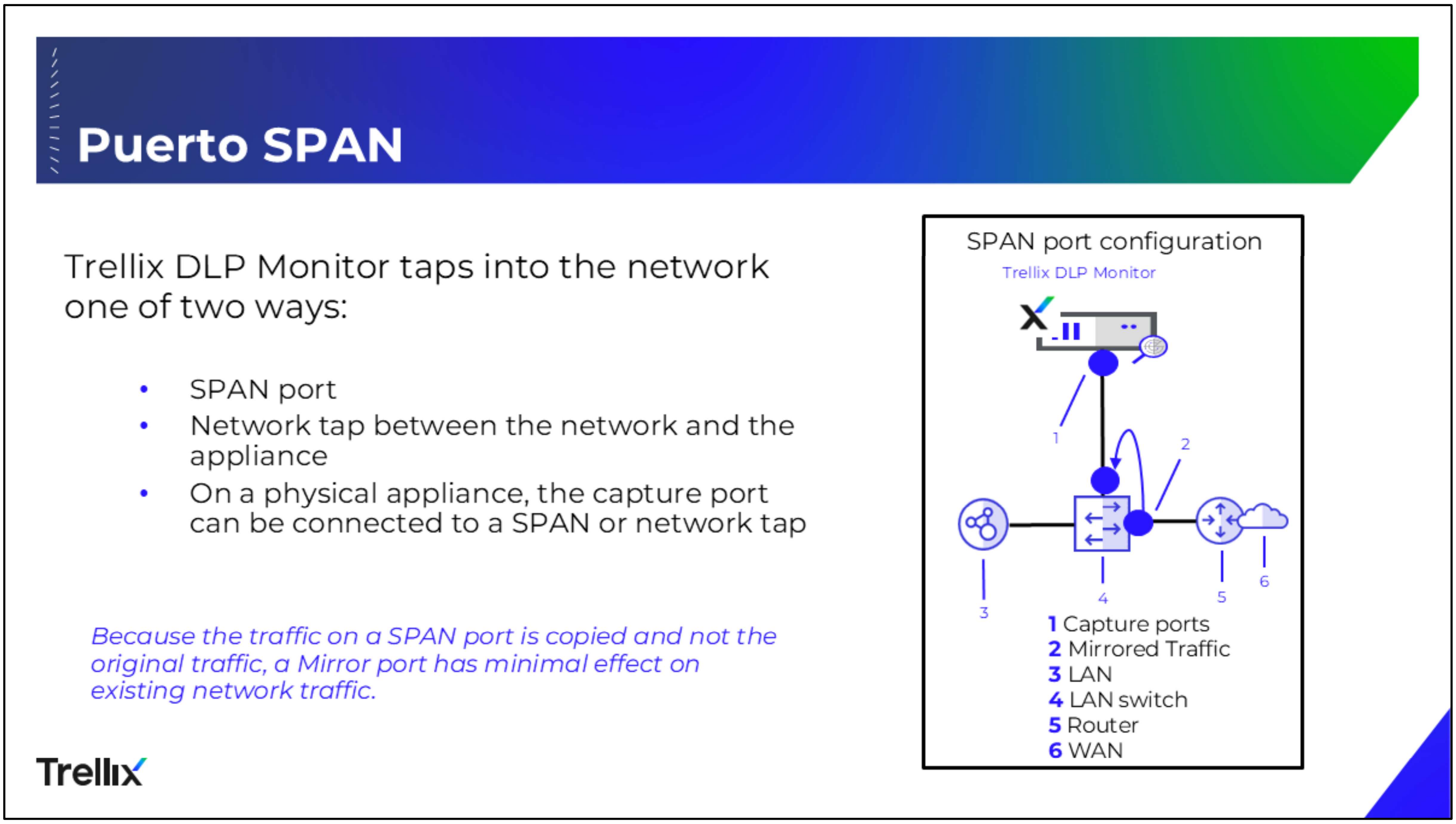
Usando Múltiples DLP Monitor

Divide the traffic

- Multiple monitors can be used to increase performance
- Specific protocols sent to different monitors to spread load
- Captured traffic – indexed, analyzed, and classified
- More efficient to send specific type of traffic

The core component of Trellix DLP Monitor is a capture engine that stores packets from network traffic using Trellix's enhanced filter drivers.

The captured traffic is indexed, analyzed, and classified. It is more efficient to send specific types of traffic to a defined monitor device in order to help improve performance and decrease load on an individual monitor.



Puerto SPAN

Trellix DLP Monitor taps into the network one of two ways:

- SPAN port
- Network tap between the network and the appliance
- On a physical appliance, the capture port can be connected to a SPAN or network tap

Because the traffic on a SPAN port is copied and not the original traffic, a Mirror port has minimal effect on existing network traffic.

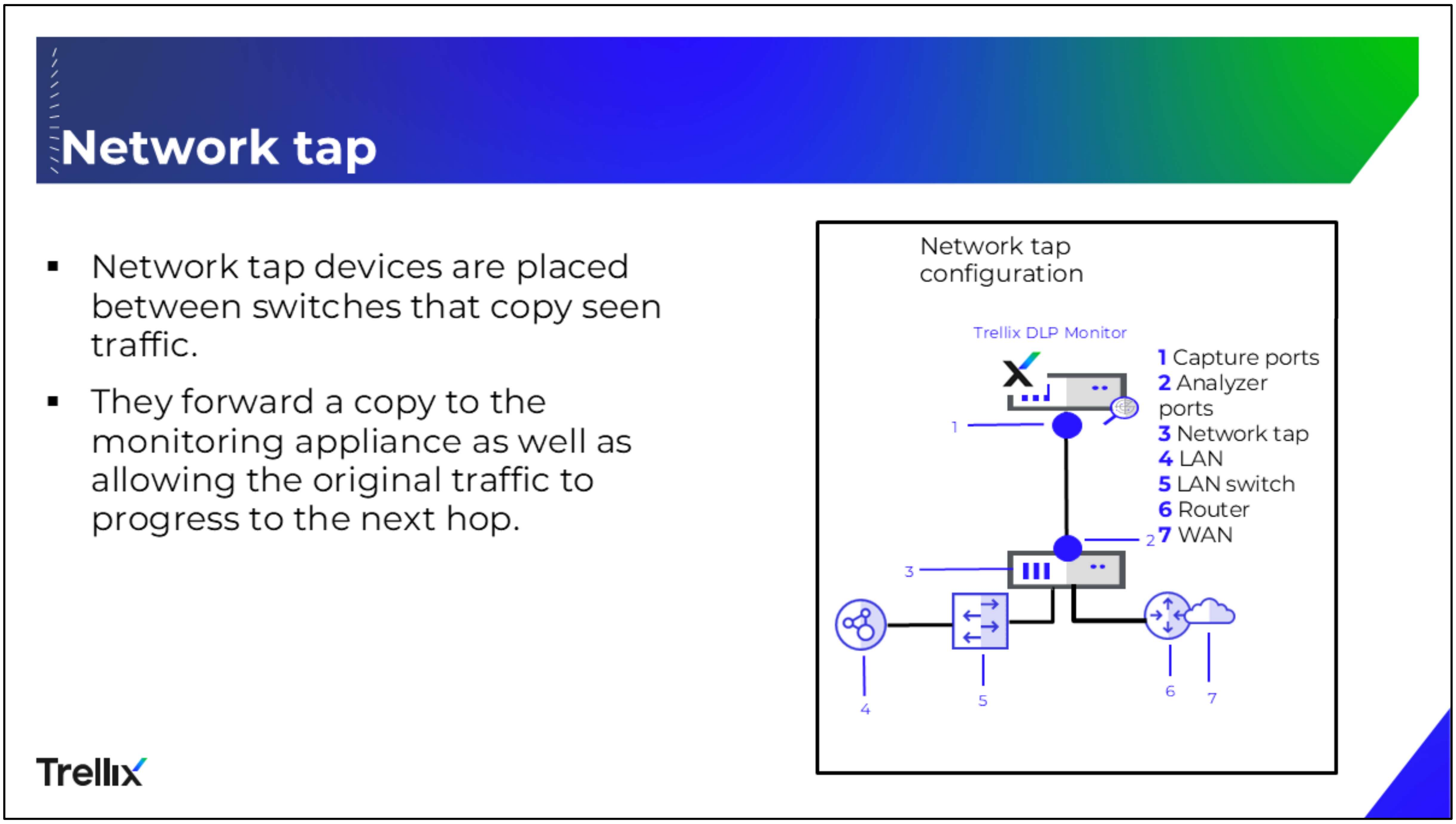
Trellix

SPAN port configuration

1 Capture ports
2 Mirrored Traffic
3 LAN
4 LAN switch
5 Router
6 WAN

Monitoring appliances regularly use SPAN ports to observe network traffic without directly impacting existing traffic. A copy of all network traffic is directed past the monitoring appliances, which have a port in promiscuous mode to listen to and analyze all traffic.

Because the traffic is copied and not the original traffic, a mirror port has minimal effect on existing network traffic.



Network tap

- Network tap devices are placed between switches that copy seen traffic.
- They forward a copy to the monitoring appliance as well as allowing the original traffic to progress to the next hop.

Network tap configuration
Trellix DLP Monitor
1 Capture ports
2 Analyzer ports
3 Network tap
4 LAN
5 LAN switch
6 Router
7 WAN
1
2
3
4
5
6
7

Trellix

The network tap sits between a WAN router and the core internal switch. All outgoing traffic passes through the network tap and is copied and sent to the Trellix DLP Monitor capture ports while the original traffic proceeds normally.

While similar to a mirror port, this configuration does not require any changes on switches or routers but can require some additional cabling and possible downtime to install the tap. Network taps are available in both copper and fiber media. They are usually installed at the last point before egress for the network between the perimeter firewall and the first internal switch.

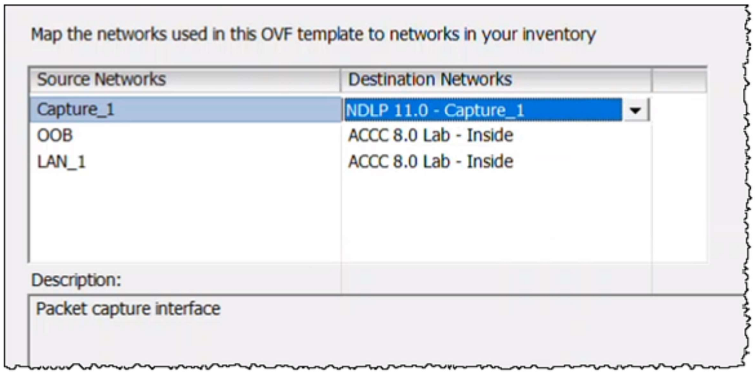
Smart Taps are network taps that are configurable to only send certain types of traffic (filtered by IP address or protocol) to the capture port. This can also be accomplished by using Network or Capture filters on the NLDP monitor, but is more efficient if done at the physical network smart tap.

Puerto de Captura para Virtual Appliance

Connect Capture port 1 to your network in a virtual environment

On a virtual appliance, the capture port is set to *promiscuous mode*

- You must enable promiscuous mode on a portgroup or virtual switch to allow the appliance to passively inspect copies of all network packets that pass through the network
- On a virtual appliance, the capture port is connected to a standard virtual switch or a portgroup on a distributed switch with promiscuous mode enabled



Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Capture_1	NDLP 11.0 - Capture_1
OOB	ACCC 8.0 Lab - Inside
LAN_1	ACCC 8.0 Lab - Inside

Description:

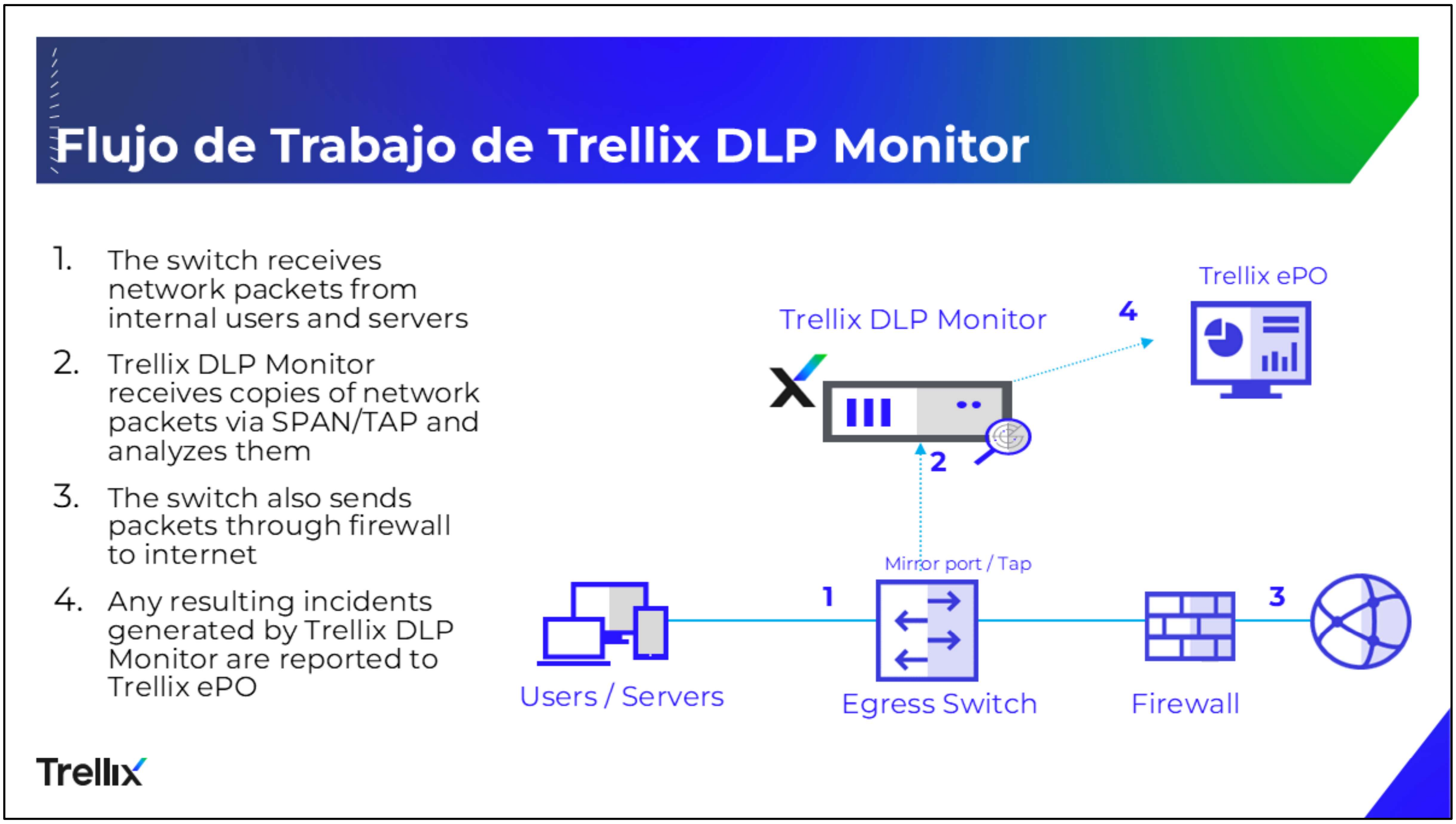
Packet capture interface

***Note:** Promiscuous mode is disabled by default on a virtual switch and should not be turned on unless specifically required. Software running inside a virtual machine may be able to monitor any and all traffic moving across a vSwitch if it is allowed to enter promiscuous mode.*

Trellix

To configure a portgroup or vitual switch for promiscuous mode:

1. Log on to the VMware ESXi or VMware ESX host, or on to vCenter Server using the vSphere Client.
2. Select the VMware ESXi or ESX host in the inventory list.
3. Click the **Configuration** tab.
4. In the **Hardware** section, click **Networking**.
5. Select the **Properties** of the virtual switch that you want to enable promiscuous mode on.
6. Select the virtual switch or portgroup you want to modify and click **Edit**.
7. Click the **Security** tab.
8. From the **Promiscuous Mode** menu, click **Accept**.



Flujo de Trabajo de Trellix DLP Monitor

1. The switch receives network packets from internal users and servers
2. Trellix DLP Monitor receives copies of network packets via SPAN/TAP and analyzes them
3. The switch also sends packets through firewall to internet
4. Any resulting incidents generated by Trellix DLP Monitor are reported to Trellix ePO

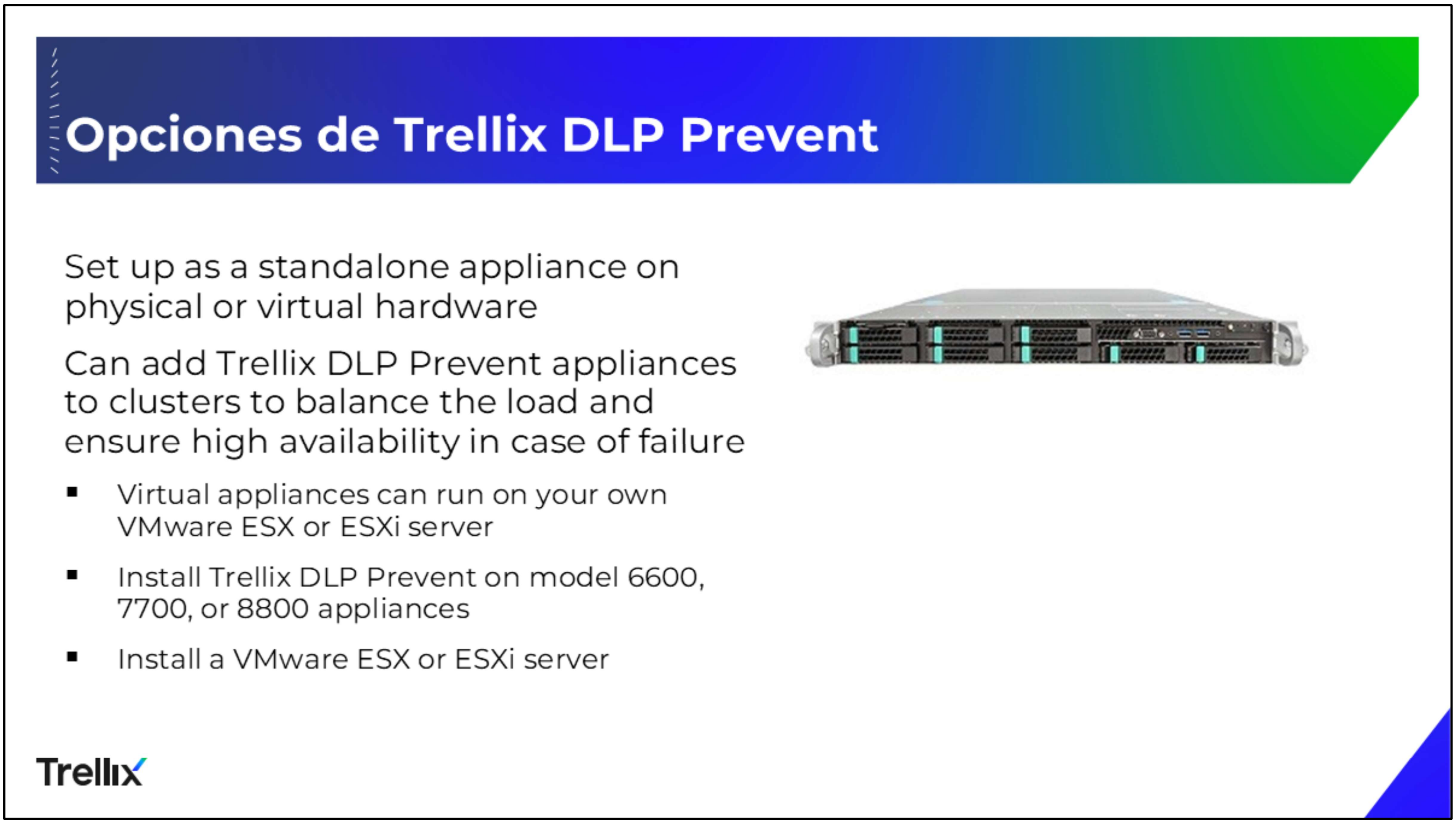
The page depicts the Trellix DLP Monitor workflow.

1. The switch receives network packets from internal users and servers
2. Trellix DLP Monitor receives copies of network packets via SPAN/TAP and analyzes them
3. The switch also sends packets through firewall to internet
4. Any resulting incidents generated by Monitor are reported to Trellix ePO

Consideraciones para DLP Monitor

Determine	Considerations
Security	▪ Use out-of-band management on a network that Trellix ePO can access to isolate management and network traffic ▪ When clustering is enabled, LAN1 traffic must not be accessible from outside your organization. You do not have to connect to LAN1 if you are not using clustering. ▪ Control who can access the physical or virtual appliance console
Network information	▪ Determine the most appropriate place in your network to attach the Trellix DLP Monitor appliance Capture port 1. For example, consider using a SPAN port or a network tap. ▪ Network interfaces: Verify that these are statically assigned IP addresses, rather than dynamically assigned IP addresses ▪ Logon account: The appliance has a local administrator account for logging on to the virtual machine shell. To make the account secure, change the default password. ▪ In a cluster environment, the virtual IP address must be in the same subnet as the appliance IP address
Remote Management Module (RMM)	▪ (Hardware appliances only) If you intend to use the RMM for appliance management, use a secure or closed network to connect to the RMM

Trellix



Opciones de Trellix DLP Prevent

Set up as a standalone appliance on physical or virtual hardware

Can add Trellix DLP Prevent appliances to clusters to balance the load and ensure high availability in case of failure

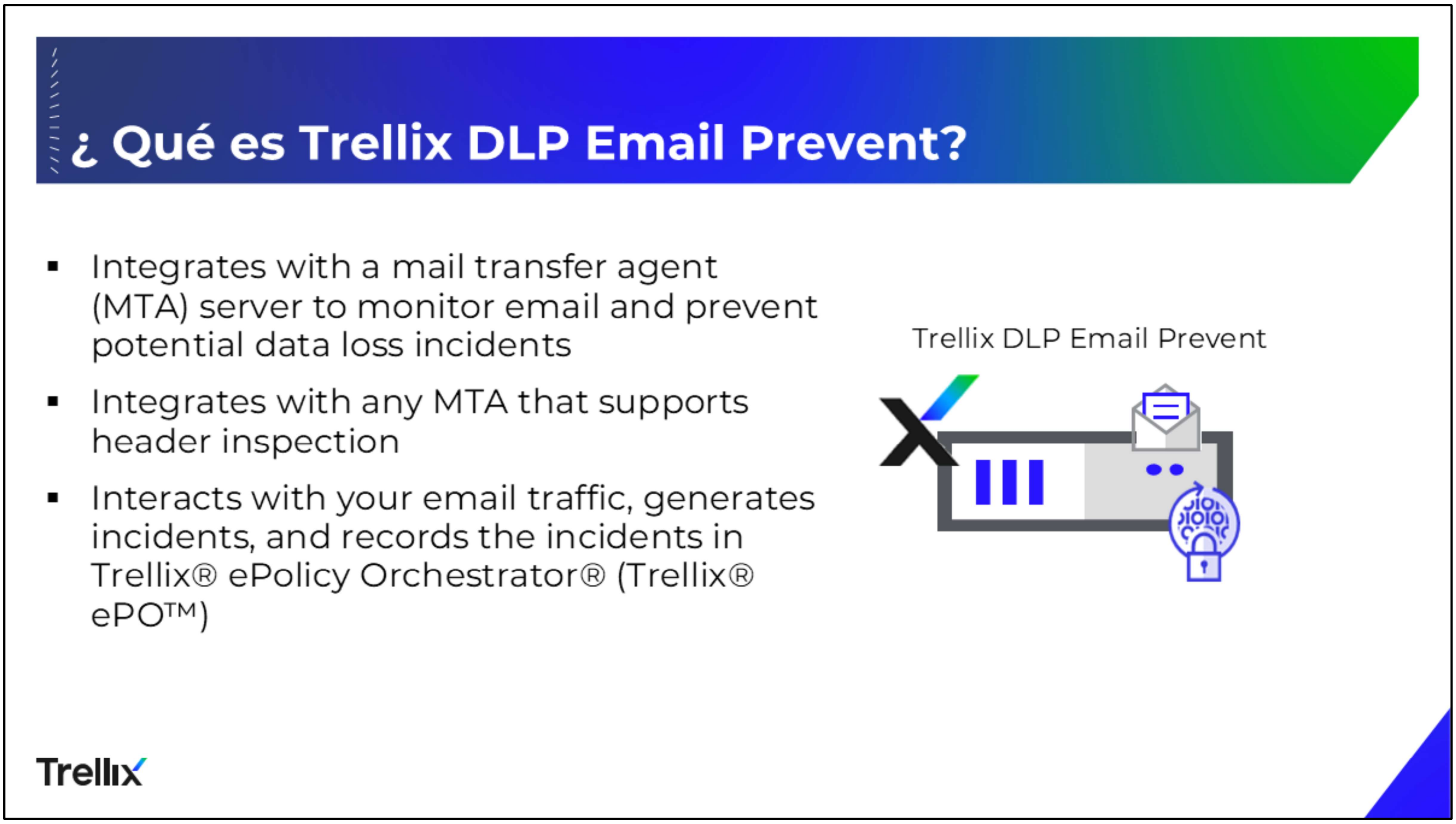
- Virtual appliances can run on your own VMware ESX or ESXi server
- Install Trellix DLP Prevent on model 6600, 7700, or 8800 appliances
- Install a VMware ESX or ESXi server

Trellix

You can add Trellix DLP Prevent appliances to clusters to balance the load and ensure high availability in case
of failure. Trellix DLP Prevent can also be set up as a standalone appliance on physical or virtual hardware.

- Virtual appliances can run on your own VMware ESX or ESXi server.
- You can install Trellix DLP Prevent on model 6600, 7700, or 8800 appliances.
- You can install a VMware ESX or ESXi server

- To purchase VMware vSphere and VMware vCenter Server, go to https://www.vmware.com.
- To purchase Windows Hyper-V, go to https://www.microsoft.com.



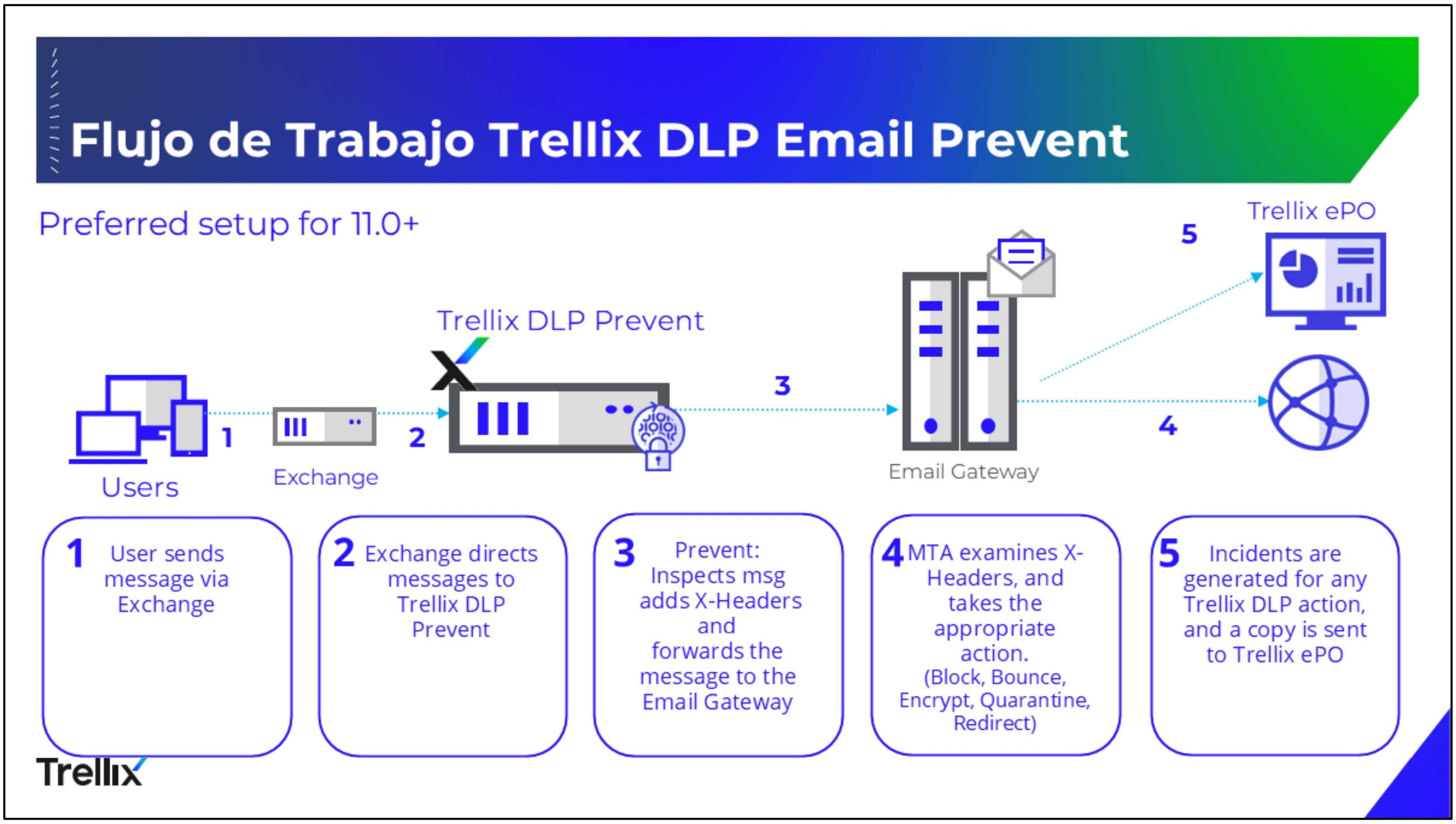
¿ Qué es Trellix DLP Email Prevent?

- Integrates with a mail transfer agent (MTA) server to monitor email and prevent potential data loss incidents
- Integrates with any MTA that supports header inspection
- Interacts with your email traffic, generates incidents, and records the incidents in Trellix® ePolicy Orchestrator® (Trellix® ePO™)

Trellix DLP Email Prevent

Trellix

Trellix DLP Prevent (Email) is used in conjunction with a mail transfer agent (MTA) server to scan and approve or disapprove any emails leaving a network. Outbound email is sent to the MTA, forwarded to Trellix DLP Prevent for scanning and then passed back to the MTA for final delivery or rejection based on headers added into the email by Trellix DLP Prevent.



Flujo de Trabajo Trellix DLP Email Prevent

Preferred setup for 11.0+

1 User sends message via Exchange

2 Exchange directs messages to Trellix DLP Prevent

3 Prevent: Inspects msg adds X-Headers and forwards the message to the Email Gateway

4 MTA examines X-Headers, and takes the appropriate action. (Block, Bounce, Encrypt, Quarantine, Redirect)

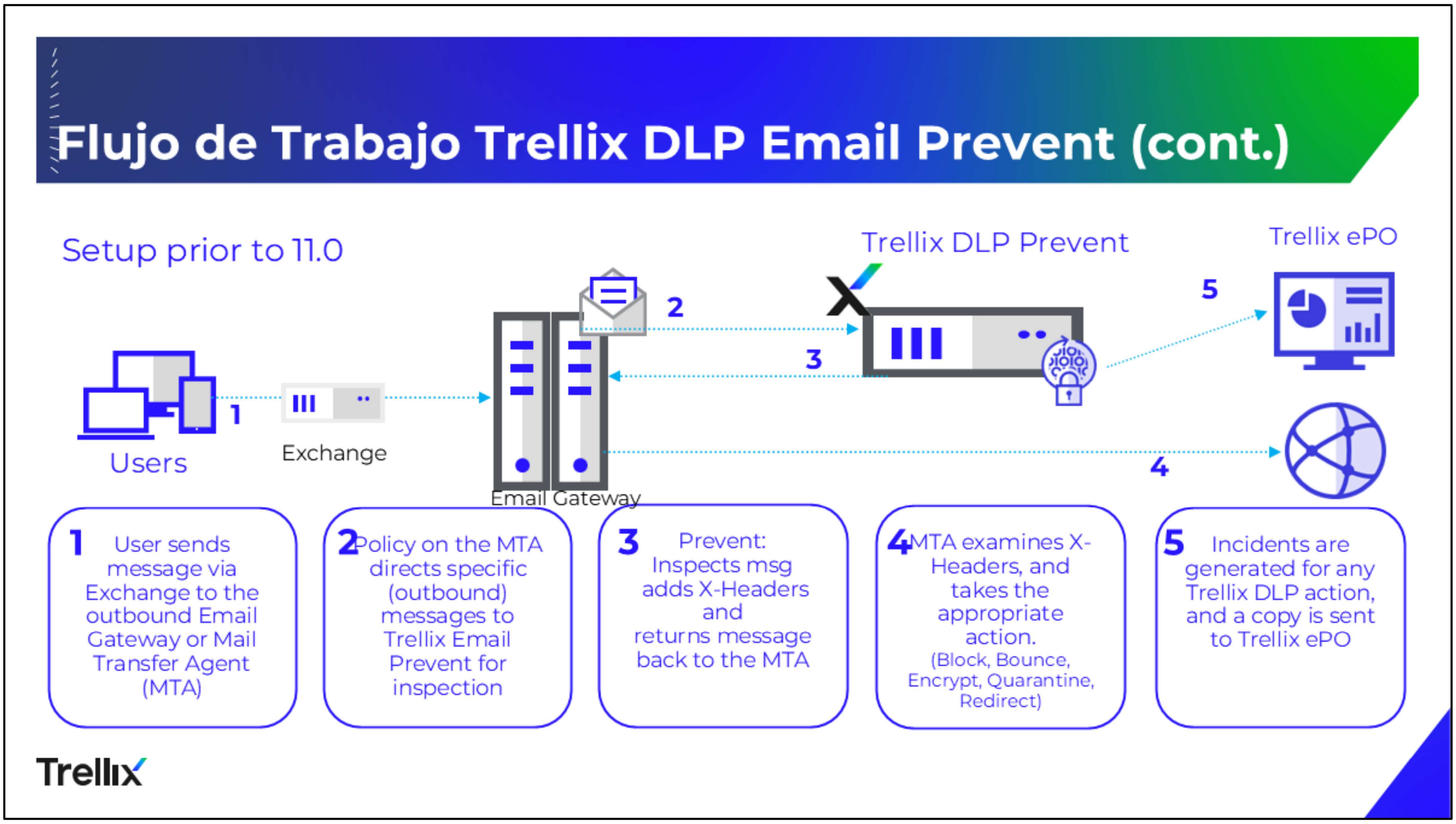
5 Incidents are generated for any Trellix DLP action, and a copy is sent to Trellix ePO

Trellix

The diagram depicts the SMTP workflow. This is the preferred setup for NDLP 11.0+ since we are not storing and forwarding email, this configuration will prevent any email looping. The Exchange server should be configured with a prioritized list for the email connections, with DLP Prevent first, and if not available, then send email directly to the Email Gateway. The Note that some of the actions that Prevent could specify in its headers include; allow, block, encrypt, bounce, and quarantine.

For the Mail Transfer Agent (MTA) and Trellix DLP Prevent to communicate properly, the MTA must understand and be able to act on the following X-RCIS-Action headers:

- ALLOW
- BLOCK
- QUART
- ENCRYPT
- BOUNCE
- REDIR
- NOTIFY



Flujo de Trabajo Trellix DLP Email Prevent (cont.)

Setup prior to 11.0

1 User sends message via Exchange to the outbound Email Gateway or Mail Transfer Agent (MTA)

2 Policy on the MTA directs specific (outbound) messages to Trellix Email Prevent for inspection

3 Prevent: Inspects msg adds X-Headers and returns message back to the MTA

4 MTA examines X-Headers, and takes the appropriate action. (Block, Bounce, Encrypt, Quarantine, Redirect)

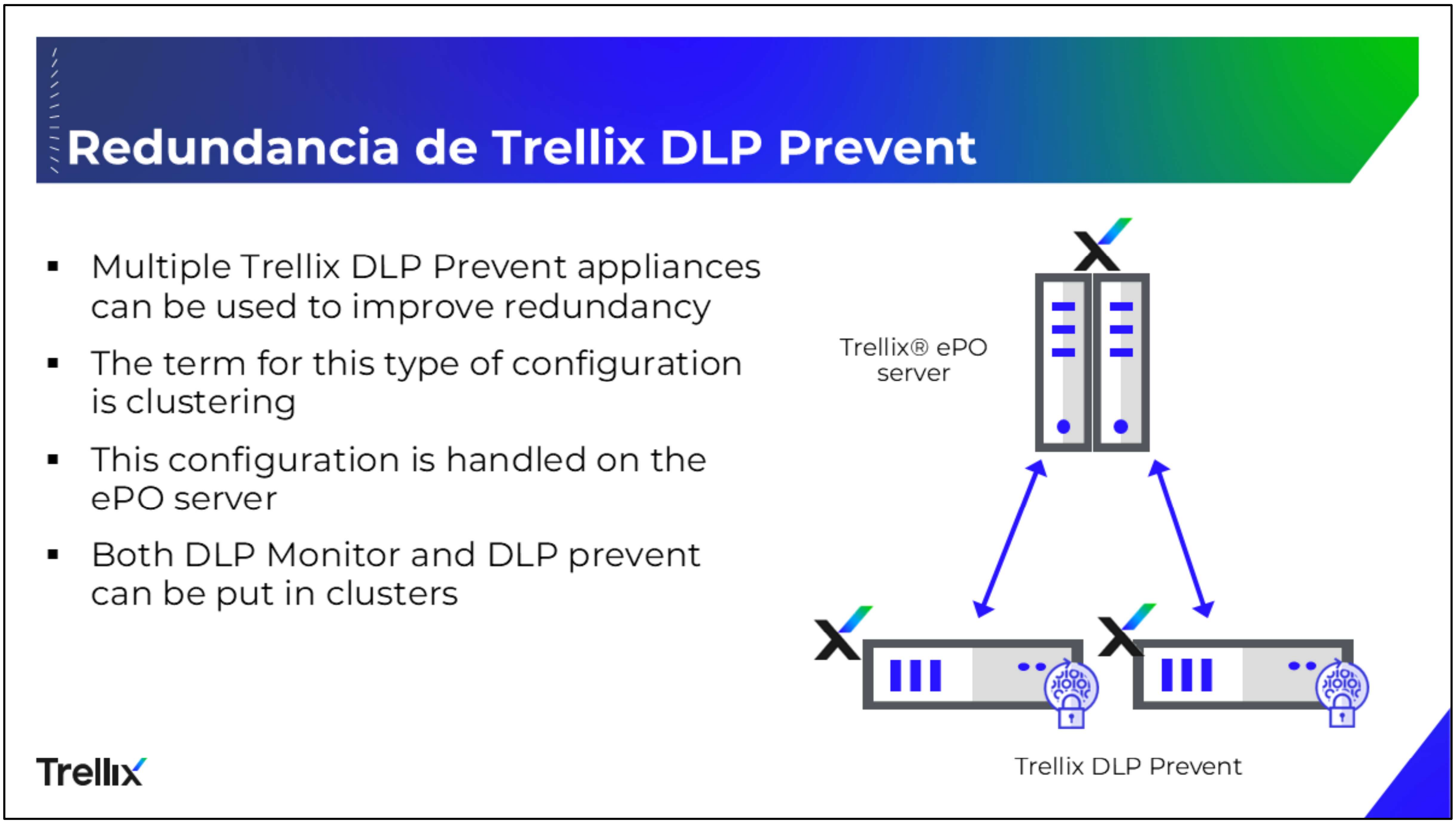
5 Incidents are generated for any Trellix DLP action, and a copy is sent to Trellix ePO

Trellix

The diagram depicts The SMTP workflow using a different setup method. Note that some of the actions that Prevent could specify in its headers include; allow, block, encrypt, bounce, and quarantine.

For the Mail Transfer Agent (MTA) and Trellix DLP Prevent to communicate properly, the MTA must understand and be able to act on the following X-RCIS-Action headers:

- ALLOW
- BLOCK
- QUART
- ENCRYPT
- BOUNCE
- REDIR
- NOTIFY



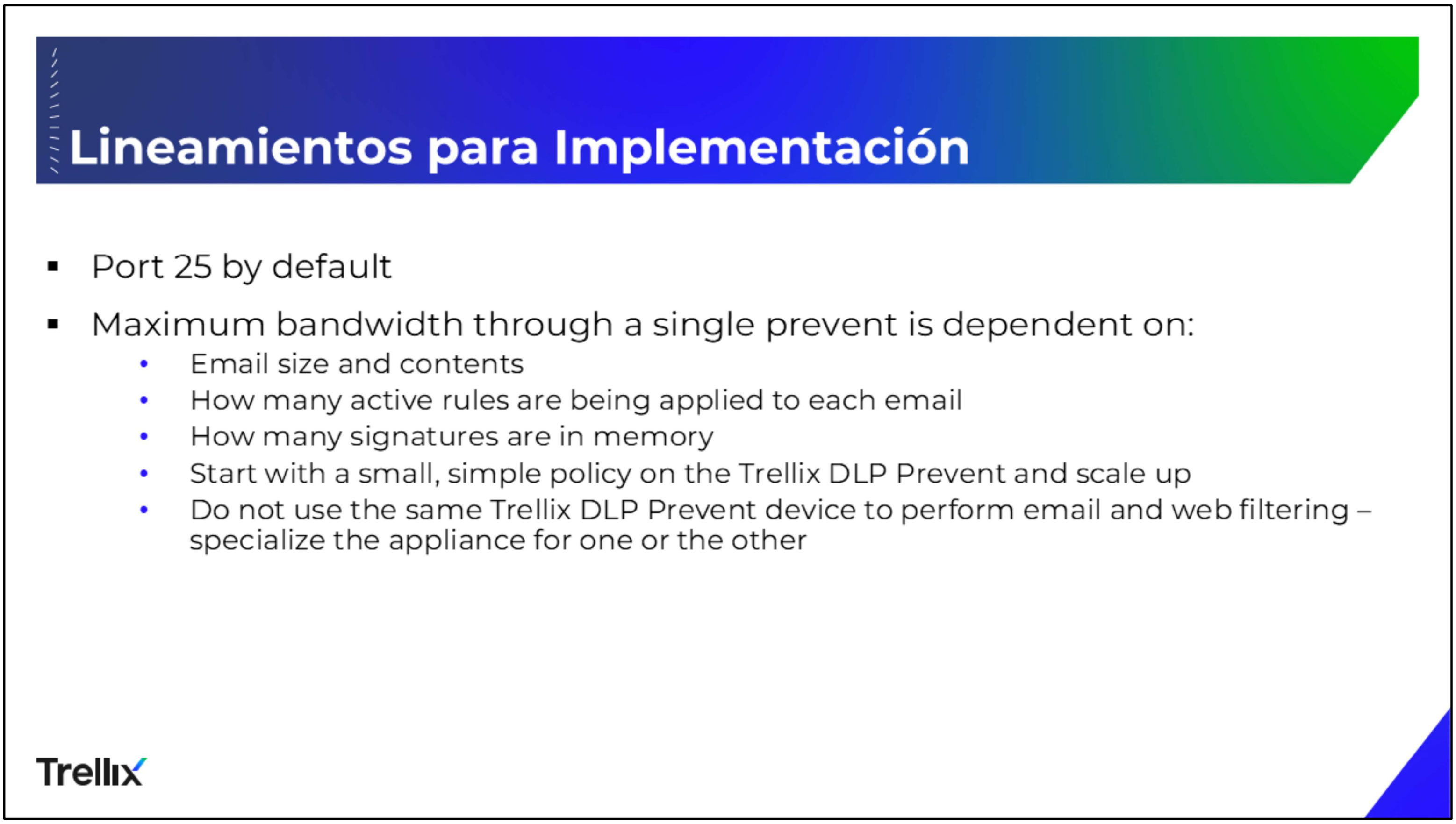
Redundancia de Trellix DLP Prevent

- Multiple Trellix DLP Prevent appliances can be used to improve redundancy
- The term for this type of configuration is clustering
- This configuration is handled on the ePO server
- Both DLP Monitor and DLP prevent can be put in clusters

Trellix® ePO server

Trellix DLP Prevent

Redundancy for Trellix DLP Prevent is possible using multiple DLP Prevent appliances in a clustered configuration. Trellix ePO pushes the configuration to all appliances in the cluster when you apply any changes.

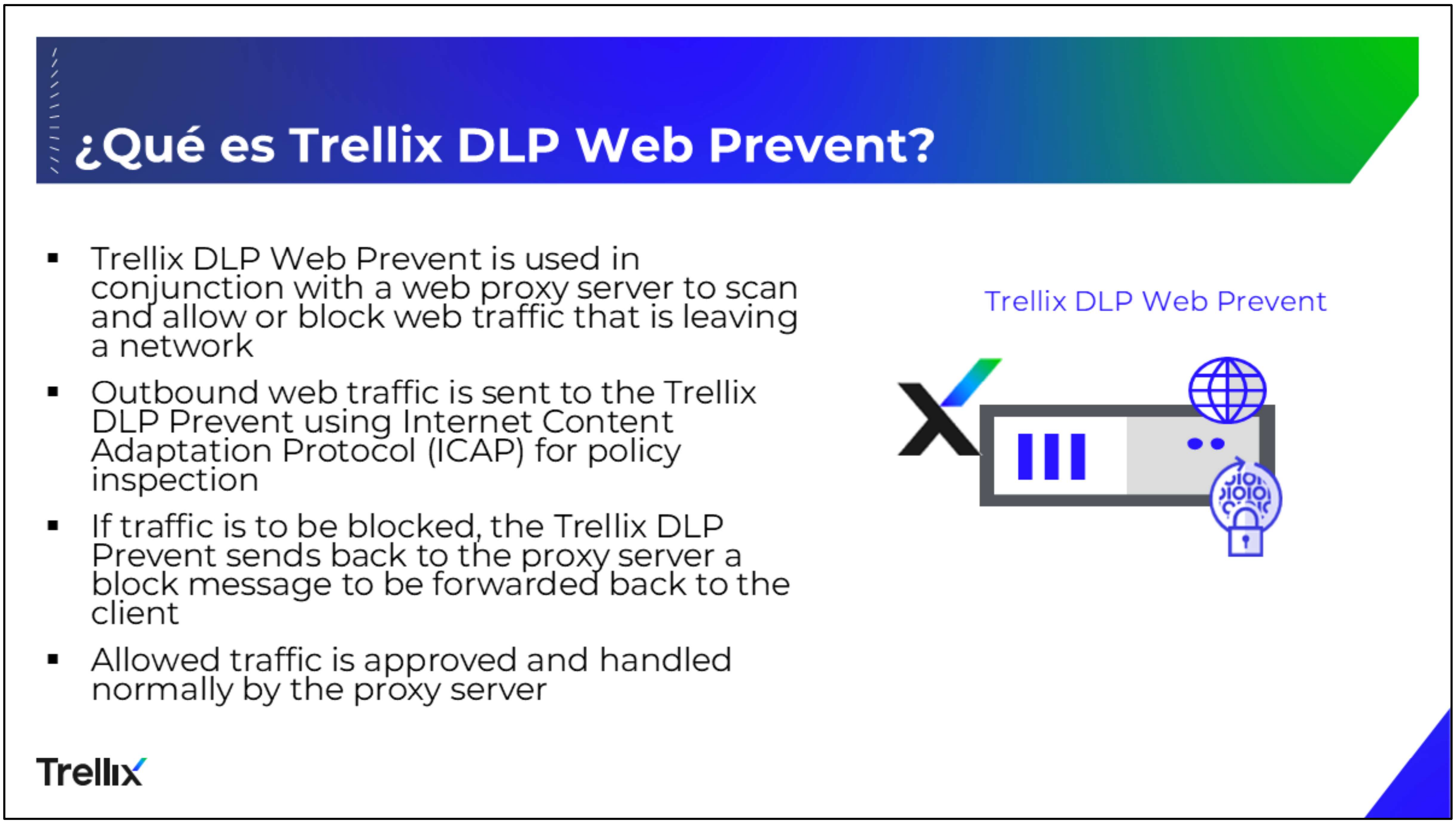


Lineamientos para Implementación

- Port 25 by default
- Maximum bandwidth through a single prevent is dependent on:
  - Email size and contents
  - How many active rules are being applied to each email
  - How many signatures are in memory
  - Start with a small, simple policy on the Trellix DLP Prevent and scale up
  - Do not use the same Trellix DLP Prevent device to perform email and web filtering – specialize the appliance for one or the other

Trellix

- Port 25 is used for communication between Mail Transfer Agent (MTA) and Trellix DLP Prevent
- Maximum number of email messages handled by Trellix DLP Prevent depends on number of TCP connections, number of emails sent in one TCP session, email size, attachment content types, and number. of active rules.
  - Example:
    - Use 30 TCP sessions to keep sending multiple emails
    - Each email with a Office file attachment that is around 200KB
    - If no active rule, Prevent can process 39 emails/second
    - Prevent can process 18 emails/second when rules are turned on
- Mail Queue on the MTA to account for peak mail load and not average
- Appropriate re-try timers to be set on MTA, incremental back off timeouts are not recommended



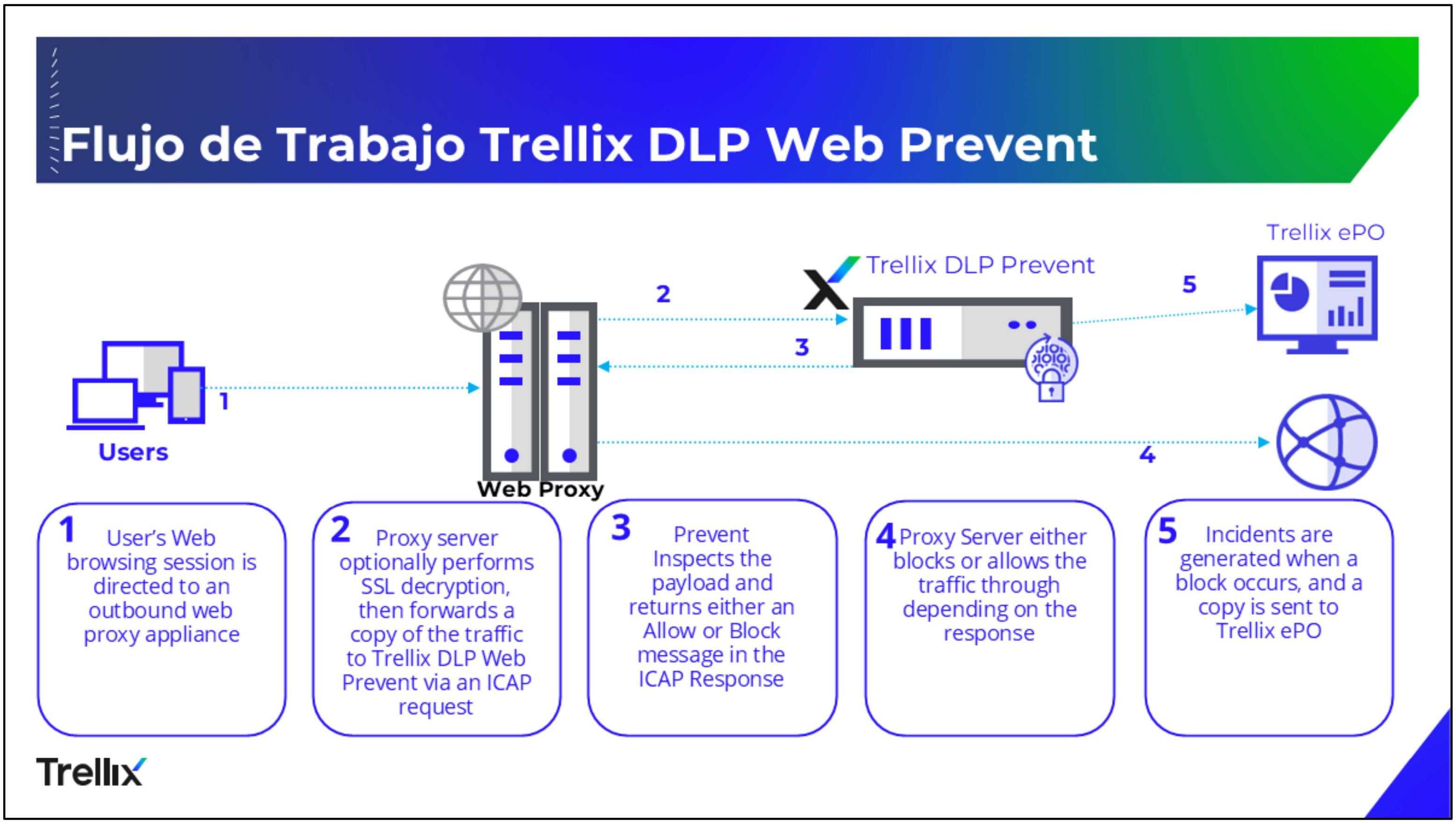
¿Qué es Trellix DLP Web Prevent?

- Trellix DLP Web Prevent is used in conjunction with a web proxy server to scan and allow or block web traffic that is leaving a network
- Outbound web traffic is sent to the Trellix DLP Prevent using Internet Content Adaptation Protocol (ICAP) for policy inspection
- If traffic is to be blocked, the Trellix DLP Prevent sends back to the proxy server a block message to be forwarded back to the client
- Allowed traffic is approved and handled normally by the proxy server

Trellix DLP Web Prevent

Trellix

Trellix DLP Web Prevent is used in conjunction with a web proxy server to scan and approve reject web traffic that is leaving a network. Outbound web traffic is sent to the Trellix DLP Prevent using Internet Content Adaptation Protocol (ICAP) for policy inspection. If traffic is to be blocked the Trellix DLP prevent sends back to the proxy server a block message to be forwarded back to the client. Allowed traffic is approved and handled normally by the proxy server.



Flujo de Trabajo Trellix DLP Web Prevent

1 User's Web browsing session is directed to an outbound web proxy appliance

2 Proxy server optionally performs SSL decryption, then forwards a copy of the traffic to Trellix DLP Web Prevent via an ICAP request

3 Prevent Inspects the payload and returns either an Allow or Block message in the ICAP Response

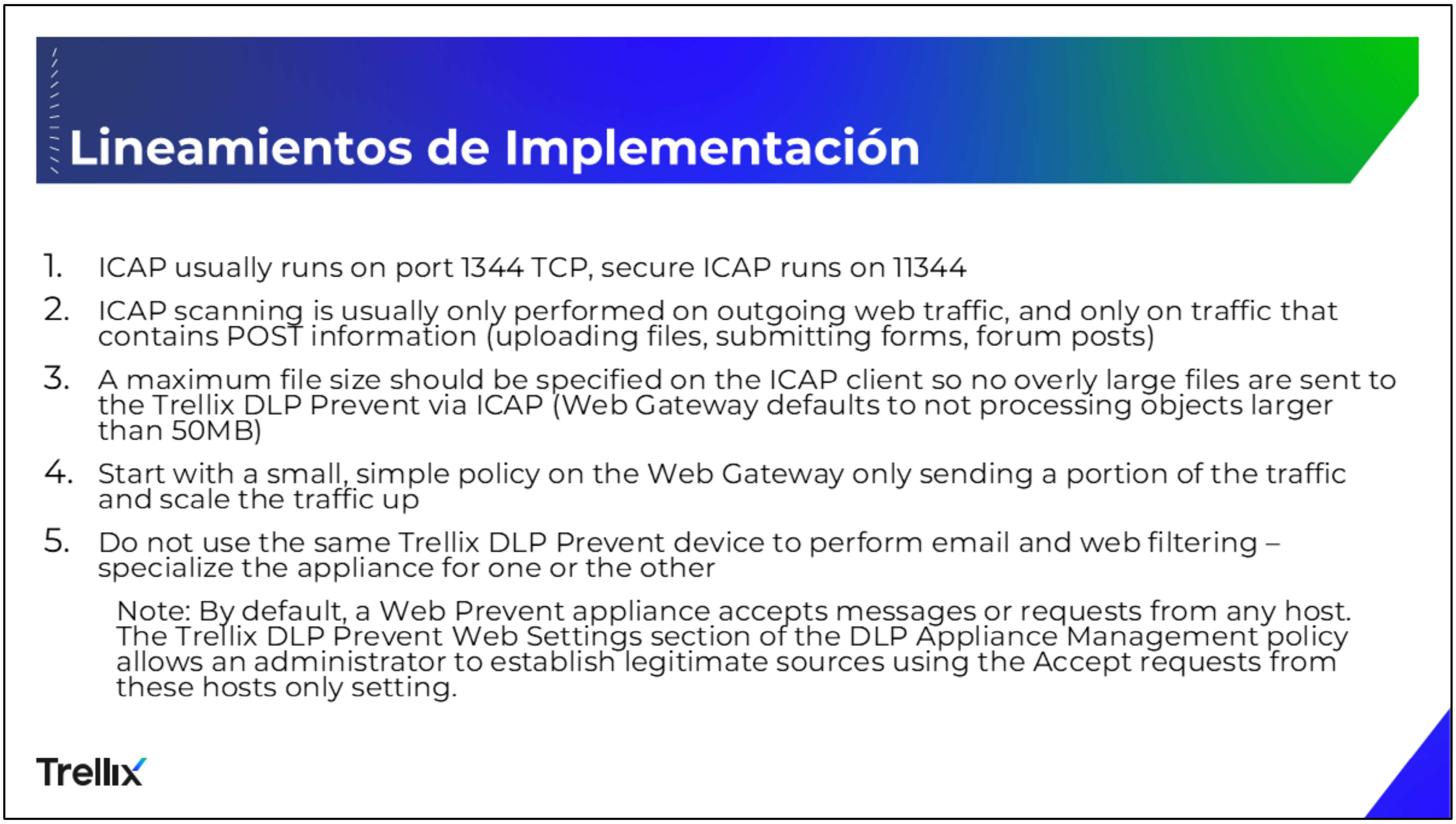
4 Proxy Server either blocks or allows the traffic through depending on the response

5 Incidents are generated when a block occurs, and a copy is sent to Trellix ePO

Trellix

A web proxy or Trellix® Web Gateway (MWG) appliance is used to take action on web requests made by client machines. These actions depend on the security policy implemented on the Trellix DLP Prevent appliance. The flow described here details how this usually takes place.

- The users' client systems forward data to a web proxy server (in this example, a Skyhigh Security Web Gateway, though any proxy server that supports ICAP will work).
- The web proxy provides an ICAP client that sends REQMOD requests with the appropriate data to Trellix DLP Prevent (the ICAP server).
- Trellix DLP Prevent sends back the action to be taken according to its configured policy, and a copy is sent to Trellix® ePolicy Orchestrator® (Trellix® ePO™).
- The request is either completed by the MWG if the Trellix DLP Prevent allows the connection, or a block page provided by the Trellix DLP Prevent in the ICAP response is forwarded back to the client.



Lineamientos de Implementación

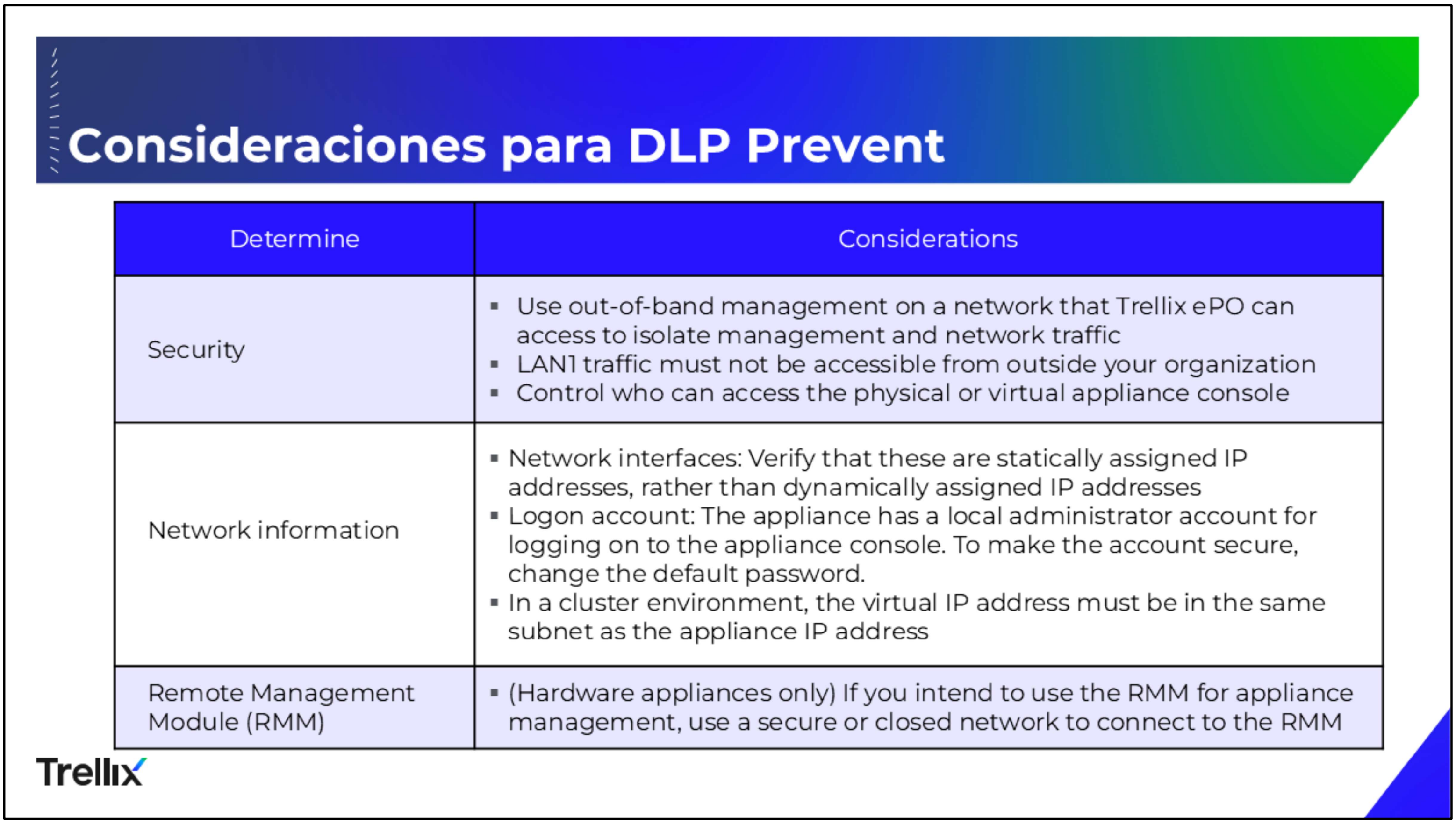
1. ICAP usually runs on port 1344 TCP, secure ICAP runs on 11344
2. ICAP scanning is usually only performed on outgoing web traffic, and only on traffic that contains POST information (uploading files, submitting forms, forum posts)
3. A maximum file size should be specified on the ICAP client so no overly large files are sent to the Trellix DLP Prevent via ICAP (Web Gateway defaults to not processing objects larger than 50MB)
4. Start with a small, simple policy on the Web Gateway only sending a portion of the traffic and scale the traffic up
5. Do not use the same Trellix DLP Prevent device to perform email and web filtering – specialize the appliance for one or the other

   Note: By default, a Web Prevent appliance accepts messages or requests from any host. The Trellix DLP Prevent Web Settings section of the DLP Appliance Management policy allows an administrator to establish legitimate sources using the Accept requests from these hosts only setting.

Trellix

- Port 1344 is used for communication between ICAP client (Web Proxy Server) and Trellix DLP Prevent.
- By default only REQMOD (Request Modification) items that have a body greater than 0 are forwarded to the Trellix DLP prevent by Skyhigh Security Web Gateway.
- Files and posts that are greater than 50mb are not forwarded to the ICAP server by default by MWG. This will help slowdowns caused by in-depth scanning of very large files.
- Do not use the same Trellix DLP Prevent device to perform email and web filtering – specialize the appliance for one or the other.

Note: By default, a Web Prevent appliance accepts messages or requests from any host. The **Trellix DLP Prevent Web Settings** section of the **DLP Appliance Management** policy allows an administrator to establish legitimate sources using the **Accept requests from these hosts** only setting.



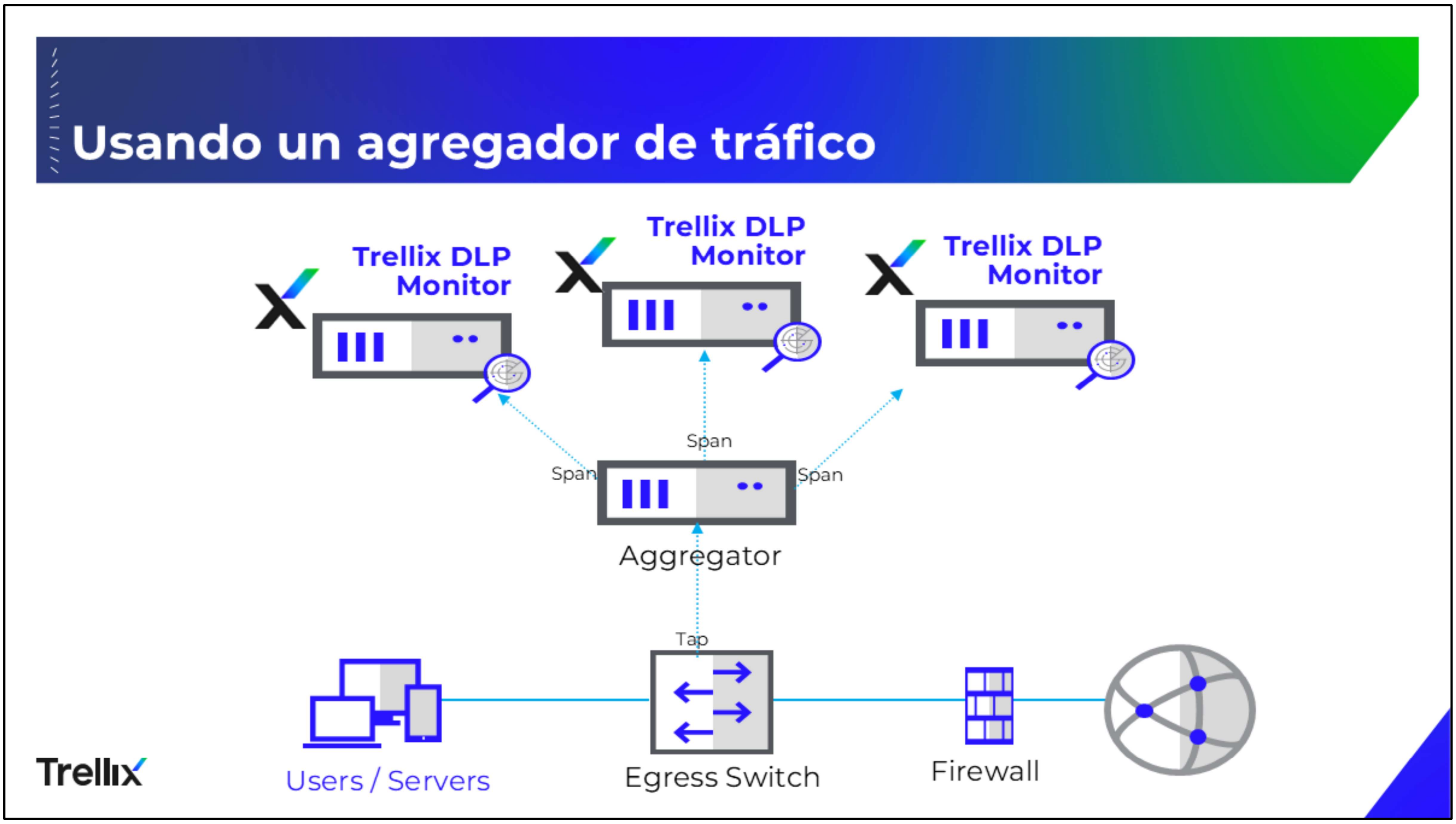
Consideraciones para DLP Prevent

Determine	Considerations
Security	▪ Use out-of-band management on a network that Trellix ePO can access to isolate management and network traffic ▪ LAN1 traffic must not be accessible from outside your organization ▪ Control who can access the physical or virtual appliance console
Network information	▪ Network interfaces: Verify that these are statically assigned IP addresses, rather than dynamically assigned IP addresses ▪ Logon account: The appliance has a local administrator account for logging on to the appliance console. To make the account secure, change the default password. ▪ In a cluster environment, the virtual IP address must be in the same subnet as the appliance IP address
Remote Management Module (RMM)	▪ (Hardware appliances only) If you intend to use the RMM for appliance management, use a secure or closed network to connect to the RMM

Trellix

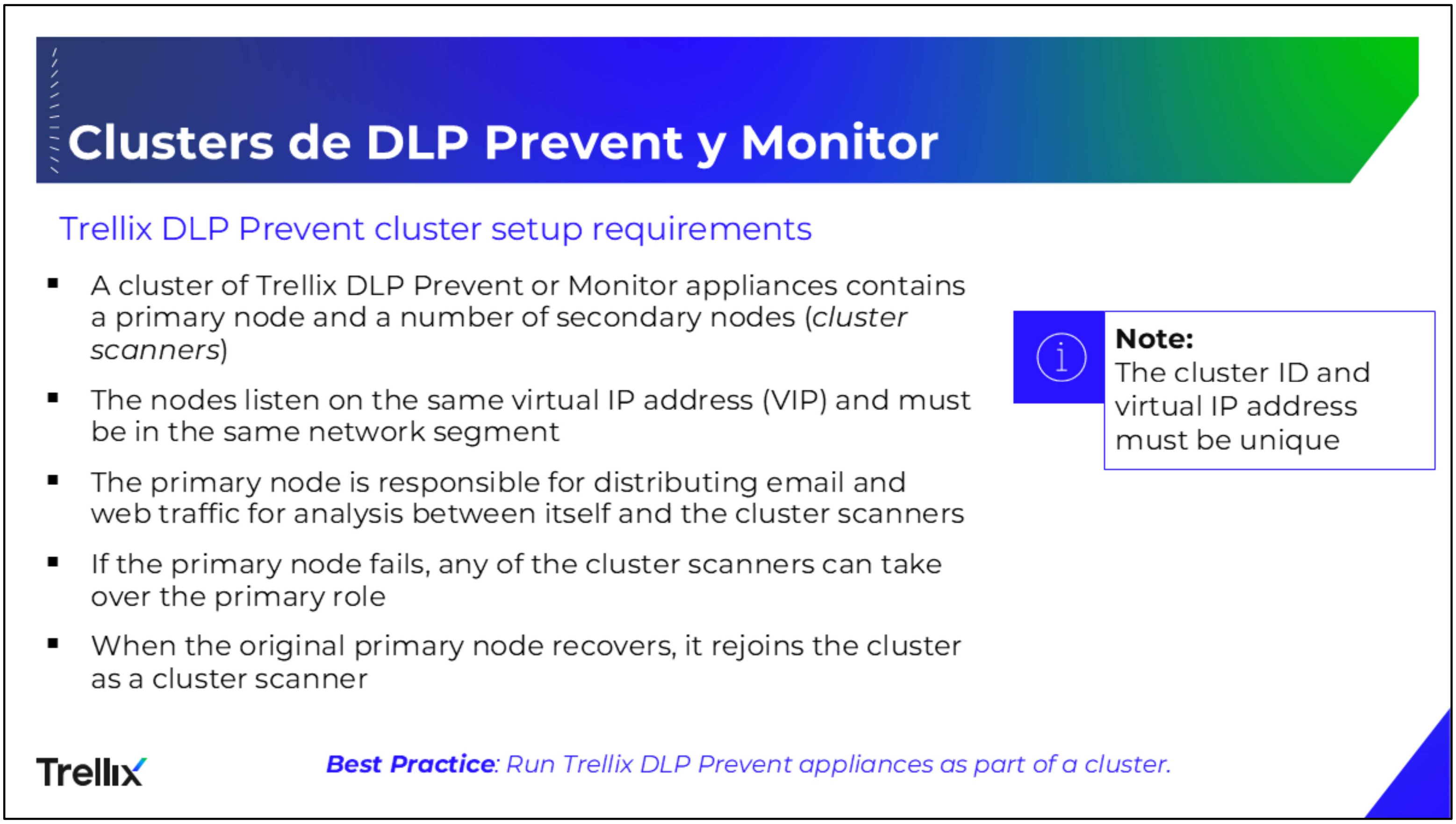
The table lists some considerations when deploying Trellix DLP Prevent.

- **Best practice:** Use the encrypted channel for your ICAP traffic.
- **Best practice:** Disable all unused services.



Usando un agregador de tráfico

An intelligent traffic aggregator device can be used to load balance sessions across multiple Trellix DLP Monitor appliances on high bandwidth segments.



Clusters de DLP Prevent y Monitor

Trellix DLP Prevent cluster setup requirements

- A cluster of Trellix DLP Prevent or Monitor appliances contains a primary node and a number of secondary nodes (*cluster scanners*)
- The nodes listen on the same virtual IP address (VIP) and must be in the same network segment
- The primary node is responsible for distributing email and web traffic for analysis between itself and the cluster scanners
- If the primary node fails, any of the cluster scanners can take over the primary role
- When the original primary node recovers, it rejoins the cluster as a cluster scanner

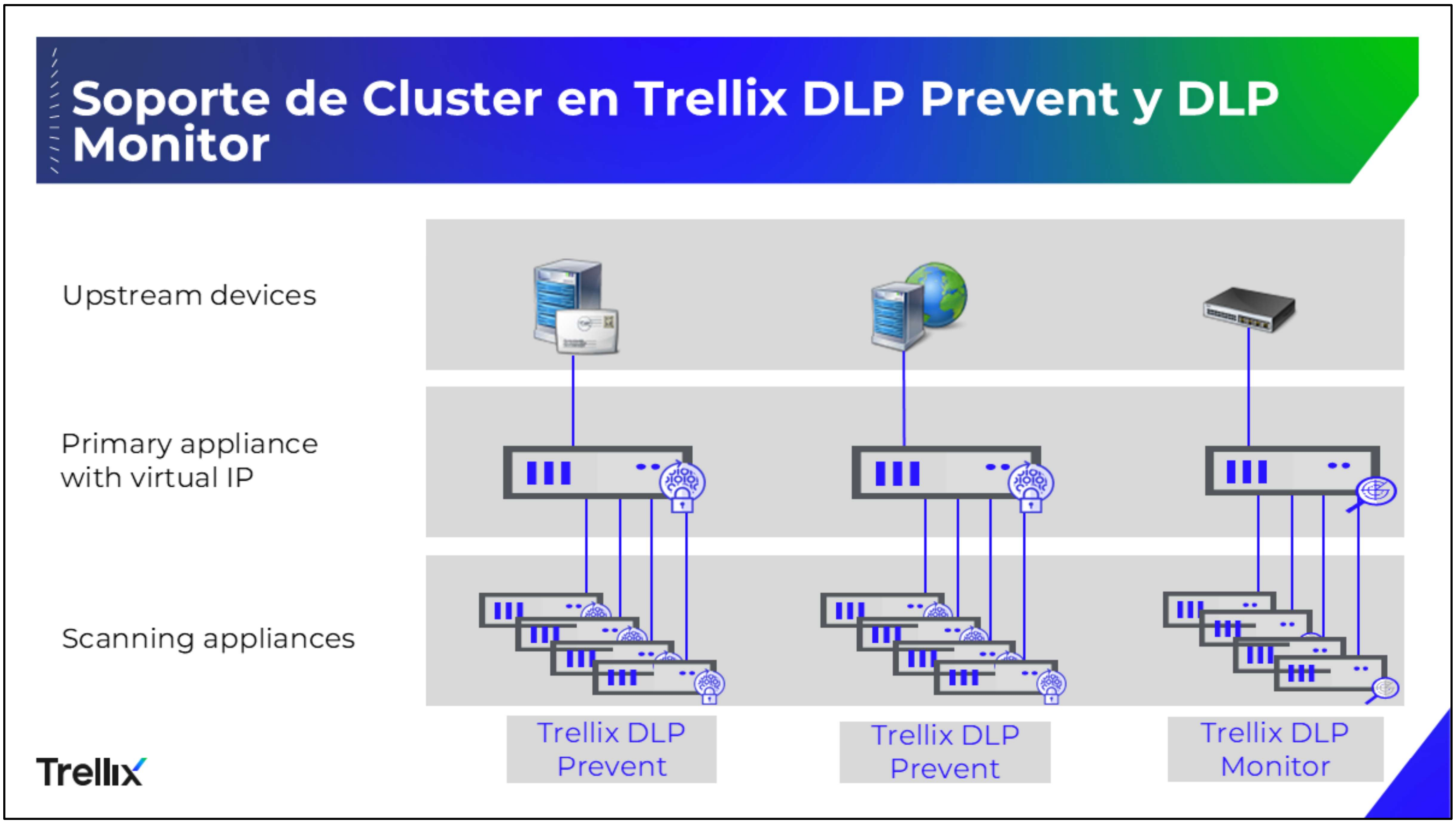
ⓘ **Note:**
The cluster ID and virtual IP address must be unique

Trellix

***Best Practice**: Run Trellix DLP Prevent appliances as part of a cluster.*

A cluster of Trellix DLP Prevent appliances contains a primary node and a number of secondary nodes (*cluster scanners*). The nodes listen on the same virtual IP address (VIP) and must be in the same network segment. The primary node is responsible for distributing email and web traffic for analysis between itself and the cluster scanners. If the primary node fails, any of the cluster scanners can take over the primary role. When the original primary node recovers, it rejoins the cluster as a cluster scanner.

Note: The cluster ID and virtual IP address must be unique.



Soporte de Cluster en Trellix DLP Prevent y DLP Monitor

Upstream devices

Primary appliance with virtual IP

Scanning appliances

Trellix DLP Prevent

Trellix DLP Prevent

Trellix DLP Monitor

You can deploy a Trellix DLP Monitor cluster or a Trellix DLP Prevent cluster or both clusters based on your environment. Deploy a Trellix DLP Monitor cluster when the network traffic monitoring and scanning capacity you want exceeds that of a standalone Trellix DLP Monitor appliance. In this scenario, a single deployment of Trellix DLP Monitor cluster monitors and scans a busy network.
Deploy a Trellix DLP Prevent cluster to load balance the incoming email and web traffic and accomplish high availability if a cluster node fails. In this scenario, a single deployment of Trellix DLP Prevent cluster analyzes and load balances the email and web traffic.

The cluster ID and the virtual IP address must be different from that of a Trellix DLP Prevent cluster ID and virtual IP address. You must not share the cluster scanners between two clusters.

Use these guidelines when setting up a Trellix DLP Monitor cluster:

- Run Trellix DLP Monitor appliances as part of a cluster to load balance the analysis of network traffic.
- Deploy two or more scanners to achieve maximum scanning capacity.
- Connect all scanners to a private scanning network and not to a public network.

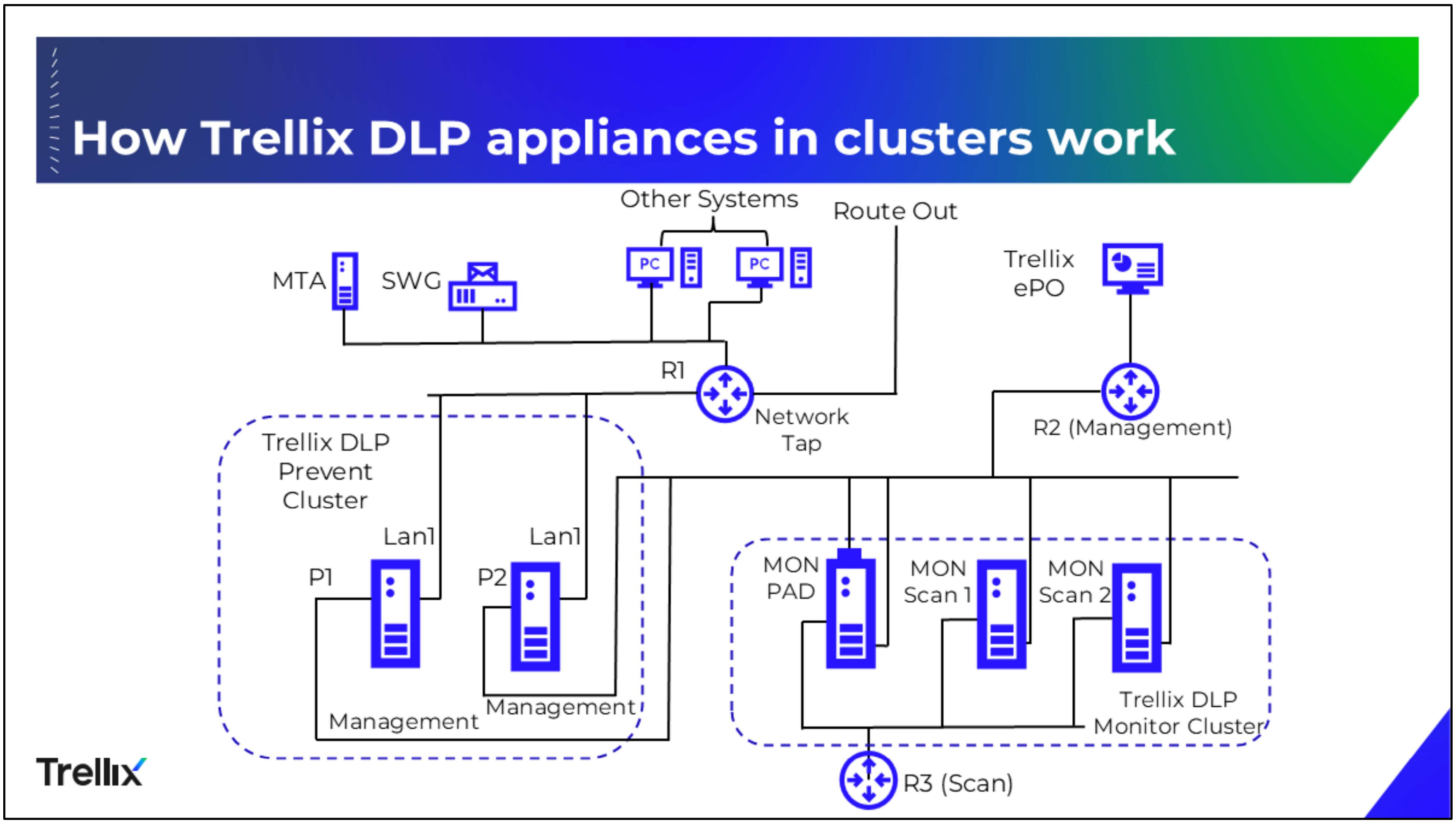
Using a DLP Monitor cluster has the following requirements:

- A dedicated Trellix DLP Monitor packet acquisition device.
- Two or more dedicated Trellix DLP Monitor scanners.

Using a Trellix DLP Prevent cluster has the following requirements:

- A Trellix DLP Prevent primary node. The primary node is responsible for distributing email and web traffic for analysis between itself and the cluster scanners. If the primary node fails, any of the cluster scanners take over the primary role.

- One or more Trellix DLP Prevent scanners.



How Trellix DLP appliances in clusters work

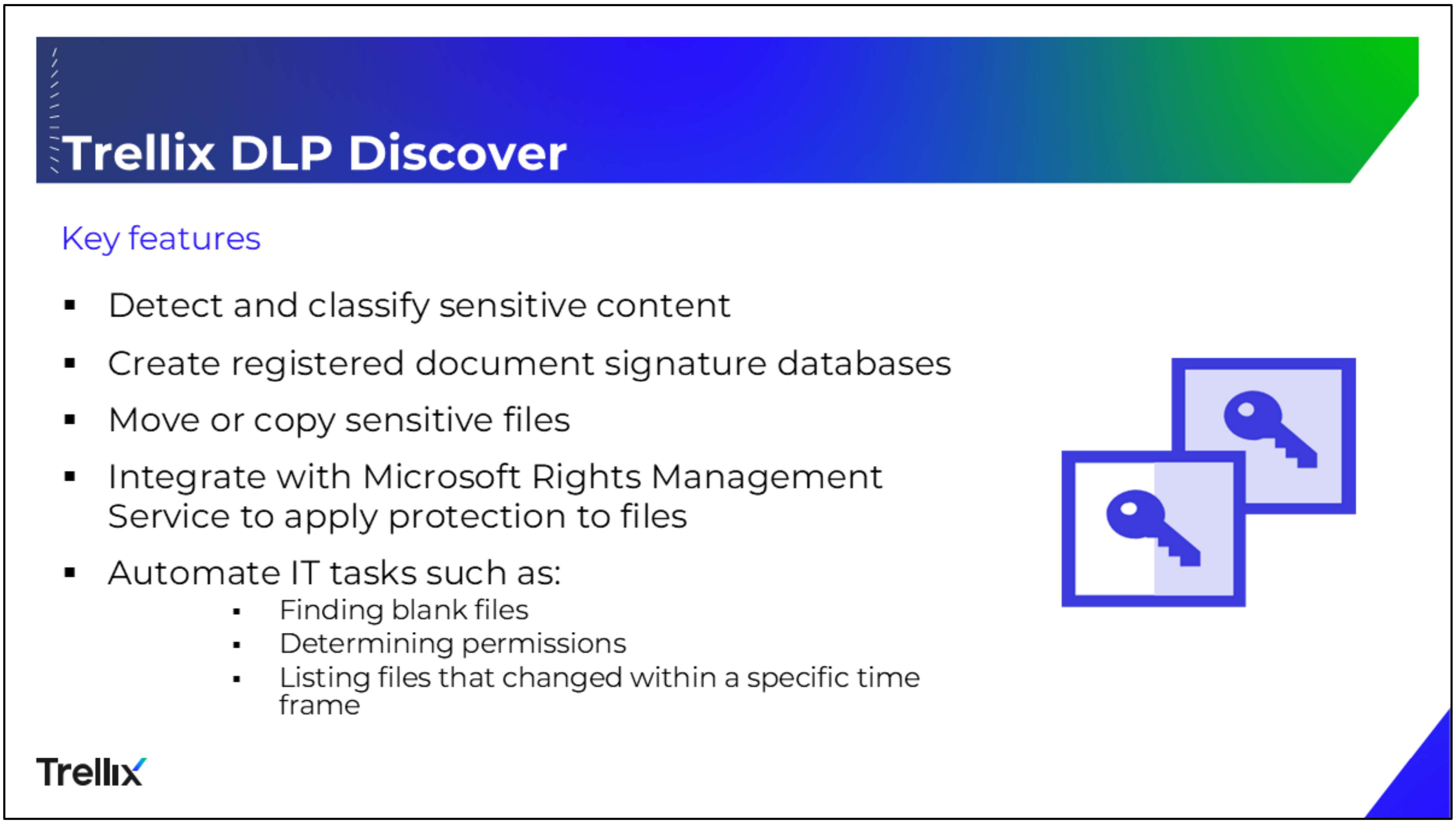
Three networks are connected to three routers:

- R1 is connected to general network traffic.
- R2 is connected to a management network with the Trellix ePO server connected to it. All Trellix DLP Monitor and Trellix DLP Prevent systems have their management interfaces connected to R2.
- R3 is connected to a private scanning network of the Trellix DLP Monitor cluster. All Trellix DLP Monitor systems have their LAN1 interfaces connected to R3.

Mail Transfer Agent (MTA) is the mail server for the R1 network, while the Web Gateway is used as the web proxy. Other systems are also connected to this network and R1 is the route out.

P1 and P2 are two Trellix DLP Prevent servers in a cluster. Their LAN1 interfaces are connected to R1. They receive email traffic from MTA and web traffic from the web gateway (MWG). The responses go back to MTA and MWG, while the events are sent to the Trellix ePO server.

A network tap mirrors all network traffic going through R1 to the capture interface on the packet acquisition device, MON PAD. The appliances, MON SCAN 1 and MON SCAN 2 are dedicated load balancing scanners and receive scanning requests from MON PAD. The scan results are sent to Trellix ePO for monitoring and tracking the incidents.



Trellix DLP Discover

Key features

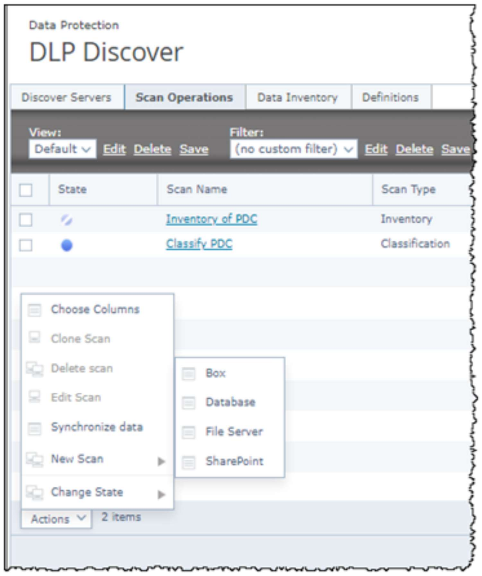
- Detect and classify sensitive content
- Create registered document signature databases
- Move or copy sensitive files
- Integrate with Microsoft Rights Management Service to apply protection to files
- Automate IT tasks such as:
  - Finding blank files
  - Determining permissions
  - Listing files that changed within a specific time frame

Use Trellix DLP Discover for:

- Detecting and classifying sensitive content
- Creating registered document signature databases
- Moving or copying sensitive files
- Integrating with Microsoft Rights Management Service to apply protection to files
- Automating IT tasks such as finding blank files, determining permissions, and listing files that changed within a specified time range

Trellix DLP Discover (cont.)

Overview



□	State	Scan Name	Scan Type
□		Inventory of PDC	Inventory
□	●	Classify PDC	Classification

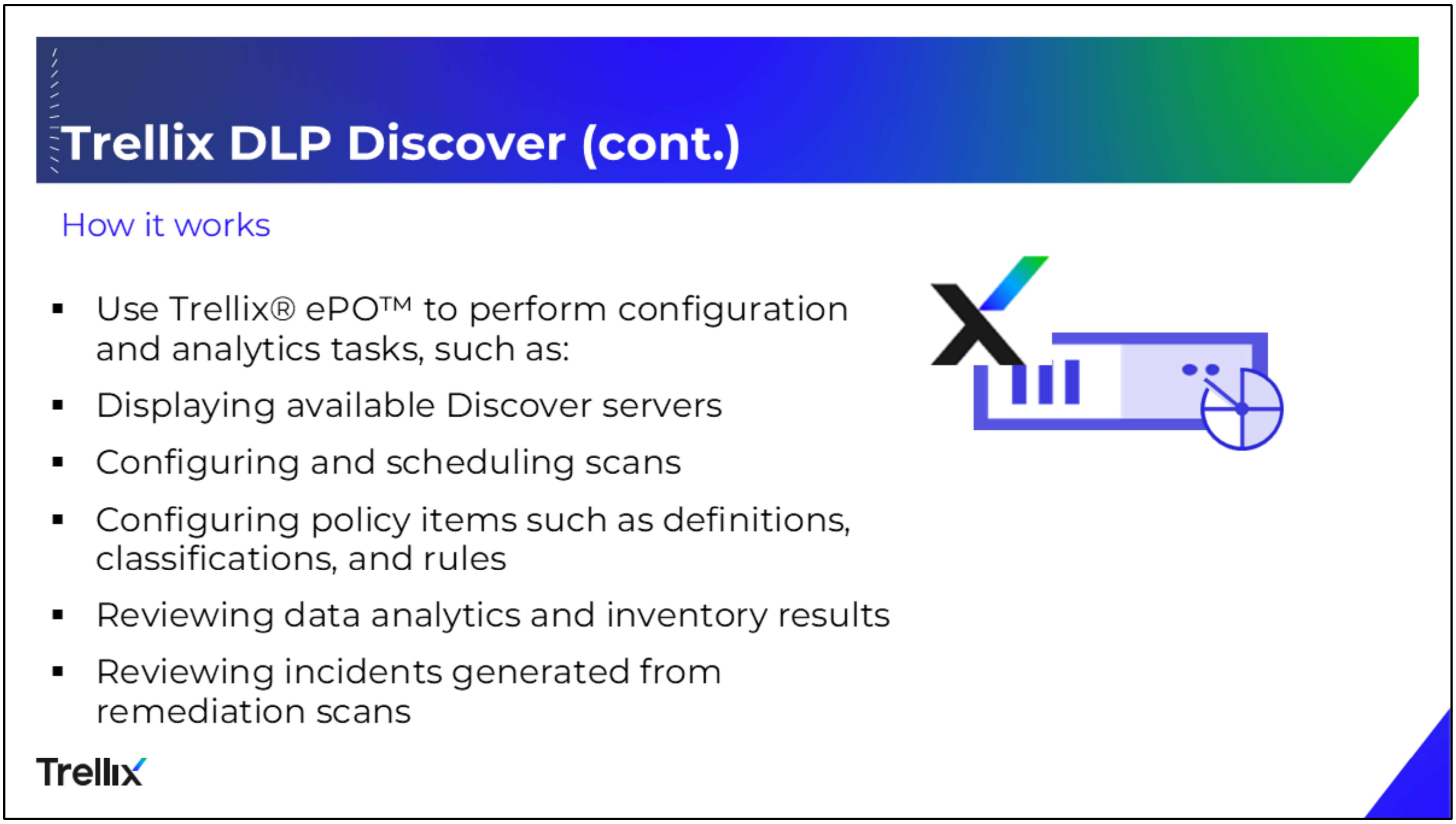
- **Discover servers**: Refer to the product documentation or student guide for a list of supported servers
- **Scan operations**: Provides ability to view current scans and create, edit, and delete scans
- **Data Analytics & Inventory**: Allows drilling into conducted scans to identify data found in Online Analytical Processing (OLAP) format
- **Definitions**: Create credentials for use with scans; setup of Box, CIFS, Database, and SharePoint scans

Trellix

Trellix DLP Discover is a scalable, extensible software system that can meet the requirements of any size
network. Deploy Trellix DLP Discover software to as many servers throughout the network as needed.

Trellix DLP Discover consists of the following functionalities:

- **Discover servers**: Windows Server 2008 R2 Standard Service Pack 1 or later, 64-bit; Windows Server 2012 Standard, 64-bit; Windows Server 2012 R2 Standard, 64-bit; Windows Server 2016 R2 Standard, 64-bit; Windows Server 2019 R2 Standard, 64-bit
- **Scan operations**: Provides ability to view current, create, edit, and delete scans
- **Data Analytics & Inventory**: Allows drilling into conducted scans to identify data found in Online Analytical Processing (OLAP) format
- **Definitions**: Create credentials for use with scans; setup of Box, CIFS, Database, and SharePoint scans



Trellix DLP Discover (cont.)

How it works

- Use Trellix® ePO™ to perform configuration and analytics tasks, such as:
- Displaying available Discover servers
- Configuring and scheduling scans
- Configuring policy items such as definitions, classifications, and rules
- Reviewing data analytics and inventory results
- Reviewing incidents generated from remediation scans

Trellix ePO uses Trellix Agent to install and deploy the Trellix DLP Discover software to a *Discover server* — a designated Windows Server.

Trellix ePO applies the scan policy to Discover servers, which scan the repository or database at the scheduled time. The data collected and the actions applied to files depend on the scan type and configuration. For database scans, the only actions available are to report the incident and store evidence.

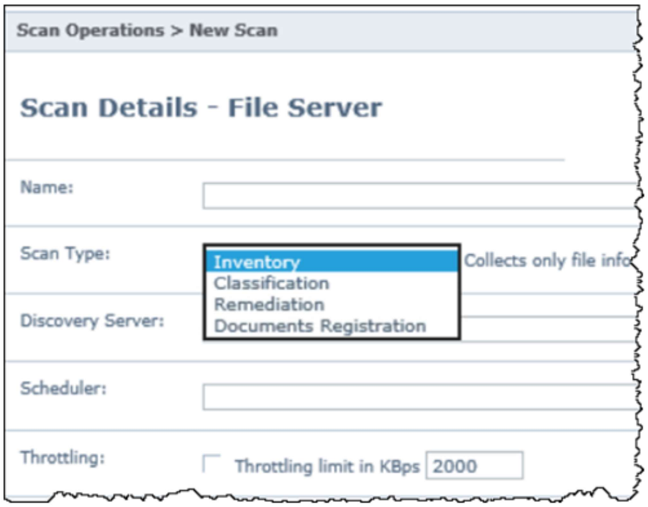
Use Trellix ePO to perform configuration and analytics tasks such as:

- Displaying available Discover servers
- Configuring and scheduling scans
- Configuring policy items such as definitions, classifications, and rules
- Reviewing data analytics and inventory results
- Reviewing incidents generated from remediation scans

Tipos de Scan

Information retrieved, actions taken, & configuration

- **Inventory**: Designed to collect file inventory data
- **Classification**: Helps in planning the protection strategy and analyze file content
- **Remediation**: Analyze files and performs remediation actions
- **Registration**: Creates file signatures that match fingerprinted criteria to identify and track files



Scan Operations > New Scan

Scan Details - File Server

Name:

Scan Type: Inventory / Classification / Remediation / Documents Registration — Collects only file info

Discovery Server:

Scheduler:

Throttling: □ Throttling limit in KBps 2000

Trellix

The type of scan you configure determines the amount of information retrieved in a scan, the actions taken during the scan, and the configuration needed for the scan.
When scanning large databases, it is recommended to register only the sensitive data, such as bank account numbers or Social Security numbers. Registering an entire database is neither practical nor useful.

Inventory scans

Use inventory scans to give you a high-level view of what types of files exist in the repository. This scan collects only metadata — the files are not fetched. Trellix DLP Discover sorts scanned metadata into different content types and analyzes attributes such as file size, location, and file extension. Use this scan to create an overview of your repository or for IT tasks such as locating infrequently used files. You can run inventory scans on all supported file repositories and databases.

Classification scans

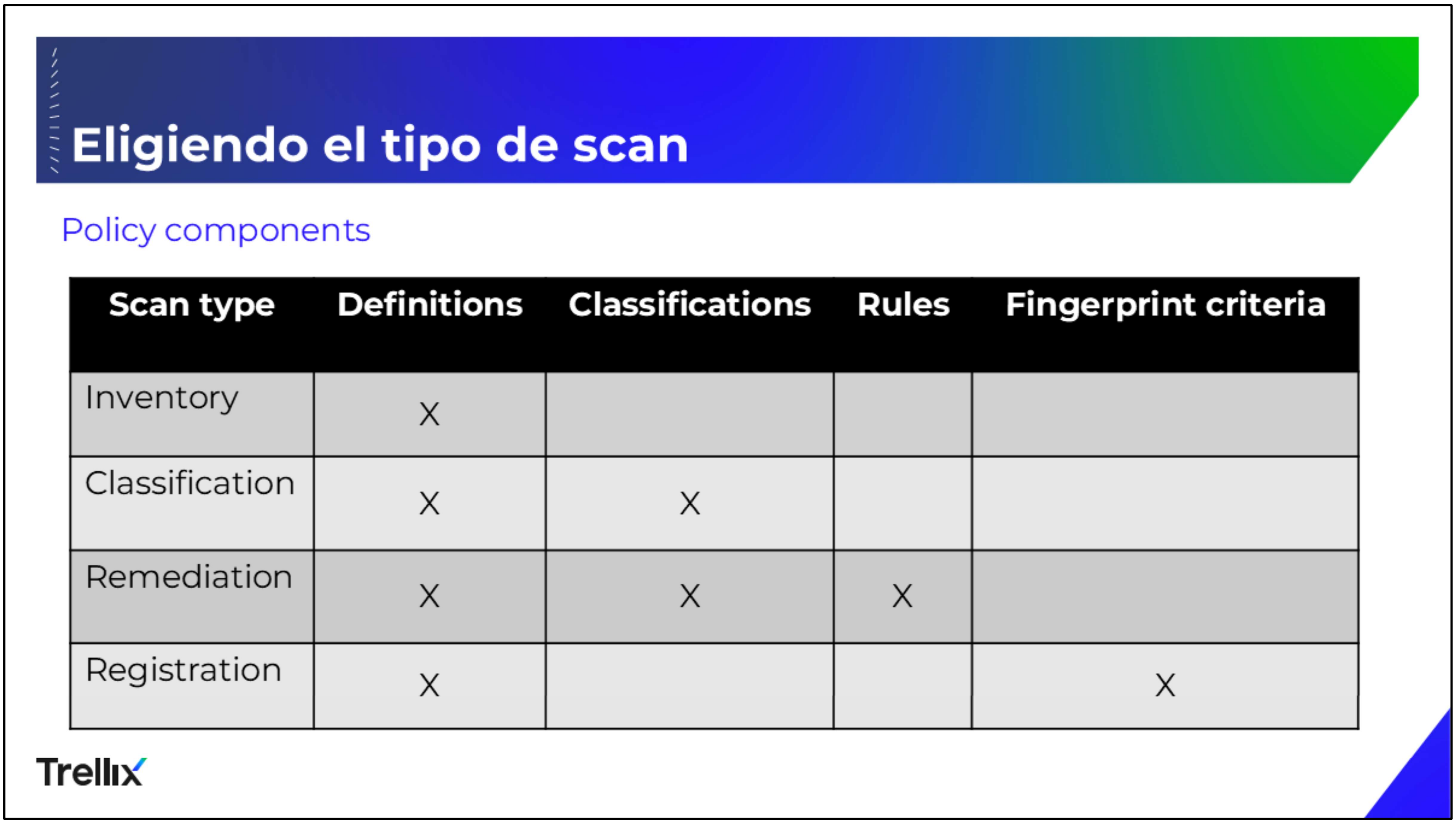
Use classification scans to help you understand the data that exists in the targeted repository. By matching scanned content to classifications such as text patterns or dictionaries, you can analyze data patterns to create optimized remediation scans. You can run classification scans on all supported file repositories and databases.

Remediation scans

Use remediation scans to find data that is in violation of a policy. You can run remediation scans on all supported file repositories and databases. You can monitor, apply a Rights Management policy, copy, or move files to an export location. All actions can produce incidents that are reported to the Incident Manager in Trellix ePO. For database scans, you can monitor, report incidents, and store evidence.

Registration scans

Use document registration scans to extract content from files based on selected fingerprint criteria, and save the data to a signature database. The registered documents can define classification and remediation scans, or policies for Trellix DLP Prevent and Trellix DLP Monitor. You can run document registration scans only on supported file repositories, not on databases. A file can potentially be picked up by more than one document registration scan. In that case, it is classified based on more than one set of criteria, and its signatures are recorded in more than one registered document.



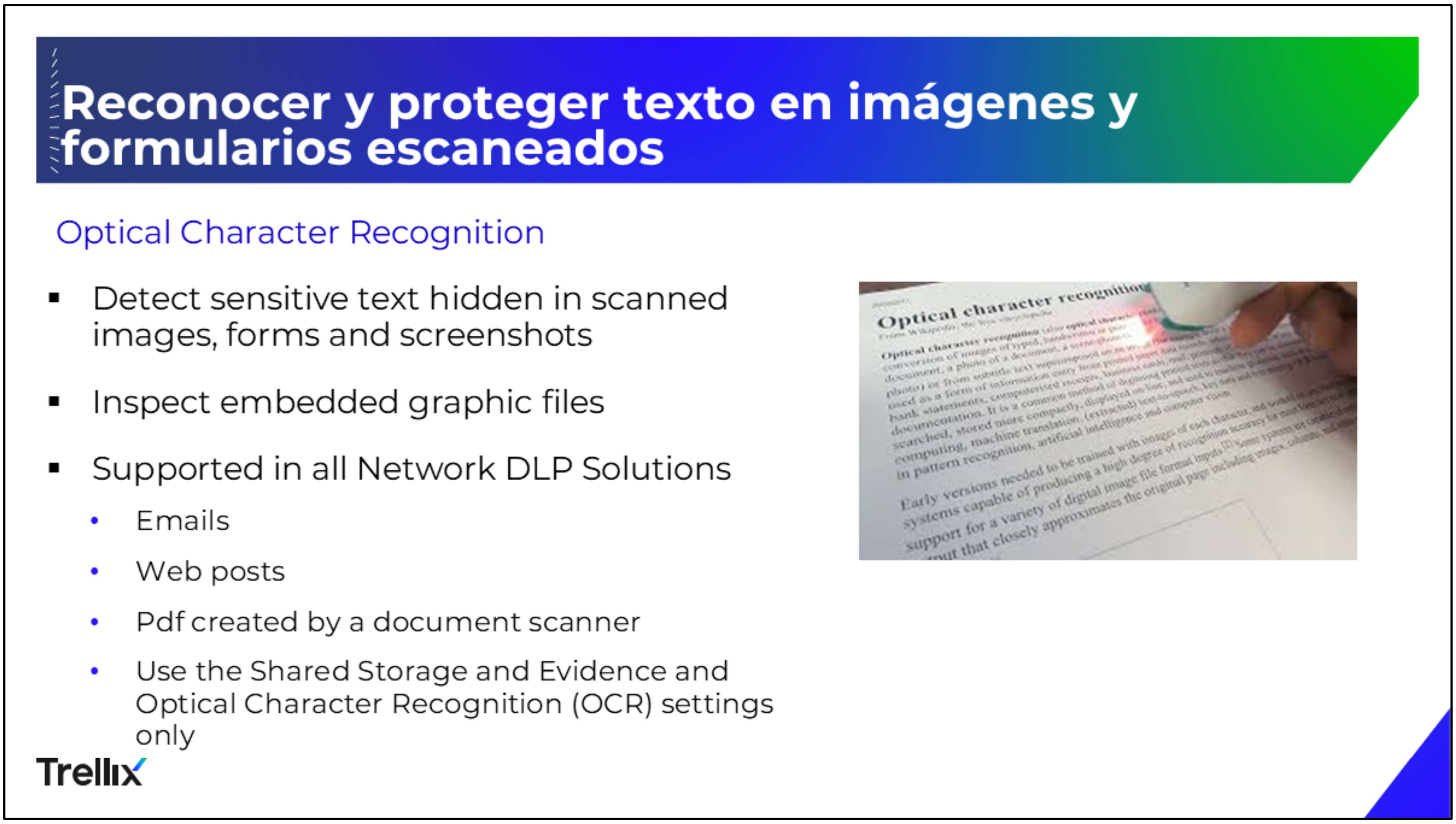
Eligiendo el tipo de scan

Policy components

Scan type	Definitions	Classifications	Rules	Fingerprint criteria
Inventory	X			
Classification	X	X		
Remediation	X	X	X	
Registration	X			X

Trellix

The policy components you must configure depend on the scan type.



Reconocer y proteger texto en imágenes y formularios escaneados

Optical Character Recognition

- Detect sensitive text hidden in scanned images, forms and screenshots
- Inspect embedded graphic files
- Supported in all Network DLP Solutions
  - Emails
  - Web posts
  - Pdf created by a document scanner
  - Use the Shared Storage and Evidence and Optical Character Recognition (OCR) settings only

Trellix

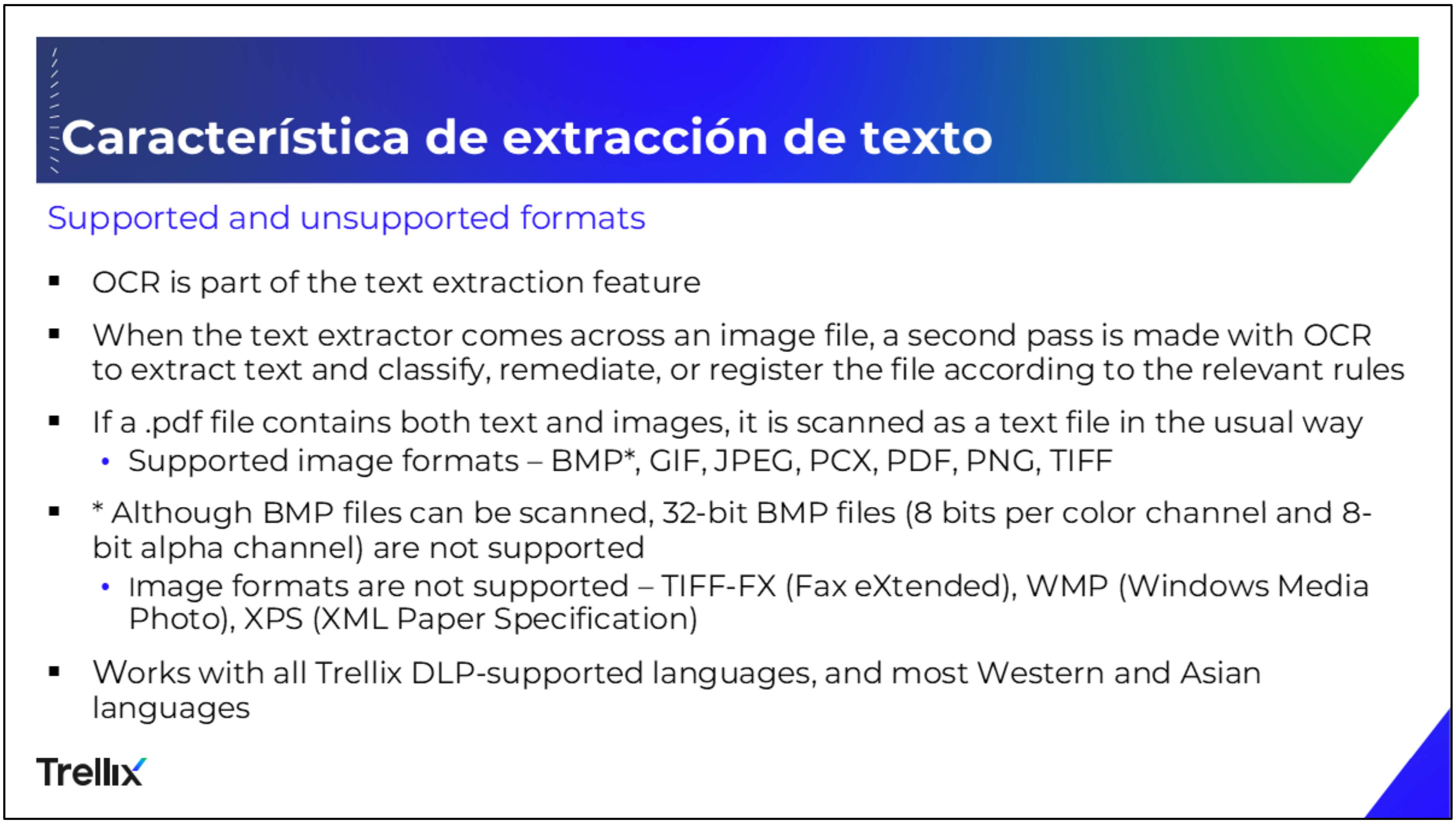
Scanning image files with OCR
Optical character recognition (OCR) scans extract text from image files.

- You can use the OCR feature for extracting text from image files. The extracted text is matched with classification definitions to classify or remediate files.
- In Trellix DLP Discover, you can use the OCR feature when scanning any file-based repository. Database scans are not supported
- In Trellix DLP appliances, you can use the OCR feature when scanning images attached to emails, uploaded in web posts, or found in other network traffic.

Note: The OCR feature is supported in Trellix DLP Discover 11.1.100 and later and in Trellix DLP appliances 11.4.0 and later.

Network DLP:

- Supports Optical Character Recognition (OCR) for scanning images attached to emails. The images can also be .pdf files created by a document scanner.
- Supports Optical Character Recognition (OCR) for scanning images attached to web posts or images found in other network traffic.
- Trellix DLP Prevent and Trellix DLP Monitor use the Shared Storage and Evidence and Optical Character Recognition (OCR) settings only.



Característica de extracción de texto

Supported and unsupported formats

- OCR is part of the text extraction feature
- When the text extractor comes across an image file, a second pass is made with OCR to extract text and classify, remediate, or register the file according to the relevant rules
- If a .pdf file contains both text and images, it is scanned as a text file in the usual way
  - Supported image formats – BMP*, GIF, JPEG, PCX, PDF, PNG, TIFF
- * Although BMP files can be scanned, 32-bit BMP files (8 bits per color channel and 8-bit alpha channel) are not supported
  - Image formats are not supported – TIFF-FX (Fax eXtended), WMP (Windows Media Photo), XPS (XML Paper Specification)
- Works with all Trellix DLP-supported languages, and most Western and Asian languages

Trellix

OCR is part of the text extraction feature. When the text extractor comes across an image file, a second pass is made with OCR to extract text and classify, remediate, or register the file according to the relevant rules. The feature also works with images saved as a .pdf file. If a .pdf file contains both text and images, it is scanned as a text file in the usual way. For example, Trellix DLP appliances monitor a hardcopy sensitive document scanned and sent in an email as a .pdf attachment. OCR scanning works with all Trellix DLP-supported languages, and most Western and Asian languages.

For information about installing and updating the OCR package in Trellix DLP Discover, see the Trellix Data Loss Prevention Discover *Installation Guide* and KB91046.

No additional software installation is needed on the Trellix DLP appliances to run the OCR feature.

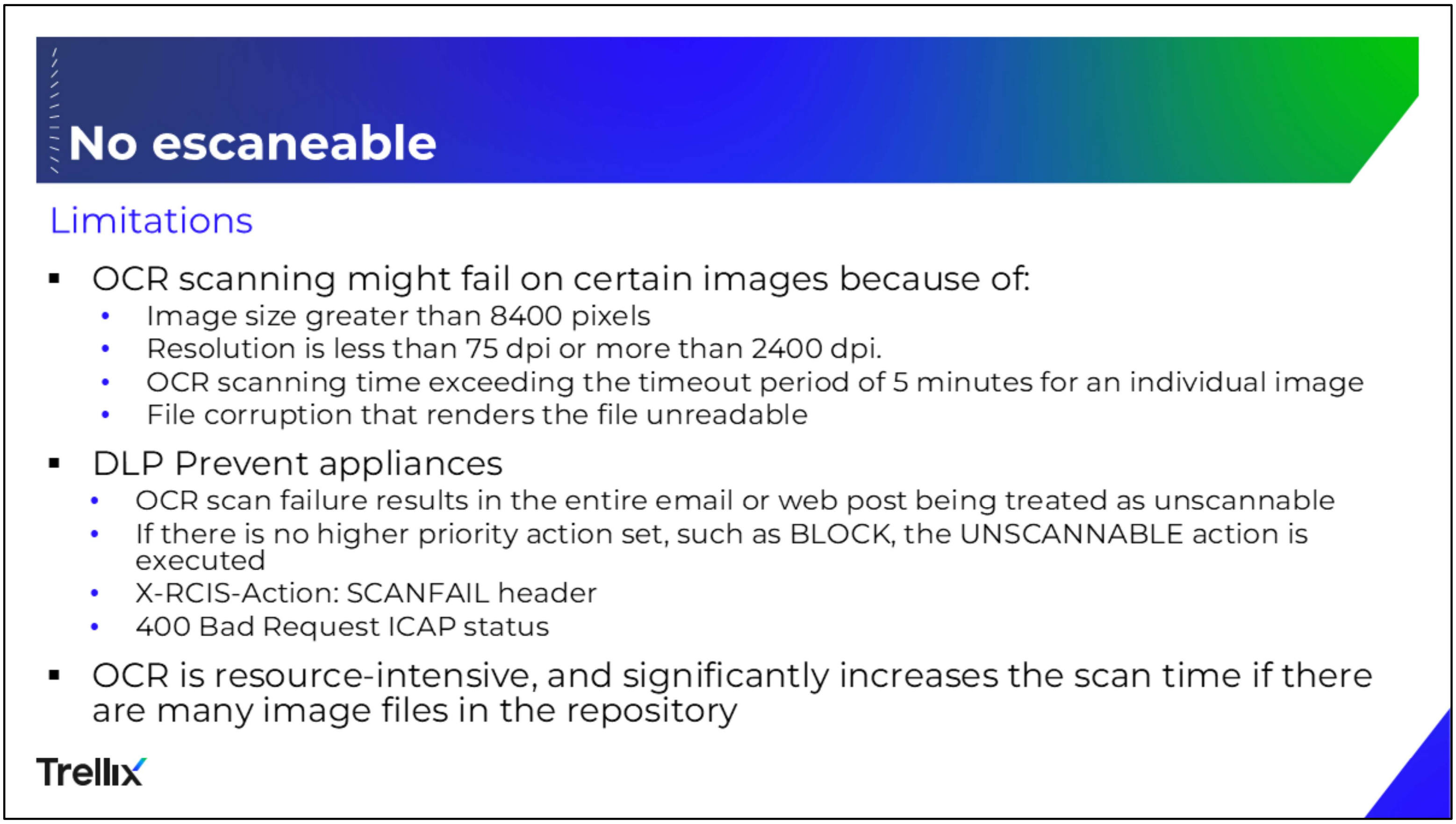
Supported image formats

- Trellix DLP Discover and Trellix DLP appliances support scanning of images of these formats:
  - BMP*
  - GIF
  - JPEG
  - PCX
  - PDF
  - PNG
  - TIFF

* Although BMP files can be scanned, 32-bit BMP files (8 bits per color channel and 8-bit alpha channel) are not supported.

The following image formats are not supported on Trellix DLP appliances but are supported on Trellix DLP Discover:

- TIFF-FX (Fax eXtended)
- WMP (Windows Media Photo)
- XPS (XML Paper Specification)



No escaneable

Limitations

- OCR scanning might fail on certain images because of:
  - Image size greater than 8400 pixels
  - Resolution is less than 75 dpi or more than 2400 dpi.
  - OCR scanning time exceeding the timeout period of 5 minutes for an individual image
  - File corruption that renders the file unreadable
- DLP Prevent appliances
  - OCR scan failure results in the entire email or web post being treated as unscannable
  - If there is no higher priority action set, such as BLOCK, the UNSCANNABLE action is executed
  - X-RCIS-Action: SCANFAIL header
  - 400 Bad Request ICAP status
- OCR is resource-intensive, and significantly increases the scan time if there are many image files in the repository

Trellix

Unscannable images with Trellix DLP appliances

OCR scanning might fail on certain images because of:

- Image size greater than 8400 pixels
- Resolution is less than 75 dpi or more than 2400 dpi.
- OCR scanning time exceeding the timeout period of 5 minutes for an individual image
- File corruption that renders the file unreadable

On Trellix DLP Prevent appliances, OCR scan failure results in the entire email or web post being treated as unscannable. If there is no higher priority action set, such as BLOCK, the UNSCANNABLE action is executed.

The Trellix DLP Prevent appliance adds X-RCIS-Action: SCANFAIL header to such unscannable emails received by the Smart Host.

For web posts, the web proxy receives a 400 Bad Request ICAP status. Any other detections in the email or web post still result in DLP incidents.

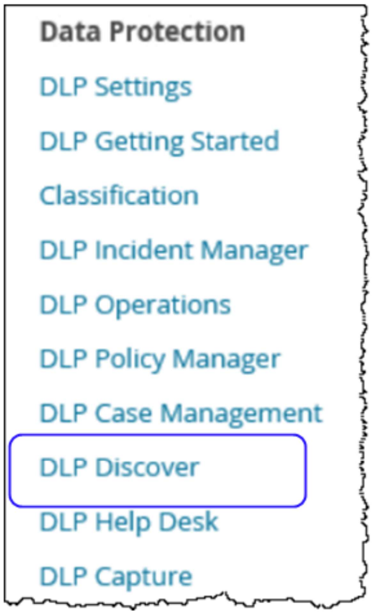
Limitations:

OCR is resource-intensive, and significantly increases the scan time if there are many image files in the repository.

For this reason, in Trellix DLP Discover, it can be disabled with a checkbox on the Text Extractor page of the Server Configuration if it is not needed.

Requerimientos DLP Discover

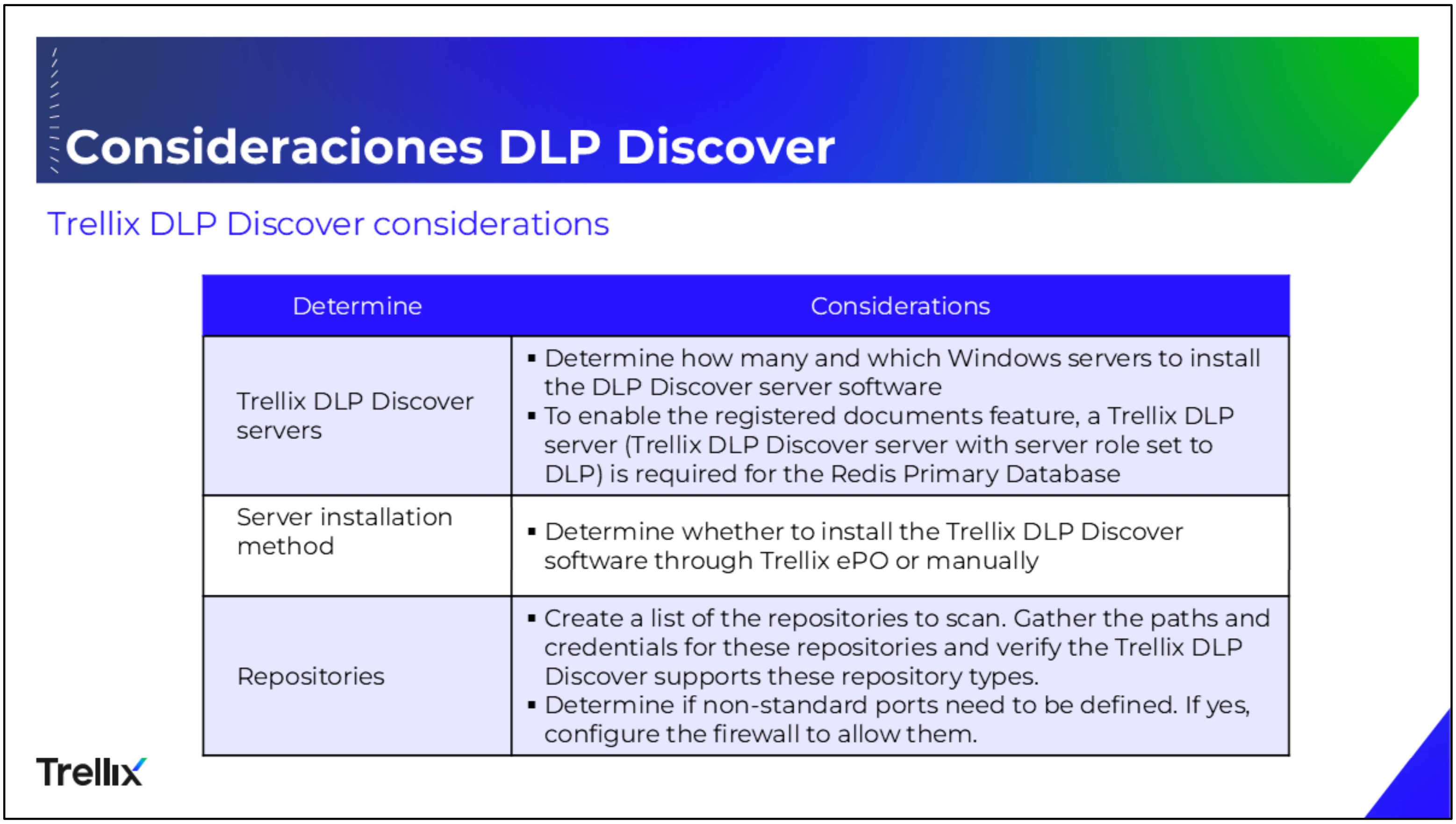
- Trellix Agent is installed and running
- Communicating with Trellix ePO
- Added to the Trellix ePO System Tree



Trellix

Make sure that any servers you use for Trellix DLP Discover meet these requirements:

- The server has Trellix Agent installed and running.
- The server is communicating with Trellix ePO.
- The server is added to the Trellix ePO System Tree.



Consideraciones DLP Discover

Trellix DLP Discover considerations

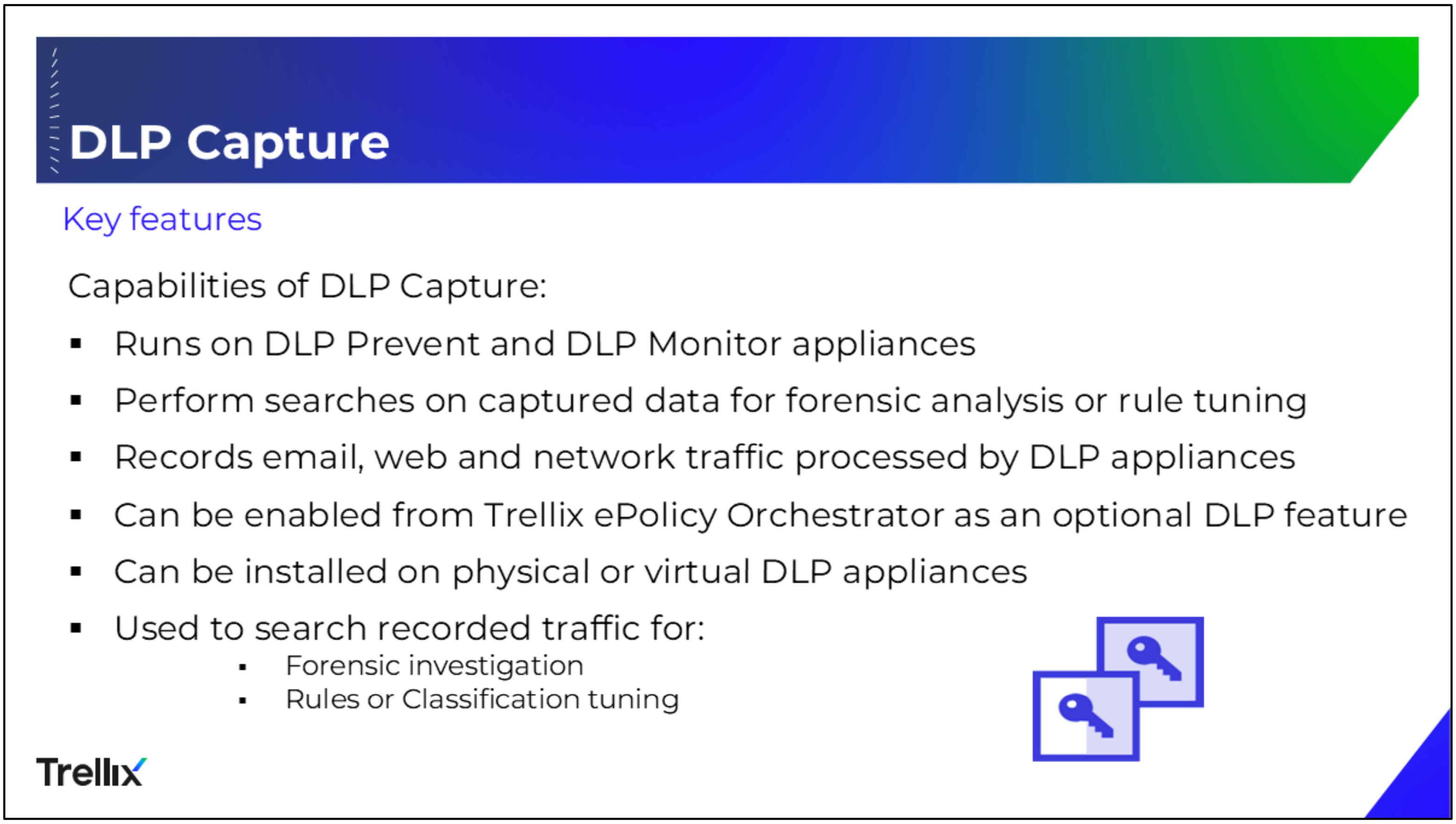
Determine	Considerations
Trellix DLP Discover servers	▪ Determine how many and which Windows servers to install the DLP Discover server software ▪ To enable the registered documents feature, a Trellix DLP server (Trellix DLP Discover server with server role set to DLP) is required for the Redis Primary Database
Server installation method	▪ Determine whether to install the Trellix DLP Discover software through Trellix ePO or manually
Repositories	▪ Create a list of the repositories to scan. Gather the paths and credentials for these repositories and verify the Trellix DLP Discover supports these repository types. ▪ Determine if non-standard ports need to be defined. If yes, configure the firewall to allow them.

Trellix

The table lists some considerations when deploying Trellix DLP Discover.

Requerimientos Trellix DLP Server

- Trellix DLP Servers are used to host a registered documents signature database
- Trellix DLP Discover servers perform the scans Trellix DLP Servers host the signature database.
- Signatures can have a large RAM impact on the DLP Server, 100 million signatures, the maximum per run, takes about 7 GB of RAM.
- The maximum size of the database is set on the Classification page in DLP Settings and can range from 10 million to 500 million signatures.
- The maximum number of registration scans, enabled and disabled, that can be listed in Scan Operations is 100.
- The DLP Server host listed on the Policy Catalog | Server Configuration | Registered Documents page must be in the same LAN as the Trellix ePO server.
- Trellix DLP Discover servers can be in another LAN or over WAN.
- User credentials provided for registration scans must have, as a minimum, READ permissions and WRITE attributes, and access to the scanned folders



DLP Capture

Key features

Capabilities of DLP Capture:

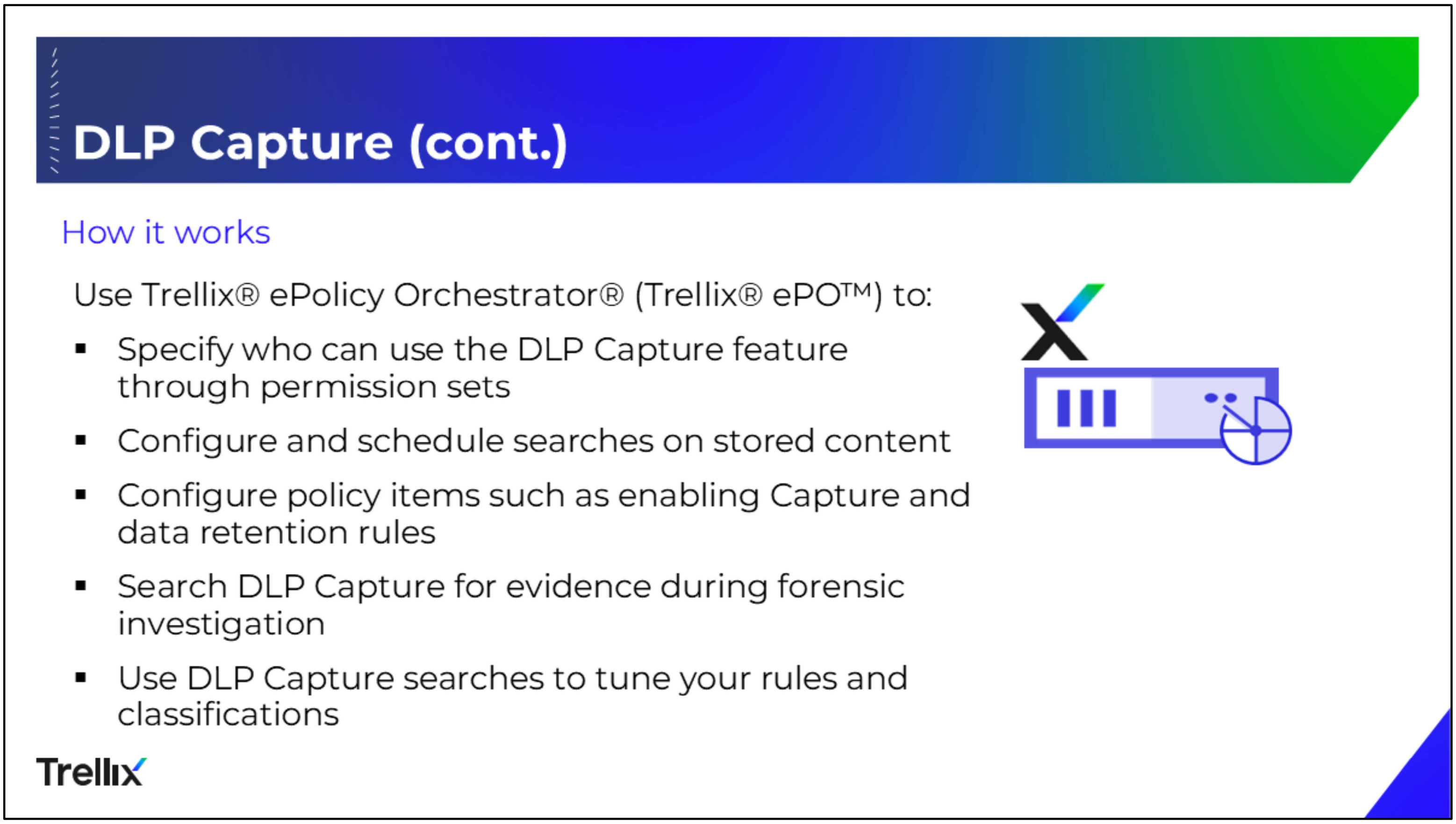
- Runs on DLP Prevent and DLP Monitor appliances
- Perform searches on captured data for forensic analysis or rule tuning
- Records email, web and network traffic processed by DLP appliances
- Can be enabled from Trellix ePolicy Orchestrator as an optional DLP feature
- Can be installed on physical or virtual DLP appliances
- Used to search recorded traffic for:
  - Forensic investigation
  - Rules or Classification tuning

Trellix

Trellix DLP capture, when enabled, allows you to store email, web, and network data analyzed by your Trellix DLP Prevent or Trellix DLP Monitor appliances. The captured data can be searched later to identify a data loss event that was missed during real-time data analysis, or used to tune rules and classification settings to reduce false positives without affecting the analysis of live data. You can create datasets that focus the search on specified properties to reduce the amount of data that will be searched on each appliance, so you get fewer and more targeted results. You can create a Trellix DLP incident from a search result, then add the incident to a new or existing case. Any evidence associated with the search result can also be added to the incident.

Capabilities of DLP Capture:

- Runs on DLP Prevent and DLP Monitor appliances
- Perform searches on captured data for forensic analysis or rule tuning
- Records email, web and network traffic processed by DLP appliances
- Can be enabled from Trellix ePolicy Orchestrator as an optional DLP feature
- Can be installed on physical or virtual DLP appliances
- Used to search recorded traffic for:
  - Forensic investigation
  - Rules or Classification tuning
- Perform searches on captured data for forensic analysis or rule tuning
- Create data sets to help focus your searches.
- Create and run searches or tune rules and classifications
- Review captured data for evidence and case tracking
- Create incidents and add evidence to cases created in ePO



DLP Capture (cont.)

How it works

Use Trellix® ePolicy Orchestrator® (Trellix® ePO™) to:

- Specify who can use the DLP Capture feature through permission sets
- Configure and schedule searches on stored content
- Configure policy items such as enabling Capture and data retention rules
- Search DLP Capture for evidence during forensic investigation
- Use DLP Capture searches to tune your rules and classifications

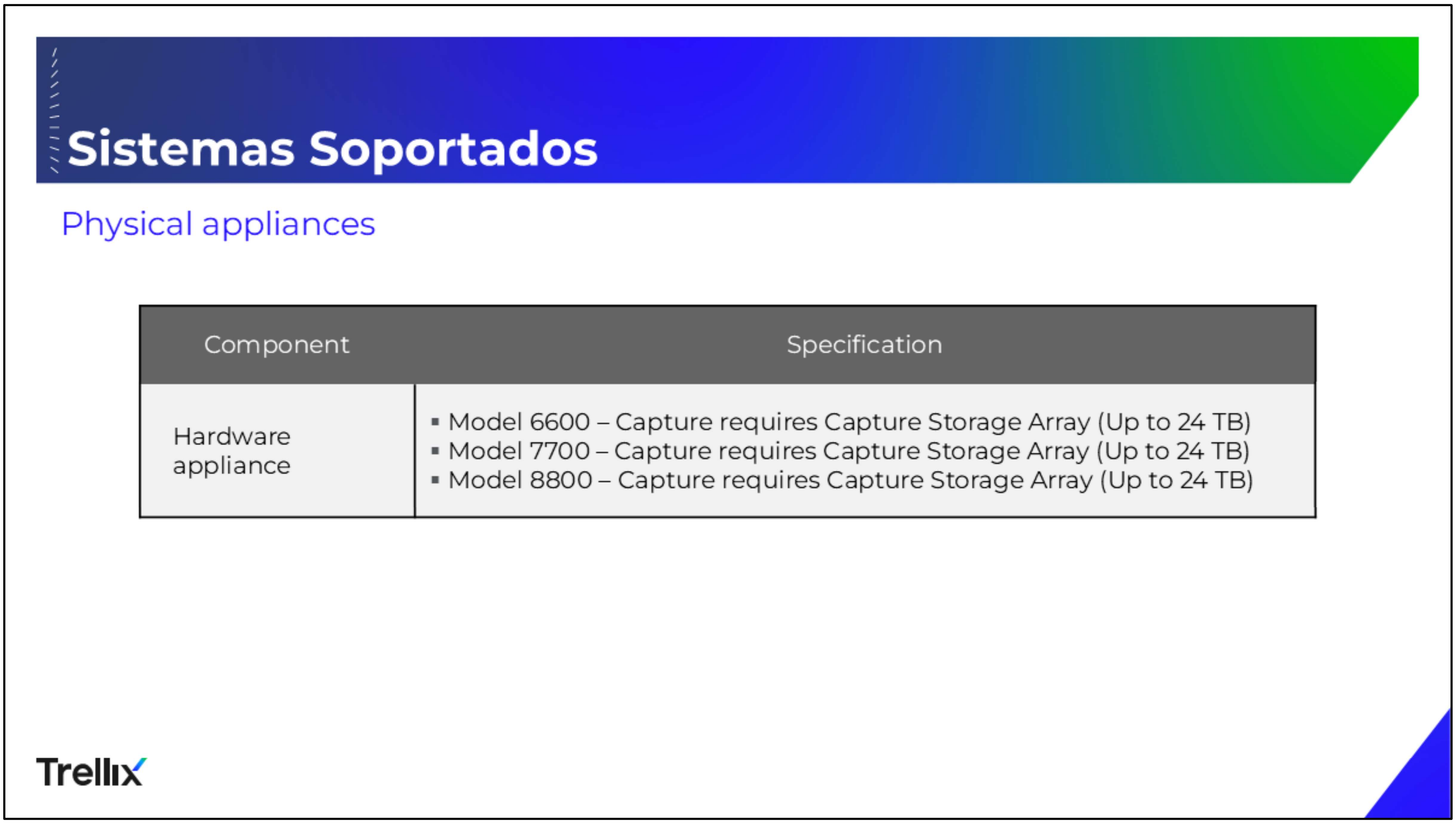
Trellix

DLP Capture allows the storage of all traffic from your DLP Prevent and DLP Monitor appliances, even if the traffic didn’t create an incident. Trellix ePO provides a consolidated location to configure settings and perform tasks on your captured DLP content.

Trellix ePO applies the Capture policy to DLP appliances. Once applied the appliances will begin capturing content for analysis and searches.

Use Trellix® ePolicy Orchestrator® (Trellix® ePO™) to:

- Specify who can use the DLP Capture feature through permission sets
- Configure and schedule searches on stored content
- Configure policy items such as enabling Capture and data retention rules
- Search DLP Capture for evidence during forensic investigation
- Use DLP Capture searches to tune your rules and classifications



Sistemas Soportados

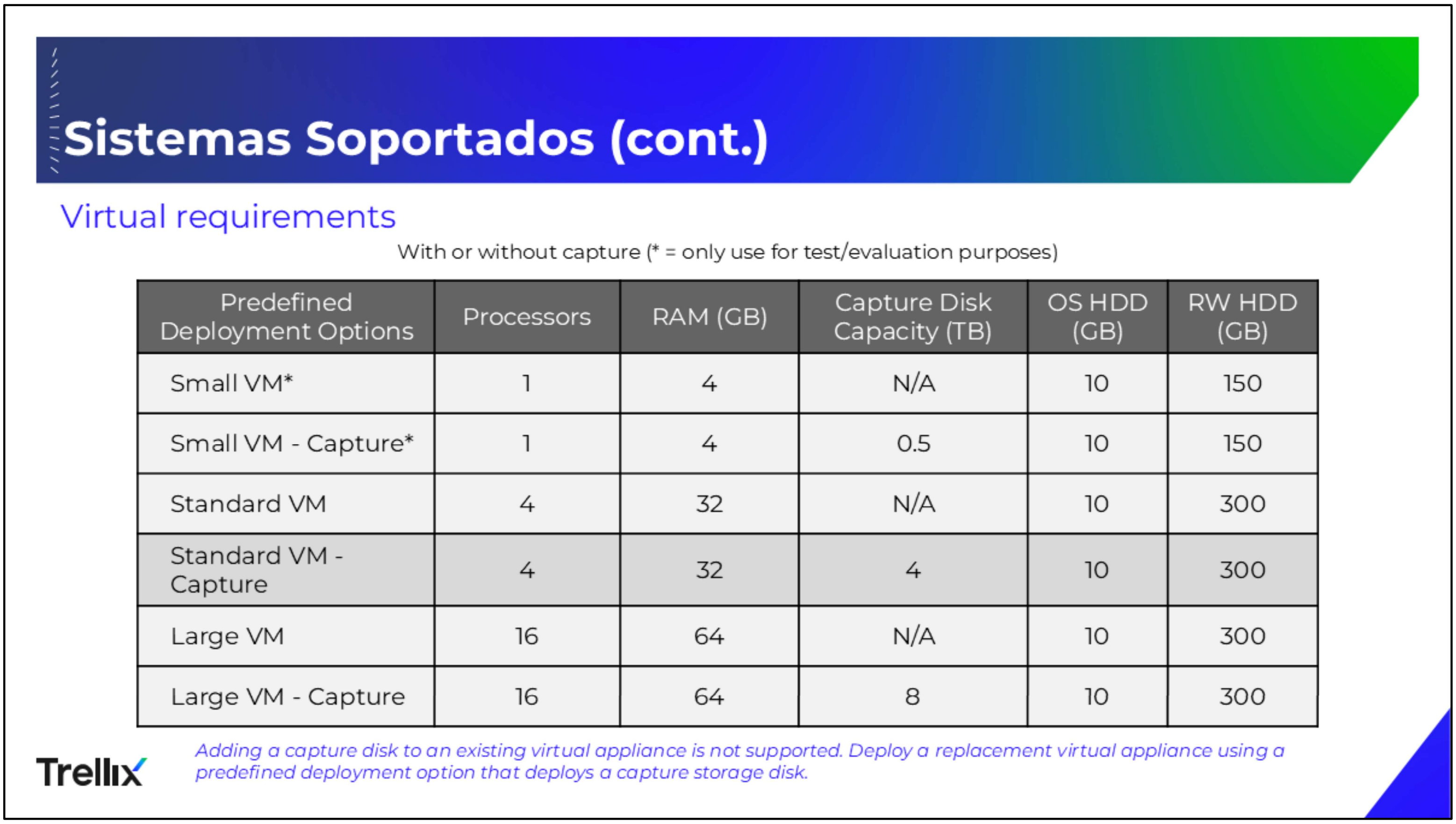
Physical appliances

Component	Specification
Hardware appliance	▪ Model 6600 – Capture requires Capture Storage Array (Up to 24 TB) ▪ Model 7700 – Capture requires Capture Storage Array (Up to 24 TB) ▪ Model 8800 – Capture requires Capture Storage Array (Up to 24 TB)

This slide shows supported systems for your DLP Prevent and Monitor appliances in order to enable DLP Capture functionality.

- 6600/7700/8800
  - Capture requires Capture Storage Array (Up to 24 TB)

  - **Note:** Each Trellix DLP 8800, Trellix DLP 7700, or Trellix DLP 6600 appliance on which you want to enable DLP Capture must have a dedicated Trellix DLP Capture Storage Array connected to it to store the captured data.



Sistemas Soportados (cont.)

Virtual requirements

With or without capture (* = only use for test/evaluation purposes)

Predefined Deployment Options	Processors	RAM (GB)	Capture Disk Capacity (TB)	OS HDD (GB)	RW HDD (GB)
Small VM*	1	4	N/A	10	150
Small VM - Capture*	1	4	0.5	10	150
Standard VM	4	32	N/A	10	300
Standard VM - Capture	4	32	4	10	300
Large VM	16	64	N/A	10	300
Large VM - Capture	16	64	8	10	300

Adding a capture disk to an existing virtual appliance is not supported. Deploy a replacement virtual appliance using a predefined deployment option that deploys a capture storage disk.

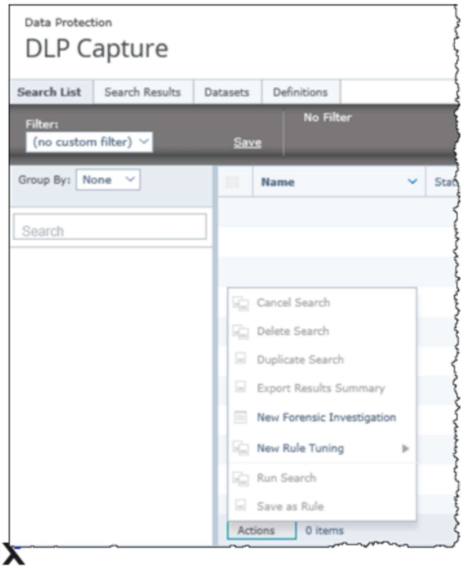
Trellix

This slide shows supported systems for your DLP Prevent and Monitor appliances in order to enable DLP Capture functionality.
Note: Use the Small VM and Small VM - Capture options only for evaluation purposes.

- Virtual
  - Pre-defined VM Sizes
  - VMware vSphere support
    - OVA supplied
    - updated to include 6.5 and 6.7
  - Hyper-V
    - Separate zip supplied
    - Windows Server 2012
    - Windows Server 2016
    - DLP Prevent only

Interfaz DLP Capture

Interface



- **Search List**: Displays information about each configured search and status of current searches
- **Search Results**: Stores results from each appliance in a dataset.
- **Datasets**: Saved entries that focus the search on specified properties to reduce the amount of data that will be searched on each appliance
- **Definitions**: A repository of definitions that can be used during searches

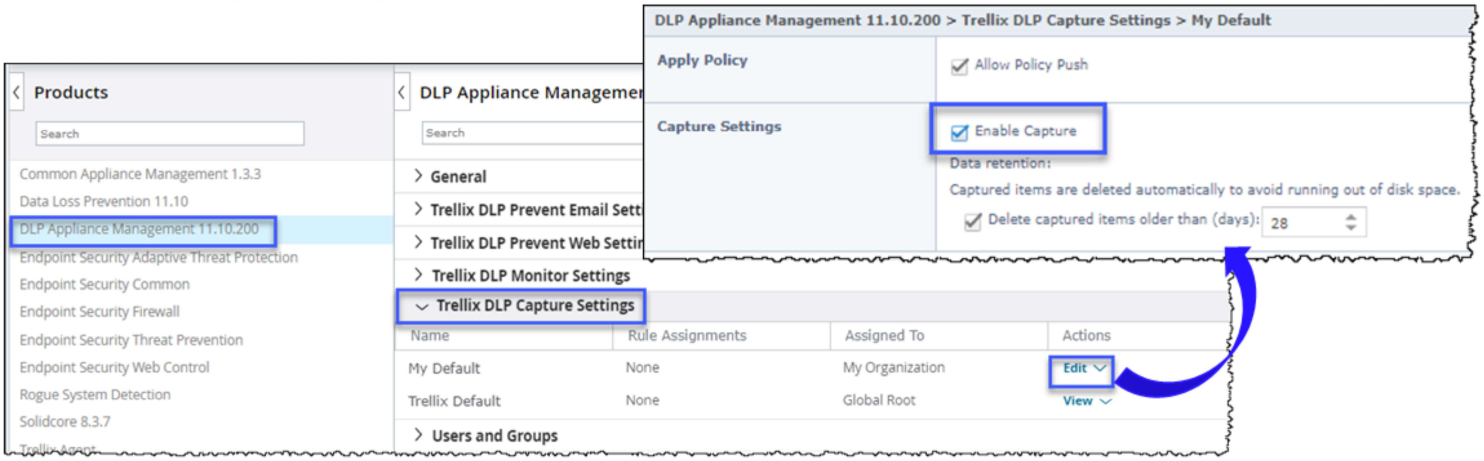
Trellix

DLP Capture interface includes the following options:

- **Search List:** Displays information about each configured search and status of current searches
- **Search Results:** Stores results of searches from each appliance.
- **Datasets:** A repository of your saved datasets. You can add more datasets here for use in your searches
- **Definitions:** A repository of definitions to use during searches.

Habilitar DLP Capture

Menu >Policy Catalog > DLP Appliance Management 11.x > DLP Capture Settings



DLP Appliance Management 11.10.200 > Trellix DLP Capture Settings > My Default

Apply Policy: ☑ Allow Policy Push

Capture Settings: ☑ Enable Capture

Data retention:

Captured items are deleted automatically to avoid running out of disk space.

☑ Delete captured items older than (days): 28

Products

Search

- Common Appliance Management 1.3.3
- Data Loss Prevention 11.10
- DLP Appliance Management 11.10.200
- Endpoint Security Adaptive Threat Protection
- Endpoint Security Common
- Endpoint Security Firewall
- Endpoint Security Threat Prevention
- Endpoint Security Web Control
- Rogue System Detection
- Solidcore 8.3.7
- Trellix Agent

DLP Appliance Managemen

Search

- General
- Trellix DLP Prevent Email Sett
- Trellix DLP Prevent Web Settir
- Trellix DLP Monitor Settings
- Trellix DLP Capture Settings

Name	Rule Assignments	Assigned To	Actions
My Default	None	My Organization	Edit
Trellix Default	None	Global Root	View

- Users and Groups

For the DLP Capture feature to appear in the ePO menu, you must add a license for DLP Monitor or DLP Prevent

Trellix

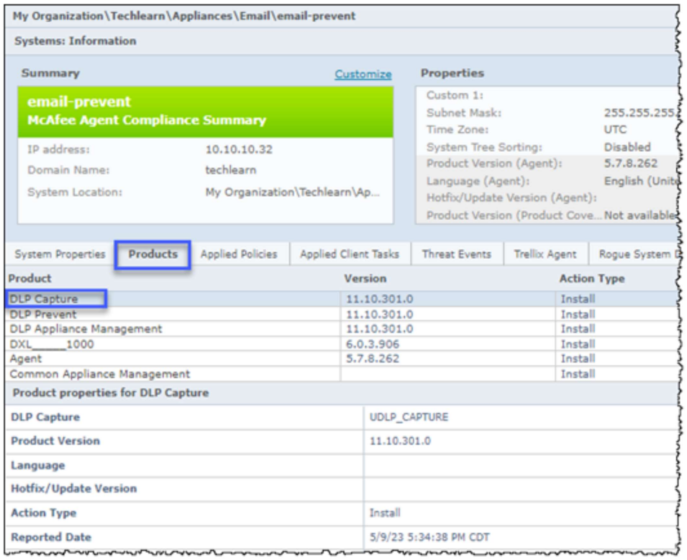
For the DLP Capture feature to appear in the ePO menu, you must add a license for DLP Monitor or DLP Prevent

To enable the DLP Capture feature:

1. In Trellix ePO, select **Menu** > **Policy Catalog** > **DLP Appliance Management > Trellix DLP Capture Settings**.
2. In the Trellix DLP Capture Settings policy under **Capture Settings** select **“Enable Capture”** to enable DLP Capture functionality. From this policy you can also set the length of time captured items are saved for review.

Verificar que DLP Capture está habilitado

Products installed



My Organization\Techlearn\Appliances\Email\email-prevent

Systems: Information

Summary

email-prevent
McAfee Agent Compliance Summary

IP address:	10.10.10.32
Domain Name:	techlearn
System Location:	My Organization\Techlearn\Ap...

Properties

Custom 1:	
Subnet Mask:	255.255.255.
Time Zone:	UTC
System Tree Sorting:	Disabled
Product Version (Agent):	5.7.8.262
Language (Agent):	English (Unit
Hotfix/Update Version (Agent):	
Product Version (Product Cove...	Not available

Product	Version	Action Type
DLP Capture	11.10.301.0	Install
DLP Prevent	11.10.301.0	Install
DLP Appliance Management	11.10.301.0	Install
DXL_____1000	6.0.3.906	Install
Agent	5.7.8.262	Install
Common Appliance Management		Install

Product properties for DLP Capture

DLP Capture	UDLP_CAPTURE
Product Version	11.10.301.0
Language	
Hotfix/Update Version	
Action Type	Install
Reported Date	5/9/23 5:34:38 PM CDT

1. From the ePO menu select System Tree
2. In the System Tree, select a DLP Appliance with capture enabled
3. On the Systems page select the Products tab
4. Select DLP Capture 11.x
5. Below the General Heading review Capture Feature Status
   - Feature is Enabled
   - Feature is Disabled
   - Feature is not supported on this platform

To ensure the Trellix DLP Capture feature is successful enabled using Trellix ePO:

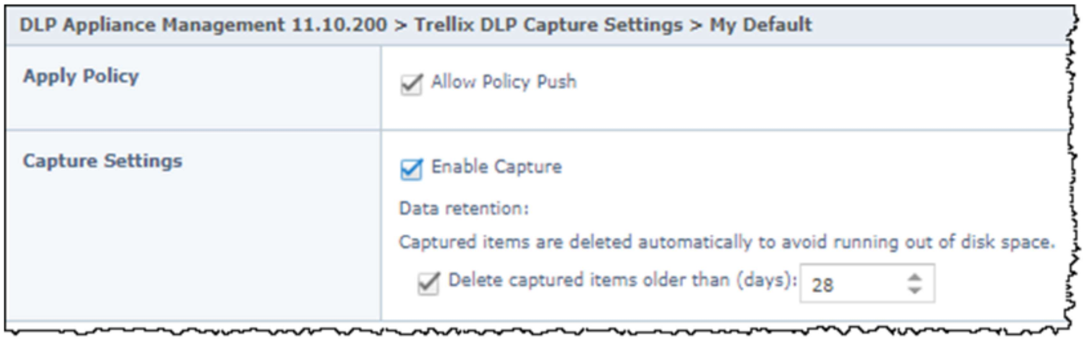
- From the ePO menu select System Tree.
- In the System Tree, select a DLP Appliance with capture enabled.
- On the Systems page, select the Products tab.
- Select DLP Capture 11.x.
- Below the General Heading review Capture Feature Status
  - 1 - Feature is Enabled
  - 2 - Feature is Disabled
  - 3 - Feature is not support on this particular platform, 3 is normally shown when the Trellix DLP Capture Storage Array needs to be attached and the appliance re-imaged.

NOTE: Users may encounter a Capture Feature Status of 3 on a Virtual Machine if an upgrade is attempted. The DLP Capture feature is not support if the VM was upgraded from older versions of DLP Monitor or DLP Prevent due to the need to provision the DLP Capture storage location on the appliance.

Retención de Datos y Almacenamiento

Policy

- Setting found at DLP Appliance Management 11.x > Trellix DLP Capture Settings
- Retained items are deleted automatically based on disk space
- Items can also be deleted based on age



DLP Appliance Management 11.10.200 > Trellix DLP Capture Settings > My Default

Apply Policy	☑ Allow Policy Push
Capture Settings	☑ Enable Capture Data retention: Captured items are deleted automatically to avoid running out of disk space. ☑ Delete captured items older than (days): 28

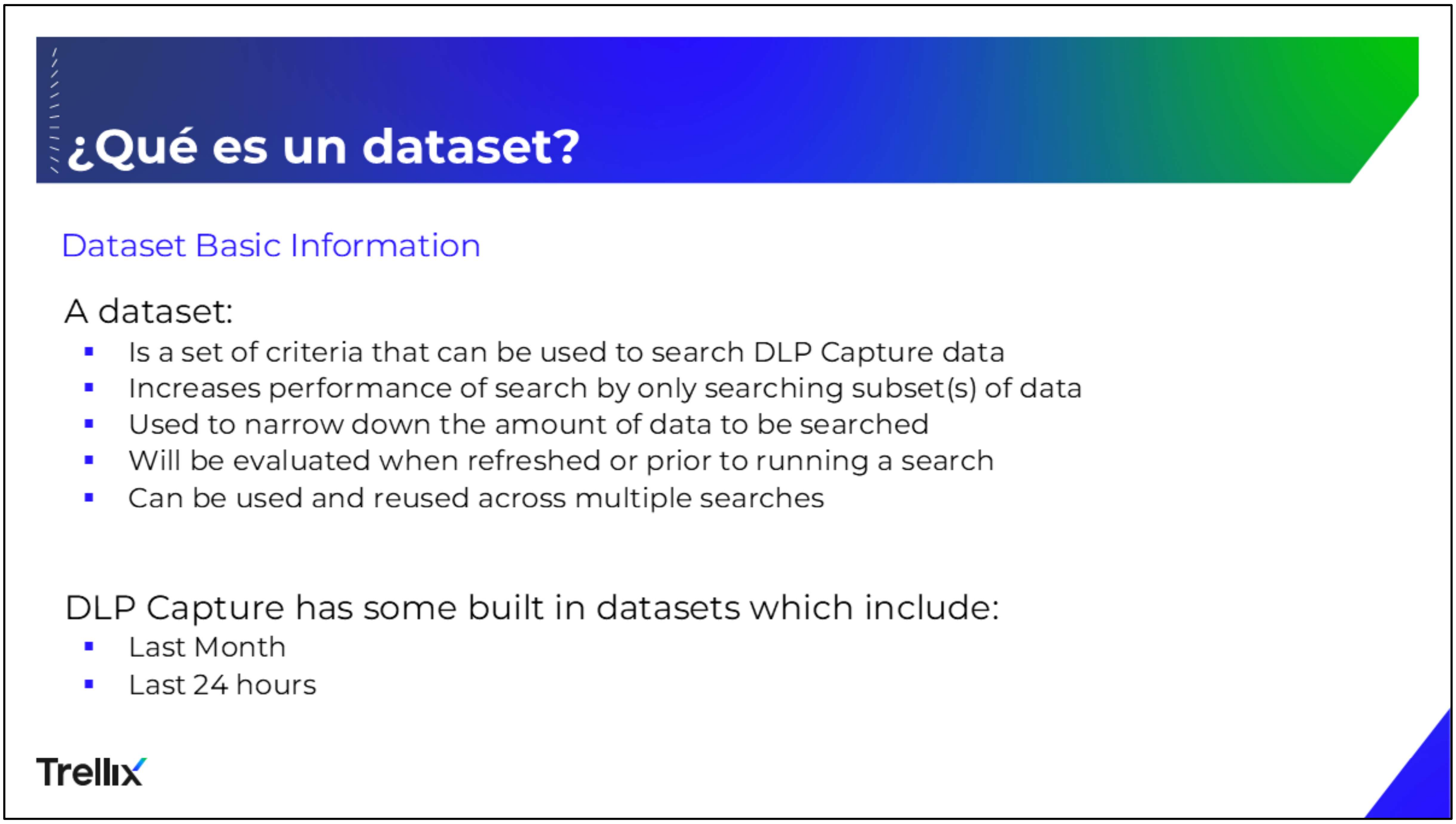
By default, captured data is removed automatically from storage after 28 days to avoid filling up the disk space however that limit may be modified. If the captured data storage nears capacity before the specified limit is reached, some older captured items are automatically removed to provide enough space for new captured data When the DLP Capture feature starts a search task, it collates the items that will be analyzed in the search. If a DLP Capture search encounters data in the storage location which should be deleted per the data retention policy, those items are skipped and the search will continue as configured. The older data will not be displayed in the search.

Captured data is stored in two parts

- Metadata about the request is stored in the ePO database
- The data requested is stored in .tar files on disk

The stored database information includes:

- .tar file name
- Offset in tar file
- Scanning service JSON size
- Captured data size



¿Qué es un dataset?

Dataset Basic Information

A dataset:

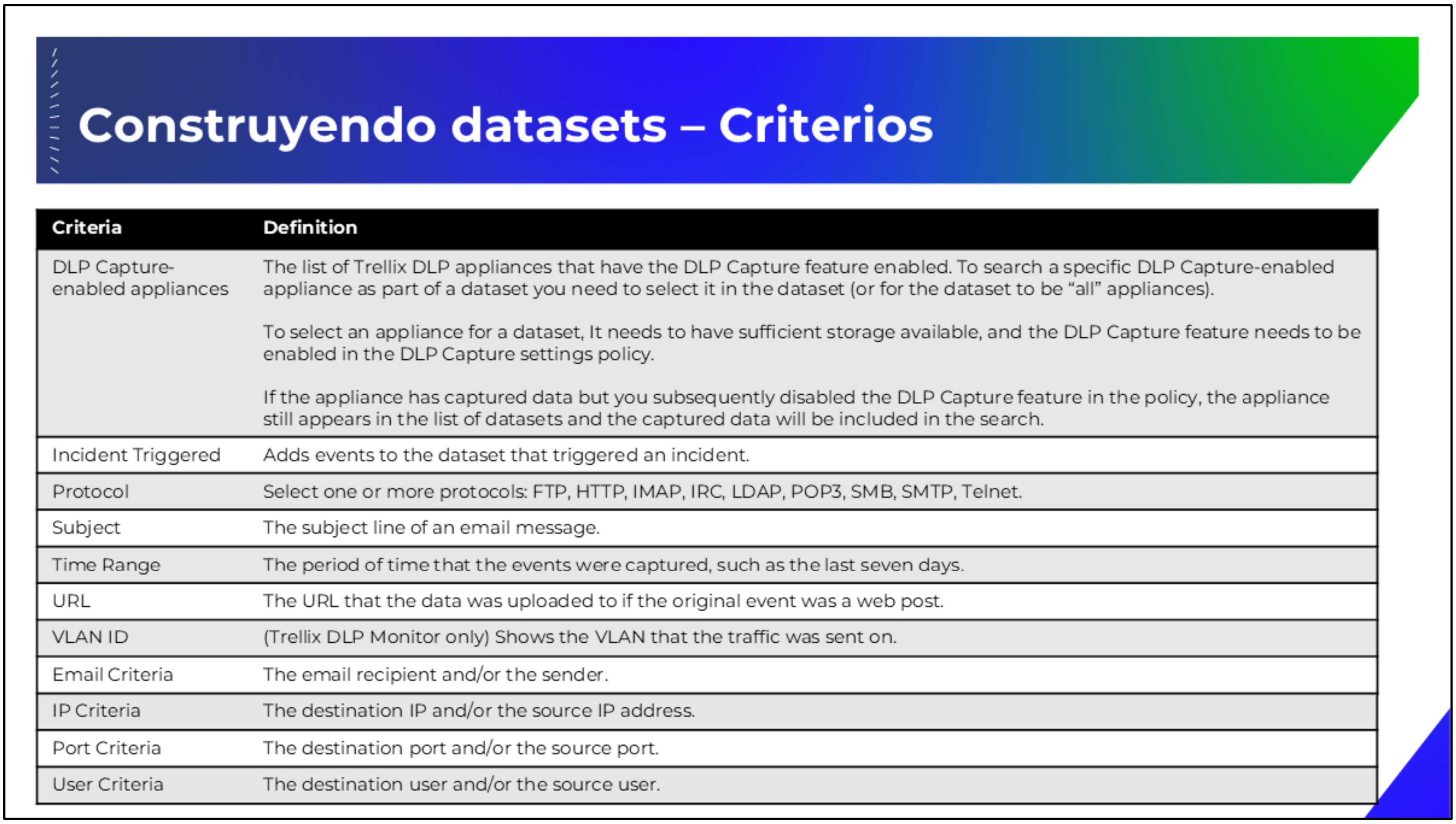
- Is a set of criteria that can be used to search DLP Capture data
- Increases performance of search by only searching subset(s) of data
- Used to narrow down the amount of data to be searched
- Will be evaluated when refreshed or prior to running a search
- Can be used and reused across multiple searches

DLP Capture has some built in datasets which include:

- Last Month
- Last 24 hours

Trellix

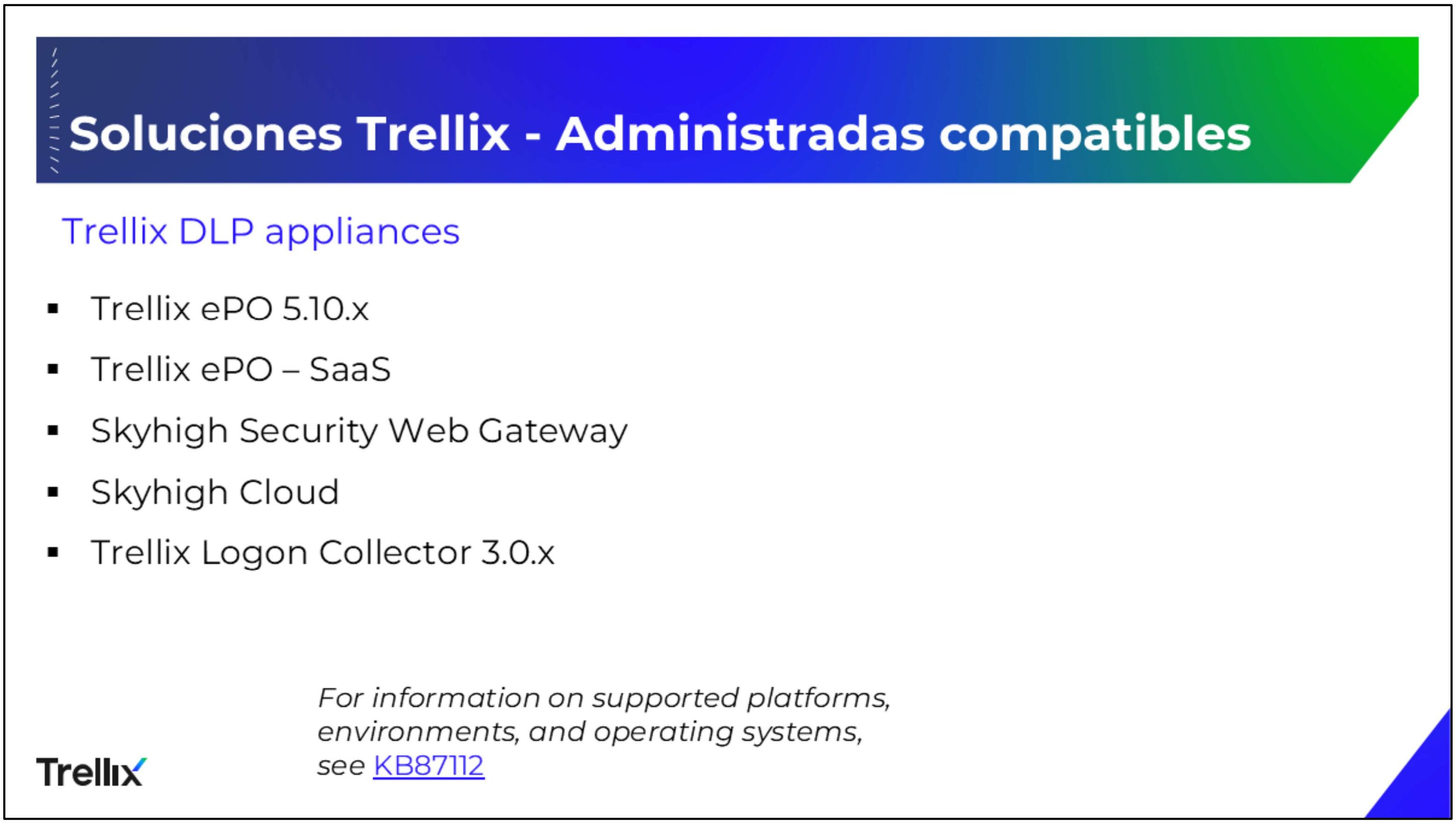
Datasets focus your rule tuning and forensic investigation searches on a subset of captured data to reduce the amount of data searched. When you search a data set, the time it takes to run the search is reduced, and the results are more useful and easier to analyze. There are some pre-defined datasets, or you can create your own based on properties such as the appliance, email criteria, or user criteria. If an appliance can support the DLP Capture feature (that is, it has disks available for storing captured data and it contains some captured data), it can be added to a dataset and the captured data searched.



Construyendo datasets – Criterios

Criteria	Definition
DLP Capture-enabled appliances	The list of Trellix DLP appliances that have the DLP Capture feature enabled. To search a specific DLP Capture-enabled appliance as part of a dataset you need to select it in the dataset (or for the dataset to be “all” appliances). To select an appliance for a dataset, It needs to have sufficient storage available, and the DLP Capture feature needs to be enabled in the DLP Capture settings policy. If the appliance has captured data but you subsequently disabled the DLP Capture feature in the policy, the appliance still appears in the list of datasets and the captured data will be included in the search.
Incident Triggered	Adds events to the dataset that triggered an incident.
Protocol	Select one or more protocols: FTP, HTTP, IMAP, IRC, LDAP, POP3, SMB, SMTP, Telnet.
Subject	The subject line of an email message.
Time Range	The period of time that the events were captured, such as the last seven days.
URL	The URL that the data was uploaded to if the original event was a web post.
VLAN ID	(Trellix DLP Monitor only) Shows the VLAN that the traffic was sent on.
Email Criteria	The email recipient and/or the sender.
IP Criteria	The destination IP and/or the source IP address.
Port Criteria	The destination port and/or the source port.
User Criteria	The destination user and/or the source user.

Use the following criteria when creating datasets



Soluciones Trellix - Administradas compatibles

Trellix DLP appliances

- Trellix ePO 5.10.x
- Trellix ePO – SaaS
- Skyhigh Security Web Gateway
- Skyhigh Cloud
- Trellix Logon Collector 3.0.x

For information on supported platforms, environments, and operating systems, see [KB87112]

Trellix

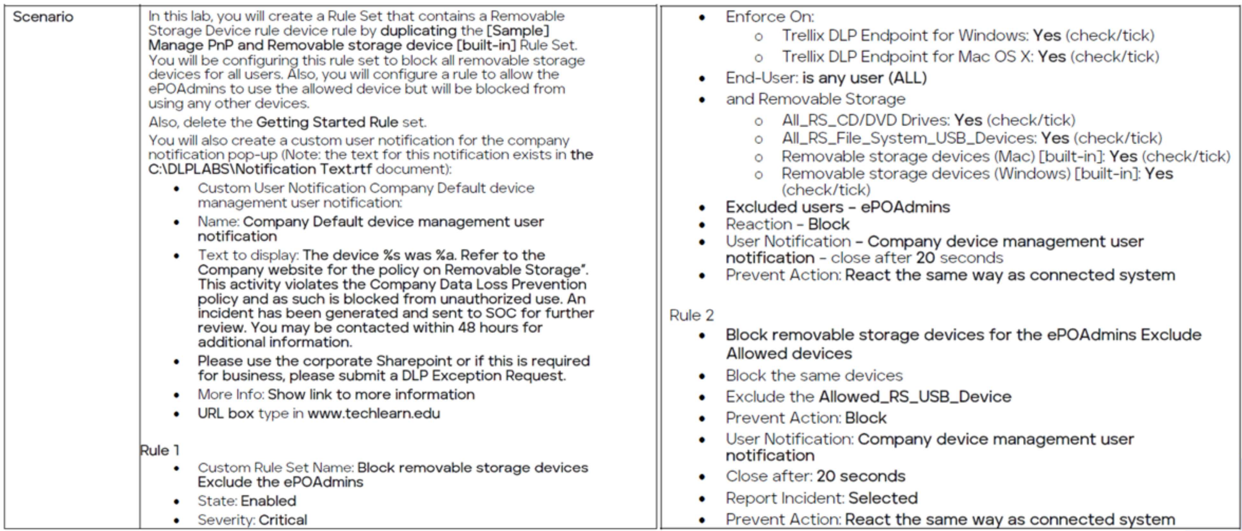
The Trellix DLP appliances have been tested for compatibility with the Trellix-managed solutions listed on the slide. For more information, see the product documentation.

Trellix

Casos de Uso de Etiquetado y Protección con DLP

Ejemplos prácticos de uso común

Monitoreo y Bloqueo con Device Control



Scenario

In this lab, you will create a Rule Set that contains a Removable Storage Device rule device rule by **duplicating** the **[Sample] Manage PnP and Removable storage device [built-in]** Rule Set. You will be configuring this rule set to block all removable storage devices for all users. Also, you will configure a rule to allow the ePOAdmins to use the allowed device but will be blocked from using any other devices.

Also, delete the **Getting Started Rule** set.

You will also create a custom user notification for the company notification pop-up (Note: the text for this notification exists in **the C:\DLPLABS\Notification Text.rtf** document):

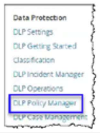
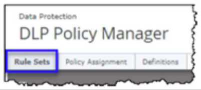
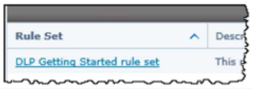
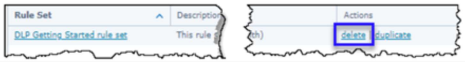
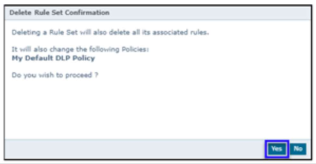
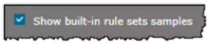
- Custom User Notification Company Default device management user notification:
- Name: **Company Default device management user notification**
- Text to display: **The device %s was %a. Refer to the Company website for the policy on Removable Storage". This activity violates the Company Data Loss Prevention policy and as such is blocked from unauthorized use. An incident has been generated and sent to SOC for further review. You may be contacted within 48 hours for additional information.**
- **Please use the corporate Sharepoint or if this is required for business, please submit a DLP Exception Request.**
- More Info: **Show link to more information**
- **URL box** type in **www.techlearn.edu**

Rule 1

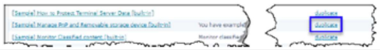
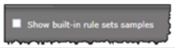
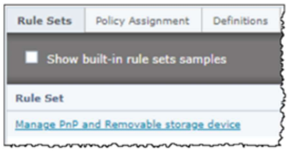
- Custom Rule Set Name: **Block removable storage devices Exclude the ePOAdmins**
- State: **Enabled**
- Severity: **Critical**
- Enforce On:
  - Trellix DLP Endpoint for Windows: **Yes** (check/tick)
  - Trellix DLP Endpoint for Mac OS X: **Yes** (check/tick)
- End-User: **is any user (ALL)**
- and Removable Storage
  - All_RS_CD/DVD Drives: **Yes** (check/tick)
  - All_RS_File_System_USB_Devices: **Yes** (check/tick)
  - Removable storage devices (Mac) [built-in]: **Yes** (check/tick)
  - Removable storage devices (Windows) [built-in]: **Yes** (check/tick)
- **Excluded users - ePOAdmins**
- Reaction - **Block**
- User Notification **- Company device management user notification** - close after **20** seconds
- Prevent Action: **React the same way as connected system**

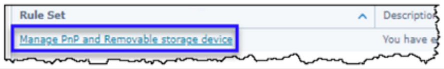
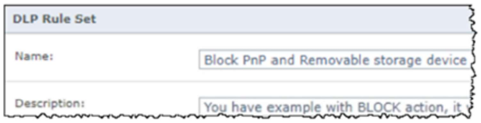
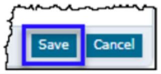
Rule 2

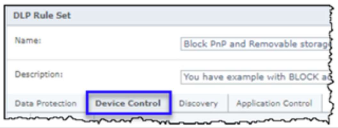
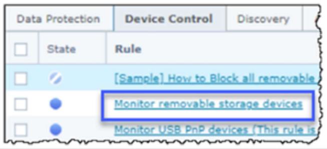
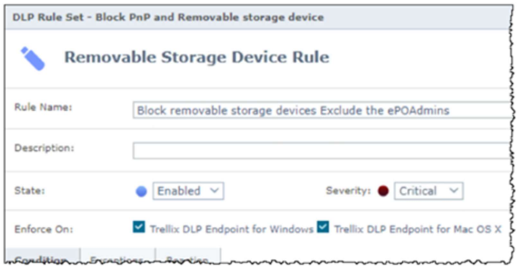
- **Block removable storage devices for the ePOAdmins Exclude Allowed devices**
- Block the same devices
- Exclude the **Allowed_RS_USB_Device**
- Prevent Action: **Block**
- User Notification: **Company device management user notification**
- Close after: **20 seconds**
- Report Incident: **Selected**
- Prevent Action: **React the same way as connected system**

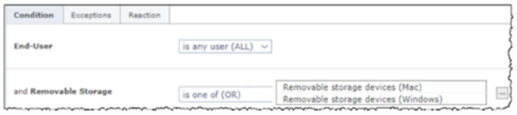
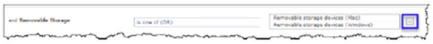
Task:	Step:	Instructions:
2	1	Make sure you are in the **DLP Policy Manager**. (Select **Data Protection > DLP Policy Manager**).  Data Protection DLP Settings DLP Getting Started Classification DLP Incident Manager DLP Operations DLP Policy Manager DLP Case Management
2	2	Click the **Rule Sets** tab.  Data Protection DLP Policy Manager Rule Sets Policy Assignment Definitions
2	3	Locate the **DLP Getting Started** rule set. 
2	4	Click **Delete**.  Rule Set Description DLP Getting Started rule set This rule Actions th) delete duplicate
2	5	Click **Yes**.  Delete Rule Set Confirmation Deleting a Rule Set will also delete all its associated rules. It will also change the following Policies: **My Default DLP Policy** Do you wish to proceed ?
2	6	Select (check/tick) **Show built-in rule sets samples**.  ☑ Show built-in rule sets samples

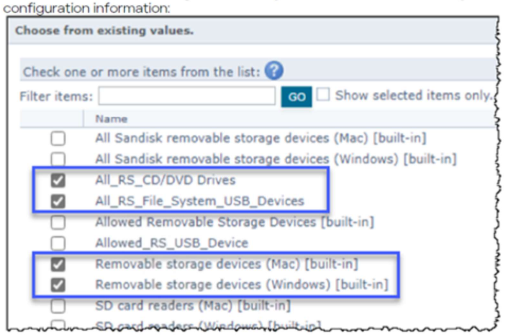
Trellix

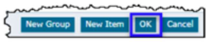
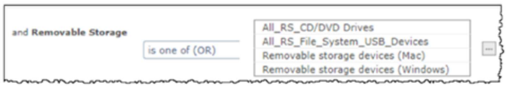
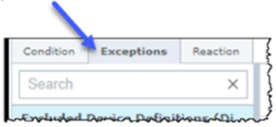
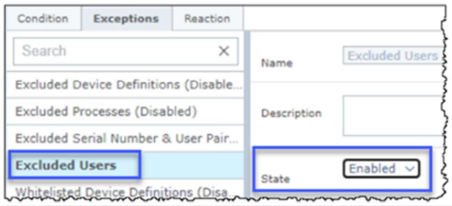
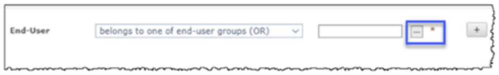
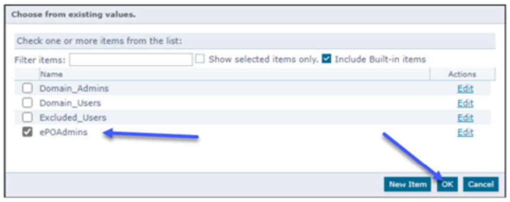
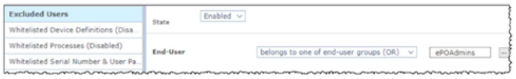
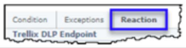
Task:	Step:	Instructions:
2	7	At the Rule Set section, locate **[Sample] Manage PnP and Removable storage device [built-in]**. Click the **duplicate** link.  [Sample] How to Protect Terminal Server Data [built-in] — duplicate [Sample] Manage PnP and Removable storage device [built-in] — You have example — duplicate [Sample] Monitor Classified content [built-in] — Monitor classified — duplicate
2	8	De-select (uncheck/tick) **Show built-in rule sets samples**.  □ Show built-in rule sets samples
2	9	Verify the duplicated **Manage PnP and Removable storage device** is added as a **Rule Set**.  □ Show built-in rule sets samples Rule Set Manage PnP and Removable storage device
		End of Task

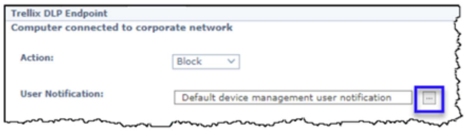
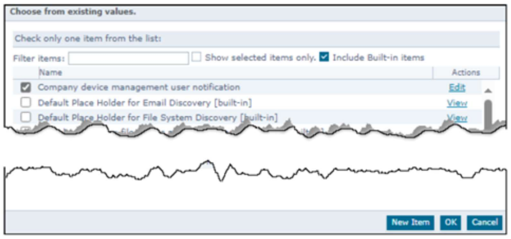
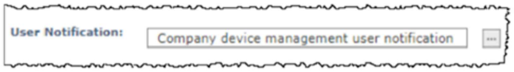
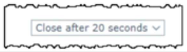
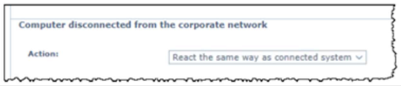
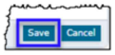
2	Create a Device Rule to block USB devices	
2	1	At the **Rule Set** section, Click the **Manage PnP and Removable storage device** link.  Rule Set — Description Manage PnP and Removable storage device — You have e
2	2	Change the name to **Block PnP and Removable storage device**  DLP Rule Set Name: Block PnP and Removable storage device Description: You have example with BLOCK action, it
2	3	In the lower right-hand corner click the **Save** button. 

2	4	Click the **Device Control** tab.  DLP Rule Set Name: Block PnP and Removable storag Description: You have example with BLOCK a Data Protection Device Control Discovery Application Control
2	5	Click the **Monitor removable storage devices** link.  □ State Rule □ [Sample] How to Block all removable □ ● Monitor removable storage devices □ ● Monitor USB PnP devices (This rule is
2	6	At the **Removable Storage Device Rule** page, enter the following configuration information:  DLP Rule Set - Block PnP and Removable storage device Removable Storage Device Rule Rule Name: Block removable storage devices Exclude the ePOAdmins Description: State: ● Enabled Severity: ● Critical Enforce On: ☑ Trellix DLP Endpoint for Windows ☑ Trellix DLP Endpoint for Mac OS X • Rule Name: **Block removable storage devices exclude the ePOAdmins** • State: **Enabled** • Severity: **Critical** • Enforce On: • Trellix DLP Endpoint for Windows: **Yes** (check/tick) • Trellix DLP Endpoint for Mac OS X: **Yes** (check/tick)

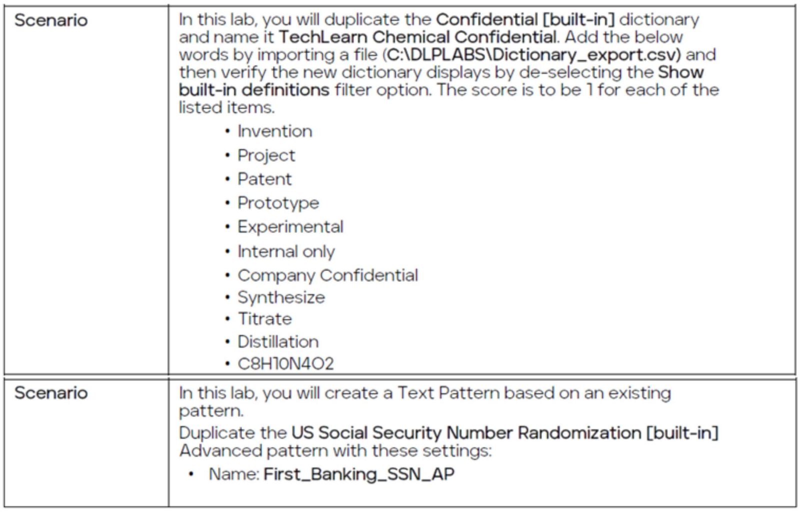
2	7	Click the **Condition** tab. Select the following configuration information:  Condition Exceptions Reaction End-User is any user (ALL) and Removable Storage is one of (OR) Removable storage devices (Mac) Removable storage devices (Windows) - **End-User**: is any user (ALL) - and **Removable Storage**: is one of (OR) - Removable storage devices (Mac) - Removable storage devices (Windows)
2	8	Click the **ellipsis** (...) button.  and Removable Storage is one of (OR) Removable storage devices (Mac) Removable storage devices (Windows)

2	9	At the **Choose from existing values** dialog window, select the following configuration information:  Choose from existing values. Check one or more items from the list: Filter items: GO ☐ Show selected items only. Name ☐ All Sandisk removable storage devices (Mac) [built-in] ☐ All Sandisk removable storage devices (Windows) [built-in] ☑ All_RS_CD/DVD Drives ☑ All_RS_File_System_USB_Devices ☐ Allowed Removable Storage Devices [built-in] ☐ Allowed_RS_USB_Device ☑ Removable storage devices (Mac) [built-in] ☑ Removable storage devices (Windows) [built-in] ☐ SD card readers (Mac) [built-in] ☐ SD card readers (Windows) [built-in] - All_RS_CD/DVD Drives: **Yes** (check/tick) - All_RS_File_System_USB_Devices: **Yes** (check/tick) - Removable storage devices (Mac) [built-in]: **Yes** (check/tick) - Removable storage devices (Windows) [built-in]: **Yes** (check/tick)

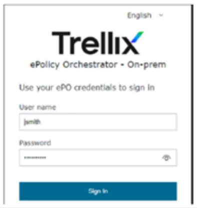
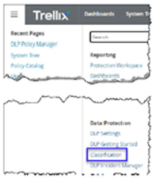
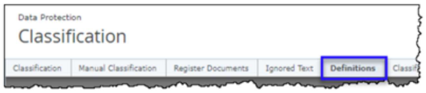
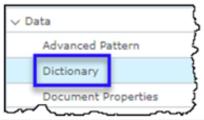
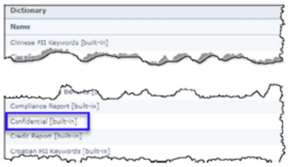
2	10	Click **OK**. 
2	11	Verify the **and Removable Storage** values.  and Removable Storage is one of (OR) All_RS_CD/DVD Drives All_RS_File_System_USB_Devices Removable storage devices (Mac) Removable storage devices (Windows)
2	12	Click on the **Exceptions** tab.  Condition Exceptions Reaction Search Excluded Device Definitions (Di...
2	13	Click to highlight and select the **Excluded Users** listing and click the drop down next to the **State** and select the option of **Enabled**.  Condition Exceptions Reaction Search Excluded Device Definitions (Disable... Excluded Processes (Disabled) Excluded Serial Number & User Pair... Excluded Users Whitelisted Device Definitions (Disa... Name Excluded Users Description State Enabled
2	14	On the line that lists **End-User** make sure the option of **belongs to one of the end-user groups (OR)** and click on the **ellipsis** (...) button  End-User belongs to one of end-user groups (OR)
2	15	Select the **ePOAdmins** group that you created and click **OK**.  Choose from existing values. Check one or more items from the list: Filter items: □ Show selected items only. ☑ Include Built-in items Name / Actions □ Domain_Admins Edit □ Domain_Users Edit □ Excluded_Users Edit ☑ ePOAdmins Edit
2	16	Make sure that the **Excluded Users** has the **ePOAdmins** selected.  Excluded Users Whitelisted Device Definitions (Disa... Whitelisted Processes (Disabled) Whitelisted Serial Number & User Pa... State Enabled End-User belongs to one of end-user groups (OR) ePOAdmins
2	17	Click the **Reaction** tab. 

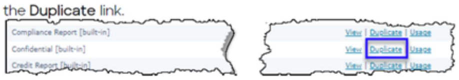
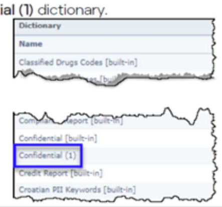
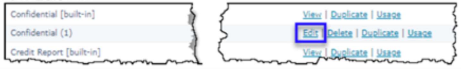
2	18	At the **Computer connect to corporate network** section, select the following configuration information:  Trellix DLP Endpoint Computer connected to corporate network Action: Block User Notification: Default device management user notification - Action: **Block** - User Notification: click the **ellipsis** (...) button.
2	19	At the **Choose from existing values** dialog window, click to select **the Company device management user notification** and click **OK**.  Choose from existing values. Check only one item from the list: Filter items: □ Show selected items only. ☑ Include Built-in items ☑ Company device management user notification — Edit □ Default Place Holder for Email Discovery [built-in] — View □ Default Place Holder for File System Discovery [built-in] — View
2	20	Verify **User Notification** is updated to reflect **Company device management user notification**.  User Notification: Company device management user notification
2	21	At the **User Notification** drop-down, select **Close after 20 seconds**.  Close after 20 seconds
2	22	Locate the **Computer disconnected from the corporate network** section. At **Action**, select, **React the same way as connected system**.  Computer disconnected from the corporate network Action: React the same way as connected system
2	23	Click **Save**. 

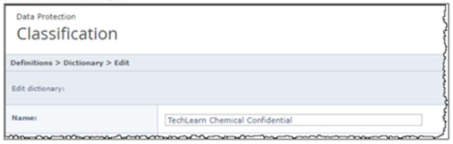
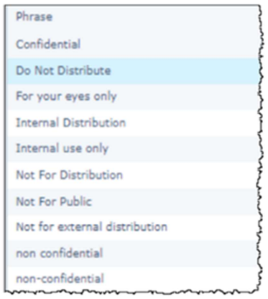
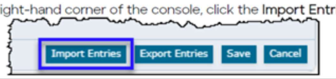
Creación de Diccionarios y Patrones Avanzados



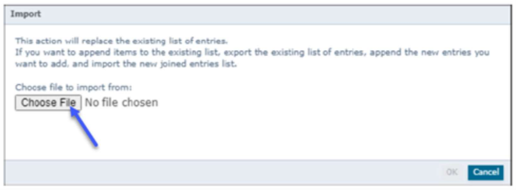
Scenario	In this lab, you will duplicate the **Confidential [built-in]** dictionary and name it **TechLearn Chemical Confidential**. Add the below words by importing a file (**C:\DLPLABS\Dictionary_export.csv**) and then verify the new dictionary displays by de-selecting the **Show built-in definitions** filter option. The score is to be 1 for each of the listed items. • Invention • Project • Patent • Prototype • Experimental • Internal only • Company Confidential • Synthesize • Titrate • Distillation • C8H10N4O2
Scenario	In this lab, you will create a Text Pattern based on an existing pattern. Duplicate the **US Social Security Number Randomization [built-in]** Advanced pattern with these settings: • Name: **First_Banking_SSN_AP**

Task:	Step:	Instructions:
1		**Create Dictionary**
1	1	Verify you are logged into the ePO console as the administrator (**jsmith/Secure123!**).  English Trellix ePolicy Orchestrator - On-prem Use your ePO credentials to sign in User name jsmith Password •••••••••• Sign In
1	2	Click the **ePO** menu. Select **Data Protection > Classification.**  Trellix Dashboards System T Recent Pages DLP Policy Manager System Tree Policy Catalog Search Reporting Protection Workspace Dashboards Data Protection DLP Settings DLP Getting Started Classification DLP Incident Manager
1	3	Click the **Definitions** tab.  Data Protection Classification Classification | Manual Classification | Register Documents | Ignored Text | Definitions | Classif
1	4	Expand **Data**. Select **Dictionary**.  Data Advanced Pattern Dictionary Document Properties
1	5	At the **Dictionary** section, locate the **Confidential [built-in]** dictionary.  Dictionary Name Chinese PII Keywords [built-in] Compliance Report [built-in] Confidential [built-in] Credit Report [built-in] Croatian PII Keywords [built-in]

1	6	Click the **Duplicate** link.  Compliance Report [built-in] Confidential [built-in] Credit Report [built-in] View | Duplicate | Usage View | Duplicate | Usage View | Duplicate | Usage
1	7	Locate the **Confidential (1)** dictionary.  Dictionary Name Classified Drugs Codes [built-in] Compliance Report [built-in] Confidential [built-in] Confidential (1) Credit Report [built-in] Croatian PII Keywords [built-in]
1	8	Click the **Edit** link.  Confidential [built-in] Confidential (1) Credit Report [built-in] View | Duplicate | Usage Edit | Delete | Duplicate | Usage View | Duplicate | Usage

1	9	At the **Edit** page, locate the **Name** section. Change the name to: **TechLearn Chemical Confidential.**  Data Protection Classification Definitions > Dictionary > Edit Edit dictionary: Name: TechLearn Chemical Confidential
1	10	Locate the **Entries** section. Note the default list of entries.  Phrase Confidential Do Not Distribute For your eyes only Internal Distribution Internal use only Not For Distribution Not For Public Not for external distribution non confidential non-confidential
1	11	In the lower right-hand corner of the console, click the **Import Entries** button. 

Task:	Step:	Instructions:
1	12	Click the **Choose File** button.



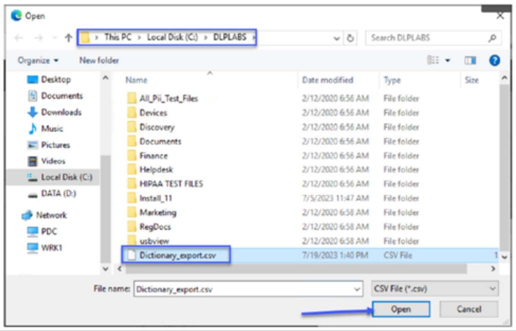
Import

This action will replace the existing list of entries.
If you want to append items to the existing list, export the existing list of entries, append the new entries you want to add, and import the new joined entries list.

Choose file to import from:

Choose File No file chosen

Task:	Step:	Instructions:
1	13	Browse and select the **C:\DLPLABS\Dictionary_export.csv** file. Click **Open**.

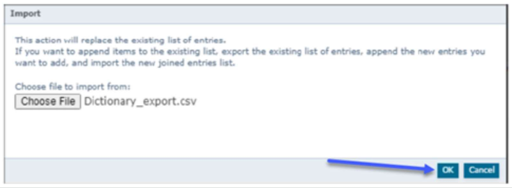


Name	Date modified	Type	Size
All_Pii_Test_Files	2/12/2020 6:56 AM	File folder	
Devices	2/12/2020 6:56 AM	File folder	
Discovery	2/12/2020 6:56 AM	File folder	
Documents	2/12/2020 6:56 AM	File folder	
Finance	2/12/2020 6:56 AM	File folder	
Helpdesk	2/12/2020 6:56 AM	File folder	
HIPAA TEST FILES	2/12/2020 6:56 AM	File folder	
Install_11	7/5/2023 11:47 AM	File folder	
Marketing	2/12/2020 6:58 AM	File folder	
RegDocs	2/12/2020 6:58 AM	File folder	
usbview	2/12/2020 6:58 AM	File folder	
Dictionary_export.csv	7/19/2023 1:40 PM	CSV File	1

File name: Dictionary_export.csv

CSV File (*.csv)

Task:	Step:	Instructions:
1	14	Click **OK**.



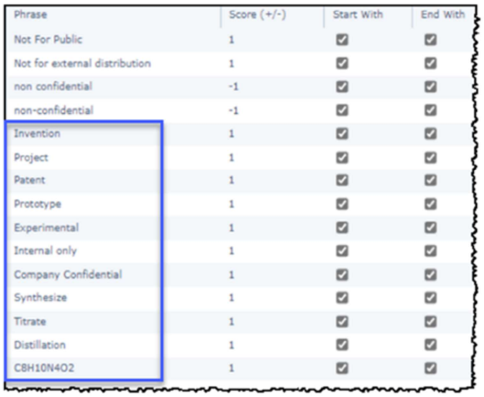
Import

This action will replace the existing list of entries.
If you want to append items to the existing list, export the existing list of entries, append the new entries you want to add, and import the new joined entries list.

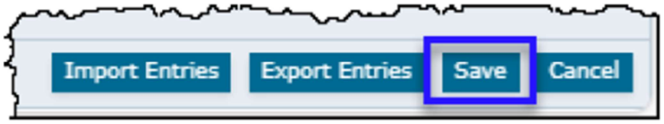
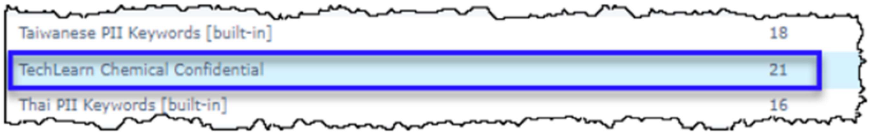
Choose file to import from:

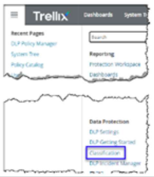
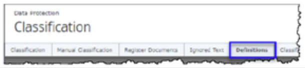
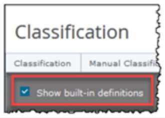
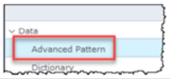
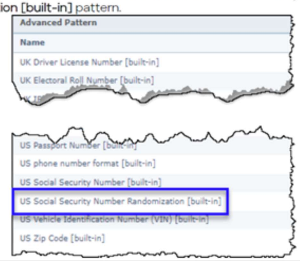
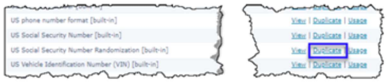
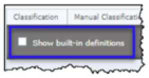
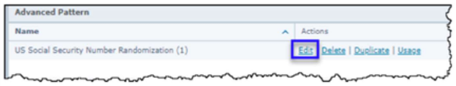
Choose File Dictionary_export.csv

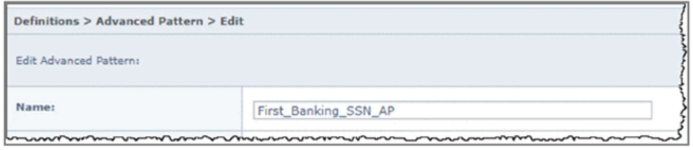
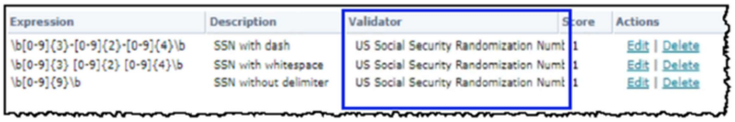
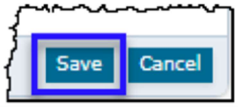
Task:	Step:	Instructions:
1	15	At the **Edit** page, verify the new phrases were successfully added to the dictionary.



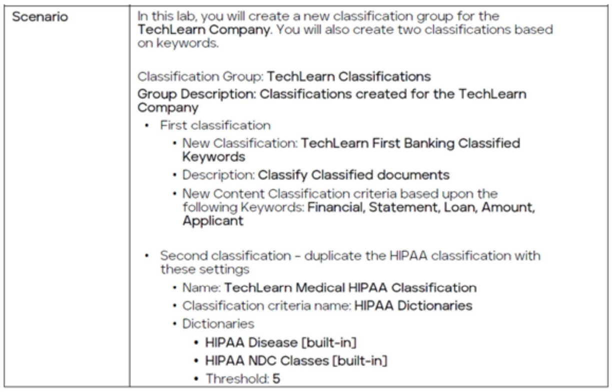
Phrase	Score (+/-)	Start With	End With
Not For Public	1	☑	☑
Not for external distribution	1	☑	☑
non confidential	-1	☑	☑
non-confidential	-1	☑	☑
Invention	1	☑	☑
Project	1	☑	☑
Patent	1	☑	☑
Prototype	1	☑	☑
Experimental	1	☑	☑
Internal only	1	☑	☑
Company Confidential	1	☑	☑
Synthesize	1	☑	☑
Titrate	1	☑	☑
Distillation	1	☑	☑
C8H10N4O2	1	☑	☑

1	16	Click **Save**. 
1	17	Verify the **TechLearn Chemical Confidential** dictionary entries column reflects the additional phrase count.  Taiwanese PII Keywords [built-in] 18 TechLearn Chemical Confidential 21 Thai PII Keywords [built-in] 16
End of Task		
End of Section		

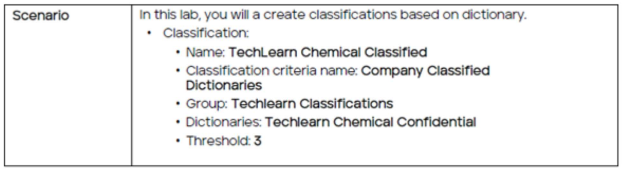
Task:	Step:	Instructions:
1		Create an Advanced Text Pattern
1	1	Make sure that you are in the **Classifications**. (Select **Data Protection** > **Classification**).  Trellix Dashboards System Tr Recent Pages DLP Policy Manager System Tree Policy Catalog Search Reporting Protection Workspace Dashboards Data Protection DLP Settings DLP Getting Started Classification DLP Incident Manager
1	2	Make sure you are in the **Definitions** section. (Click the **Definitions** tab).  Data Protection Classification Classification Manual Classification Register Documents Ignored Text Definitions Classif
1	3	Verify **Show built-in definitions** option is **Yes** (checked).  Classification Classification Manual Classifi ☑ Show built-in definitions
1	4	Expand the **Data** menu. Select **Advanced Pattern**. 
1	5	At the **Advanced Pattern** section, locate the **US Social Security Number Randomization [built-in]** pattern.  Advanced Pattern Name UK Driver License Number [built-in] UK Electoral Roll Number [built-in] US Passport Number [built-in] US phone number format [built-in] US Social Security Number [built-in] US Social Security Number Randomization [built-in] US Vehicle Identification Number (VIN) [built-in] US Zip Code [built-in]
1	6	Click the **Duplicate** link.  US phone number format [built-in] US Social Security Number [built-in] US Social Security Number Randomization [built-in] US Vehicle Identification Number (VIN) [built-in] View | Duplicate | Usage View | Duplicate | Usage View | Duplicate | Usage View | Duplicate | Usage
1	7	**Uncheck** Show built-in definitions:  Classification Manual Classificati □ Show built-in definitions
1	8	Locate the **US Social Security Number Randomization (1)** Advanced Pattern. Click the **Edit** link.  Advanced Pattern Name Actions US Social Security Number Randomization (1) Edit | Delete | Duplicate | Usage

<table>
<tr><th>Task:</th><th>Step:</th><th>Instructions:</th></tr>
<tr><td>1</td><td>9</td><td>At the <b>Edit</b> page, locate the <b>Name</b> section. Enter the name: First_Banking_SSN_AP.

Definitions &gt; Advanced Pattern &gt; Edit
Edit Advanced Pattern:
Name: First_Banking_SSN_AP</td></tr>
<tr><td>1</td><td>10</td><td>Verify each <b>Matched Expression</b> has a <b>US Social Security Randomization Number Validator.</b>
<table>
<tr><th>Expression</th><th>Description</th><th>Validator</th><th>Score</th><th>Actions</th></tr>
<tr><td>\b[0-9]{3}-[0-9]{2}-[0-9]{4}\b</td><td>SSN with dash</td><td>US Social Security Randomization Numt</td><td>1</td><td>Edit | Delete</td></tr>
<tr><td>\b[0-9]{3} [0-9]{2} [0-9]{4}\b</td><td>SSN with whitespace</td><td>US Social Security Randomization Numt</td><td>1</td><td>Edit | Delete</td></tr>
<tr><td>\b[0-9]{9}\b</td><td>SSN without delimiter</td><td>US Social Security Randomization Numt</td><td>1</td><td>Edit | Delete</td></tr>
</table></td></tr>
<tr><td>1</td><td>11</td><td>Click <b>Save</b>.

 </td></tr>
<tr><td colspan="3">End of Task</td></tr>
<tr><td colspan="3">End of Section</td></tr>
</table>

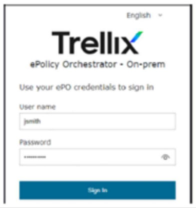
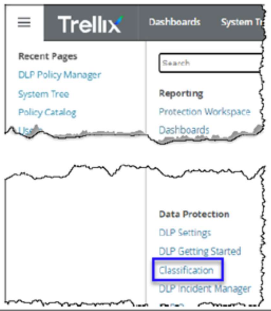
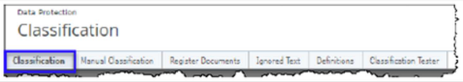
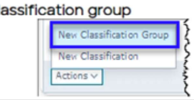
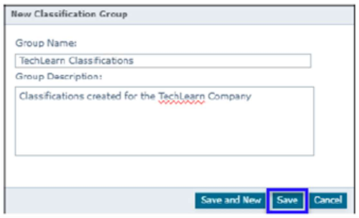
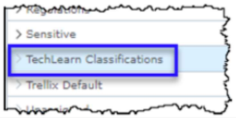
Trabajando con Clasificaciones

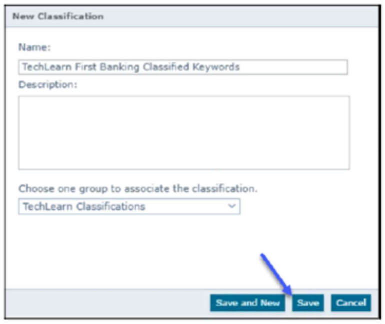
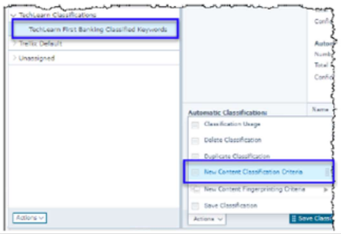
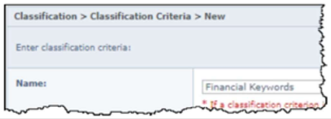
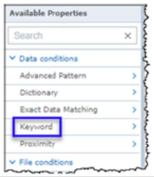
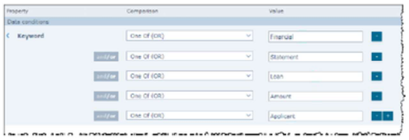


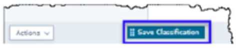
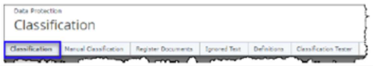
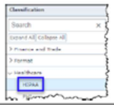
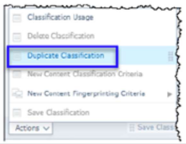
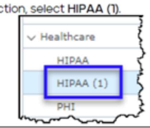
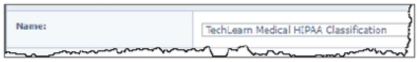
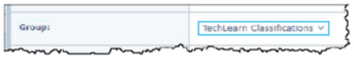
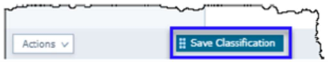
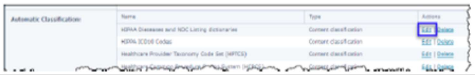
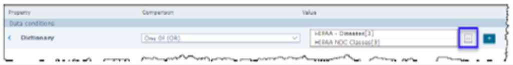
Scenario	In this lab, you will create a new classification group for the **TechLearn Company**. You will also create two classifications based on keywords. Classification Group: **TechLearn Classifications** **Group Description: Classifications created for the TechLearn Company** • First classification • New Classification: **TechLearn First Banking Classified Keywords** • Description: **Classify Classified documents** • New Content Classification criteria based upon the following Keywords: **Financial, Statement, Loan, Amount, Applicant** • Second classification – duplicate the HIPAA classification with these settings • Name: **TechLearn Medical HIPAA Classification** • Classification criteria name: **HIPAA Dictionaries** • Dictionaries • **HIPAA Disease [built-in]** • **HIPAA NDC Classes [built-in]** • Threshold: **5**

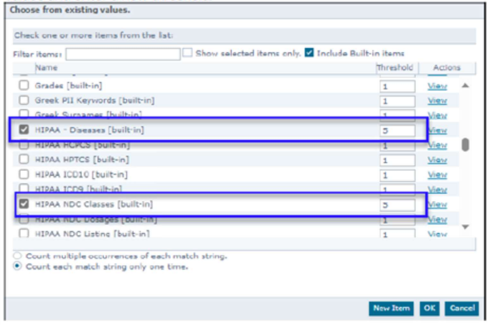
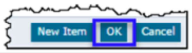
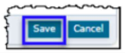
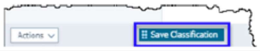


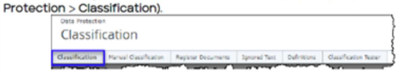
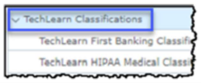
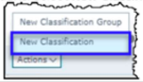
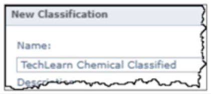
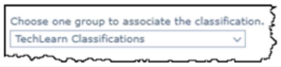
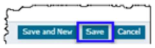
Scenario	In this lab, you will a create classifications based on dictionary. • Classification: • Name: **TechLearn Chemical Classified** • Classification criteria name: **Company Classified Dictionaries** • Group: **Techlearn Classifications** • Dictionaries: **Techlearn Chemical Confidential** • Threshold: **3**

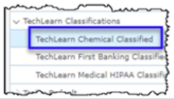
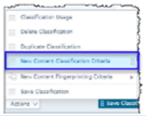
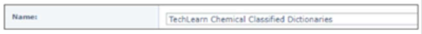
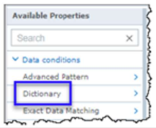
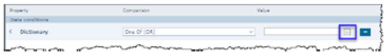
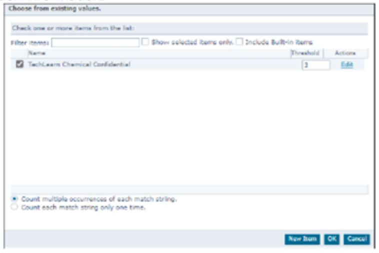
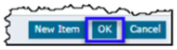
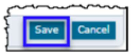
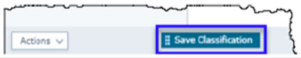
Task:	Step:	Instructions:
1	First Classification – Create TechLearn Medical Classified keywords	
1	1	Make sure you are logged into the ePO console as the administrator (jsmith/Secure123!).  English Trellix ePolicy Orchestrator - On-prem Use your ePO credentials to sign in Sign In User name: jsmith Password: ••••••••••
1	2	Click the **ePO** menu. Select **Data Protection** > **Classification.**  Trellix Dashboards System Tr Recent Pages DLP Policy Manager System Tree Policy Catalog Search Reporting Protection Workspace Dashboards Data Protection DLP Settings DLP Getting Started Classification DLP Incident Manager
1	3	Click the **Classification** tab.  Data Protection Classification Classification Manual Classification Register Documents Ignored Text Definitions Classification Tester
1	4	Click **Actions > New Classification group** 
1	5	In the group name field, enter **TechLearn Classifications.** In the **Group Description** field, enter **Classifications created for the TechLearn Company.** Click **Save.**  Group Name: TechLearn Classifications Group Description: Classifications created for the TechLearn Company
1	6	Click to highlight and select the **TechLearn Classifications**. Select the **Actions > New Classification**  Regulations Sensitive TechLearn Classifications Trellix Default

1	7	Name the new classification **TechLearn First Banking Classified Keywords**. Click **Save**.  New Classification Name: TechLearn First Banking Classified Keywords Description: Choose one group to associate the classification. TechLearn Classifications
1	8	At the **Classification** section, make sure that you have the **TechLearn First Banking Classified Keywords** classification selected. In the right-side of the console select the **Actions > New Content Classification Criteria**.  TechLearn Classifications TechLearn First Banking Classified Keywords Trellix Default Unassigned Automatic Classification: Name Classification Usage Delete Classification Duplicate Classification New Content Classification Criteria New Content Fingerprinting Criteria Save Classification Actions Save Classi
1	9	Name the Classification Criteria **Financial Keywords**  Classification > Classification Criteria > New Enter classification criteria: Name: Financial Keywords * If a classification criterion
1	10	At the **Available Properties** section, select **Keyword**.  Available Properties Search Data conditions Advanced Pattern Dictionary Exact Data Matching Keyword Proximity File conditions
1	11	At the **Property** section, locate **Keyword** properties. Enter the following configuration information:  Property / Comparison / Value Data conditions Keyword: One Of (OR) Financial and/or One Of (OR) Statement and/or One Of (OR) Loan and/or One Of (OR) Amount and/or One Of (OR) Applicant • Comparison: **One Of (OR)** Value: **Financial** • Comparison: **One Of (OR)** Value: **Statement** • Comparison: **One Of (OR)** Value: **Loan** • Comparison: **One Of (OR)** Value: **Amount** • Comparison: **One Of (OR)** Value: **Applicant**
1	12	Click **Save**.

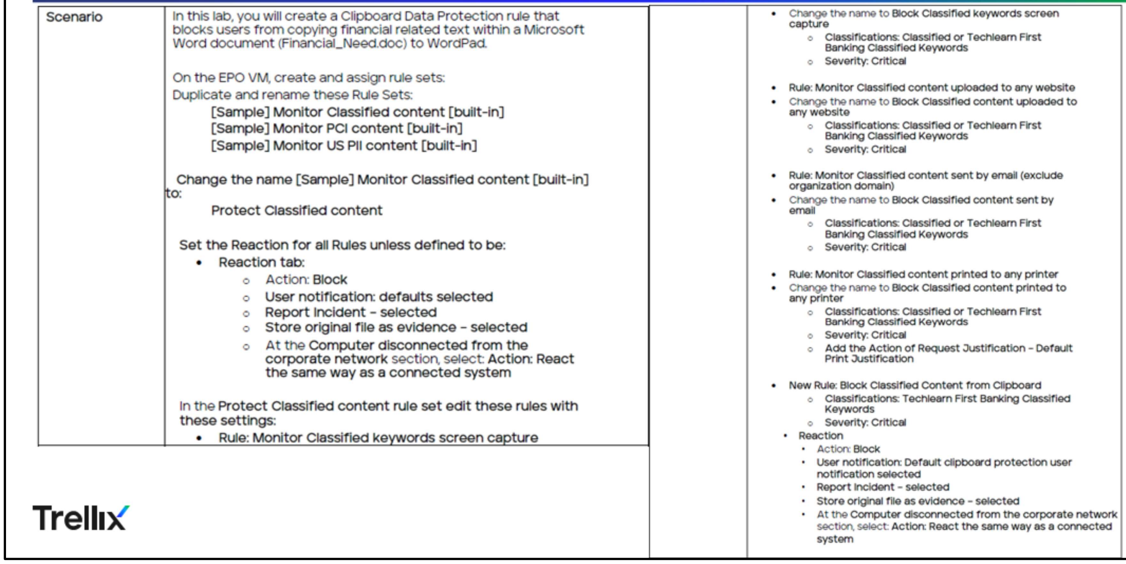
1	13	Select **Save Classification.** 
End of Task		
2	Second Classification – Create the TechLearn Medical HIPAA Classification	
2	1	Make sure you are on the **Classification** tab.  Data Protection Classification Classification Manual Classification Register Documents Ignored Text Definitions Classification Tester
2	2	At the **Classification** section, expand the **Healthcare** section. Select **HIPAA.**  Classification Search Expand All Collapse All Finance and Trade Format Healthcare HIPAA
2	3	Click **Actions.** Select **Duplicate Classification.**  Classification Usage Delete Classification Duplicate Classification New Content Classification Criteria New Content Fingerprinting Criteria Save Classification Actions
2	4	At the **Classification** section, select **HIPAA (1).** 
2	5	At the **Name** section, enter: **TechLearn Medical HIPAA Classification.**  Name: TechLearn Medical HIPAA Classification
2	6	At the **Group** section, select **TechLearn Classifications** if it is not already selected.  Group: TechLearn Classifications
2	7	Click **Save Classification.** 
2	8	At the **Automatic Classification** section, locate the entry **HIPAA Diseases and NDC Listing dictionaries.** Click the **Edit** link.  Automatic Classification Name | Type | Actions HIPAA Diseases and NDC Listing dictionaries | Content classification | Edit | Delete HIPAA ICD10 Codes | Content classification | Edit | Delete Healthcare Provider Taxonomy Code Set (HPTCS) | Content classification | Edit | Delete
2	9	Locate the **Property** section. At **Dictionary** property, click the **ellipsis (...)** button.  Property | Comparison | Value Data conditions Dictionary | One Of (OR) | HIPAA - Diseases[3] HIPAA NDC Classes[9]

2	10	At the **Choose from existing values** dialog window, select the following values and enter a new threshold:  **Choose from existing values.** Check one or more items from the list: Filter items: □ Show selected items only. ☑ Include Built-in items Name / Threshold / Actions □ Grades [built-in] / 1 / View □ Greek PII Keywords [built-in] / 1 / View □ Greek Surnames [built-in] / 1 / View ☑ HIPAA - Diseases [built-in] / 5 / View □ HIPAA HCPCS [built-in] / 1 / View □ HIPAA HPTCS [built-in] / 1 / View □ HIPAA ICD10 [built-in] / 1 / View □ HIPAA ICD9 [built-in] / 1 / View ☑ HIPAA NDC Classes [built-in] / 5 / View □ HIPAA NDC Dosages [built-in] / 1 / View □ HIPAA NDC Listing [built-in] / 1 / View ○ Count multiple occurrences of each match string. ● Count each match string only one time. • Name: **HIPAA – Diseases [built-in]** Threshold: **5** • Name: **HIPAA NDC Classes [built-in]** Threshold: **5**
2	11	Click **OK**. 
2	12	Click **Save**. 
2	13	At the **Classification** section, click **Save Classification**. 
End of Task		
End of Section		

Task:	Step:	Instructions:
1		First classification - TechLearn Chemical Classified Classification
1	1	Make sure that you have the **Classification** tab selected. (Select **Data Protection > Classification**).  Data Protection Classification Classification Manual Classification Register Documents Ignored Text Definitions Classification Tester
1	2	Make sure you have the **TechLearn Classifications** group highlighted and selected.  TechLearn Classifications TechLearn First Banking Classifi TechLearn HIPAA Medical Classi
1	3	At **Classification**, click **Actions**. Select **New Classification**. 
1	4	At **Name** enter: **TechLearn Chemical Classified**  New Classification Name: TechLearn Chemical Classified Descr
1	5	At the **Group** section, select **TechLearn Classifications** if it is not already selected.  Choose one group to associate the classification. TechLearn Classifications
1	6	Click **Save**. 

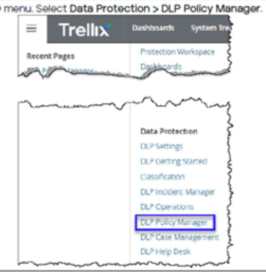
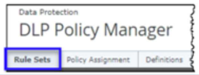
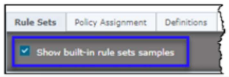
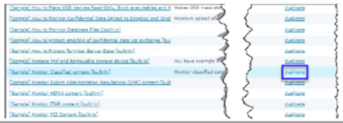
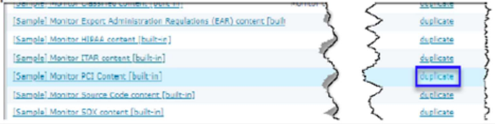
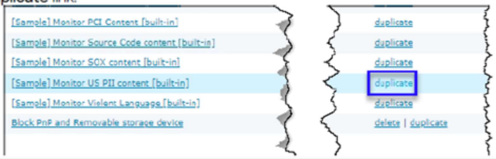
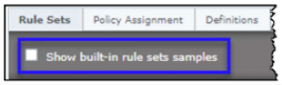
Task:	Step:	Instructions:
1	7	Make sure that you have the **TechLearn Chemical Classified** selected.  TechLearn Classifications TechLearn Chemical Classified TechLearn First Banking Classifie TechLearn Medical HIPAA Classifi
1	8	Click **Actions**. Select **New Content Classification Criteria**.  Classification Usage Delete Classification Duplicate Classification New Content Classification Criteria New Content Fingerprinting Criteria Save Classification Actions Save Classi
1	9	At **Name**, enter: **TechLearn Chemical Classified Dictionaries**.  Name: TechLearn Chemical Classified Dictionaries
1	10	At **Available Properties**, expand **Data Conditions**. Select **Dictionary**.  Available Properties Search Data conditions Advanced Pattern Dictionary Exact Data Matching
1	11	At the **Property** section, locate the **Dictionary** properties. Select the following configuration information:  Property Comparison Value Data conditions Dictionary One Of (OR) • Comparison: **One Of (OR)** • Value: **Click the ellipsis button (...)**.
1	12	At the **Choose from existing values** dialog window, select the following configuration information:  Choose from existing values. Check one or more items from the list: Filter items: □ Show selected items only. □ Include Built-in Items Name / Threshold / Actions ☑ TechLearn Chemical Confidential / 3 / Edit ● Count multiple occurrences of each match string. ○ Count each match string only one time. • Name: **TechLearn Chemical Confidential** • Threshold: **3**
1	13	Click **OK**. 
1	14	Click **Save**. 
1	15	Click **Save Classification**. 
		End of Task
		End of Section

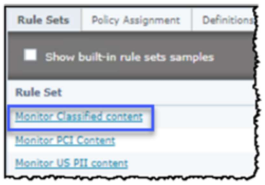
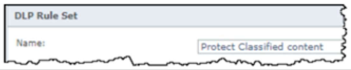
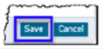
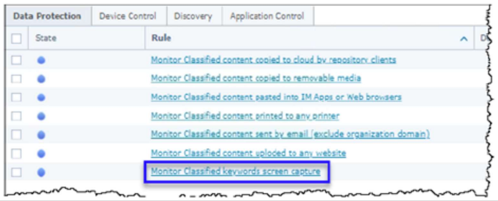
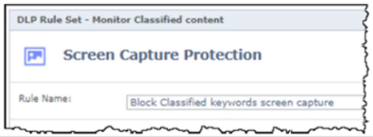
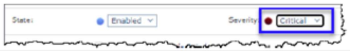
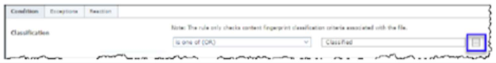
Trabajando con Reglas de Protección de Datos

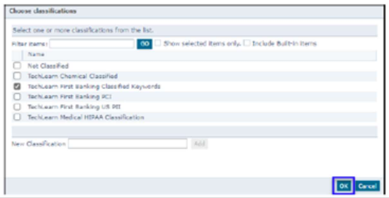
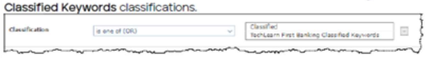
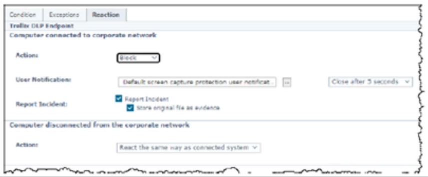
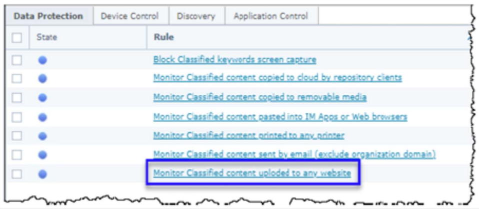
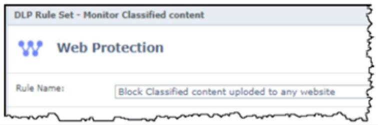
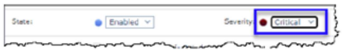
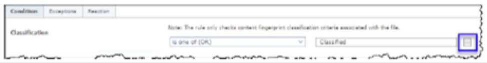


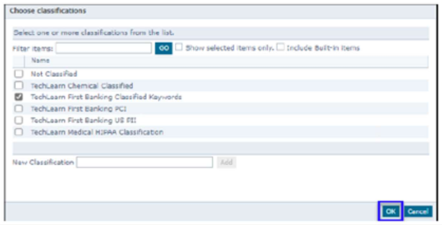
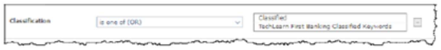
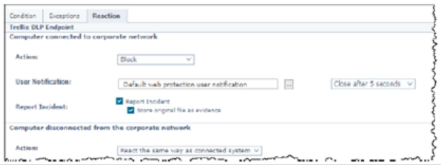
Scenario	In this lab, you will create a Clipboard Data Protection rule that blocks users from copying financial related text within a Microsoft Word document (Financial_Need.doc) to WordPad. On the EPO VM, create and assign rule sets: Duplicate and rename these Rule Sets: [Sample] Monitor Classified content [built-in] [Sample] Monitor PCI content [built-in] [Sample] Monitor US PII content [built-in] Change the name [Sample] Monitor Classified content [built-in] to: Protect Classified content Set the Reaction for all Rules unless defined to be: • Reaction tab: ○ Action: Block ○ User notification: defaults selected ○ Report Incident – selected ○ Store original file as evidence – selected ○ At the Computer disconnected from the corporate network section, select: Action: React the same way as a connected system In the Protect Classified content rule set edit these rules with these settings: • Rule: Monitor Classified keywords screen capture • Change the name to Block Classified keywords screen capture ○ Classifications: Classified or Techlearn First Banking Classified Keywords ○ Severity: Critical • Rule: Monitor Classified content uploaded to any website • Change the name to Block Classified content uploaded to any website ○ Classifications: Classified or Techlearn First Banking Classified Keywords ○ Severity: Critical • Rule: Monitor Classified content sent by email (exclude organization domain) • Change the name to Block Classified content sent by email ○ Classifications: Classified or Techlearn First Banking Classified Keywords ○ Severity: Critical • Rule: Monitor Classified content printed to any printer • Change the name to Block Classified content printed to any printer ○ Classifications: Classified or Techlearn First Banking Classified Keywords ○ Severity: Critical ○ Add the Action of Request Justification – Default Print Justification • New Rule: Block Classified Content from Clipboard ○ Classifications: Techlearn First Banking Classified Keywords ○ Severity: Critical • Reaction • Action: Block • User notification: Default clipboard protection user notification selected • Report Incident – selected • Store original file as evidence – selected • At the Computer disconnected from the corporate network section, select: Action: React the same way as a connected system

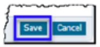
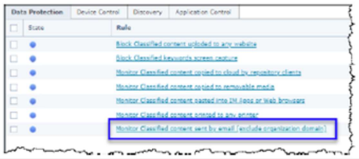
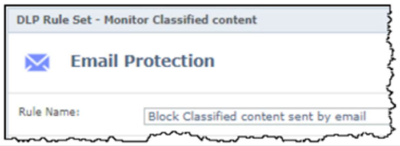
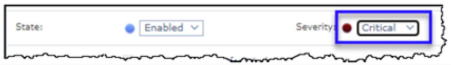
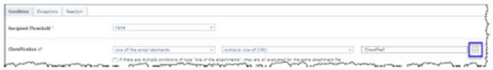
Trellix

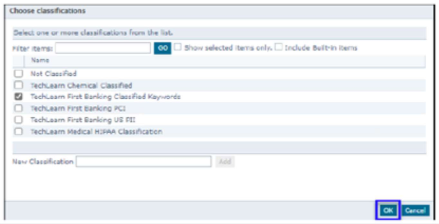
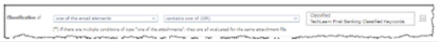
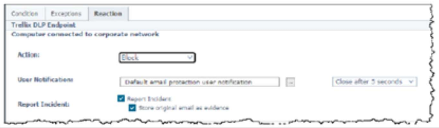
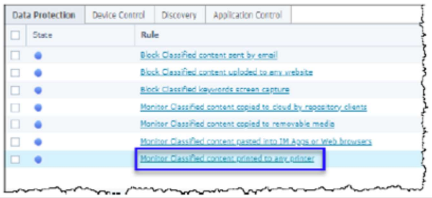
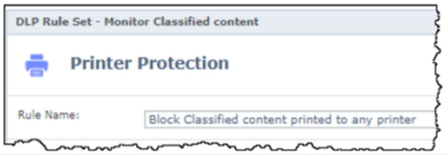
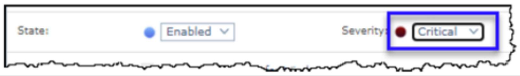
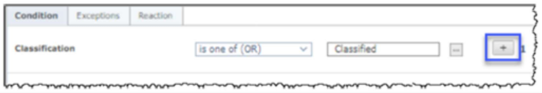
Task:	Step:	Instructions:
1	Create Rule Sets and rules	
1	1	Click the EPO menu. Select **Data Protection > DLP Policy Manager**.  ☰ Trellix Dashboards System Tre Recent Pages Protection Workspace Dashboards Data Protection DLP Settings DLP Getting Started Classification DLP Incident Manager DLP Operations DLP Policy Manager DLP Case Management DLP Help Desk
1	2	Click the **Rule Sets** tab.  Data Protection DLP Policy Manager Rule Sets Policy Assignment Definitions
1	3	Make sure that the option for **Show built-in rule sets samples** is selected.  Rule Sets Policy Assignment Definitions ☑ Show built-in rule sets samples
1	4	On the line that lists the **[Sample] Monitor Classified content [built-in]** click the **duplicate** link.  [Sample] How to Make USB devices Read-Only, Block executables and A ... duplicate [Sample] How to Monitor Confidential Data Upload to Dropbox and One ... duplicate [Sample] How to Monitor Database Files [built-in] ... duplicate [Sample] How to protect emailing of confidential data via exchange [bu ... duplicate [Sample] How to Protect Terminal Server Data [built-in] ... duplicate [Sample] Manage PnP and Removable storage device [built-in] ... duplicate [Sample] Monitor Classified content [built-in] ... duplicate [Sample] Monitor Export Administration Regulations (EAR) content [buil ... duplicate [Sample] Monitor HIPAA content [built-in] ... duplicate [Sample] Monitor ITAR content [built-in] ... duplicate [Sample] Monitor PCI Content [built-in] ... duplicate
1	5	On the line that lists the **[Sample] Monitor PCI content [built-in]** click the **duplicate** link.  [Sample] Monitor Export Administration Regulations (EAR) content [buil ... duplicate [Sample] Monitor HIPAA content [built-in] ... duplicate [Sample] Monitor ITAR content [built-in] ... duplicate [Sample] Monitor PCI Content [built-in] ... duplicate [Sample] Monitor Source Code content [built-in] ... duplicate [Sample] Monitor SOX content [built-in] ... duplicate
1	6	On the line that lists the **[Sample] Monitor US PII content [built-in]** click the **duplicate** link.  [Sample] Monitor PCI Content [built-in] ... duplicate [Sample] Monitor Source Code content [built-in] ... duplicate [Sample] Monitor SOX content [built-in] ... duplicate [Sample] Monitor US PII content [built-in] ... duplicate [Sample] Monitor Violent Language [built-in] ... duplicate Block PnP and Removable storage device ... delete | duplicate
1	7	At the top of the **Rule Sets** console **remove** the check/tick mark next to the **Show built-in rule sets samples** so that you see only the rule sets that you can edit.  Rule Sets Policy Assignment Definitions □ Show built-in rule sets samples
End of Task		

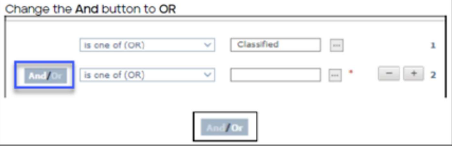
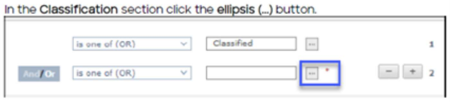
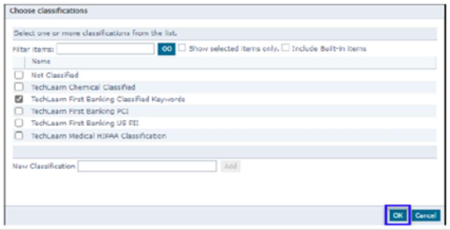
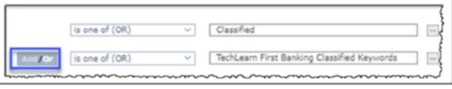
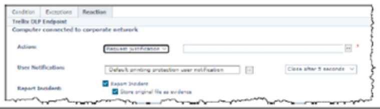
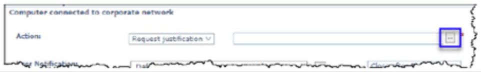
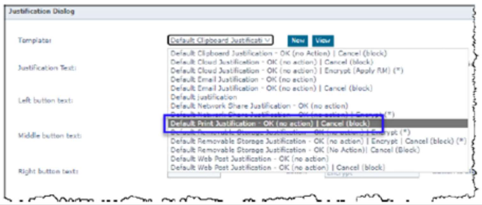
2		**Edit the Monitor Classified content rule set**
2	1	Click on the **Monitor Classified content** rule set.  Rule Sets | Policy Assignment | Definitions □ Show built-in rule sets samples Rule Set Monitor Classified content Monitor PCI Content Monitor US PII content
2	2	Change the name to **Protect Classified content.**  DLP Rule Set Name: Protect Classified content
2	3	In the lower right-hand corner click **Save**.  Save Cancel
2	4	Click on the **Monitor Classified keywords Screen capture** rule.  Data Protection | Device Control | Discovery | Application Control □ State | Rule □ ● Monitor Classified content copied to cloud by repository clients □ ● Monitor Classified content copied to removable media □ ● Monitor Classified content pasted into IM Apps or Web browsers □ ● Monitor Classified content printed to any printer □ ● Monitor Classified content sent by email (exclude organization domain) □ ● Monitor Classified content uploded to any website □ ● Monitor Classified keywords screen capture
2	5	Change the name to **Block Classified keywords screen capture.**  DLP Rule Set - Monitor Classified content Screen Capture Protection Rule Name: Block Classified keywords screen capture
2	6	Change the **Severity** to **Critical**.  State: ● Enabled Severity: ● Critical
2	7	In the **Classification** section click the **ellipsis** (...) button.  Condition | Exceptions | Reaction Classification Note: The rule only checks content fingerprint classification criteria associated with the file. is one of (OR) | Classified

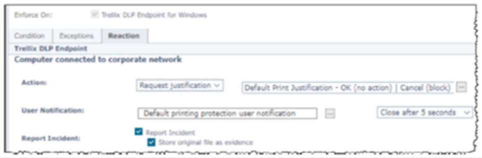
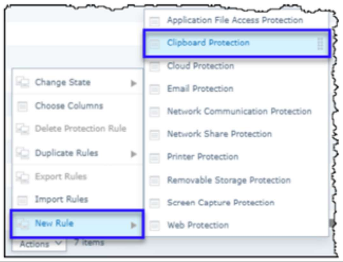
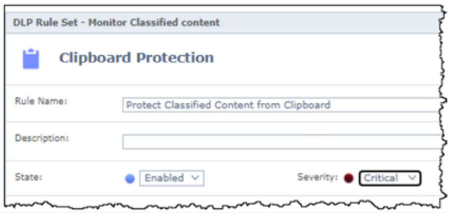
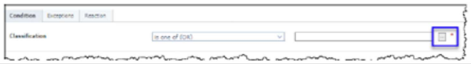
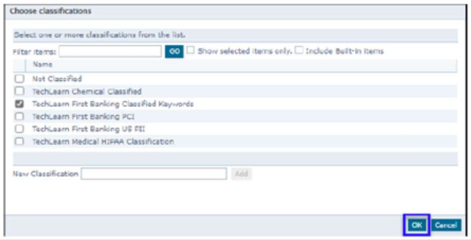
Task:	Step:	Instructions:
2	8	Remove the **Include Built-in items** option and select the **Techlearn First Banking Classified Keywords** classification. You can leave the **Classified [built-in]** selected. Click **OK**.  Choose classifications Select one or more classifications from the list. Filter items: GO □ Show selected items only. □ Include Built-in items Name □ Not Classified □ TechLearn Chemical Classified ☑ TechLearn First Banking Classified Keywords □ TechLearn First Banking PCI □ TechLearn First Banking US PII □ TechLearn Medical HIPAA Classification New Classification: Add OK Cancel
2	9	Make sure that you have the **Classified** and **Techlearn First Banking Classified Keywords** classifications.  Classification: is one of (OR) — Classified, TechLearn First Banking Classified Keywords
2	10	Click the **Reaction** tab and select these options: • Action: **Block** • **User notification: defaults selected** • **Report Incident – selected** • **Store original file as evidence – selected** • At the **Computer disconnected from the corporate network** section, select: **Action: React the same way as a connected system**  Condition | Exceptions | Reaction Trellix DLP Endpoint Computer connected to corporate network Action: Block User Notification: Default screen capture protection user notificat... — Close after 5 seconds Report Incident: ☑ Report Incident ☑ Store original file as evidence Computer disconnected from the corporate network Action: React the same way as connected system
2	11	Click **Save**. Save Cancel
2	12	Click on the **Monitor Classified content uploaded to any website** rule.  Data Protection | Device Control | Discovery | Application Control State — Rule ● Block Classified keywords screen capture ● Monitor Classified content copied to cloud by repository clients ● Monitor Classified content copied to removable media ● Monitor Classified content pasted into IM Apps or Web browsers ● Monitor Classified content printed to any printer ● Monitor Classified content sent by email (exclude organization domain) ● Monitor Classified content uploded to any website
2	13	Change the name to **Block Classified content uploaded to any website**  DLP Rule Set - Monitor Classified content Web Protection Rule Name: Block Classified content uploded to any website
2	14	Change the **Severity** to **Critical**.  State: ● Enabled — Severity: ● Critical
2	15	In the **Classification** section click the **ellipsis** (...) button.  Condition | Exceptions | Reaction Classification — Note: The rule only checks content fingerprint classification criteria associated with the file. is one of (OR) — Classified

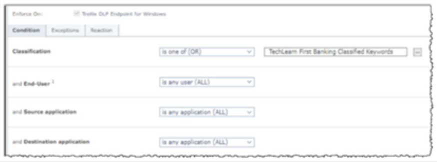
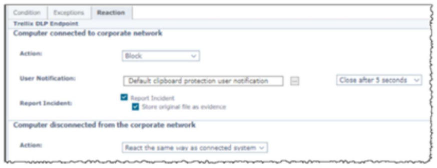
2	16	Remove the **Include Built-in items** option and select the **Techlearn First Banking Classified Keywords** classification. Click **OK**.  Choose classifications Select one or more classifications from the list. Filter items: GO □ Show selected items only. □ Include Built-in items Name □ Not Classified □ TechLearn Chemical Classified ☑ TechLearn First Banking Classified Keywords □ TechLearn First Banking PCI □ TechLearn First Banking US PII □ TechLearn Medical HIPAA Classification New Classification Add OK Cancel
2	17	Note that the two classifications have been selected.  Classification: is one of (OR) — Classified, TechLearn First Banking Classified Keywords
2	18	Click the **Reaction** tab and select these options: (Note that the Report Incident options are already selected. This is due to the DLP Settings tab) • Action: **Block** • **User notification: defaults selected** • **Report Incident – selected** • **Store original file as evidence – selected** • At the **Computer disconnected from the corporate network** section, select: **Action: React the same way as a connected system**  Condition | Exceptions | Reaction Trellix DLP Endpoint Computer connected to corporate network Action: Block User Notification: Default web protection user notification … Close after 5 seconds Report Incident: ☑ Report Incident ☑ Store original file as evidence Computer disconnected from the corporate network Action: React the same way as connected system

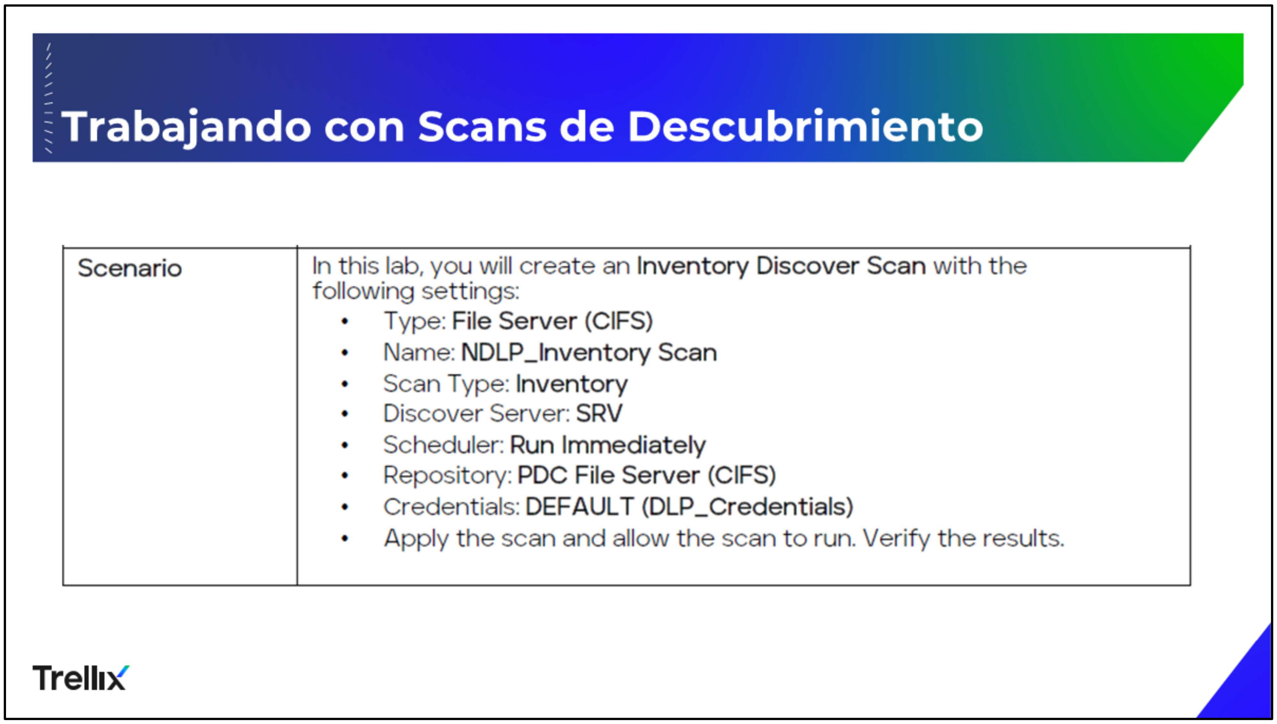
2	19	Click **Save** to save the changes to this rule.  Save Cancel
2	20	Click on the **Monitor Classified content sent by email (exclude organization domain)** rule  Data Protection | Device Control | Discovery | Application Control State | Rule ● Block Classified content uploded to any website ● Block Classified keywords screen capture ● Monitor Classified content copied to cloud by repository clients ● Monitor Classified content copied to removable media ● Monitor Classified content pasted into IM Apps or Web browsers ● Monitor Classified content printed to any printer ● Monitor Classified content sent by email (exclude organization domain)
2	21	Change the name to **Block Classified content sent by email.**  DLP Rule Set - Monitor Classified content Email Protection Rule Name: Block Classified content sent by email
2	22	Change the **Severity** to **Critical.**  State: ● Enabled Severity: ● Critical
2	23	In the **Classification** section click the **ellipsis** (...) button.  Condition | Exceptions | Reaction Recipient Threshold *: None Classification (*): one of the email elements — contains one of (OR) — Classified … (*) If there are multiple conditions of type "one of the attachments", they are all evaluated for the same attachment file.

2	24	Remove the **Include Built-in items** option and select the **Techlearn First Banking Classified Keywords** classification. Click **OK**.  Choose classifications Select one or more classifications from the list. Filter items: GO □ Show selected items only. □ Include Built-in items Name □ Not Classified □ TechLearn Chemical Classified ☑ TechLearn First Banking Classified Keywords □ TechLearn First Banking PCI □ TechLearn First Banking US PII □ TechLearn Medical HIPAA Classification New Classification Add OK Cancel
2	25	Note that the two classifications have been selected.  Classification of: one of the email elements · contains one of (OR) · Classified TechLearn First Banking Classified Keywords (*) if there are multiple conditions of type "one of the attachments", they are all evaluated for the same attachment file
2	26	Click the **Reaction** tab and select these options: • Action: **Block** • **User notification: defaults selected** • **Report Incident – selected** • **Store original file as evidence – selected** • At the **Computer disconnected from the corporate network** section, select: **Action: React the same way as a connected system**  Condition · Exceptions · Reaction Trellix DLP Endpoint Computer connected to corporate network Action: Block User Notification: Default email protection user notification · Close after 5 seconds Report Incident: ☑ Report Incident ☑ Store original email as evidence
2	27	Click **Save** to save the changes to this rule. Save Cancel
2	28	Click on the **Monitor Classified content printed to any printer** rule  Data Protection · Device Control · Discovery · Application Control State · Rule ● Block Classified content sent by email ● Block Classified content uploded to any website ● Block Classified keywords screen capture ● Monitor Classified content copied to cloud by repository clients ● Monitor Classified content copied to removable media ● Monitor Classified content pasted into IM Apps or Web browsers ● Monitor Classified content printed to any printer
2	29	Change the name to **Block Classified content printed to any printer.**  DLP Rule Set - Monitor Classified content Printer Protection Rule Name: Block Classified content printed to any printer
2	30	Change the **Severity** to **Critical.**  State: ● Enabled Severity: ● Critical
2	31	In the **Classification** section click the **plus (+)** button.  Condition · Exceptions · Reaction Classification: is one of (OR) · Classified · +

2	32	Change the **And** button to **OR**  is one of (OR) Classified 1 is one of (OR) 2
2	33	In the **Classification** section click the **ellipsis** (...) button.  is one of (OR) Classified 1 is one of (OR) 2
2	34	Remove the **Include Built-in items** option and select the **Techlearn First Banking Classified Keywords** classification. Click **OK**.  Choose classifications Select one or more classifications from the list. Filter items: GO □ Show selected items only. □ Include Built-in items Name □ Not Classified □ TechLearn Chemical Classified ☑ TechLearn First Banking Classified Keywords □ TechLearn First Banking PCI □ TechLearn First Banking US PII □ TechLearn Medical HIPAA Classification New Classification Add
2	35	Note that both classifications are selected. Make sure that the **OR** condition is selected.  is one of (OR) Classified is one of (OR) TechLearn First Banking Classified Keywords
2	36	Click the **Reaction** tab and select these options: • Action: **Request justification – default Print justification selected** • **User notification: default selected** • **Report Incident – selected** • **Store original file as evidence – selected** • At the **Computer disconnected from the corporate network** section, select: **Action: React the same way as a connected system**  Trellix DLP Endpoint Computer connected to corporate network Action: Request justification User Notification: Default printing protection user notification Close after 5 seconds Report Incident: ☑ Report Incident ☑ Store original file as evidence
2	37	In the **Action** section click the **ellipsis** (...) button.  Computer connected to corporate network Action: Request justification
2	38	Select the **Default Print Justification – OK (no action) | Cancel (block)**.  Justification Dialog Template: Default Clipboard Justificati Default Clipboard Justification - OK (no Action) | Cancel (block) Default Cloud Justification - OK (no action) | Cancel (block) Default Cloud Justification - OK (no action) | Encrypt (Apply RM) (*) Default Email Justification - OK (no action) Default Email Justification - OK (no action) | Cancel (block) Default justification Default Network Share Justification - OK (no action) Default Network Share Justification - OK (no action) | Encrypt (*) Default Print Justification - OK (no action) | Cancel (block) Default Removable Storage Justification - OK (no action) | Encrypt (*) Default Removable Storage Justification - OK (no action) | Encrypt | Cancel (block) (*) Default Removable Storage Justification - OK (No Action)| Cancel (Block) Default Web Post Justification - OK (no action) Default Web Post Justification - OK (no action) | Cancel (block) Justification Text: Left button text: Middle button text: Right button text:
2	39	Click **OK**.

Task:	Step:	Instructions:
2	40	Leave the default **User Notification** selected.  Enforce On: ☑ Trellix DLP Endpoint for Windows Condition | Exceptions | **Reaction** **Trellix DLP Endpoint** **Computer connected to corporate network** **Action:** Request justification ⌄ Default Print Justification - OK (no action) | Cancel (block) … **User Notification:** Default printing protection user notification … Close after 5 seconds ⌄ **Report Incident:** ☑ Report Incident ☑ Store original file as evidence
2	41	Click **Save** to save the changes to this rule. Save Cancel
End of Task		
3	Create a Clipboard Protection rule	
3	1	To create a Clipboard protection rule, click the **Actions > New Rule > Clipboard Protection**  Change State ▶ Choose Columns Delete Protection Rule Duplicate Rules ▶ Export Rules Import Rules New Rule ▶ Actions ⌄ 7 items Application File Access Protection Clipboard Protection Cloud Protection Email Protection Network Communication Protection Network Share Protection Printer Protection Removable Storage Protection Screen Capture Protection Web Protection
3	2	Name the rule **Protect Classified Content from Clipboard.** Make sure that the **State** is **Enabled** and the **Severity** is **Critical.**  **DLP Rule Set - Monitor Classified content** **Clipboard Protection** Rule Name: Protect Classified Content from Clipboard Description: State: ● Enabled ⌄ Severity: ● Critical ⌄
3	3	In the **Classification** section click the **ellipsis** (...) button.  Condition | Exceptions | Reaction Classification is one of (OR) ⌄ … *
3	4	Remove the **Include Built-in items** option and select the **Techlearn First Banking Classified Keywords** classification. Click **OK**.  **Choose classifications** Select one or more classifications from the list. Filter items: GO □ Show selected items only. □ Include Built-in items Name □ Not Classified □ TechLearn Chemical Classified ☑ TechLearn First Banking Classified Keywords □ TechLearn First Banking PCI □ TechLearn First Banking US PII □ TechLearn Medical HIPAA Classification New Classification Add OK Cancel

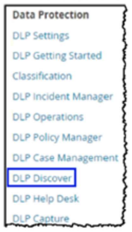
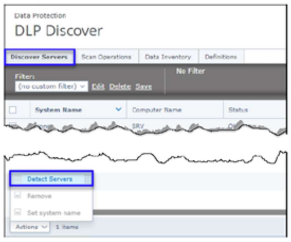
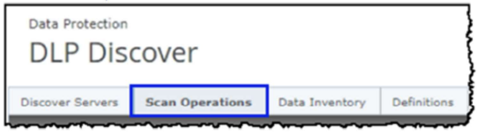
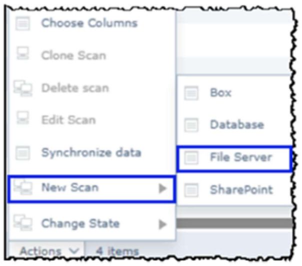
Task:	Step:	Instructions:
3	5	Make sure that you have the **Techlearn First Banking Classified Keywords** classification listed. Leave the default settings for: • End-User is any user (ALL) • Source application is any application (ALL) • Destination application is any application (ALL)  Enforce On: ☑ Trellix DLP Endpoint for Windows Classification: is one of (OR) · TechLearn First Banking Classified Keywords and End-User [1]: is any user (ALL) and Source application: is any application (ALL) and Destination application: is any application (ALL)
3	6	Click the **Reaction** tab and select these options: • Action: **Block** • **User notification: Default clipboard protection user notification selected** • **Report Incident – selected** • **Store original file as evidence – selected** • At the **Computer disconnected from the corporate network** section, select: **Action: React the same way as a connected system**  Trellix DLP Endpoint Computer connected to corporate network Action: Block User Notification: Default clipboard protection user notification · Close after 5 seconds Report Incident: ☑ Report Incident ☑ Store original file as evidence Computer disconnected from the corporate network Action: React the same way as connected system
3	7	Click **Save** to save the rule.
3	8	Click **Close** to close the rule set. (Note: we are not configuring the other rules within this rule set at this time. In your environment you would need to also edit all of the rules for the settings that you want configured).
End of Task		
End of Section		



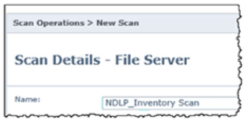
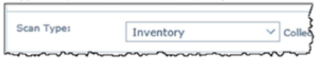
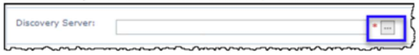
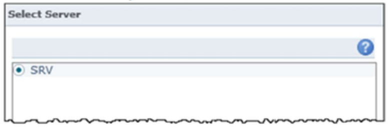
Trabajando con Scans de Descubrimiento

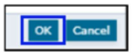
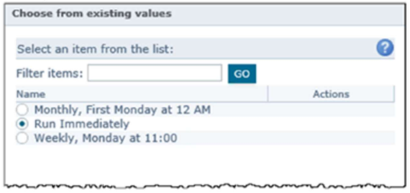
Scenario	In this lab, you will create an **Inventory Discover Scan** with the following settings: • Type: **File Server (CIFS)** • Name: **NDLP_Inventory Scan** • Scan Type: **Inventory** • Discover Server: **SRV** • Scheduler: **Run Immediately** • Repository: **PDC File Server (CIFS)** • Credentials: **DEFAULT (DLP_Credentials)** • Apply the scan and allow the scan to run. Verify the results.

Trellix

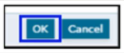
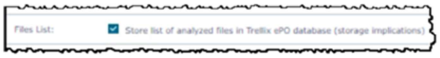
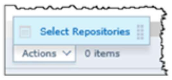
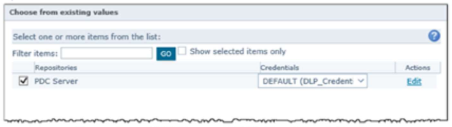
Task:	Step:	Instructions:
1	Configure an inventory Discover Scan	
1	1	Click the **ePO** menu button. Select **Data Protection > DLP Discover.**  Data Protection DLP Settings DLP Getting Started Classification DLP Incident Manager DLP Operations DLP Policy Manager DLP Case Management DLP Discover DLP Help Desk DLP Capture
1	2	Click the **Discover Servers** tab. Select **Actions > Detect Servers** to refresh the list of servers.  Data Protection DLP Discover Discover Servers Scan Operations Data Inventory Definitions Filters (no custom filter) Edit Delete Save No Filter System Name Computer Name Status SRV Detect Servers Remove Set system name Actions 1 items
1	3	Click the **Scan Operations** tab.  Data Protection DLP Discover Discover Servers Scan Operations Data Inventory Definitions
1	4	Click the **Actions** button. Select **New Scan** > **File Server.**  Choose Columns Clone Scan Delete scan Edit Scan Synchronize data New Scan Change State Box Database File Server SharePoint Actions 4 items
1	5	At the **Name** section, enter: **NDLP_Inventory Scan.**

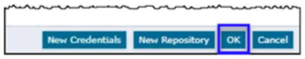
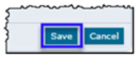
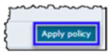
Trellix

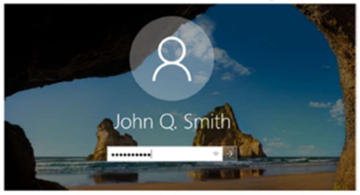
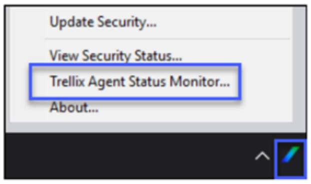
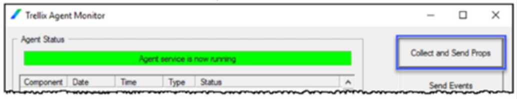
		 Scan Operations > New Scan Scan Details - File Server Name: NDLP_Inventory Scan
1	6	At the **Scan Type** drop-down, select: **Inventory.**  Scan Type: Inventory Colle
1	7	At the **Discovery Server** section, click the ellipsis (...) button.  Discovery Server: * ...
1	8	At the Select Server dialog window, select **SRV.**  Select Server ● SRV

1	9	Click the **OK** button.  OK Cancel
1	10	At the **Scheduler** section, click the ellipse button. Select **Run Immediately.**  Choose from existing values Select an item from the list: Filter items: GO Name Actions ○ Monthly, First Monday at 12 AM ● Run Immediately ○ Weekly, Monday at 11:00
1	11	Click the **OK** button.

Trellix

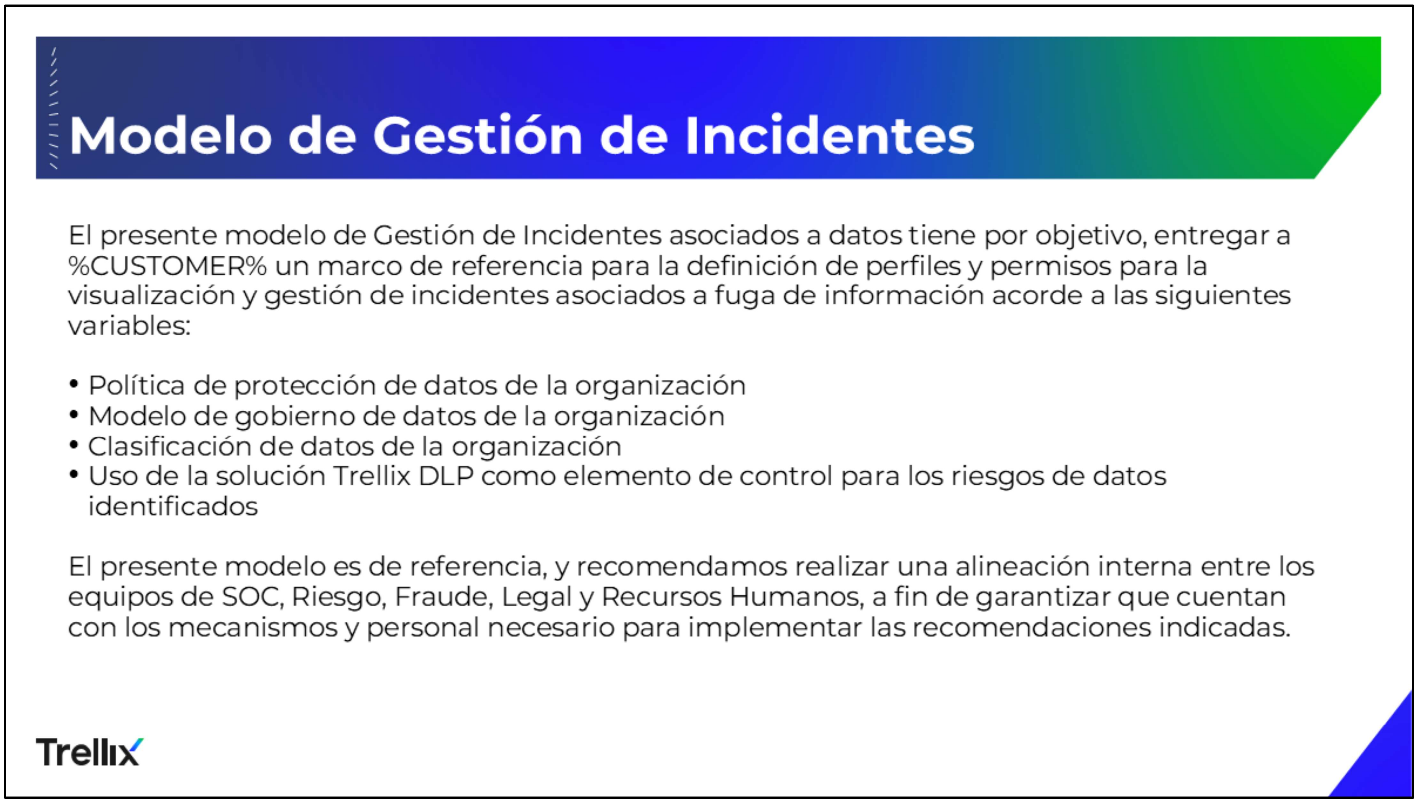
		 OK Cancel
1	12	At the **Files List** section, check/tick the box to **Store list of analyzed files in Trellix ePO Database.**  Files List: ☑ Store list of analyzed files in Trellix ePO database (storage implications)
1	13	Click the **Actions** button. Select **Select Repositories.**  Select Repositories Actions 0 items
1	14	At the **Choose from existing values** dialog window, select the following options:  Choose from existing values Select one or more items from the list: Filter items: GO □ Show selected items only Repositories | Credentials | Actions ☑ PDC Server | DEFAULT (DLP_Credent | Edit • Repository: **PDC Server (CIFS): Yes** (check/tick) • Credentials: **Default (DLP_Credentials)**

1	15	Click the **OK** button.  New Credentials New Repository OK Cancel
1	16	Click the **Save** button.  Save Cancel
1	17	Click the **Apply Policy** button.  Apply policy
End of Task		
2	Update SRV	

Task:	Step:	Instructions:
2	1	Login to the **SRV** virtual machine with the following credentials:  • User Name: **TechLearn\JSmith** • Password: **Secure123!**
2	2	At the system tray click the **Trellix Agent** icon. Select **Trellix Agent Status Monitor.**  Update Security... View Security Status... Trellix Agent Status Monitor... About...
2	3	Click the **Collect and Send Props** button.  Trellix Agent Monitor Agent Status Collect and Send Props Send Events Agent service is now running Component | Date | Time | Type | Status
End of Task		

Trellix

Gestión de Incidentes y Casos con DLP



Modelo de Gestión de Incidentes

El presente modelo de Gestión de Incidentes asociados a datos tiene por objetivo, entregar a %CUSTOMER% un marco de referencia para la definición de perfiles y permisos para la visualización y gestión de incidentes asociados a fuga de información acorde a las siguientes variables:

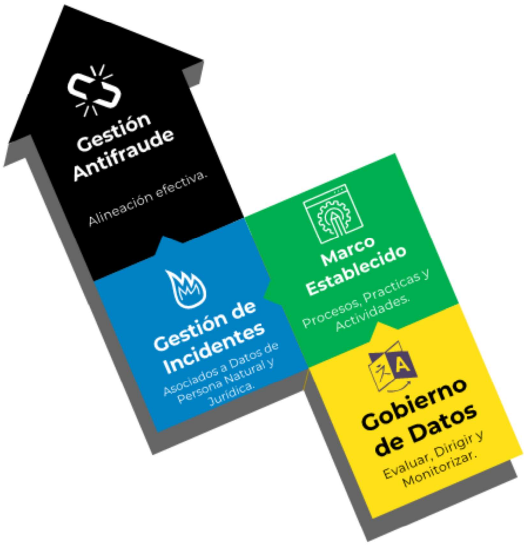
- Política de protección de datos de la organización
- Modelo de gobierno de datos de la organización
- Clasificación de datos de la organización
- Uso de la solución Trellix DLP como elemento de control para los riesgos de datos identificados

El presente modelo es de referencia, y recomendamos realizar una alineación interna entre los equipos de SOC, Riesgo, Fraude, Legal y Recursos Humanos, a fin de garantizar que cuentan con los mecanismos y personal necesario para implementar las recomendaciones indicadas.

Modelo de Gestión - Ejemplo

El presente modelo de Gestión de Incidentes asociados a datos, busca una alineación perfecta con los términos de **Gestión Antifraude** que posea el cliente, así como con el **Marco de Referencia en Gobierno de Datos** establecido por el mismo.

El presente Modelo establece el **Flujo de Trabajo**, **Roles y Responsabilidades**, así como el correspondiente **periodo de tiempo “Time Frame”** y **Estrategias de Monitoreo** correspondientes.

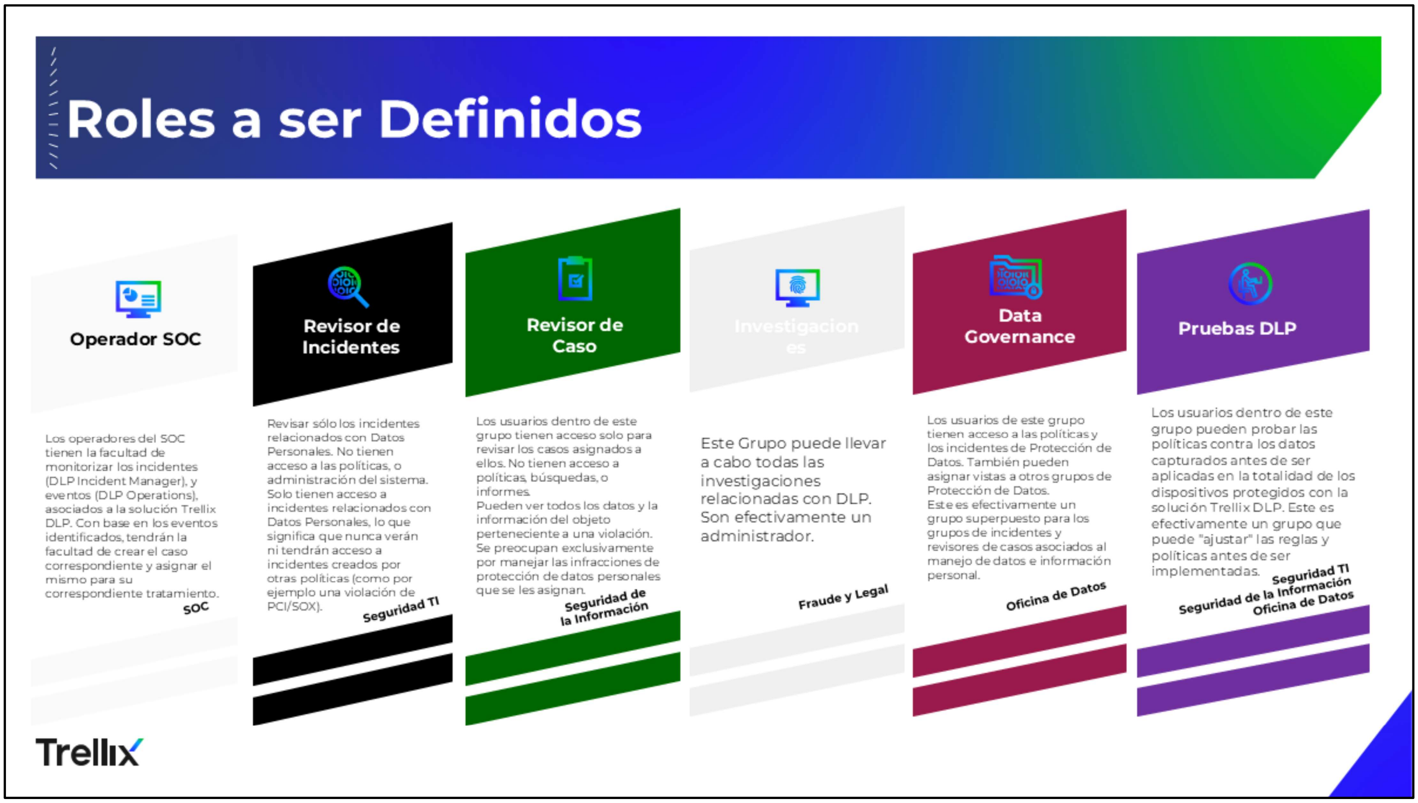


Gestión Antifraude
Alineación efectiva.

Marco Establecido
Procesos, Practicas y Actividades.

Gestión de Incidentes
Asociados a Datos de Persona Natural y Jurídica.

Gobierno de Datos
Evaluar, Dirigir y Monitorizar.



Roles a ser Definidos

Operador SOC

Los operadores del SOC tienen la facultad de monitorizar los incidentes (DLP Incident Manager), y eventos (DLP Operations), asociados a la solución Trellix DLP. Con base en los eventos identificados, tendrán la facultad de crear el caso correspondiente y asignar el mismo para su correspondiente tratamiento.

SOC

Revisor de Incidentes

Revisar sólo los incidentes relacionados con Datos Personales. No tienen acceso a las políticas, o administración del sistema. Solo tienen acceso a incidentes relacionados con Datos Personales, lo que significa que nunca verán ni tendrán acceso a incidentes creados por otras políticas (como por ejemplo una violación de PCI/SOX).

Seguridad TI

Revisor de Caso

Los usuarios dentro de este grupo tienen acceso solo para revisar los casos asignados a ellos. No tienen acceso a políticas, búsquedas, o informes.

Pueden ver todos los datos y la información del objeto perteneciente a una violación. Se preocupan exclusivamente por manejar las infracciones de protección de datos personales que se les asignan.

Seguridad de la Información

Investigaciones

Este Grupo puede llevar a cabo todas las investigaciones relacionadas con DLP. Son efectivamente un administrador.

Fraude y Legal

Data Governance

Los usuarios de este grupo tienen acceso a las políticas y los incidentes de Protección de Datos. También pueden asignar vistas a otros grupos de Protección de Datos.

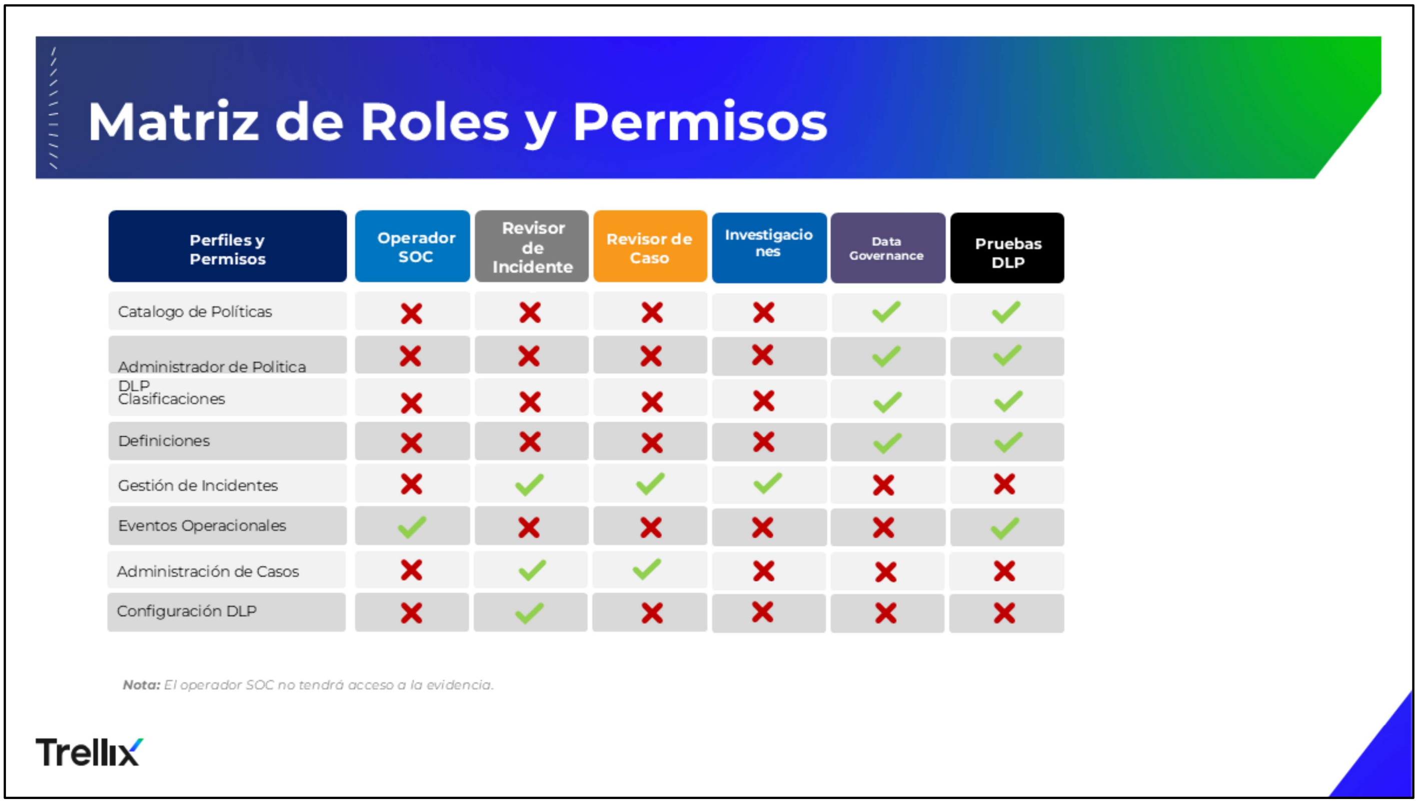
Este es efectivamente un grupo superpuesto para los grupos de incidentes y revisores de casos asociados al manejo de datos e información personal.

Oficina de Datos

Pruebas DLP

Los usuarios dentro de este grupo pueden probar las políticas contra los datos capturados antes de ser aplicadas en la totalidad de los dispositivos protegidos con la solución Trellix DLP. Este es efectivamente un grupo que puede "ajustar" las reglas y políticas antes de ser implementadas.

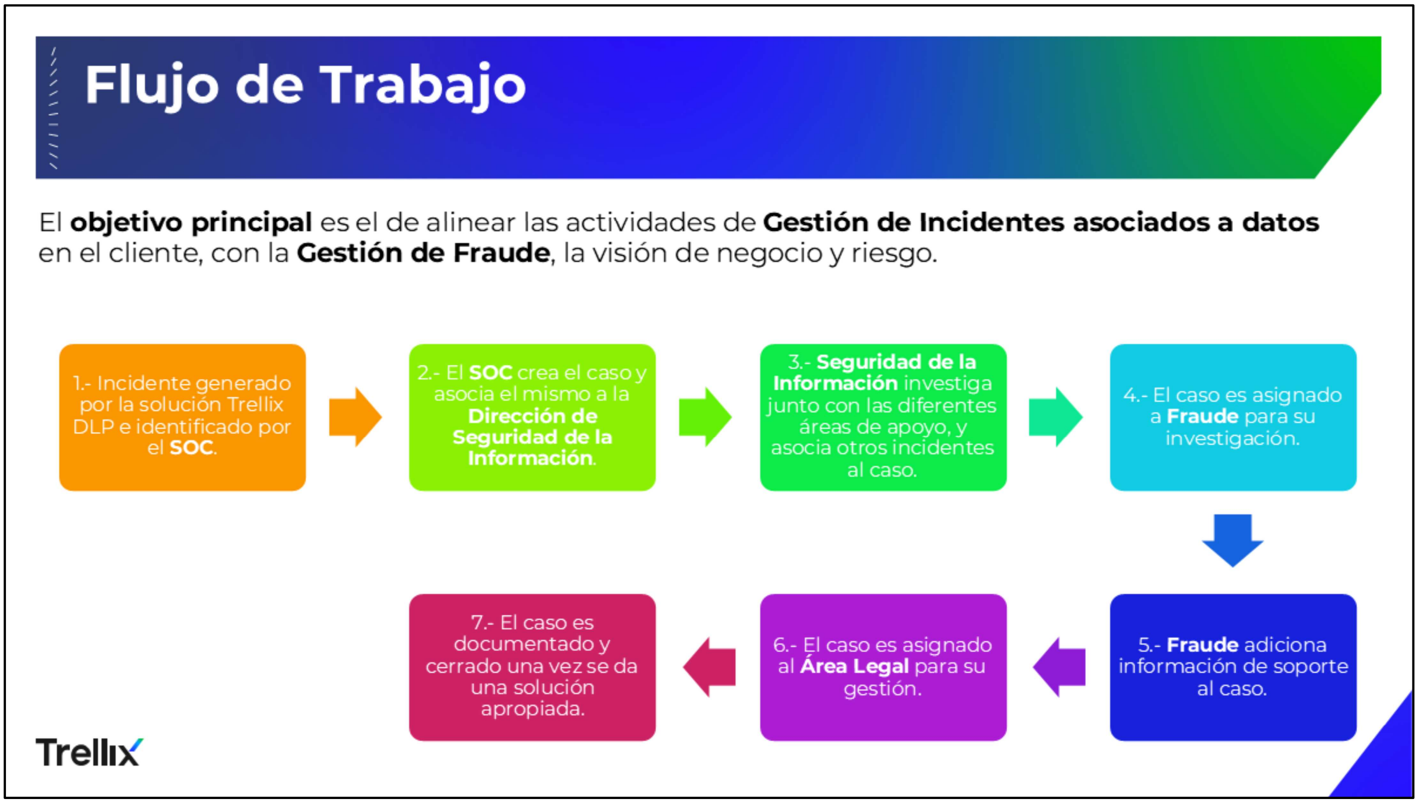
Seguridad TI
Seguridad de la Información
Oficina de Datos



Matriz de Roles y Permisos

Perfiles y Permisos	Operador SOC	Revisor de Incidente	Revisor de Caso	Investigaciones	Data Governance	Pruebas DLP
Catalogo de Políticas	✗	✗	✗	✗	✓	✓
Administrador de Politica DLP	✗	✗	✗	✗	✓	✓
Clasificaciones	✗	✗	✗	✗	✓	✓
Definiciones	✗	✗	✗	✗	✓	✓
Gestión de Incidentes	✗	✓	✓	✓	✗	✗
Eventos Operacionales	✓	✗	✗	✗	✗	✓
Administración de Casos	✗	✓	✓	✗	✗	✗
Configuración DLP	✗	✓	✗	✗	✗	✗

Nota: *El operador SOC no tendrá acceso a la evidencia.*



Flujo de Trabajo

El **objetivo principal** es el de alinear las actividades de **Gestión de Incidentes asociados a datos** en el cliente, con la **Gestión de Fraude**, la visión de negocio y riesgo.

1.- Incidente generado por la solución Trellix DLP e identificado por el **SOC**.

2.- El **SOC** crea el caso y asocia el mismo a la **Dirección de Seguridad de la Información**.

3.- **Seguridad de la Información** investiga junto con las diferentes áreas de apoyo, y asocia otros incidentes al caso.

4.- El caso es asignado a **Fraude** para su investigación.

5.- **Fraude** adiciona información de soporte al caso.

6.- El caso es asignado al **Área Legal** para su gestión.

7.- El caso es documentado y cerrado una vez se da una solución apropiada.

Trellix

Estrategia de Monitoreo

Prioridad 1 - Declinación

Durante la primera hora del Descubrimiento/Detección

Dato Privado bajo Ley XYZ / PCI / Otra.

Prioridad 2 - Alta

Durante las dos primeras horas del Descubrimiento / Detección

Dato Semi-Privado bajo Ley XYZ / PCI / Otra.

Prioridad 3 - Media

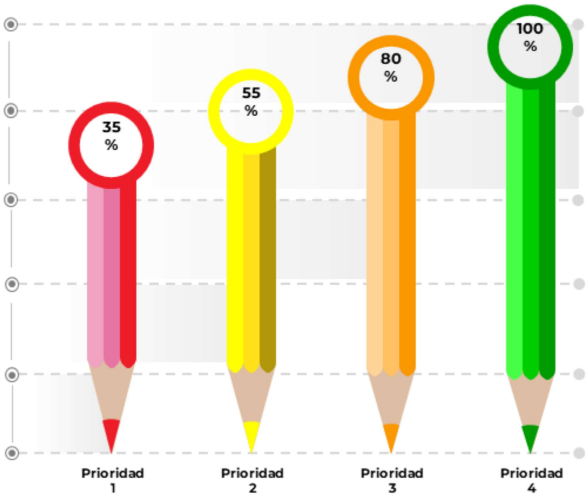
Diariamente. Durante las cuatro primeras horas del Descubrimiento/Detección

Dato Sensible bajo Ley XYZ / PCI / Otra.

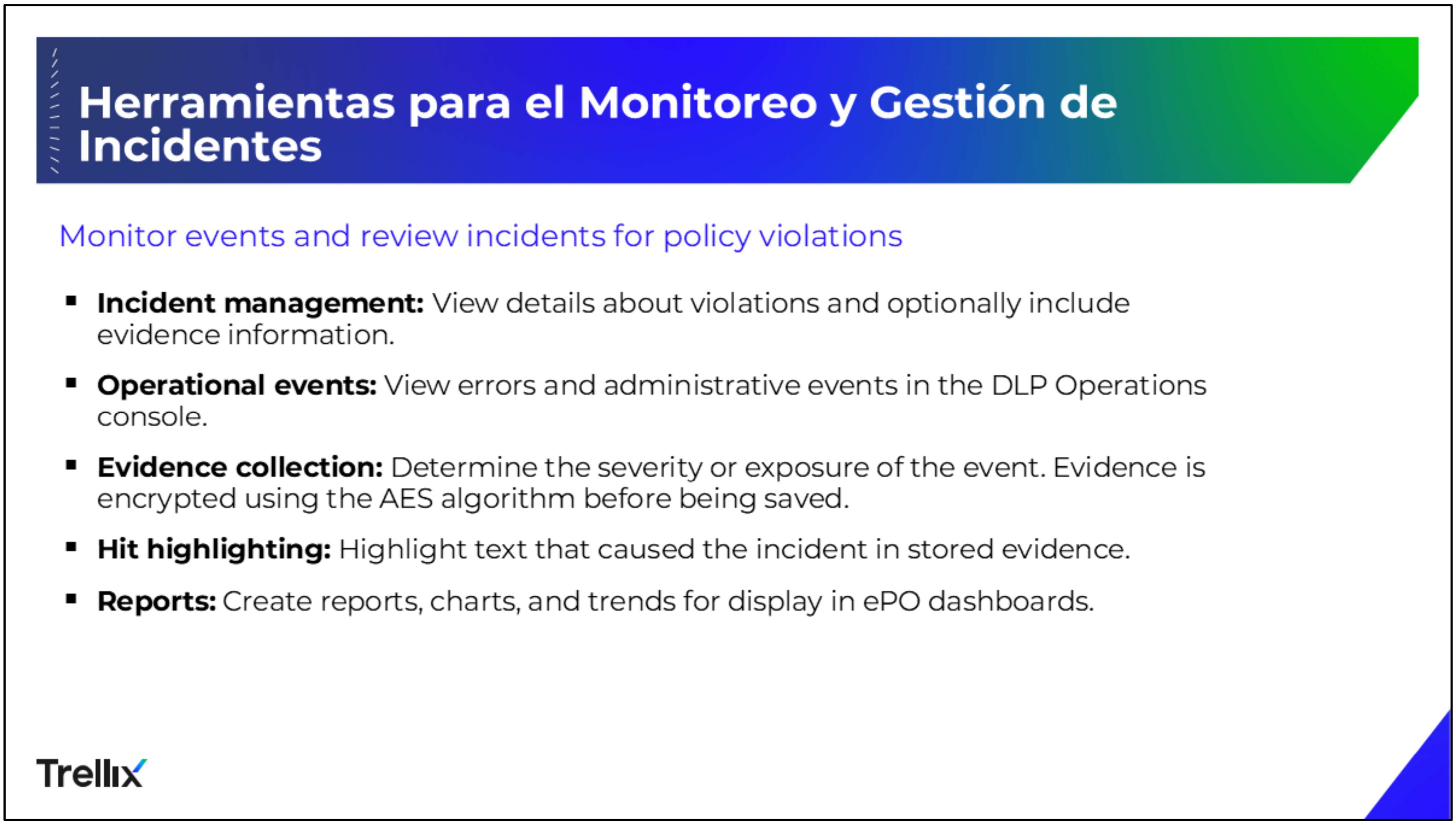
Prioridad 4 - Baja

Diariamente. Durante las ocho primeras horas del Descubrimiento/Detección

Información de Uso Confidencial bajo Manual de Seguridad de la Información de CUSTOMER.



Trellix



Herramientas para el Monitoreo y Gestión de Incidentes

Monitor events and review incidents for policy violations

- **Incident management:** View details about violations and optionally include evidence information.
- **Operational events:** View errors and administrative events in the DLP Operations console.
- **Evidence collection:** Determine the severity or exposure of the event. Evidence is encrypted using the AES algorithm before being saved.
- **Hit highlighting:** Highlight text that caused the incident in stored evidence.
- **Reports:** Create reports, charts, and trends for display in ePO dashboards.

Monitoring functions include:

- **Incident management**: Incidents are sent to the ePO Event Parser and stored in a database. Incidents contain the details about the violation and can optionally include evidence information. You can view incidents and evidence as they are received in the DLP Incident Manager console.

- **Operational events**: View errors and administrative events in the DLP Operations console.

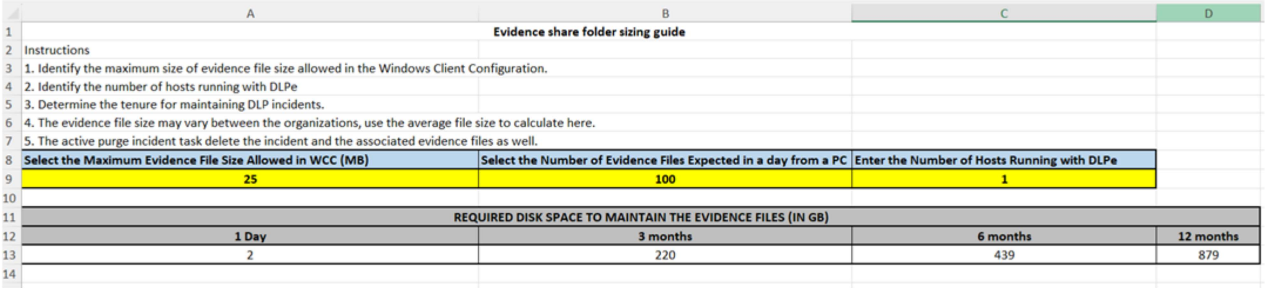
- **Evidence collection**: For rules that are configured to collect evidence, a copy of the data or file is saved and linked to the specific incident. This information can help determine the severity or exposure of the event. Evidence is encrypted using the AES algorithm before being saved.

- **Hit highlighting**: Evidence can be saved with highlighting of the text that caused the incident. Highlighted evidence is stored as a separate encrypted HTML file.

- **Reports**: DLP Endpoint can create reports, charts, and trends for display in ePO dashboards.

Dimensionamiento de Evidencia

Use the tools provided by Trellix for evidence sizing: https://thrive.trellix.com/s/article/KB96298



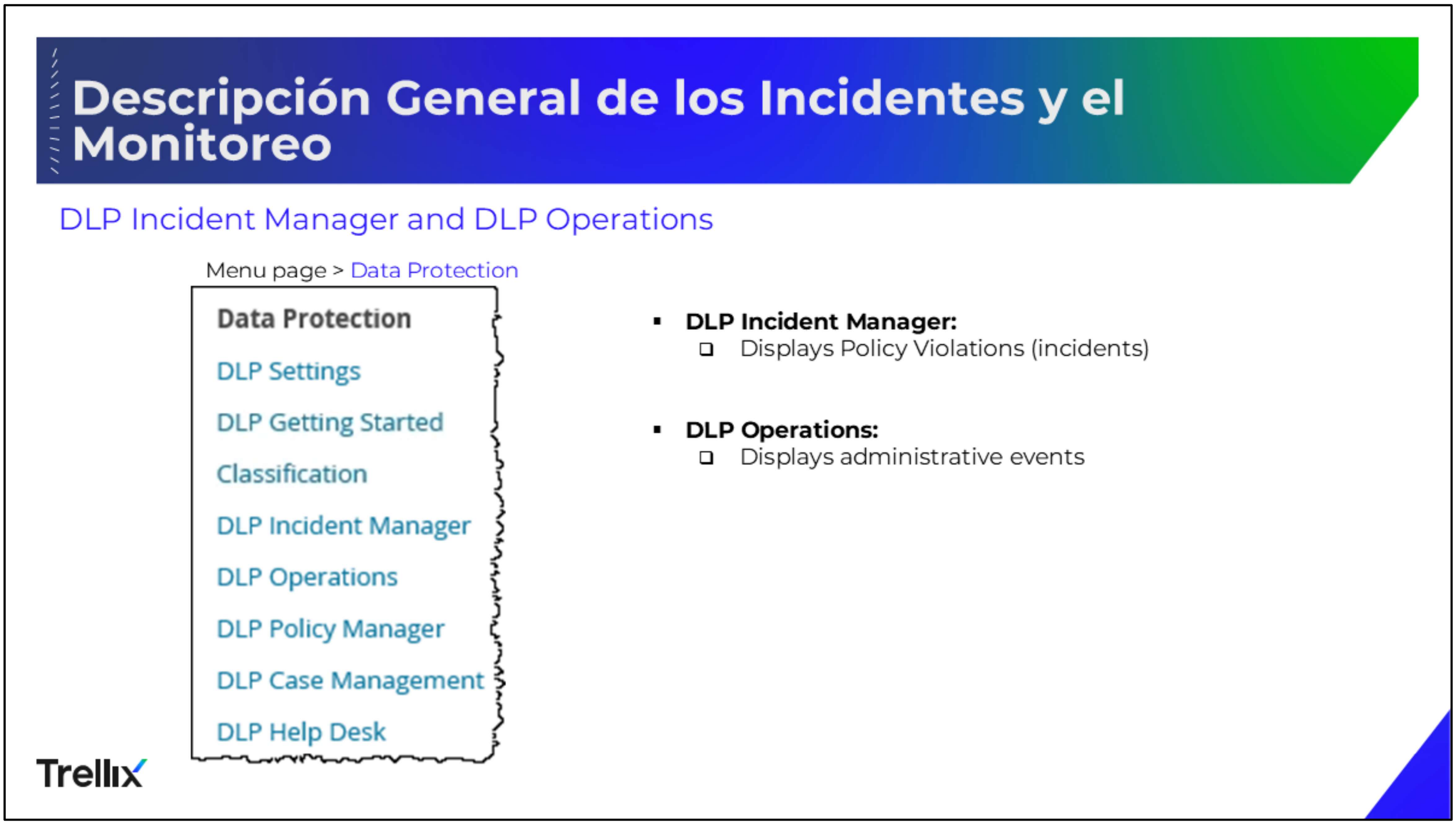
Evidence share folder sizing guide

Instructions

1. Identify the maximum size of evidence file size allowed in the Windows Client Configuration.
2. Identify the number of hosts running with DLPe
3. Determine the tenure for maintaining DLP incidents.
4. The evidence file size may vary between the organizations, use the average file size to calculate here.
5. The active purge incident task delete the incident and the associated evidence files as well.

Select the Maximum Evidence File Size Allowed in WCC (MB)	Select the Number of Evidence Files Expected in a day from a PC	Enter the Number of Hosts Running with DLPe
25	100	1

REQUIRED DISK SPACE TO MAINTAIN THE EVIDENCE FILES (IN GB)			
1 Day	3 months	6 months	12 months
2	220	439	879



Descripción General de los Incidentes y el Monitoreo

DLP Incident Manager and DLP Operations

Menu page > Data Protection

Data Protection

DLP Settings

DLP Getting Started

Classification

DLP Incident Manager

DLP Operations

DLP Policy Manager

DLP Case Management

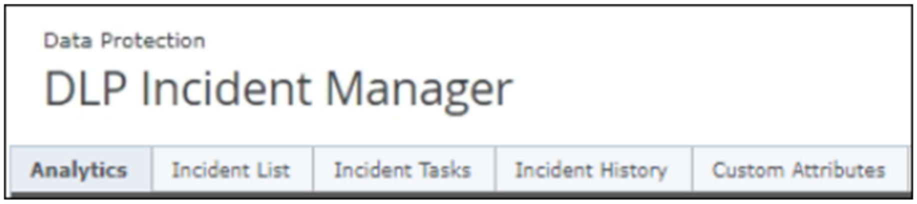
DLP Help Desk

- **DLP Incident Manager:**
  - ❑ Displays Policy Violations (incidents)
- **DLP Operations:**
  - ❑ Displays administrative events

DLPe divides events into two classes: incidents (policy violations) and administrative events. You view these events in the two pages: DLP Incident Manager and DLP Operational Events (**Menu** > **Data Protection**).

DLP Incident Manager

- View and manage incidents (policy violations).
- DLP Operational Events page works in a similar manner with administrative events.



- **Analytics tab**: Six charts summarizing the incident list
- **Incident List tab**: Current policy violation events
- **Incident Tasks tab**: Actions to take on all or part of list
- **Incident History tab**: Historic incidents
- **Custom Attributes**: Create custom attributes

Trellix

Use the **DLP Incident Manager** to view the incidents from policy violations. The page has four tabbed sections:

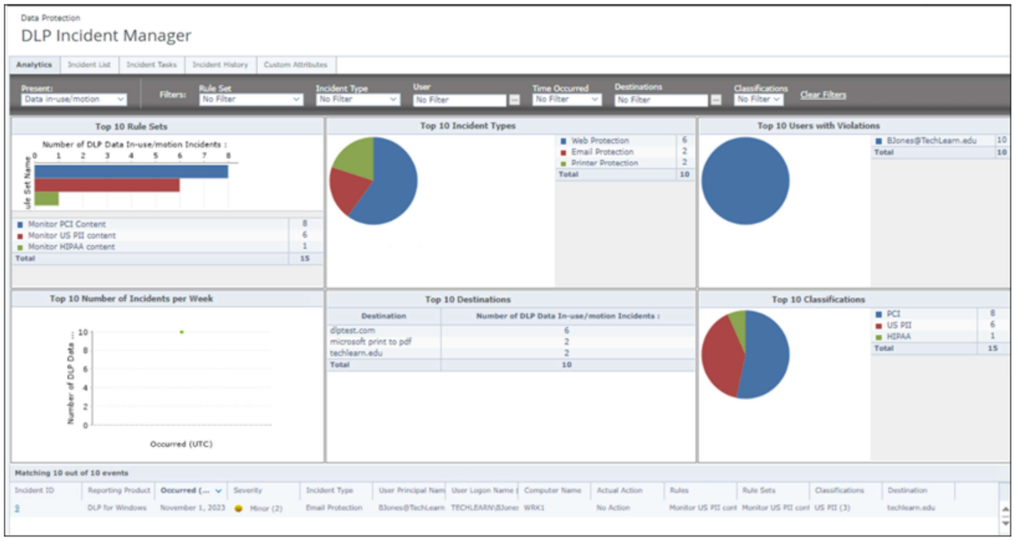
- **Analytics**: The Analytics tab contains a display of six charts that summarize the incident list. Each chart has a filter to adjust the display.
- **Incident List**: The Incident List tab of the DLP Incident Manager provides administrators with a list of events triggered by policy rules. The page lists incidents from DLPe and DLP Discover, if both products are installed. The list can be filtered for easier viewing. The Incident List displays only policy violations. Administrative events such as agent updates are displayed on the DLP Operational Events page. The Incident List tab works with ePO Queries & Reports to create reports and display data on ePO dashboards.
- **Incident Tasks**: The Incident Tasks tab list of actions you can take on the list or selected parts of it. They include assigning reviewers to incidents, setting automatic email notifications, and purging all or part of the list.
- **Incident History**: A list containing all historic incidents. Purging the incident list does not affect the history.
- Custom Attributes: You can create custom attributes that can be

applied to incidents or users.

DLP Incident Manager: Analytics

Dashboard-based quick filtering of incidents

- Top 10 Rule Sets
- Incidents per Type
- Top 10 Users with Violations
- Number of Incidents per Day
- Top 10 Destinations
- Top 10 Classifications



🟦 Monitor PCI Content	8
🟥 Monitor US PII content	6
🟩 Monitor HIPAA content	1
Total	15

🟦 Web Protection	6
🟥 Email Protection	2
🟩 Printer Protection	2
Total	10

🟦 BJones@TechLearn.edu	10
Total	10

Destination	Number of DLP Data In-use/motion Incidents :
dlptest.com	6
microsoft print to pdf	2
techlearn.edu	2
Total	10

🟦 PCI	8
🟥 US PII	6
🟩 HIPAA	1
Total	15

Matching 10 out of 10 events

Incident ID	Reporting Product	Occurred (...	Severity	Incident Type	User Principal Nam	User Logon Name (	Computer Name	Actual Action	Rules	Rule Sets	Classifications	Destination
9	DLP for Windows	November 1, 2023	● Minor (2)	Email Protection	BJones@TechLearn	TECHLEARN\BJone:	WRK1	No Action	Monitor US PII cont	Monitor US PII cont	US PII (3)	techlearn.edu

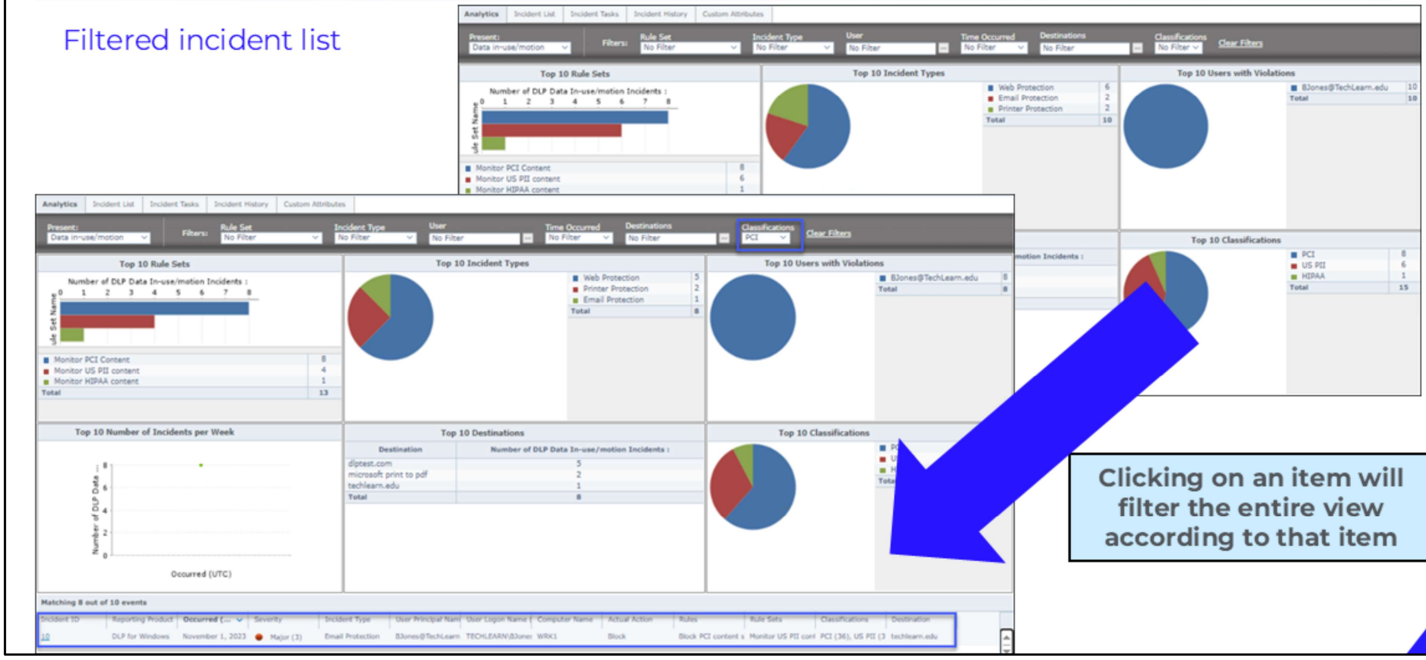
Trellix

The Incident Analytics tab in DLP Incident Manager provides a dashboard-based quick filtering of incidents. There are six charts that summarize the incident list. Each chart has a filter to adjust the display The charts display:

- Top 10 Rule Sets
- Incidents per Type
- Top 10 Users with Violations
- Number of Incidents per Day
- Top 10 Destinations
- Top 10 Classifications

DLP Incident Manager: Analytics (cont.)

Filtered incident list



Present: Data in-use/motion | Filters: Rule Set: No Filter | Incident Type: No Filter | User: No Filter | Time Occurred: No Filter | Destinations: No Filter | Classifications: No Filter

Top 10 Rule Sets

🟦 Monitor PCI Content	8
🟥 Monitor US PII content	6
🟩 Monitor HIPAA content	1

Top 10 Incident Types

🟦 Web Protection	6
🟥 Email Protection	2
🟩 Printer Protection	2
Total	10

Top 10 Users with Violations

🟦 BJones@TechLearn.edu	10
Total	10

Top 10 Classifications

🟦 PCI	8
🟥 US PII	6
🟩 HIPAA	1
Total	15

Present: Data in-use/motion | Filters: Rule Set: No Filter | Incident Type: No Filter | User: No Filter | Time Occurred: No Filter | Destinations: No Filter | Classifications: PCI

Top 10 Rule Sets

🟦 Monitor PCI Content	8
🟥 Monitor US PII content	4
🟩 Monitor HIPAA content	1
Total	13

Top 10 Incident Types

🟦 Web Protection	5
🟥 Printer Protection	2
🟩 Email Protection	1
Total	8

Top 10 Users with Violations

🟦 BJones@TechLearn.edu	8
Total	8

Top 10 Number of Incidents per Week

Top 10 Destinations

Destination	Number of DLP Data In-use/motion Incidents :
dlptest.com	5
microsoft print to pdf	2
techlearn.edu	1
Total	8

Top 10 Classifications

Matching 8 out of 10 events

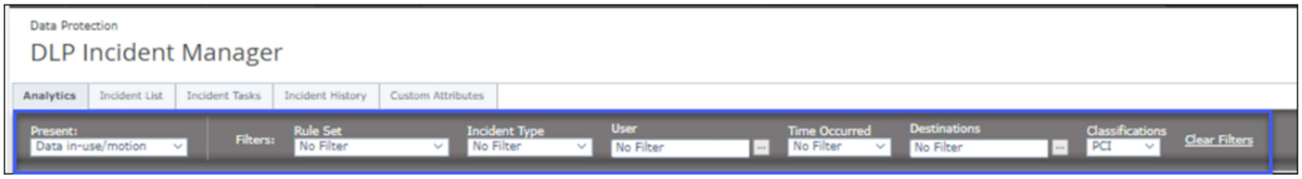
Incident ID	Reporting Product	Occurred (...	Severity	Incident Type	User Principal Nam	User Logon Name (	Computer Name	Actual Action	Rules	Rule Sets	Classifications	Destination
10	DLP for Windows	November 1, 2023	● Major (3)	Email Protection	BJones@TechLearn	TECHLEARN\BJone:	WRK1	Block	Block PCI content s	Monitor US PII cont	PCI (36), US PII (3	techlearn.edu

Clicking on an item will filter the entire view according to that item

Clicking on an item will filter the entire view according to that item.

DLP Incident Manager: Analytics (cont)

Menu bar



Present: Data in-use/motion

Filters: Rule Set: No Filter | Incident Type: No Filter | User: No Filter | Time Occurred: No Filter | Destinations: No Filter | Classifications: PCI

Trellix

On each page the Present drop-down list determines the data set displayed:
Menu bar options include:

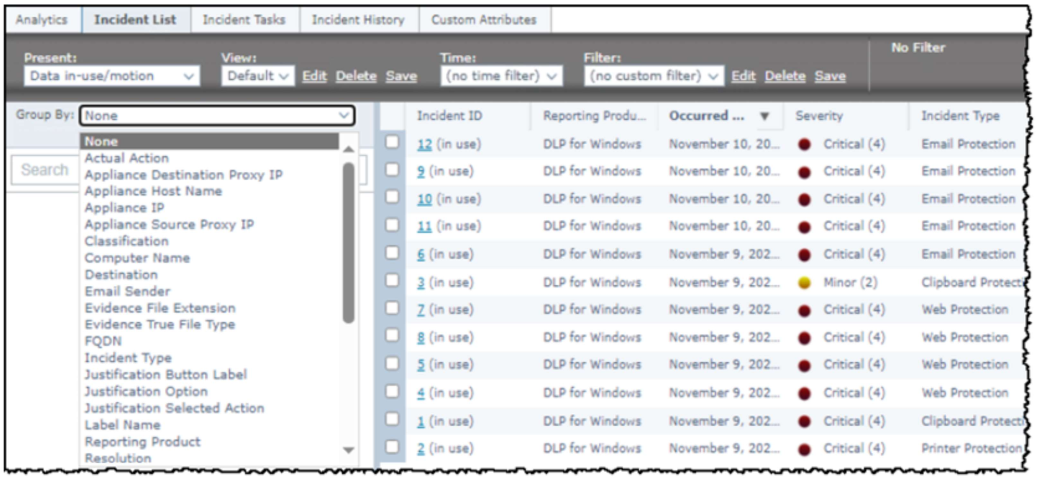
- **Present**: Drop-down list to display to display incidents according to the application that produced them:
  - **Data in-use/motion**
    - Trellix DLP Endpoint
    - Device Control
    - Trellix DLP Prevent
    - Trellix DLP Monitor
    - Trellix® Data Loss Prevention for Mobile Email (Trellix® DLP for Mobile Email)
  - **Data at rest (endpoint)**
    - Trellix DLP Endpoint discovery
  - **Data at rest (Network)**
    - Trellix DLP Discover
- **Filters**:
  - Incident Type
  - User
  - Time Occurred
  - Destinations
  - Classifications

- **Clear Filters**

DLP Incident Manager: Lista de Incidentes

Menu Bar

- **Present**: Data-in-use/motion or Data-at-rest.
- **View**: Default view or custom view (if created).
- **Time**: None, Last 24 hours, Last 7 days, Last 30 days, or Last year.
- **Filter**: No filter or custom filter (if created).
- **Group by**: Vary based on Present setting.



Present: Data in-use/motion
View: Default
Time: (no time filter)
Filter: (no custom filter)
Group By: None

	Incident ID	Reporting Produ...	Occurred ... ▼	Severity	Incident Type
□	12 (in use)	DLP for Windows	November 10, 20...	● Critical (4)	Email Protection
□	9 (in use)	DLP for Windows	November 10, 20...	● Critical (4)	Email Protection
□	10 (in use)	DLP for Windows	November 10, 20...	● Critical (4)	Email Protection
□	11 (in use)	DLP for Windows	November 10, 20...	● Critical (4)	Email Protection
□	6 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Email Protection
□	3 (in use)	DLP for Windows	November 9, 202...	● Minor (2)	Clipboard Protecti
□	7 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Web Protection
□	8 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Web Protection
□	5 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Web Protection
□	4 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Web Protection
□	1 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Clipboard Protecti
□	2 (in use)	DLP for Windows	November 9, 202...	● Critical (4)	Printer Protection

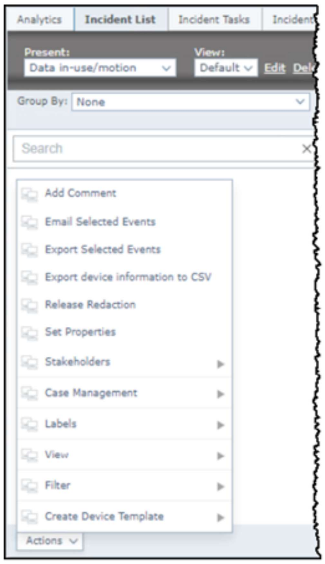
Trellix

Menu bar options include:

- **Present**: Drop-down list to display either Data-in-use/motion, Data-at-rest (Endpoint) (DLP Endpoint data), or Data-at-rest (Network) (DLP Discover data).
- **View**: Drop-down list to display the view. Use Edit to create a view. The view can alternately be applied and switched off during the current session. Use **Save** to use a view between sessions.
- **Time** (DLP Endpoint only): Drop-down list to display the time filter.
- **Filter**: Drop-down list to select the display filter. Use Edit to create a filter. The available properties vary according to the Present setting. The filter can alternately be applied and switched off during the current session. Use Save to use a filter between sessions.
- **Group by**: Drop-down list to organize data. The available filters vary according to the Present setting.

DLP Incident Manager: Lista de Incidentes (cont.)

Columns and actions



Present: Data in-use/motion

View: Default

Group By: None

- Sort columns
- Show/hide columns
- Add Comment
- Email Selected Events
- View
- Filter
- Export Device Parameters (Data in-use/motion list only)
- Release Redaction
- Case Management
- Set Properties
- Manage Labels

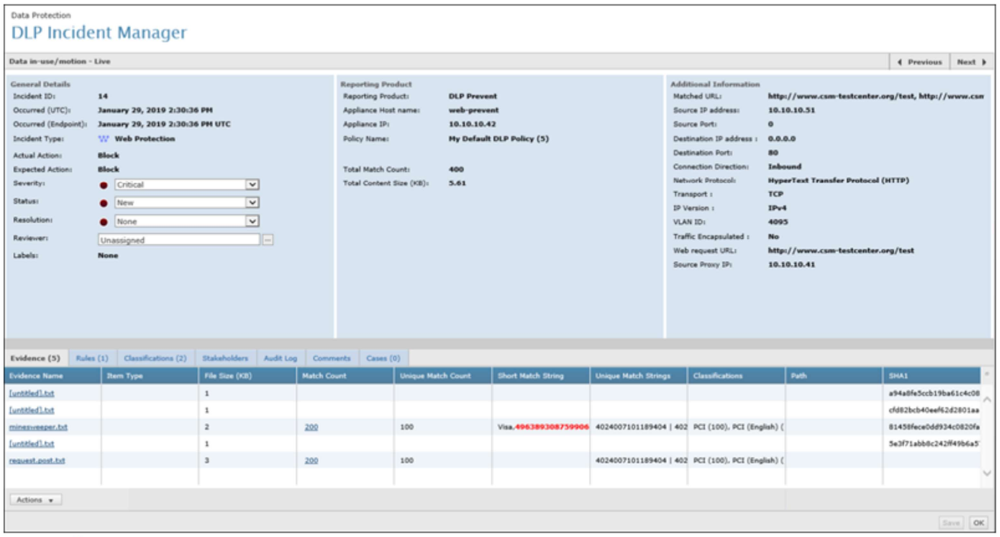
Trellix

The incidents display in columns, which you can sort, show, or hide.
Supported actions are:

- **Add Comment**: Active when at least one incident is selected. Opens a text box for comments of up to 500 characters.
- **Email Selected Events**: Opens an email set-up window to send selected events.
- **Release Redaction**: Opens an authorization dialog box for entering user name and password.
- **Case Management**: Allows you to add incidents to an existing or new case. This is available with DLP 9.4.1 and later.
- **Set Properties**: Opens a dialog box that allows editing of properties (Severity, Status, and so forth) for all selected incidents.
- **Manage Labels**: Opens dialog boxes to attach, detach, or delete labels.
- **View**: Allows the customization of the list view. You can rearrange, display, or hide columns. You can save the view as a named view, with options for Save group by, Save time filter, and Save column filter. Saved views can be public or private.
- **Filter**: Allows you to edit, save, or export filters to Incident Tasks. Click **Filter** > **Edit** to open the Edit Filter Criteria page for selection and definition of filter parameters.
- **Export Device Parameters (Data in-use/motion list only)**: Exports the device parameters of selected incidents to a CSV file and displays the file name as a link.

DLP Incident Manager: Detalle de Incidentes

Drill down to incident details



Data Protection

DLP Incident Manager

Data in-use/motion - Live

◀ Previous | Next ▶

General Details

Incident ID:	14
Occurred (UTC):	January 29, 2019 2:30:36 PM
Occurred (Endpoint):	January 29, 2019 2:30:36 PM UTC
Incident Type:	Web Protection
Actual Action:	Block
Expected Action:	Block
Severity:	● Critical
Status:	● New
Resolution:	● None
Reviewer:	Unassigned
Labels:	None

Reporting Product

Reporting Product:	DLP Prevent
Appliance Host name:	web-prevent
Appliance IP:	10.10.10.42
Policy Name:	My Default DLP Policy (5)
Total Match Count:	400
Total Content Size (KB):	5.61

Additional Information

Matched URL:	http://www.csm-testcenter.org/test, http://www.csm
Source IP address:	10.10.10.51
Source Port:	0
Destination IP address :	0.0.0.0
Destination Port:	80
Connection Direction:	Inbound
Network Protocol:	HyperText Transfer Protocol (HTTP)
Transport :	TCP
IP Version :	IPv4
VLAN ID:	4095
Traffic Encapsulated :	No
Web request URL:	http://www.csm-testcenter.org/test
Source Proxy IP:	10.10.10.41

Evidence (5) | Rules (1) | Classifications (2) | Stakeholders | Audit Log | Comments | Cases (0)

Evidence Name	Item Type	File Size (KB)	Match Count	Unique Match Count	Short Match String	Unique Match Strings	Classifications	Path	SHA1
[untitled].txt		1							a94a8fe5ccb19ba61c4c08
[untitled].txt		1							cfd82bcb40eef62d2801aa
minesweeper.txt		2	200	100	Visa.4963893087599906	4024007101189404 | 402	PCI (100), PCI (English) (		81458fece0dd934c0820fa
[untitled].txt		1							5e3f71abb8c242ff49b6a5
request.post.txt		3	200	100		4024007101189404 | 402	PCI (100), PCI (English) (		

- Time/Date
- Incident Type
- Severity/Status/Resolution
- Reviewer
- URL info
- Evidence Files
- Rule(s) that triggered incident
- Classification(s) matched
- Stakeholders
- Audit
- Comments
- Cases Incident is added to

To display the **User Principal Name** and **User Logon Name** in Trellix DLP appliance incidents, add an LDAP server to the **DLP Appliance Management** policy (**Users and Groups** category). You must do this even if your email protection rules do not use LDAP.

To view incident details:

1. Click an **Incident ID**.

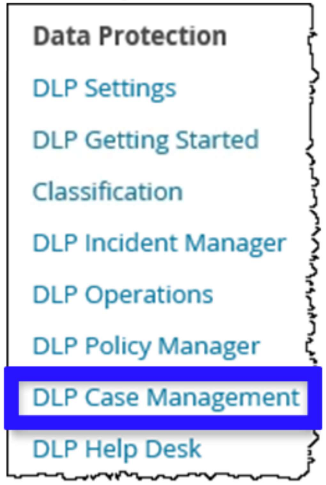
   For Trellix DLP Endpoint, Trellix DLP Monitor, and Trellix DLP Prevent incidents, the page displays general details and source information. Depending on the incident type, destination or device details appear. For Trellix DLP Discover incidents, the page displays general details about the incident.
2. To view additional information, perform any of these tasks.
   - To view user information for Trellix DLP Endpoint incidents, click the user name in the **Source** area.
   - To view evidence files:
3. Click the **Evidence** tab.
4. Click a file name to open the file with an appropriate program.

The **Evidence** tab also displays the **Short Match String**, which contains up to three hit highlights as a single string.

- To view rules that triggered the incident, click the **Rules** tab.
- To view classifications, click the **Classifications** tab.
- To view incident history, click the **Audit Logs** tab.
- To view comments added to the incident, click the **Comments** tab.
- To email the incident details, including decrypted evidence and hit highlight files, select **Actions** > **Email Selected Events**.
- To return to the Incident Manager, click **OK**.

Descripción General de DLP Case Management

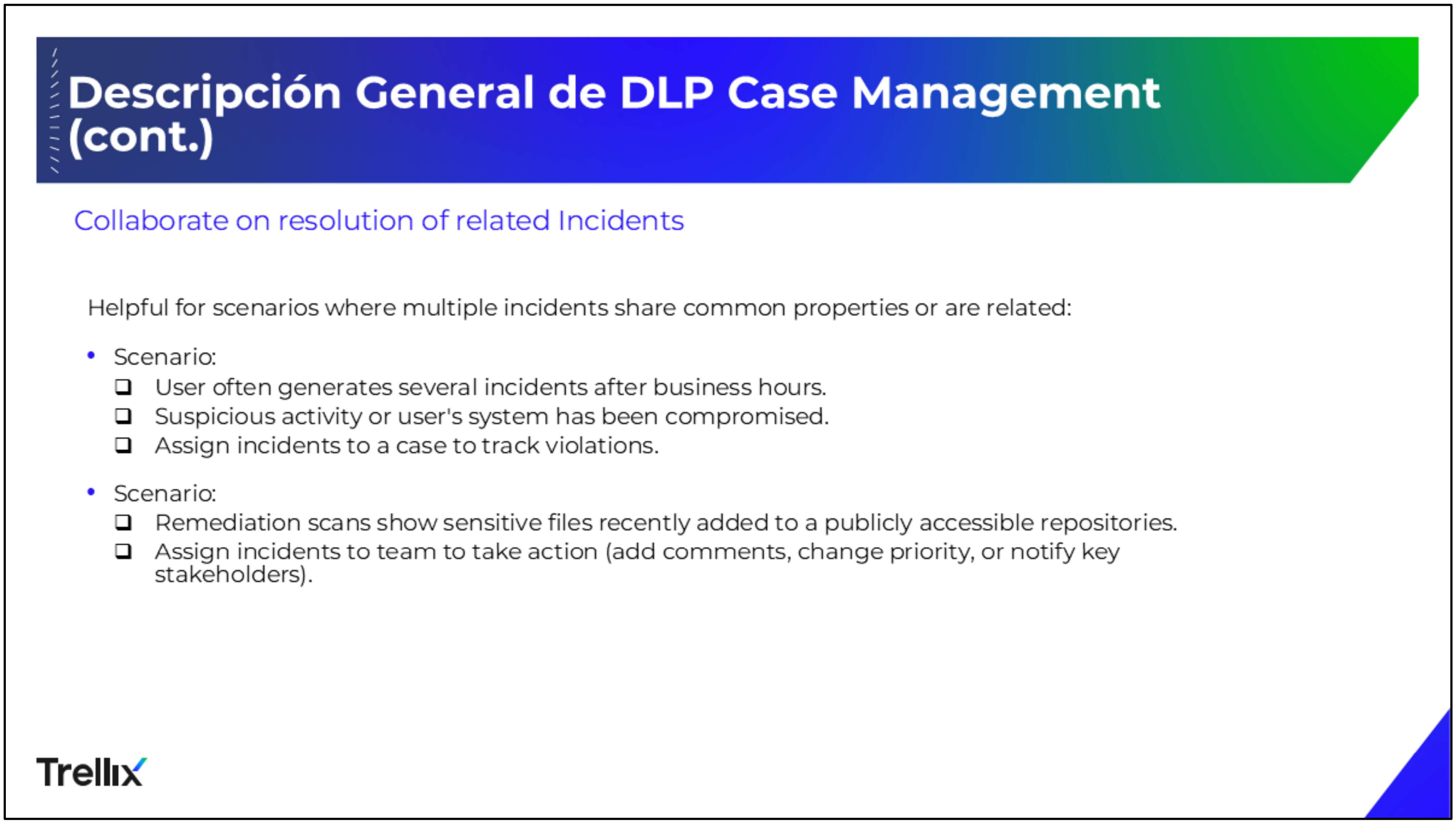
Menu Page > Data Protection



- **DLP Case Management:**
  - ❑ Allows administrators to collaborate on the resolution of related incidents.
  - ❑ Available with DLP 9.4.1 and later.

Trellix

The DLP Case Management feature allows administrators to collaborate on the resolution of related incidents.



Descripción General de DLP Case Management (cont.)

Collaborate on resolution of related Incidents

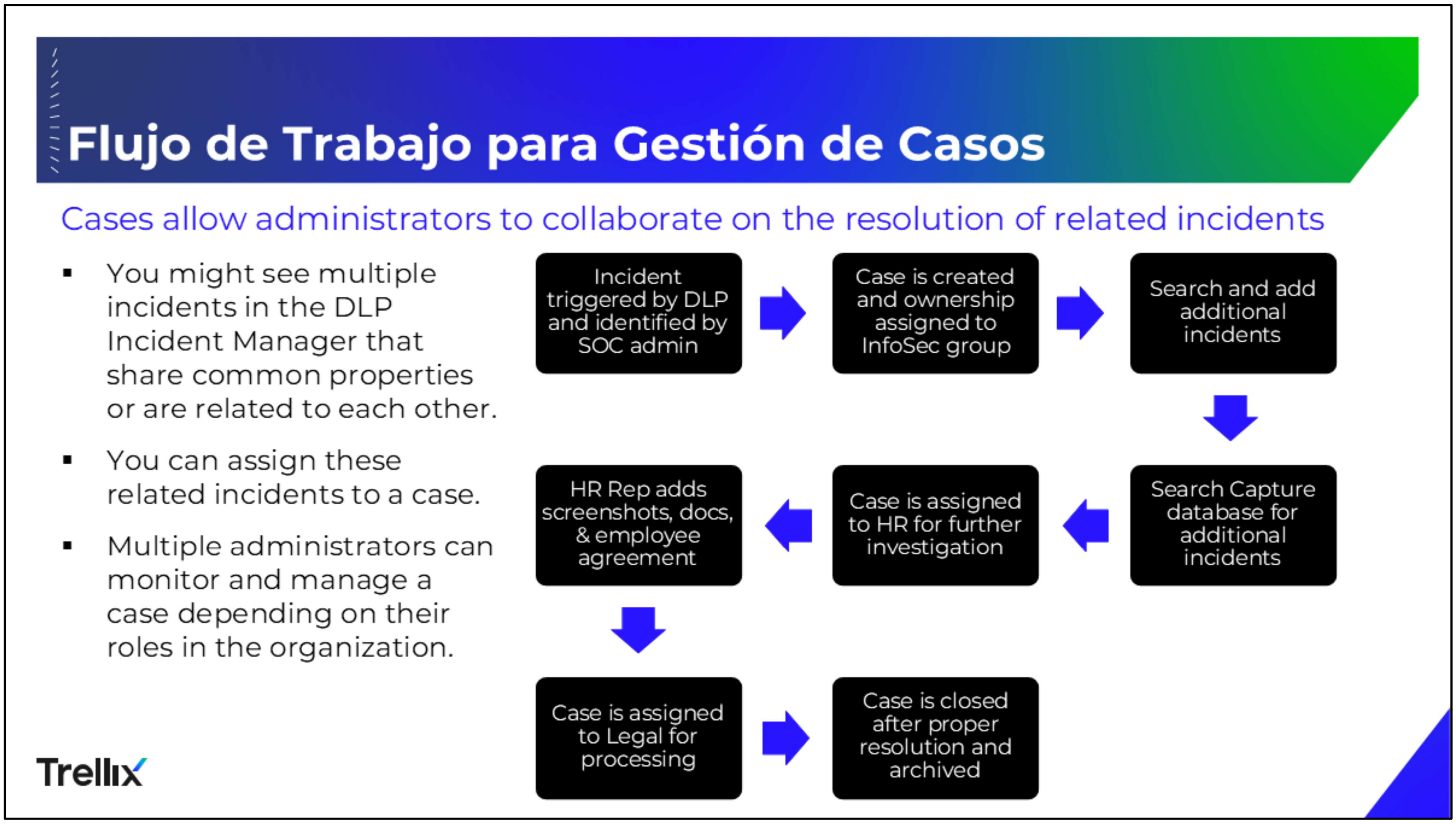
Helpful for scenarios where multiple incidents share common properties or are related:

- Scenario:
  - □ User often generates several incidents after business hours.
  - □ Suspicious activity or user's system has been compromised.
  - □ Assign incidents to a case to track violations.
- Scenario:
  - □ Remediation scans show sensitive files recently added to a publicly accessible repositories.
  - □ Assign incidents to team to take action (add comments, change priority, or notify key stakeholders).

Trellix

Cases allow administrators to collaborate on the resolution of related incidents.
In many situations, a single incident is not an isolated event. You might see multiple incidents in the DLP Incident Manager that share common properties or are related to each other. You can assign these related incidents to a case. Multiple administrators can monitor and manage a case depending on their roles in the organization. As examples:

- **Scenario**: You notice that a particular user often generates several incidents after business hours. This could indicate that the user is engaging in suspicious activity or that the user's system has been compromised. Assign these incidents to a case to keep track of when and how many of these violations occur.
- **Scenario**: Incidents generated from a remediation scan show that many sensitive files were recently added to a publicly accessible repository. Another remediation scan shows that these files have also been added to a different public repository. Depending on the nature of the violations, you might need to alert the HR or legal teams about these incidents. You can allow members of these teams to work on the case, such as adding comments, changing the priority, or notifying key stakeholders.



Flujo de Trabajo para Gestión de Casos

Cases allow administrators to collaborate on the resolution of related incidents

- You might see multiple incidents in the DLP Incident Manager that share common properties or are related to each other.
- You can assign these related incidents to a case.
- Multiple administrators can monitor and manage a case depending on their roles in the organization.

Incident triggered by DLP and identified by SOC admin

Case is created and ownership assigned to InfoSec group

Search and add additional incidents

Search Capture database for additional incidents

Case is assigned to HR for further investigation

HR Rep adds screenshots, docs, & employee agreement

Case is assigned to Legal for processing

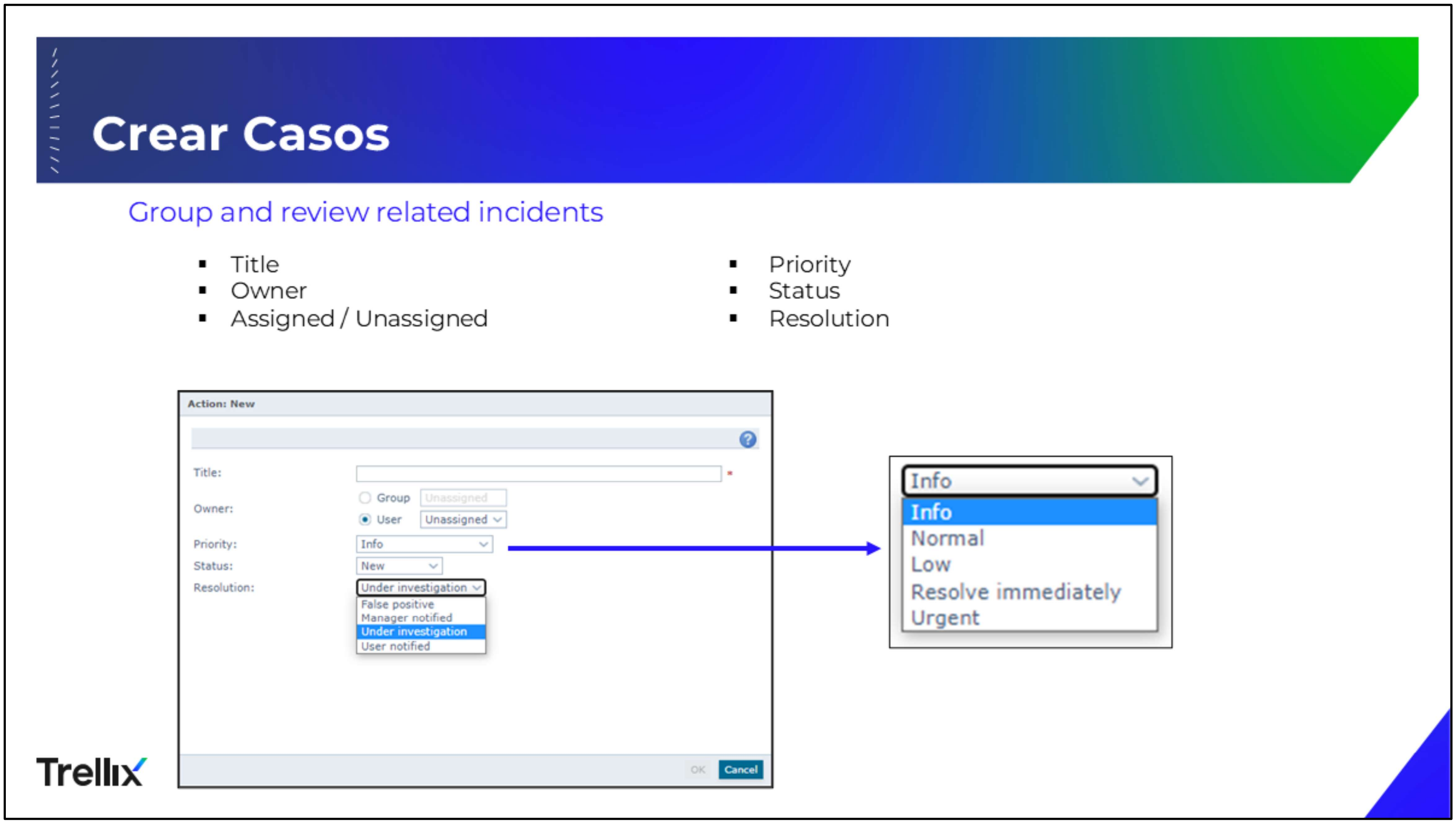
Case is closed after proper resolution and archived

Trellix

Cases allow administrators to collaborate on the resolution of related incidents. In many situations, a single incident is not an isolated event. You might see multiple incidents in the DLP Incident Manager that share common properties or are related to each other. You can assign these related incidents to a case. Multiple administrators can monitor and manage a case depending on their roles in the organization.

Notes:

1. During normal operations, a security specialist identifies an incident from an internal user. The user has emailed a confidential document to an external account.
2. A case is created with the single incident and assigned to the InfoSec group for further research.
3. The InfoSec group looks for any additional incidents in the Incident Manager and adds them to the case.
4. Additional capture searches are performed on the suspect user’s IP address, username, and email address, and additional violations are discovered. These capture database elements and incidents are attached to the case.
5. The case is assigned to the HR group for further processing.
6. HR representative attaches screenshots from the user’s desktop, the relevant employee contract, and additional evidence to the case.
7. The case is assigned to Legal for final remediation actions – In this case, an interview with the employee, Legal, and HR to determine further actions.
8. The case is closed and archived for future reference.



Crear Casos

Group and review related incidents

- Title
- Owner
- Assigned / Unassigned
- Priority
- Status
- Resolution

Action: New

Title:

Owner: ○ Group Unassigned

● User Unassigned

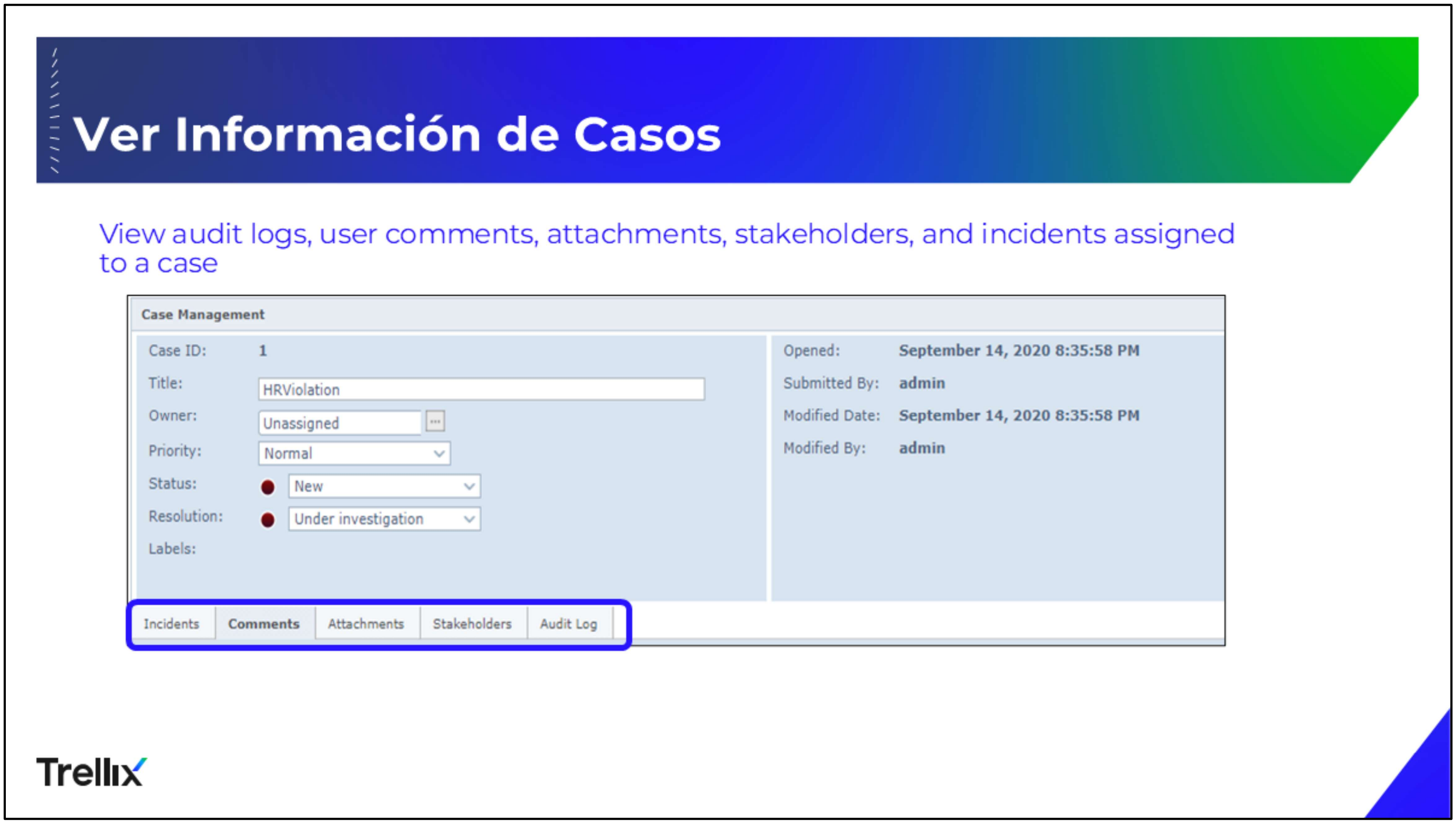
Priority: Info

Status: New

Resolution: Under investigation

To create a case to group and review related incidents, complete these steps from the ePO console.

1. From the menu page, select **Data Protection** > **DLP Case Management**.
2. Select **Actions** > **New**.
3. Type a title name and configure the options.
4. Click **OK**.



Ver Información de Casos

View audit logs, user comments, attachments, stakeholders, and incidents assigned to a case

Case Management

Case ID:	1
Title:	HRViolation
Owner:	Unassigned
Priority:	Normal
Status:	● New
Resolution:	● Under investigation
Labels:	

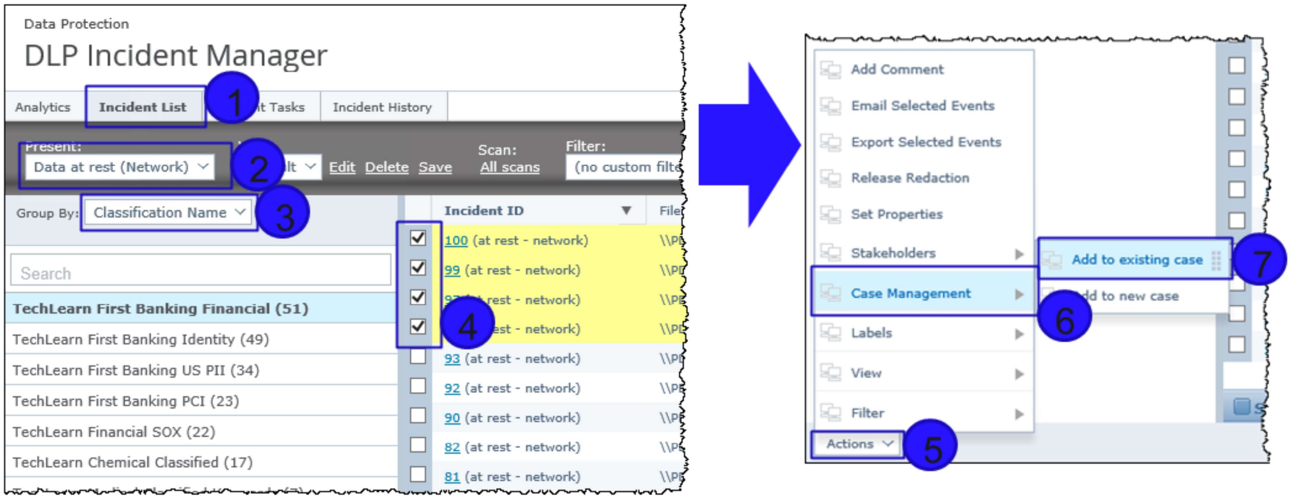
Opened:	**September 14, 2020 8:35:58 PM**
Submitted By:	**admin**
Modified Date:	**September 14, 2020 8:35:58 PM**
Modified By:	**admin**

To **View case** information:

1. In ePO, select **Menu** > **Data Protection** > **DLP Case Management**.
2. Click on a case ID.
3. Perform any of these tasks.
    - To view incidents assigned to the case, click the **Incidents** tab.
    - To view user comments, click the **Comments** tab.
    - To view attachments to the case, click the **Attachments** tab.
    - To view stake holders' information, click the **Stakeholders** tab.
    - To view the audit logs, click the **Audit Log** tab.
4. Click **OK**.

Asignar Incidentes a un Caso

Add related incidents to a new or existing case



Trellix

*Use options such as **Filter** or **Group By** to show related incidents. To update all incidents displayed by the current filter, click **Select all in this page**.*

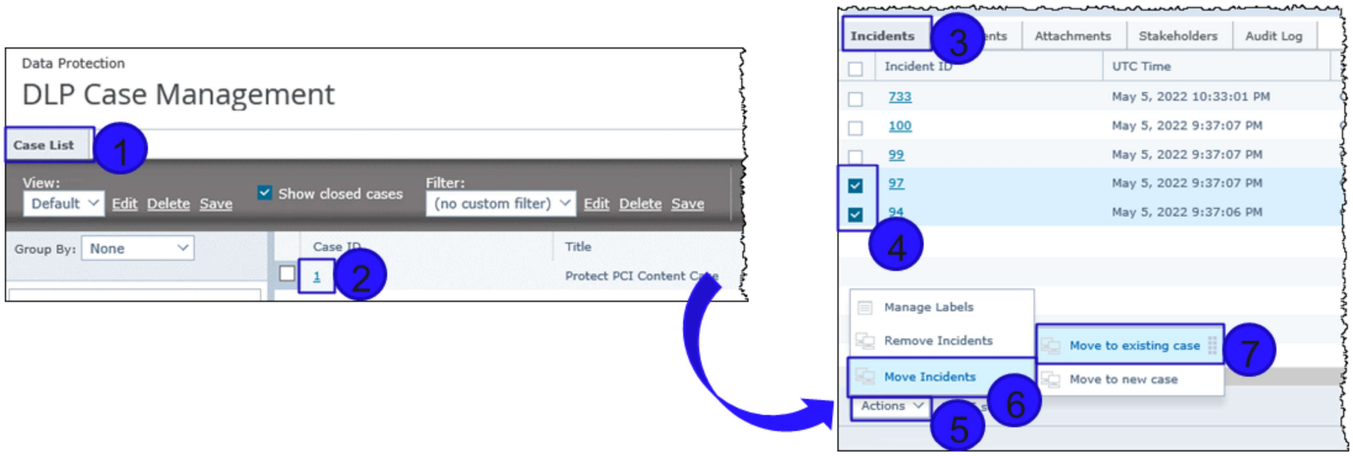
To add related incidents to a new or existing case:

1. In Trellix ePO, select **Menu** > **Data Protection** > **DLP Incident Manager**.
2. From the **Present** drop-down list, select an incident type. For **Data at rest (Network),** click the **Scan** link to set the scan if needed.
3. Select the checkboxes of one or more incidents.

   Note: Use options such as **Filter** or **Group By** to show related incidents. To update all incidents displayed by the current filter, click **Select all in this page**.
4. Assign the incidents to a case.
   - To add to a new case, select **Actions** > **Case Management** > **Add to new case**, enter a title name, and configure the options.
   - To add to an existing case, select **Actions** > **Case Management** > **Add to existing case**, filter by the case ID or title, and select the case.
5. Click **OK**.

Mover o remover incidentes de un caso

Move or remove irrelevant incidents



*You can also move or remove one incident from the **Incidents** tab by clicking **Move** or **Remove** in the **Actions** column*

Trellix

If an incident is no longer relevant to a case, you can remove it from the case or move it to another case.

1. In Trellix ePO, select **Menu** > **Data Protection** > **DLP Case Management**.
2. Click a case ID.
3. Perform any of these tasks.
   - To move incidents from one case to another:
     1. Click the **Incidents** tab and select the incidents.
     2. Select **Actions** > **Move**, then select whether to move to an existing or new case.
     3. Select the existing case or configure options for a new case, then click OK.
   - To remove incidents from the case:
     1. Click the Incidents tab and select the incidents.
     2. Select Actions > Remove, then click Yes.
     3. Click OK.

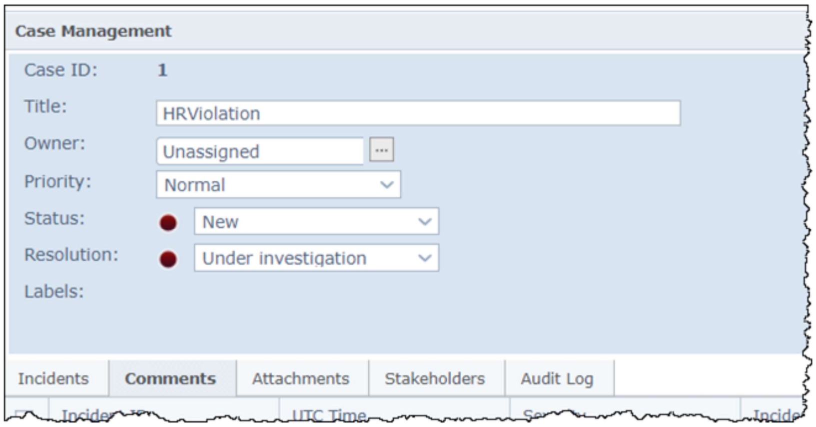
Note: You can also move or remove one incident from the **Incidents** tab by clicking **Move** or **Remove** in the **Actions** column.

Actualización de Casos

Change owner, send notifications, or add comments

Notifications are sent to the case creator, case owner, and selected users when:

- An email is added or changed
- Incidents are added to or deleted from the case
- Case title is changed
- Owner details are changed
- Priority is changed
- Resolution is changed
- Comments are added
- Attachment is added



Case Management

Case ID: 1

Title: HRViolation

Owner: Unassigned

Priority: Normal

Status: ● New

Resolution: ● Under investigation

Labels:

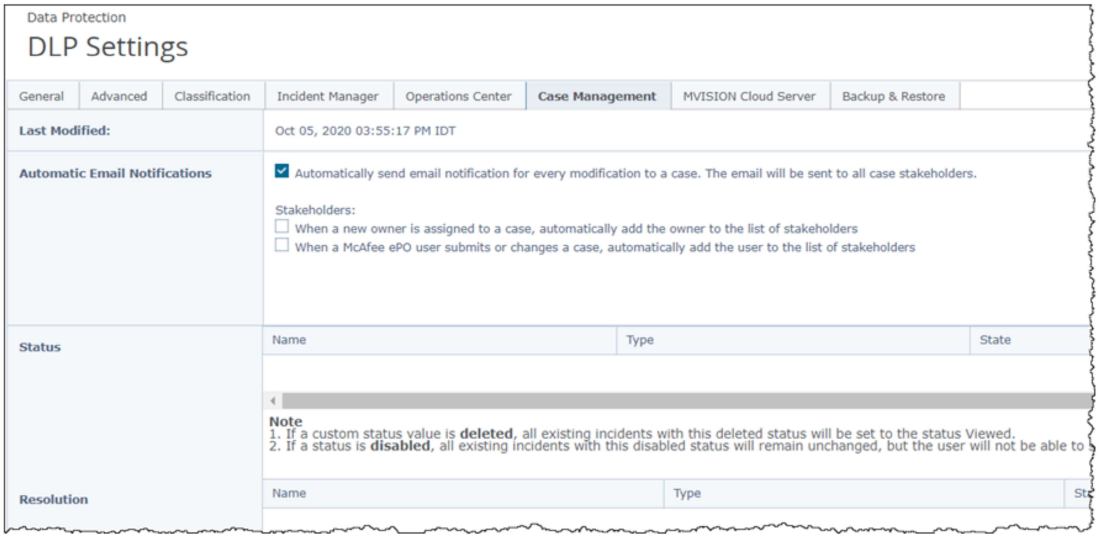
To update case information:

1. In Trellix ePO, select **Menu** > **Data Protection** > **DLP Case Management**.
2. Click a case ID.
3. Perform any of these tasks.
   - To update the case name, in the **Title** field, enter a new name, then click **Save**.
   - To update the owner:
     1. Next to the **Owner** field, click **...**
     2. Select the group or user.
     3. Click **OK**.
     4. Click **Save**.
   - To update the **Priority**, **Status**, or **Resolution** options, use the drop-down lists to select the items, then click **Save**.
   - To add a comment to the case:
     1. Click the **Comments** tab.
     2. Enter the comment in the text field.
     3. Click **Add Comment**.
     4. Click **OK**.

Continued on the next page.

Actualización de Casos (cont.)

Send email notifications



Last Modified: Oct 05, 2020 03:55:17 PM IDT

Automatic Email Notifications

☑ Automatically send email notification for every modification to a case. The email will be sent to all case stakeholders.

Stakeholders:

□ When a new owner is assigned to a case, automatically add the owner to the list of stakeholders

□ When a McAfee ePO user submits or changes a case, automatically add the user to the list of stakeholders

Status

Name	Type	State

Note
1. If a custom status value is **deleted**, all existing incidents with this deleted status will be set to the status Viewed.
2. If a status is **disabled**, all existing incidents with this disabled status will remain unchanged, but the user will not be able to

Resolution

Name	Type	St

Trellix

*You can disable automatic email notifications to the case creator and owner from **Menu** > **Configuration** > **Server Settings** > **Data Loss Prevention***

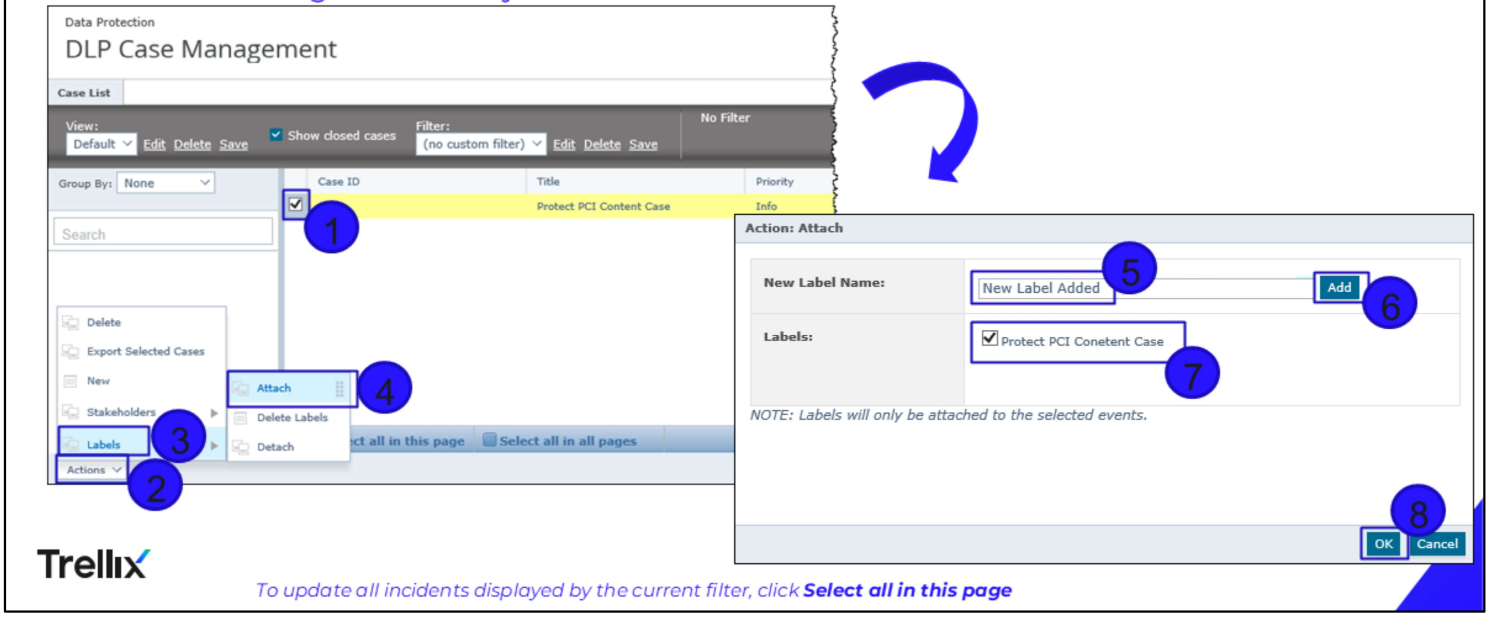
To send email notifications:

1. Next to the **Send notifications to** field, click **...**
2. Select the users to send notifications to.

   Note: If no contacts are listed, specify an email server for Trellix ePO and add email addresses for users. Configure the email server from **Menu** > **Configuration** > **Server Settings** > **Email Server**. Configure users from **Menu** > **User Management** > **Users**.
3. Click **Save**.

Agregar o remover etiquetas de un caso

Use labels to distinguish cases by a custom attribute



View: Default

☑ Show closed cases

Filter: (no custom filter)

Group By: None

☑ Protect PCI Content Case — Info

Action: Attach

New Label Name: New Label Added

Labels: ☑ Protect PCI Conetent Case

NOTE: Labels will only be attached to the selected events.

Trellix

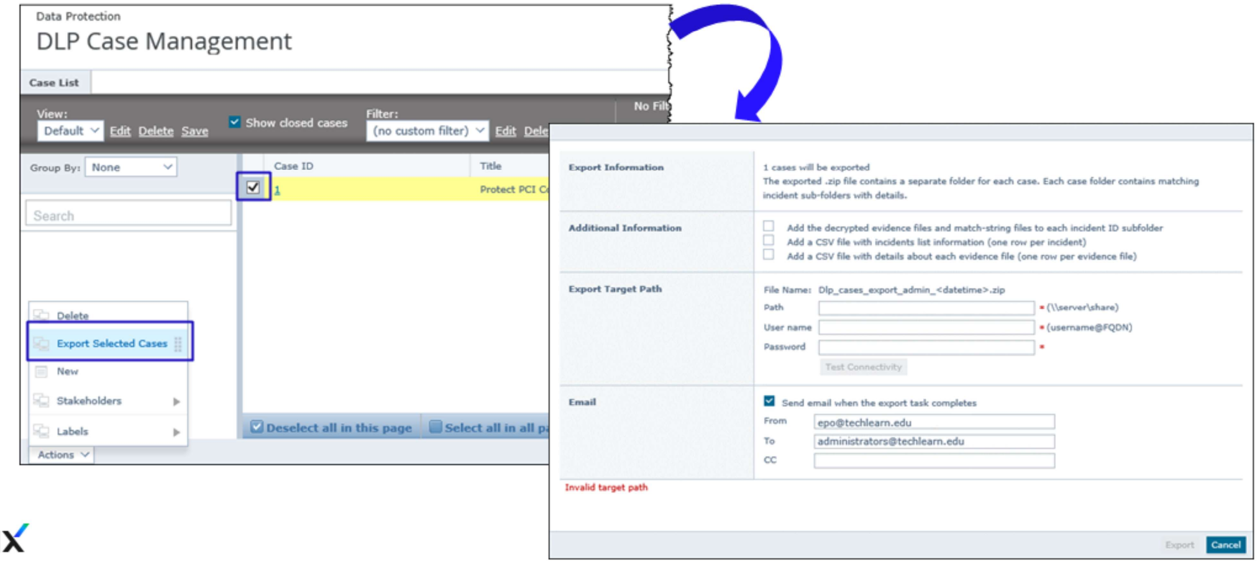
To update all incidents displayed by the current filter, click ***Select all in this page***

To add or remove labels to a case:

1. In Trellix ePO, select **Menu** > **Data Protection** > **DLP Case Management**.
2. Select the checkboxes of one or more cases.
3. Perform any of these tasks.
   - To add labels to the selected cases:
     1. Select **Actions** > **Labels** > **Attach**.
     2. To add a new label, enter a name and click **Add**.
     3. Select one or more labels. The labels will be attached to the selected events.
     4. Click **OK**.
   - To remove labels from the selected cases:
     1. Select **Actions** > **Manage Labels** > **Detach**.
     2. Select the labels to remove.
     3. Click **OK**.

Exportar casos

Export selected events as a zip file



☑ Show closed cases

	Case ID	Title
☑	1	Protect PCI C

Export Information

1 cases will be exported
The exported .zip file contains a separate folder for each case. Each case folder contains matching incident sub-folders with details.

Additional Information

□ Add the decrypted evidence files and match-string files to each incident ID subfolder
□ Add a CSV file with incidents list information (one row per incident)
□ Add a CSV file with details about each evidence file (one row per evidence file)

Export Target Path

File Name: Dlp_cases_export_admin_<datetime>.zip
Path * (\\server\share)
User name * (username@FQDN)
Password *

Email

☑ Send email when the export task completes
From epo@techlearn.edu
To administrators@techlearn.edu
CC

Invalid target path

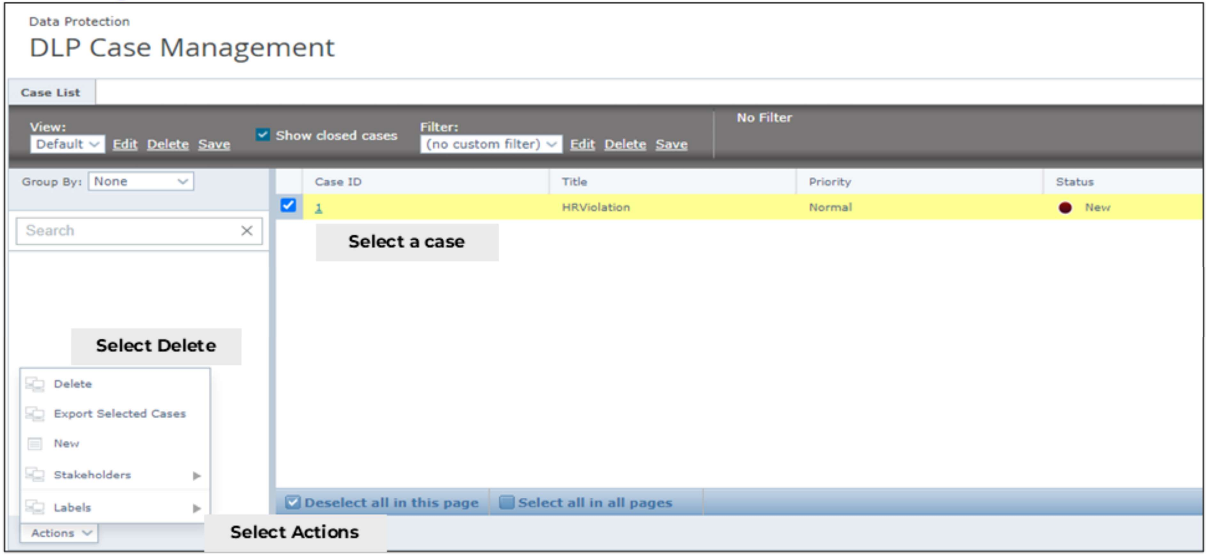
Trellix

To export selected events to a zip file:

1. In Trellix ePO, select **Menu** > **Data Protection** > **DLP Case Management**.
2. Select the checkboxes of one or more cases.
3. Select **Actions** > **Export Selected Cases** > **TBD**.

Borrar Casos

Delete cases no longer needed



☑ Show closed cases

	Case ID	Title	Priority	Status
☑	1	HRViolation	Normal	● New

Select a case

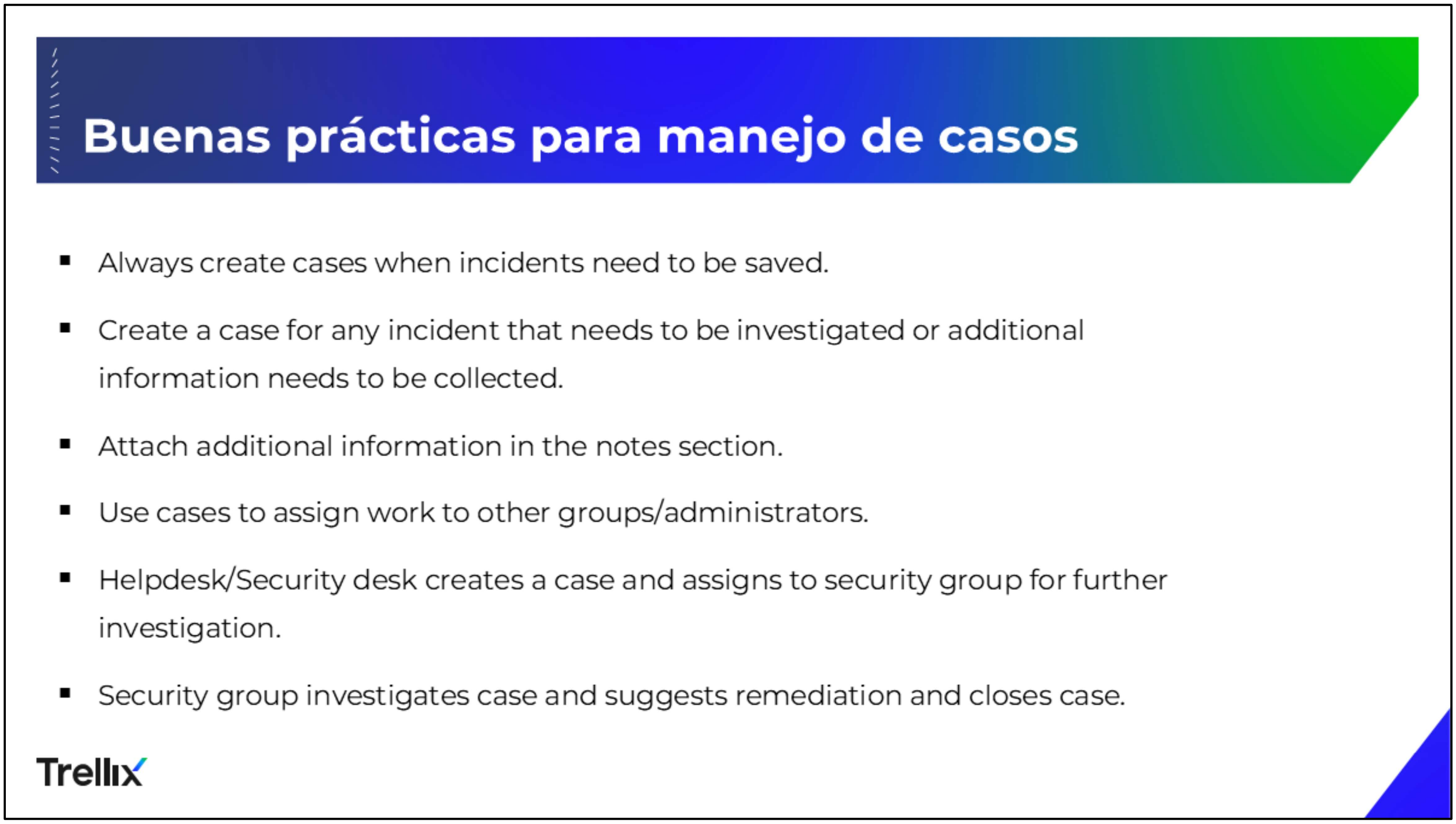
Select Delete

Select Actions

To delete all cases displayed by the current filter, click ***Select all in this page***

To **Delete cases** that are no longer needed:

1. In ePO, select **Menu** > **Data Protection** > **DLP Case Management**.
2. Select the checkboxes of one or more cases.
3. Select **Actions** > **Delete**, then click **Yes**.



Buenas prácticas para manejo de casos

- Always create cases when incidents need to be saved.
- Create a case for any incident that needs to be investigated or additional information needs to be collected.
- Attach additional information in the notes section.
- Use cases to assign work to other groups/administrators.
- Helpdesk/Security desk creates a case and assigns to security group for further investigation.
- Security group investigates case and suggests remediation and closes case.

Trellix