Trellix

Welcome!

Partner Tech Summit – Lisbon

Data Security

AGENDA

- Welcome
- Product Line
- Use Cases
- Demonstration Guidance
- POV Product Deployment / Best Practices / Tuning
- Milestones and Latest Updates
- Trellix Differentiators – Competitive Intelligence
- Q&A

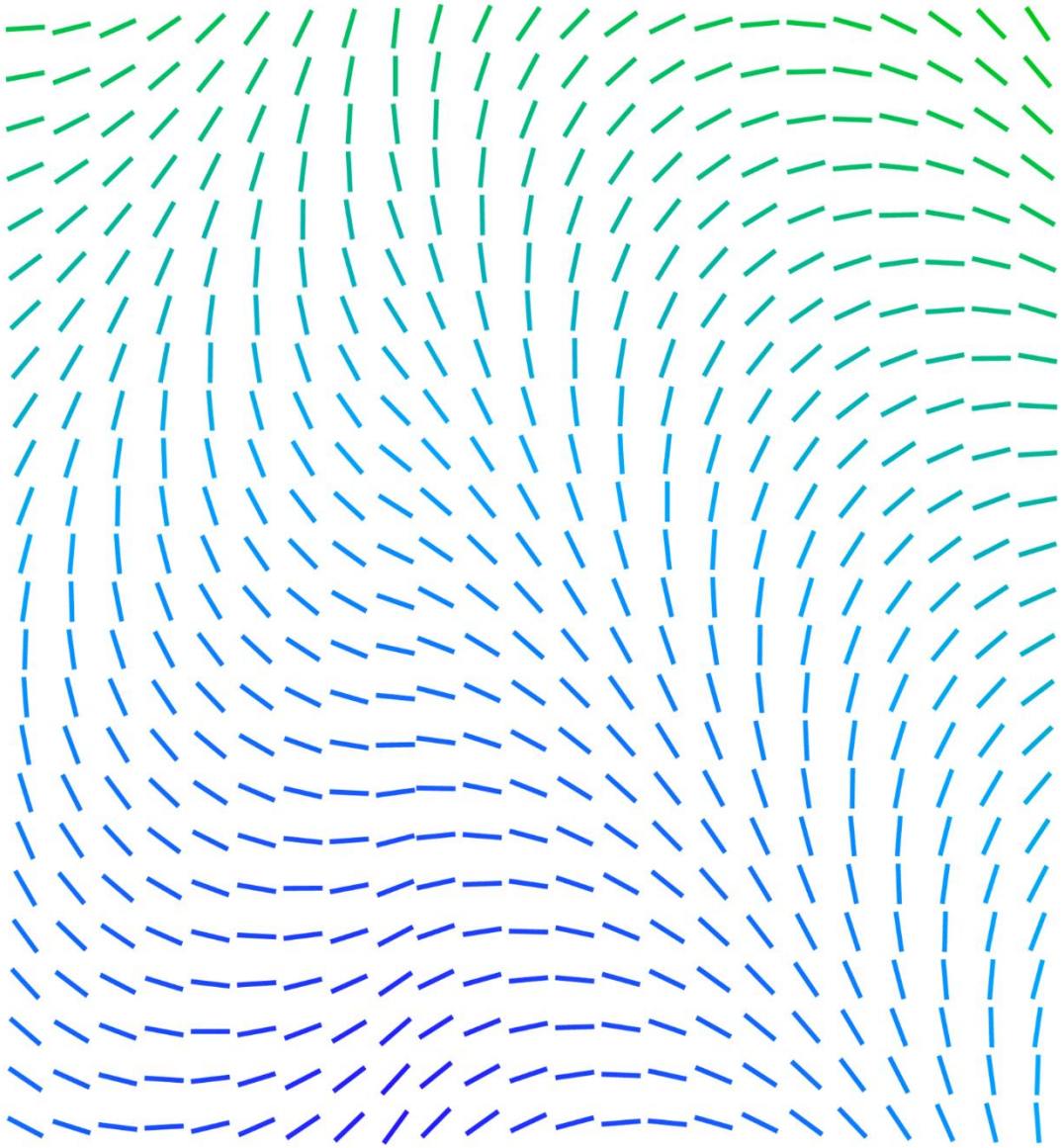
Trellix

Welcome

Trellix

Leon Matthasen

Senior Pre Sales Engineer



Do you know where your data is?

Trellix

Do you know what data is sensitive?

Trellix

How do you protect your sensitive data?

Trellix

Trellix

Product Line

Data Security

Today's Challenges

Insider Risk / Threats
Accidental and Malicious

Regulatory Landscape
Complex and Time Consuming

Expanding Information
Lack of Visibility and Control

Technology Management
Too Many Tools, Too Few People

Ransomware Threats
Data Exfiltration and Policy Updates

Insider Threats

Continue to be a Major Driver of Data Breaches

74% of Breaches

Include a Human Element

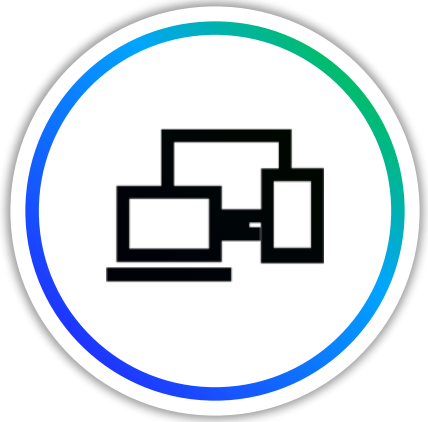
19% of breaches

Driven by Internal Malicious Actors

Top 3 Sources of Compromise

Misdelivery, Miscommunication, Misconfiguration

Top Compromised Assets



Web Apps, Email, Desktop/Laptop

Source: Verizon Data Breach Investigations Report 2023

Trellix

Compliance

One of the Biggest Concerns Across Industries

35% of CISOs surveyed consider ‘changing mandates’ and the legal landscape one of their biggest challenges*

Privacy	Payment Information	Healthcare	Financial Reporting
GDPR	PCI DSS COMPLIANT	HIPAA COMPLIANT HITRUST	SOX

** Trellix - Mind of the CISO Report*

Trellix

Trellix Platform

XConsole

Endpoint Security

Data Security

Cloud Security

Email Security

Network Security

3rd Party Engine

Core Engines

XDR

Advanced Research Center

Product Research

Threat Intelligence

Threat Intelligence & Advocacy

Data Science ML / AI

Research Engineering

Data Lake

Data Security Completes Your XDR

Threat Actors
Nation States
Organized Crime
Hacktivists / Terrorists
Anarchists
Insiders

Motivation
Espionage or Cyber Warfare
Financial Gain
Ideological Causes
Chaos
Disgruntlement

Tactics, Techniques, & Procedures	
Malware	Social Engineering
Phishing	Ransomware
DDoS	Man in the Middle
Exploits	SQL Injection
DNS Attack	APTs

Trellix

XDR Is Not Complete Without Data Security

Objectives

Endzone Defense Around the Attacker's Ultimate Objective…

Your Data

Trellix

What's Needed for Data Security

Data Loss Prevention

- Discovery and Classification
- Compliance Policies
- User Coaching
- Real-time Visibility
- Detection
- Reporting
- Open Architecture
- Centralized Management

Data Encryption

- Files / Data Protected Anywhere
- Compliance Reporting
- Bitlocker & FileVault Centralized
- Removable Media
- Unified Management
- Seamless Login
- Self-Service Recovery
- Integrate with DLP

Database Security

- Database Discovery
- Sensitive Data Discovery
- Block Unauthorized Access
- Address Vulnerabilities
- Ensure Performance
- Real-time Monitoring
- Centralized Administration

Trellix

The Future with a Trellix Solution

With Data Security from Trellix, protect the data that matters to your organization.

1) Protected Against Insider Risk
   Prevent Exfiltration and Coach Users

2) Quickly Demonstrate Compliance
   Out of the Box Policies and Reports

3) Visibility Across Data Storage
   Discovery and Classification, 400+ Content types

4) Streamlined Tools & Event Handling
   Unified Management, Detection and Events

5) Address Ransomware Threats
   Blocking, Integration with Incident Management

Trellix

Trellix Data Security

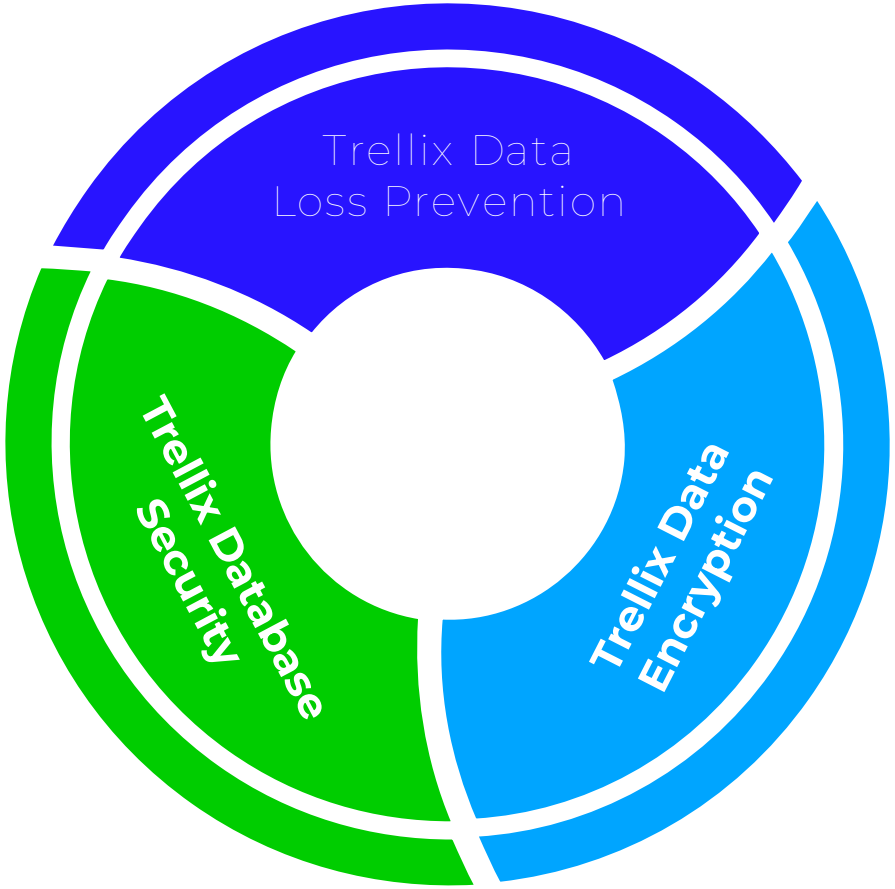
Protect the Data that Matters

Trellix Data Loss Prevention:

Safeguard against intentional and accidental data leaks.

Trellix Database Security:

Find and defend databases and the information they contain.



Trellix Data Security

Trellix Data Encryption:

Protect enterprise and removable device data.

Trellix

Trellix Data Loss Prevention (DLP)

Safeguard against intentional and accidental data leaks

Before

- Lack of visibility
- Time consuming compliance
- Disconnected systems
- Data events go undetected
- User share sensitive information
- Event handling is slow and uncoordinated
- Unauthorized devices installed on endpoints

How We Help

- Discover 400+ content types
- Out of the box classifications
- Single, unified console
- Open architecture
- Real-time event detection and dashboards
- Users blocked/coached when violating policy
- Workflows and automation speed event handling
- Only authorized devices can connect to endpoints

After

- Protecting the data that matters
- Passing audits with ease
- Interconnected ecosystem
- Respond to incidents faster and more effectively
- Fewer data leaks
- Less user policy violations
- More secure environment

Trellix

Trellix Data Loss Prevention - Products

Safeguard against intentional and accidental data leaks

Trellix Data Loss Prevention Endpoint Complete

- Protect workstations and servers (Win and macOS)
- Find sensitive & 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 & 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 Encryption

Protect enterprise and removable device data

Before

- Unprotected enterprise devices and removable media
- No authentication on shared devices
- Unable to demonstrate separation of duties
- Managing Bitlocker and FileVault separately
- Cumbersome login and recovery for users
- Lack of security controls on devices

How We Help

- Enterprise-grade encryption for devices and media
- Multi-user authentication
- Connections to Active Directory
- Enable file and media access for authorized users
- Single console to manage Bitlocker and FileVault
- Seamless login and self service recovery options
- Key management, pin activation on devices

After

- Enterprise devices and removable media protected
- Prove encryption status easily
- Enforce policies encryption at scale
- Comply with access controls
- Lower administrative burden
- A better, more secure end user experience with less burden on administrators

Trellix

Trellix Data Encryption Products

Protect enterprise and removable device data

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 Database Security

Find and defend databases and the information they contain

Before

- Rogue and unprotected databases
- PII like payment data unprotected
- Any user can access database information
- Databases contain unpatched vulnerabilities
- Misconfigurations and code issues impacting performance
- No visibility when a violation of policy occurs

How We Help

- Databases found and protected
- Identify where PII resides in databases
- Manage user access to databases
- Block attempts to access sensitive information
- Scan, patch and secure databases quickly
- Perform regular checks of database health
- Alert on abnormal database usage

After

- Visibility across all databases and into what they contain
- PII and other sensitive data secure
- Meet compliance standards for user access
- Up to date on database patches
- Optimize database performance
- Potential data breaches identified quickly

Trellix

Trellix Database Security

Find and defend databases and the information they contain

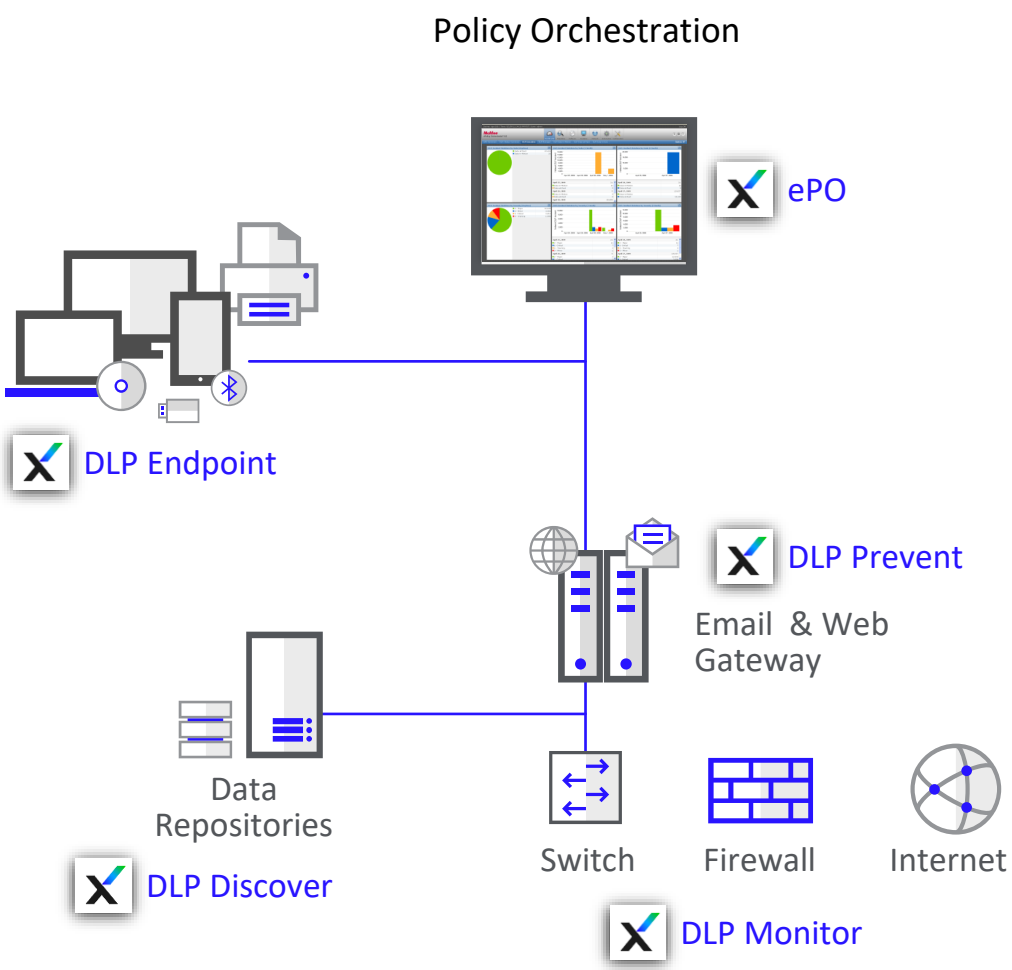
- Find rogue databases
- Get comprehensive data discovery
- Manage user access to sensitive information
- Block unauthorized access
- Address vulnerabilities
- Prevent data breaches
- Report on compliance
- Monitor database health
- Identify misconfigurations, code issues and other errors

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.

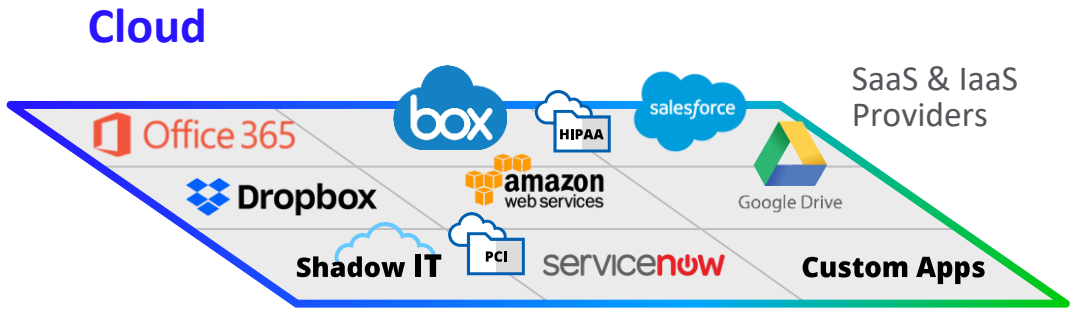
Trellix

Protect Data Wherever it Resides

Native Capabilities



Partner Integration



Trellix

Trellix DLP solution

Cover Endpoints, Networks, and Cloud Environments

Trellix ePO

Trellix ePolicy Orchestrator

- Central web based administration console for all Trellix products
- Enterprise class – highly scalable - RBAC
- DLP Policy is created here and pushed out to various control points
- Incidents are aggregated here for and available for analysis
- Powerful reporting engine

Trellix

Trellix DLP Classification

Identify and track sensitive content

Manual	Allow end-users to manually classify documents
Automatic	Content & Context based automatic classification
Fingerprint	Structured / Unstructured data fingerprint
	Exact Data Matching
3rd Party Integrations	Integrate with MIP, Titus, Bolden James

Trellix

Trellix DLP solution

Cover Endpoints, Networks, and Cloud Environments

Endpoint Data Protection

DLP Endpoint Agent

- Covers Windows and Macintosh platforms
- Policy is enforced even when system is disconnected.
- Vectors Covered: Email, Web, Cloud, Removable storage, Network transfers, Printing, Clipboard, Screen Capture
- Local discovery of File system and Mailboxes
- Provides for User Coaching dialogs
- Provides more visibility & Control than network can, due to proximity to data origin.

Trellix

Trellix DLP Endpoint

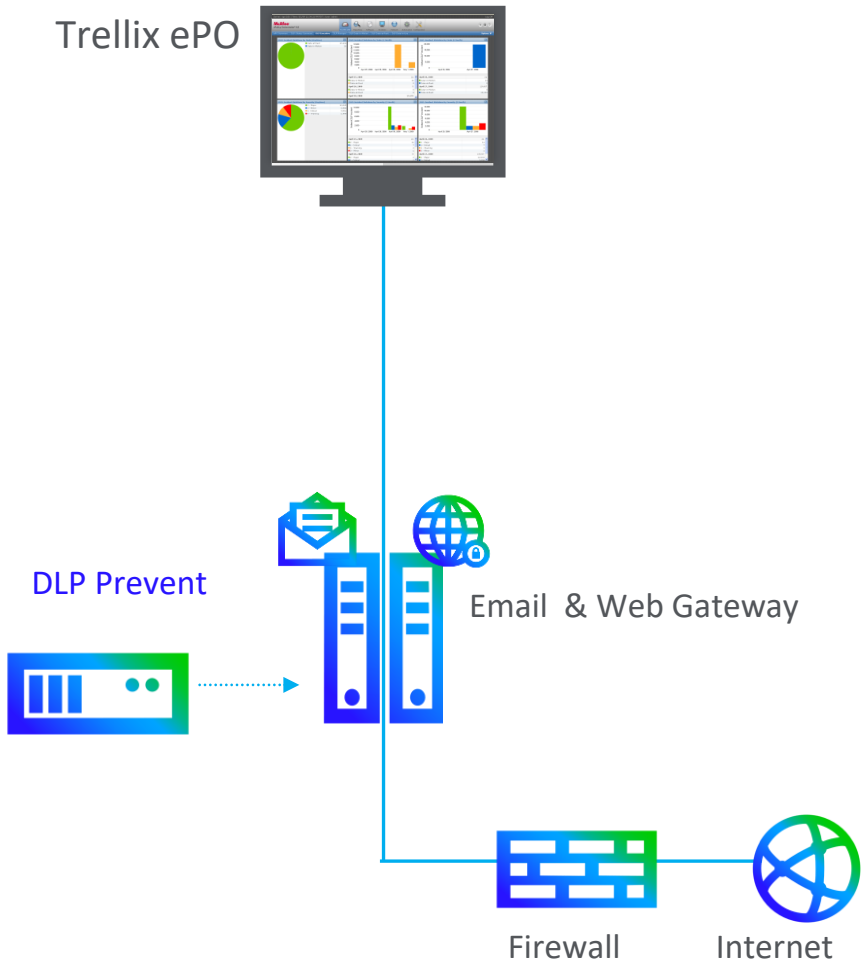
Extend Your Data Security to the Endpoint

Device Control	Prevent unauthorized external devices connecting to your corporate network
Protect data loss	Monitor & Protect sensitive data such as PCI, PII, and PHI from multiple endpoint vectors
Discover sensitive data	Discover sensitive files including OST & PST
User Awareness	Show user notifications providing feedback on their actions, and request business justification when needed

Trellix

Trellix DLP solution

Cover Endpoints, Networks, and Cloud Environments



DLP Prevent

- Network appliance (Hardware or VM)
- Inspects out bound email and Web traffic against your DLP Policy and passes Allow / Block decision to outbound Mail and Web Gateways
- Feeds DLP incidents back to ePO
- Works with any ICAP capable Proxy
- Works with any SMTP mail Gateway
- Can receive SSL Decrypted Session from Proxy for inspection

Trellix

Trellix DLP Prevent

Enforce Network Policies

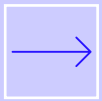
Web

Email

Prevent the movement of sensitive data

Integrate with any commercially available email and web gateway products using SMTP or ICAP.

Add X-RCIS Action headers to emails for gateway to act



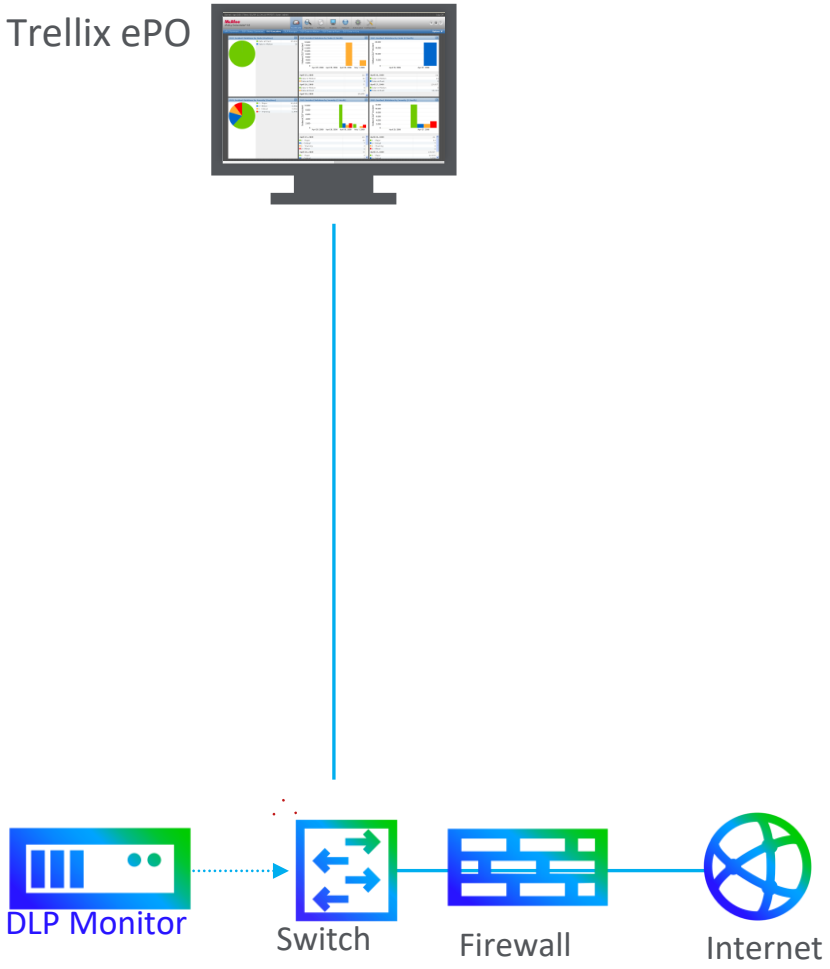
Web gateways get ICAP response action post inspection

Enable capture of every information for forensics & policy finetuning

Trellix

Trellix DLP solution

Cover Endpoints, Networks, and Cloud Environments



DLP Monitor

- Network Appliance (Hardware or VM)
- Passive device that monitors traffic and generates incidents, **but can not block**.
- Receives copy of outbound traffic from switch via a SPAN or TAP.
- Monitors more protocols than Web/Email
- Last line of defense
- Requires upstream SSL Decryption

Trellix

Trellix DLP Monitor

Safeguard vital data

Email

Web

Network

Integrated with egress devices using SPAN or TAP

Analyze network packets for type of data and its content

Supports multiple protocols:

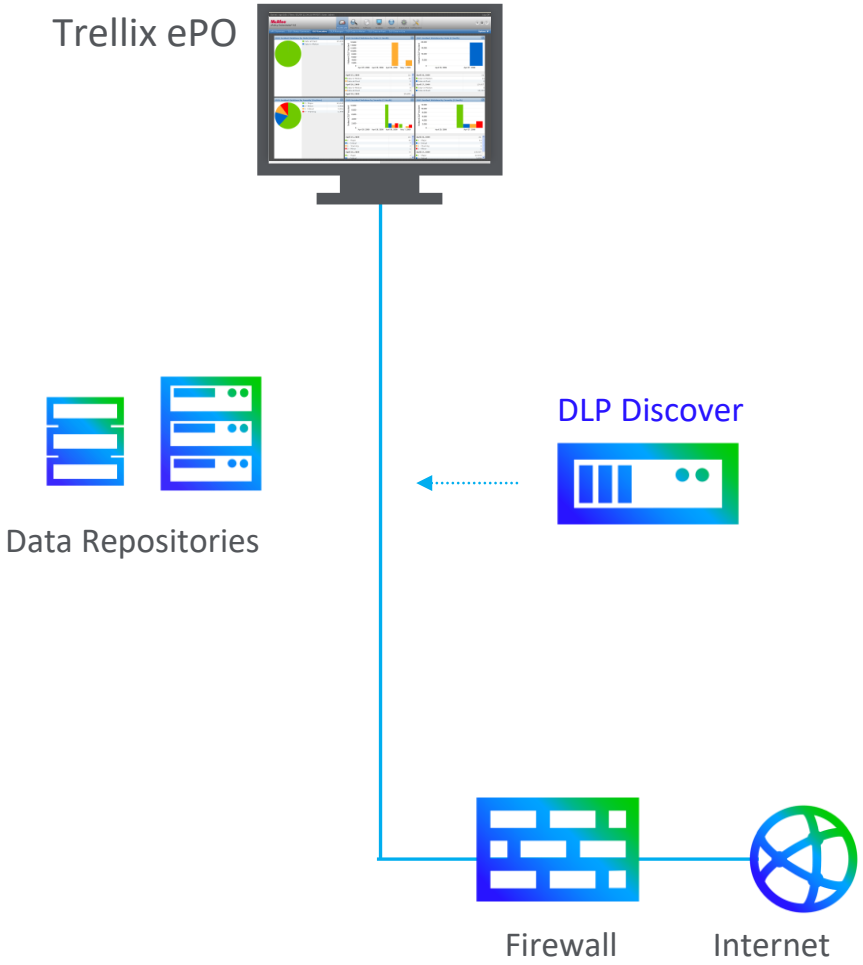
SMTP, IMAP, POP3, HTTP, LDAP, Telnet, FTP, IRC, SMB, SOCKS

Enable capture of every information for forensics & policy finetuning

Trellix

Trellix DLP solution

Cover Endpoints, Networks, and Cloud Environments



DLP Discover

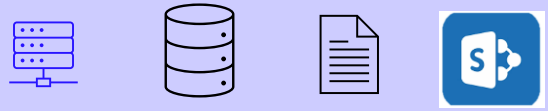
- Software based server deployed to a windows server OS via ePO
- Scans large Data repositories looking for files that match your DLP policy
- Supports CIFS and NFS shares, Sharepoint, MS-SQL, MySQL, Oracle and DB2

- Remediation actions include Report, Copy, Move, Apply Azure Information protection (AIP) tags, Fingerprint, and Apply classification (Tag)

Trellix

Trellix DLP Discover

Discover and protect sensitive data in storage locations

Inventory	 CIFS SQL MySQL SharePoint NFS Oracle DB2 Box
Classify	 Inspect content in files / DB tables to identify sensitive content
Remediate	 Move and encrypt to protect sensitive content from unauthorized locations
Fingerprint	 Scan files to generate fingerprints to be used in protection rules

Trellix

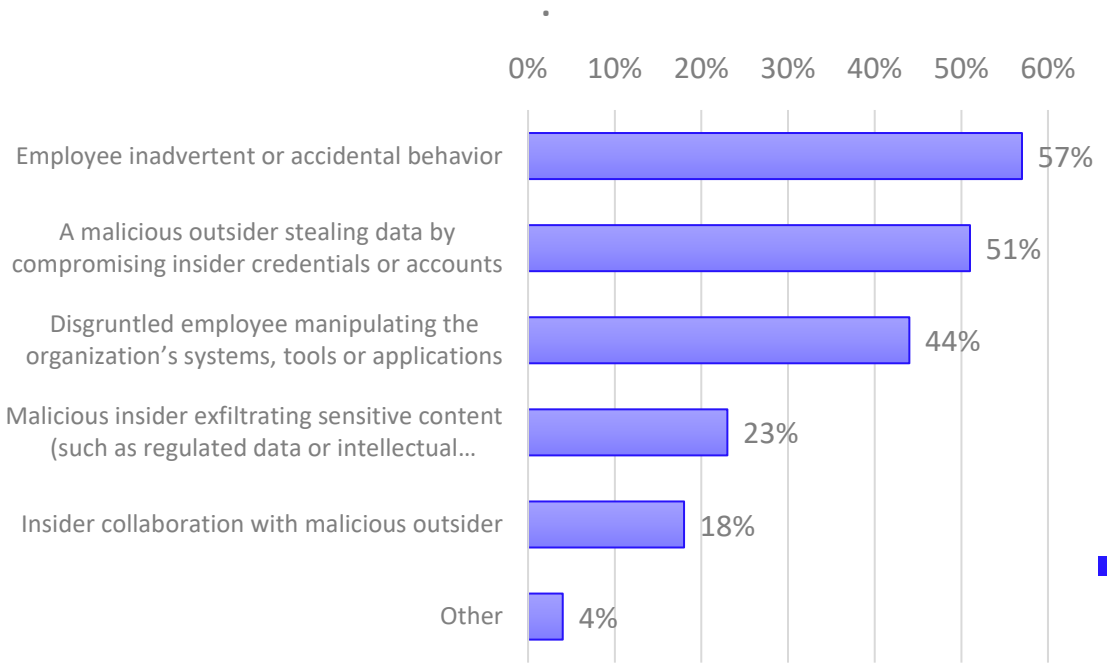
Trellix

Use Cases

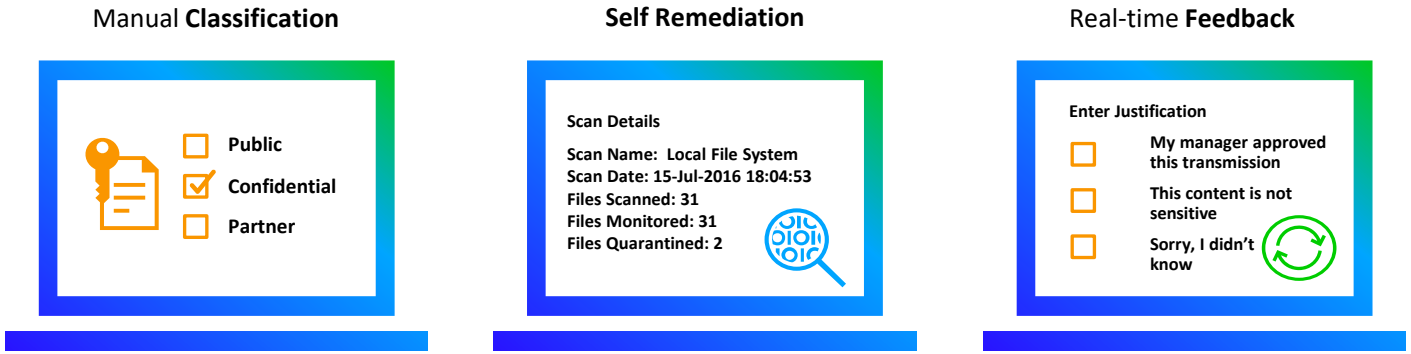
Data Security

Insider Threat

Negligent employees and credential thieves are the root causes of most insider incidents



Trellix allows administrators to coach and monitor end-user Behavior



Reference: 2022 COST OF INSIDER THREATS GLOBAL REPORT by Ponemon Institute

Trellix

Data Privacy

Legislation in 120 countries to secure data and privacy.

- PII
- GDPR
- PCI
- SOX
- And more...

- In-built definitions and rules for quicker visibility and control
- Fingerprinting ensure accurate detection of data
- Detect sensitive text hidden in scanned images, forms, screenshots and embedded graphics
- Discover and monitor across multiple data loss vectors
- Unified console for management, dashboard and reporting

Trellix

Proactive Data Protection

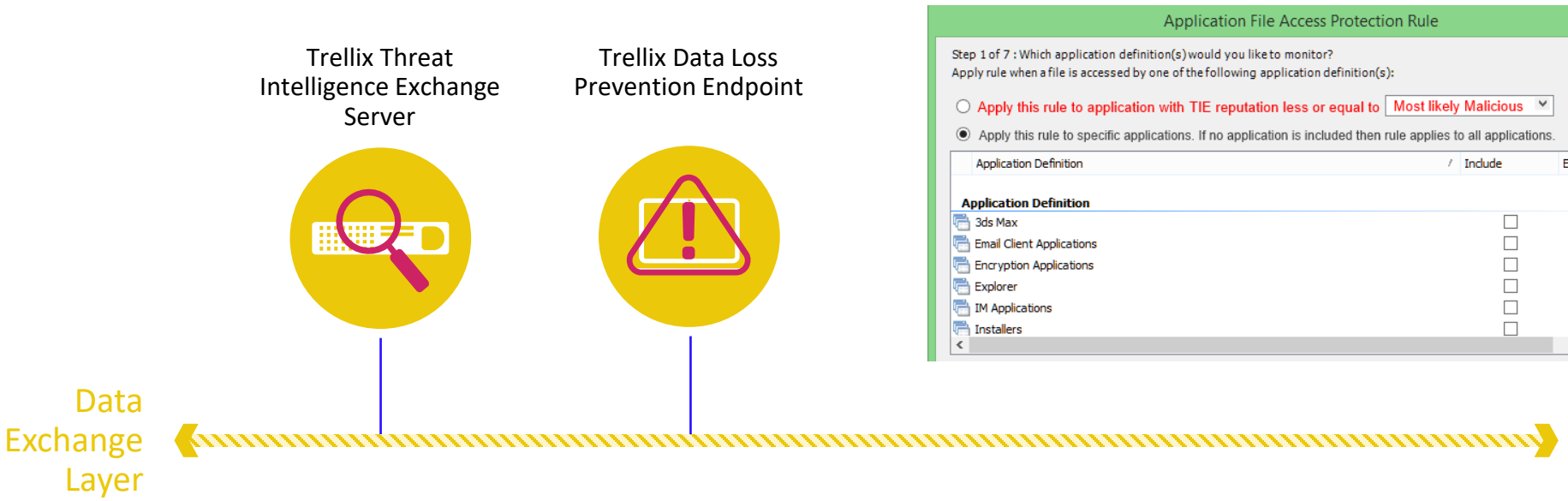
1 DLPE Identifies new process (ProcessA.exe) starts running

2 DLPE post TIE request for ProcessA.exe reputation

3 TIE performs reputation lookup for ProcessA.exe

4 TIE post reply: ProcessA.exe Most Likely Malicious

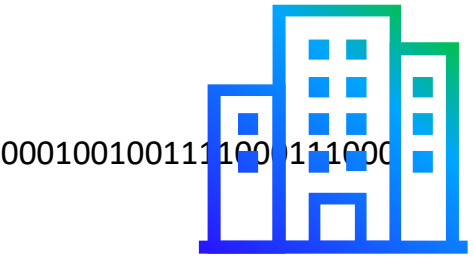
5 DLPE start monitoring ProcessA.exe for Any/Sensitive file access



Trellix

Forensics Capabilities

Forensic and learning ability



Egress

Internet

DLP Policies

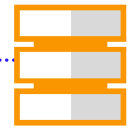
PCI
HIPAA
Intellectual Properties
Acceptable Use

All Matches

Mine data with Google-like search capabilities

Forensic search of historical data

Bonus = Help catch theft of critical data



Traditional Vendor

- False negatives destroyed
- Cannot LEARN and adjust policies
- Assumes you know what to protect

Violations Database

- Pre-set Policies
- Dashboard reports
- Distributed notification of violations and reports

Trellix Capture Database

- Everything captured
- “Information gap” solved
- Ability to LEARN from the past

Trellix

SecOps Use cases

Data Forensics

Trellix DLP Capture database ingests events about every data transfer across the network providing forensic ability

Data Context

With sensitive data classified and identified across multiple egress points, provides the data that is at most risk

User Context

Every user action monitored and logged with source and destination information of sensitive data transfer, identify user risk

Application Risk

DLP endpoint integrated with Trellix Threat Intelligence Exchange (TIE), can stop malicious applications accessing sensitive data

Trellix

Trellix

Demonstration Guidance

Data Security

Demo’s

Trellix

Trellix

POV Product Deployment Best Practices

Data Security

Data Governance & Components

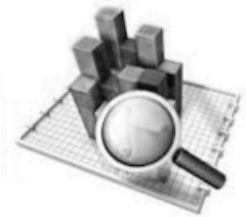
Effective User Behavior Shaping

+

Data Protection Objectives Met

Trellix

DLP Policy Lifecycle



Review

Provide reports and metrics, tune policy as required per business changes.

Plan

Engage Business Unit Owner for Intellectual Property and sensitive date.

Define

Create DLP Policy, implement, monitor and tune policy, create baseline.

Business Remediation

Update business policies as needed, educate employees, create event remediation workflow.

Implement

Modify DLP work flows as needed, enable DLP Policy to ensure identified information is secure.

Trellix

DLP Policy Construction elements

Definitions

Building blocks for policy creation

DATA:

RegEx, Dictionary, Doc properties, File Extension, File information, True File type, Validation Algorithms

SOURCE / DESTINATION:

Application, Network Share, URL List, Email List, User list, Device, File Repositories

Classifications

Use definitions to build out customized logic for identifying data

- Automatic Classification based on
  - Application
  - File location
  - Content Inspection
- Manual Classification
- Content fingerprinting

Protection Rules

Tie classifications to specific protection vectors (email, web, clipboard, Print Screen, Printing, Cloud, Network, etc)

- **Condition** – Match condition for the rule
- **Exception** – Exceptions to the match conditions
- **Reaction** - Expected outcome for the rule

Rule Sets

Collection of related protection rules

- Multiple rules sets can be created and Shared across different DLP Policies.
- Geo specific, Production, Test, Lockdown, Watch list, etc…

DLP Policy

Top level DLP Policy Object associated with a managed system

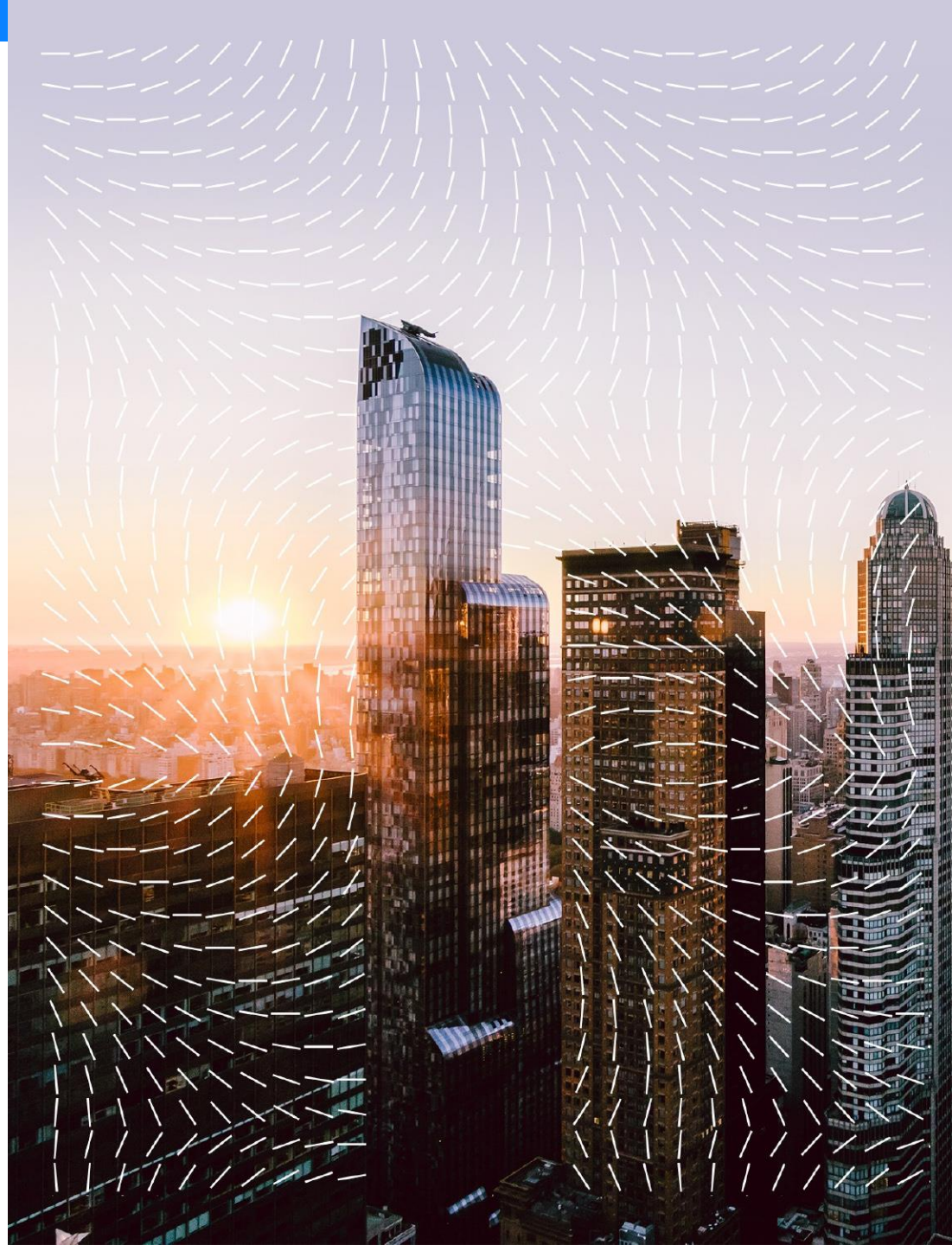
- Can be Assigned to systems or groups via the System Tree.
- Multiple DLP Policies can be configured in ePO
- Can be re-assigned dynamically to a system via System Tags and Policy assignment Rules

Assigned to systems

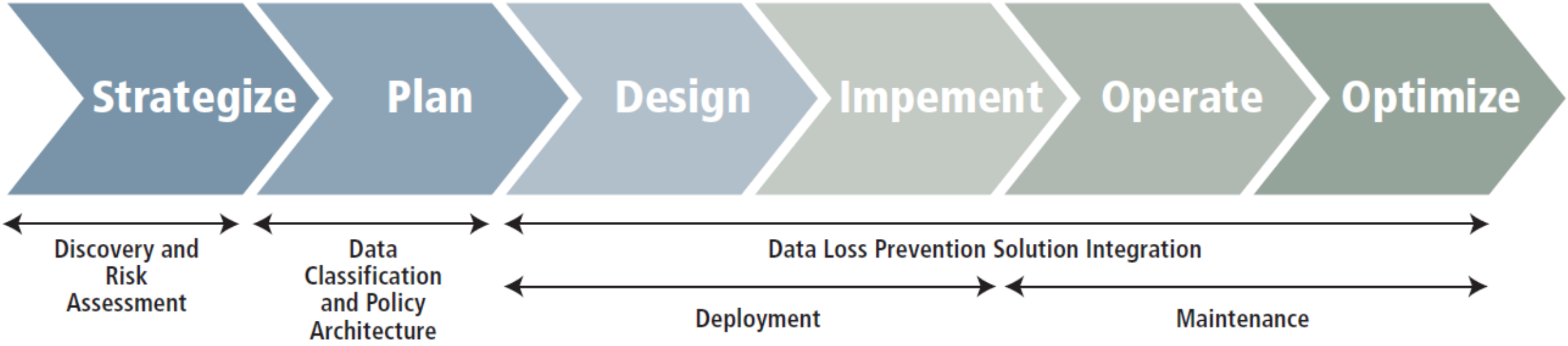
Trellix

Trellix

Implementation Best Practices



Implemention Best Practices Methodology



Trellix

Trellix

Milestones and Latest Updates

Data Security

Trellix

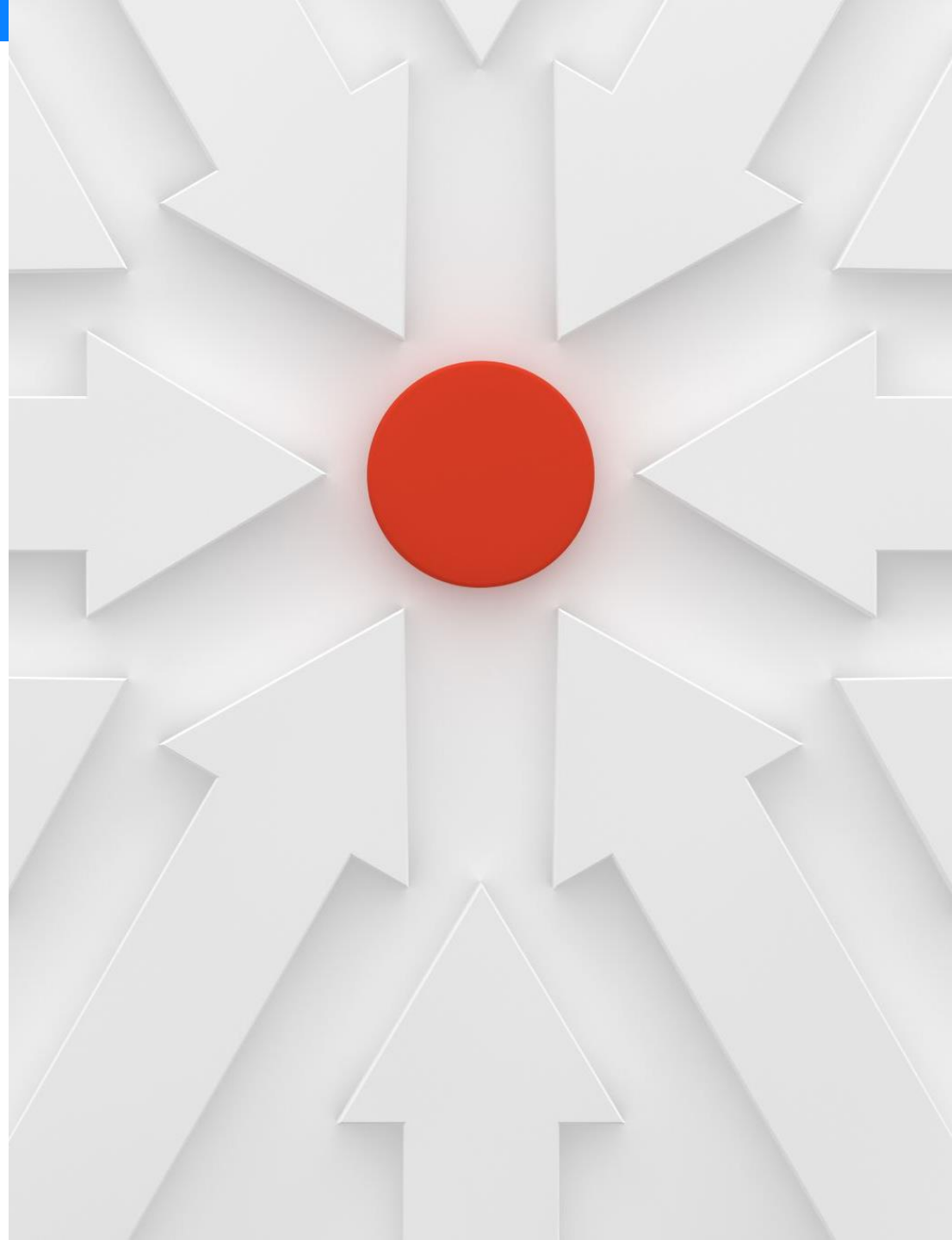
Trellix Differentiators

Data Security

Competitive Landscape

In this module, you will learn about:

1. Competitors to Trellix in the DLP space.
2. Strengths and weaknesses of competitive solutions
3. Objection Handling
4. Key use cases and how we deliver better outcomes



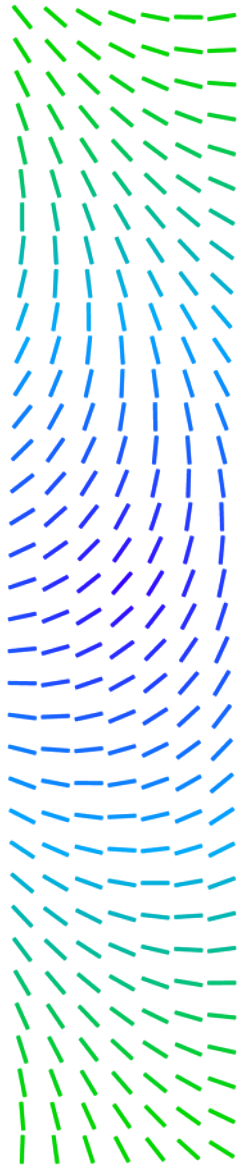
Top Competitors

Microsoft– Platform vendor with DLP capability built into their productivity platform

Broadcom/Symantec – A leading enterprise grade DLP offering serving limited large enterprises

Forcepoint – Secure Service Edge (SSE), DLP and Network Security solutions focusing on User Behavior Analytics (UBA) and Risk-based capabilities.

Trellix – Squarely in the leader's section beating MS with current offering, beating Broadcom/Symantec with strategy, and beating Forcepoint in both.



Trellix

Microsoft Overview

Compliance/Data Governance rebranded “Microsoft Purview”

Unless customer has full E5 licensing is complex

Customers may not know what outcomes they may be solving for based on licensing

Information protection	Microsoft 365 E3	Microsoft 365 E5	Microsoft 365 E5 Compliance[1]
Azure Information Protection Plan 1	•		
Azure Information Protection Plan 2		•	•
Manual, default, and mandatory sensitivity labeling in Office 365	•	•	
Automatic sensitivity labeling in Office 365 apps		•	•
Manual labeling with the AIP app and plugin	•	•	
Automatic labeling in the AIP plugin		•	•
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive		•	•
Sensitivity labels based on Machine		•	•

Data lifecycle management					
Manual retention labels	•	•	•		
Basic org-wide or location-wide retention policies	•	•	•	•	
Rules-based automatic retention policies		•	•	•	
Machine Learning-based retention		•	•		
Teams message retention policies	•	•	•	•	
Records Management		•	•	•	

[1] 30-day minimum retention period. (No maximum retention period.)

eDiscovery and auditing					
Content Search	•	•	•	•	
eDiscovery (Standard) (including Hold and Export)	•	•	•	•	
Litigation Hold	•	•	•	•	
eDiscovery (Premium)		•	•	•	
Audit (Standard)	•	•	•	•	
Audit (Premium)		•	•	•	

Insider risk management					
Insider Risk Management		•	•	•	
Communication Compliance		•	•	•	
Information Barriers		•	•	•	
Customer Lockbox		•	•	•	
Privileged Access Management		•	•	•	

Trellix

Strengths/Weaknesses

Strengths

- Native DLP Capabilities in platform esp. O365
- Perceived low cost of acquisition
- Trainable classifiers, ML
- DLP Integrated with XDR

Weakness

- Limited endpoint functionality
- Weak reporting
- Complex Incident Workflow:
  - Limited context
  - Multiple consoles

Trellix contrasts with:

Trellix DLP is managed by ePO which is an industry leading security IT operations mgmt platform

- Focused on security easier and less complex to achieve outcomes, efficiencies

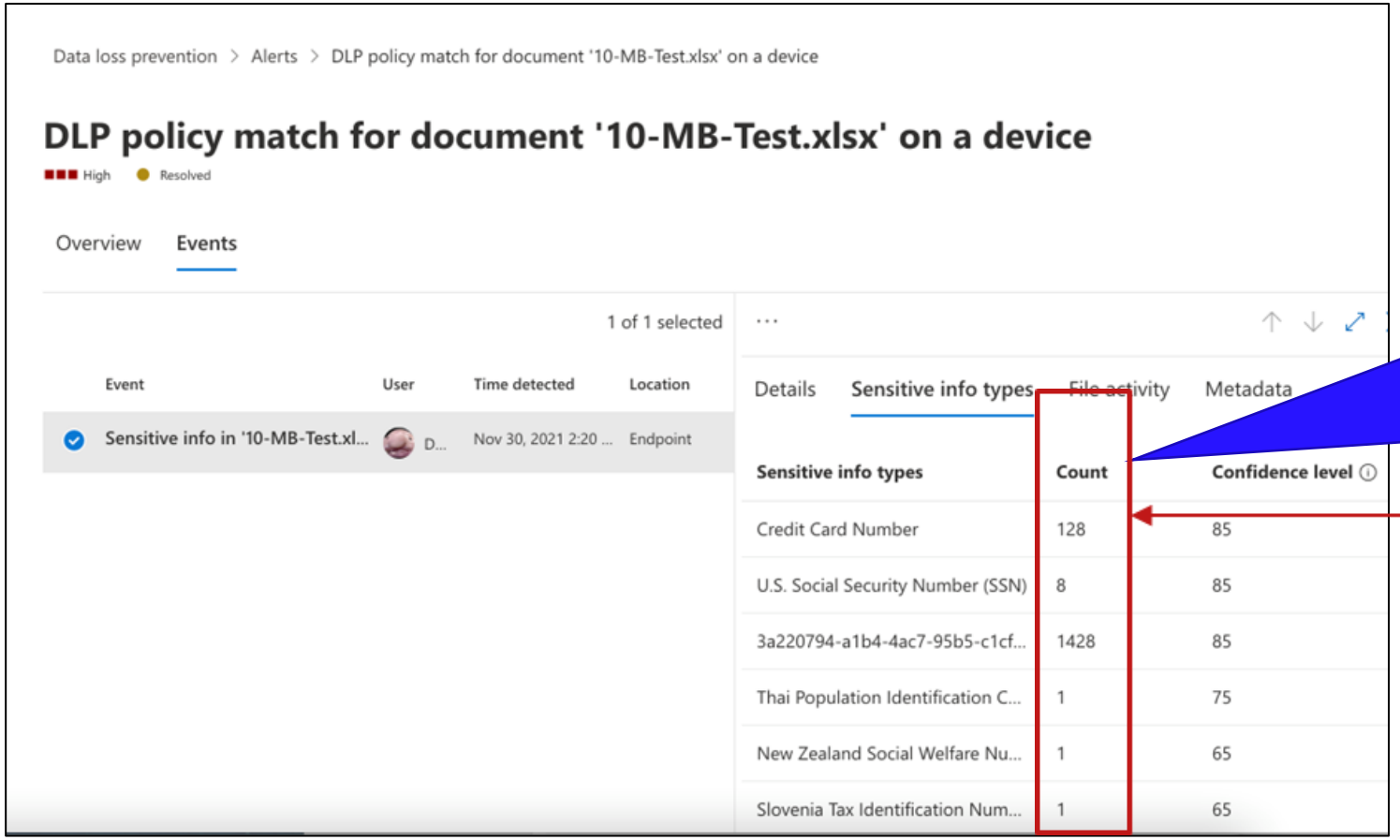
Strong reporting and efficient incident workflows in ePO

Integration with TIE blocks untrusted processes from touching sensitive data

Trellix

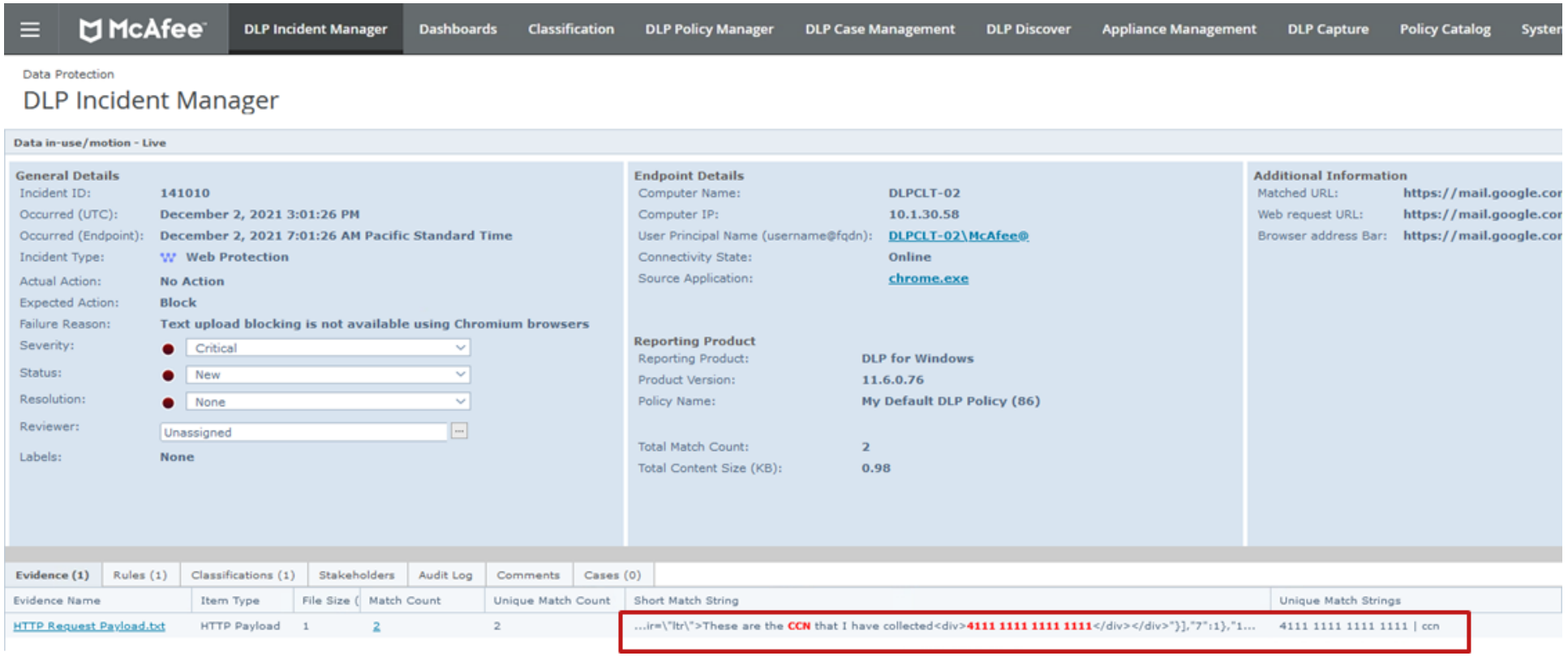
DLP in the SOC - Minimize Time to Respond

Not enough context for responders to understand an Endpoint DLP Incidents



Microsoft Endpoint DLP doesn't provide details about matches or context around the matches, just the number of matches and the confidence level

DLP in the SOC – Minimize Time to Respond



Trellix DLP shows context in Endpoint DLP incidents for quicker situational awareness:

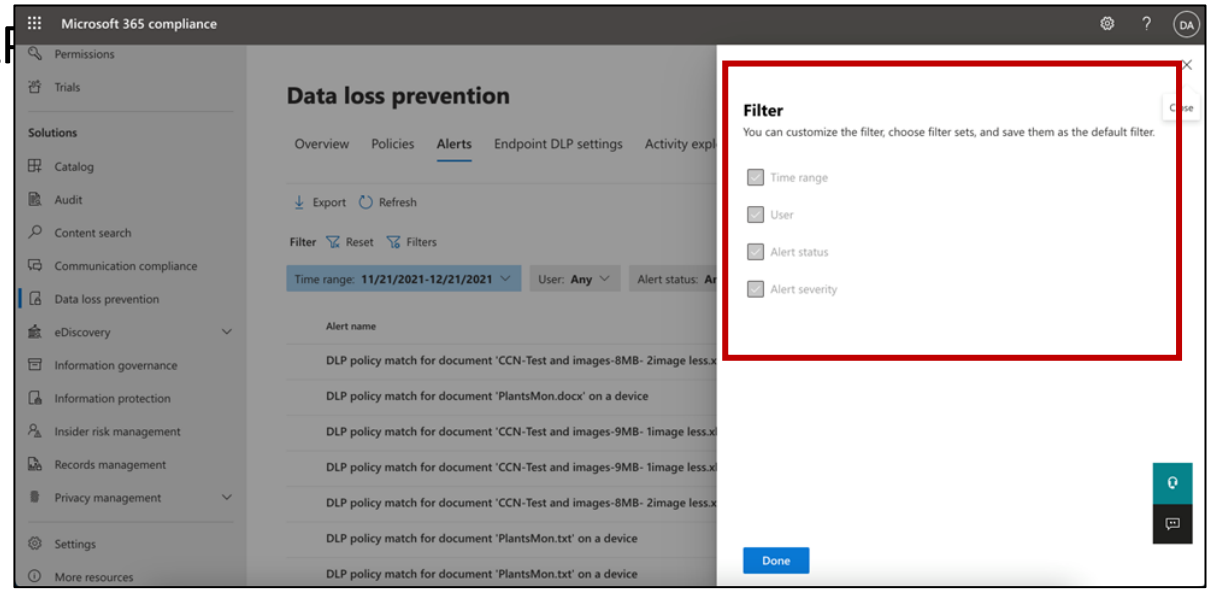
- Policy triggers
- Unique Match Counts, Match Strings, etc . . .

Trellix

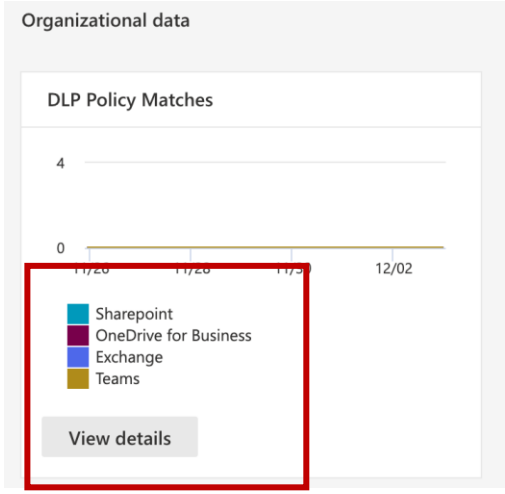
DLP for Privacy, PII, and Compliance - Reporting

Limited reporting for Microsoft Endpoint DLP Alerts

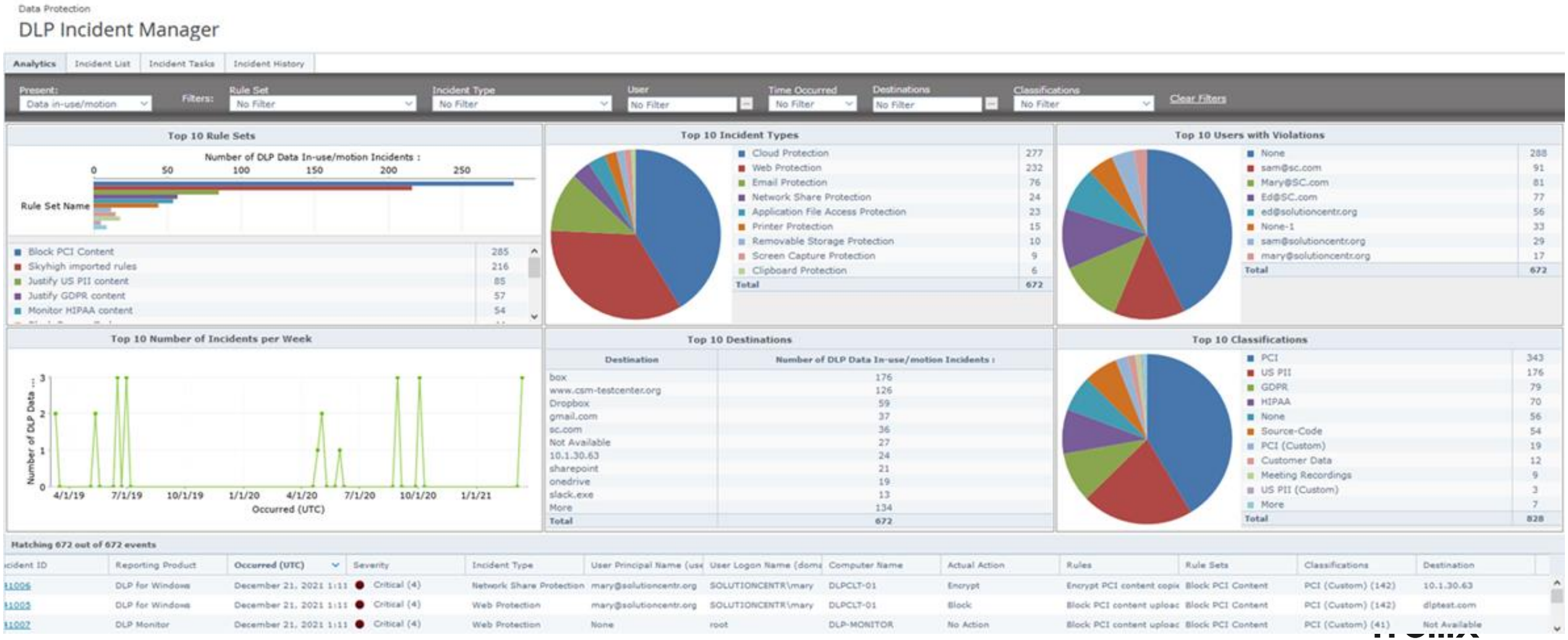
- Does not provide any graphs
- Just filter based on 4 parameters
- Cannot filter by channel
- Not possible to see the user with more alerts



Endpoint DLP incidents do **not appear** in the "Reports" section of M365 Compliance

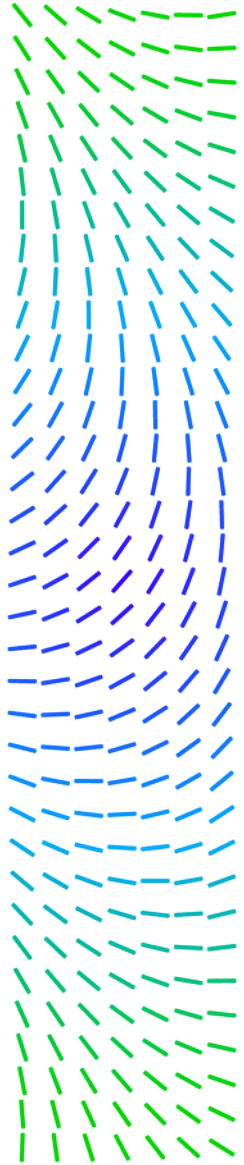


Trellix DLP has Rich and Detailed Reporting



Microsoft Takeaways

Microsoft has a powerful productivity platform	• However built-in security is complex to manage with gaps in coverage
Microsoft licensing is complex, confusion about what DLP outcomes with which license	• Trellix DLP offerings are easy to understand and have broad coverage
Microsoft has integrated DLP into their XDR platform.	• Trellix already has integrations between TIE and DLP for data aware protection as well and will continue to focus on DLP and XDR.



Trellix

Trellix

Broadcom/Symantec DLP Overview

2 DLP offerings: on-prem and cloud

Data Loss Prevention Core Solution

- DLP Endpoint Discover / Prevent
- DLP Network Discover / Protect / Monitor
- DLP Network Prevent for Email / Web
- DLP Sensitive Image Recognition
- Information Centric Analytics

Data Loss Prevention Cloud Solution

- CloudSOC Audit / CASB / Gateway
- DLP Cloud Detection Service
- DLP Cloud Detection for Web Security Service
- DLP for Office 365 Email and Gmail

Trellix DLP Competes with the Core Solution

Skyhigh Security competes with the Cloud Solution

Trellix

Strengths/Weaknesses

Strengths

- Unified management (data channels)
- EDM, IDM, Vector ML (on-prem only)
- Incident workflows

Weakness

- Heavy on-prem requirements
- Weak reporting, additional tool needed
- Shrinking customer base

Trellix contrasts with:

Trellix DLP also has unified management across data channels but is easier to manage with ePO

Strong reporting and efficient incident workflows in ePO

Can support and solve for outcomes in broad customer base, not only the largest enterprises

Trellix
Trellix

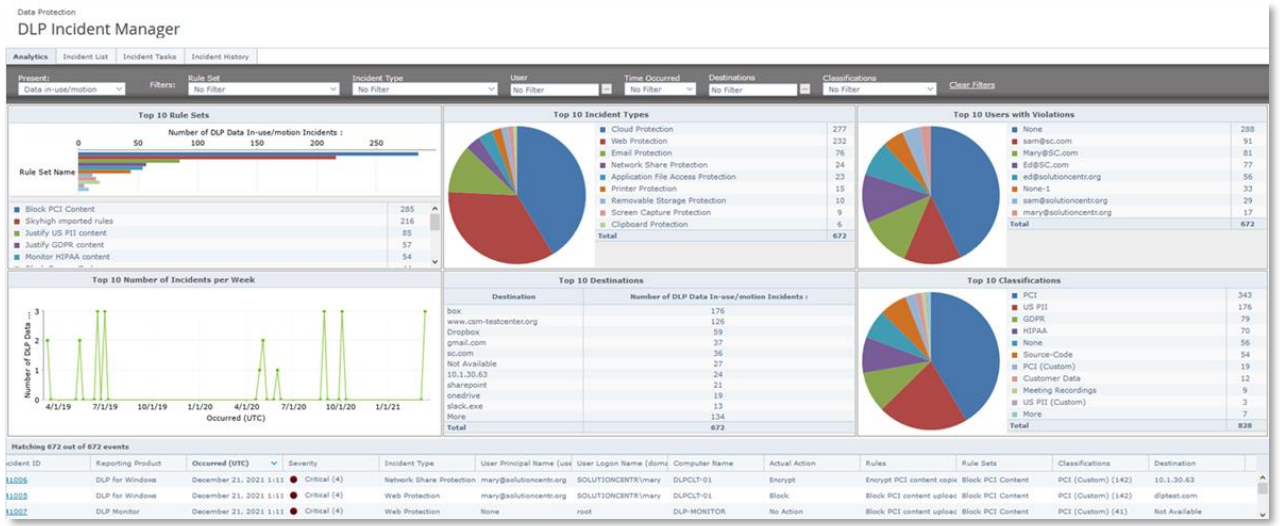
DLP for Privacy, PII, and Compliance

- **How they do it:** Broadcom/Symantec has weak reporting and recommends IT Analytics, a separate reporting tool. This adds complexity to an already heavy and complex deployment.
- **How we do it better:** Trellix DLP provides ability to query all data, regardless of DLP component, natively in ePO

In addition to infrastructure prerequisites, the IT Analytics Server instance requires the following:

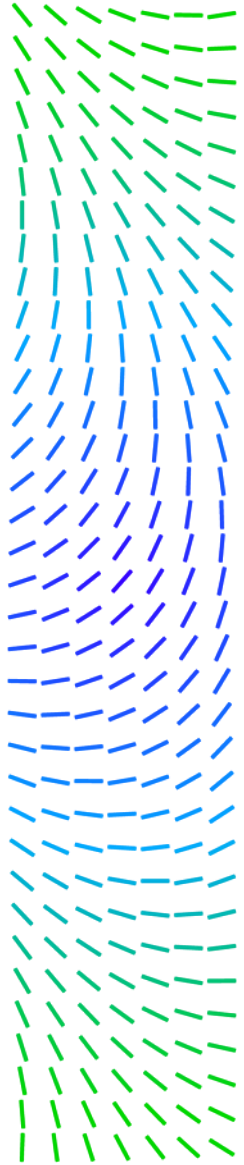
- Microsoft SQL Server 2012 Management Objects 11 For SQL Server 2012
- For SQL Server 2012 Service Pack 1
- Microsoft SQL Server 2012 System CLR Types 11. For SQL Server 2012
- For SQL Server 2012 Service Pack 1
- Oracle Database 11g Release 2 Client (11.2.0.1.0) or later for Microsoft Windows

IT Analytics for Symantec DLP versions 14, 15, and 15.1 require Oracle Database Client (12.1.0.2.0).



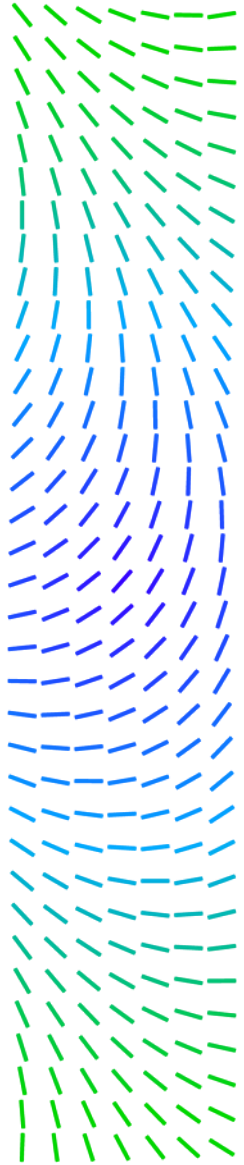
Broadcom/Symantec DLP Takeaways

Symantec has a powerful enterprise DLP offering	• However it is heavy and complex to deploy and manage compared to Trellix with ePO
Symantec has limited reporting requiring additional tools	• Trellix DLP uses comprehensive native reporting in ePO for broad visibility
Symantec customers are dissatisfied with pricing and support since Broadcom acquisition	• Trellix DLP can support mid-market to enterprise and our Professional Services can make the switch to Trellix easy



Trellix

Forcepoint



Trellix

Forcepoint Overview

2 DLP offerings: on-prem and cloud

Forcepoint Data Security

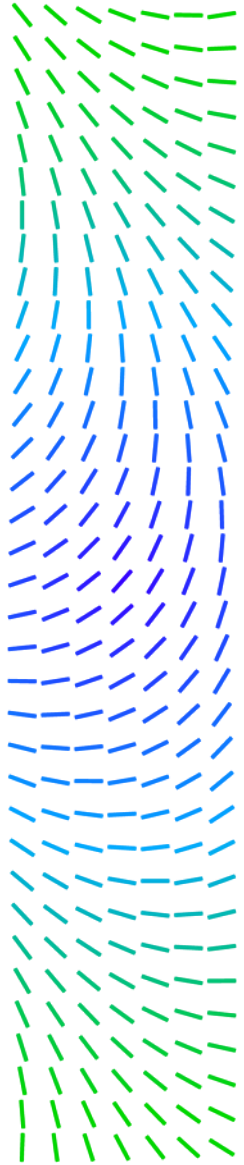
- DLP
- Risk-adaptive DLP

Forcepoint One

- Cloud Access Security Broker
- Zero Trust Network Access
- Secure Web Gateway

Trellix DLP Competes with Forcepoint Data Security

Skyhigh Security competes with Forcepoint One



Trellix

Strengths/Weaknesses

Strengths

- Behavior-based, Risk adaptive approach
- Out of box policies
- Broad customer base across enterprise and mid-market

Weakness

- Encryption/device control
- Limited integration/API
- Complex deployment and mgmt
- Complex report builders

Trellix contrasts with:

Trellix DLP also has many out of box policies and powerful discovery and classification capabilities

Easier to manage DLP with ePO as well as threat protection capability that Forcepoint doesn’t have

Integrated encryption and device control in DLP offering, Forcepoint is still catching up

Trellix
Trellix

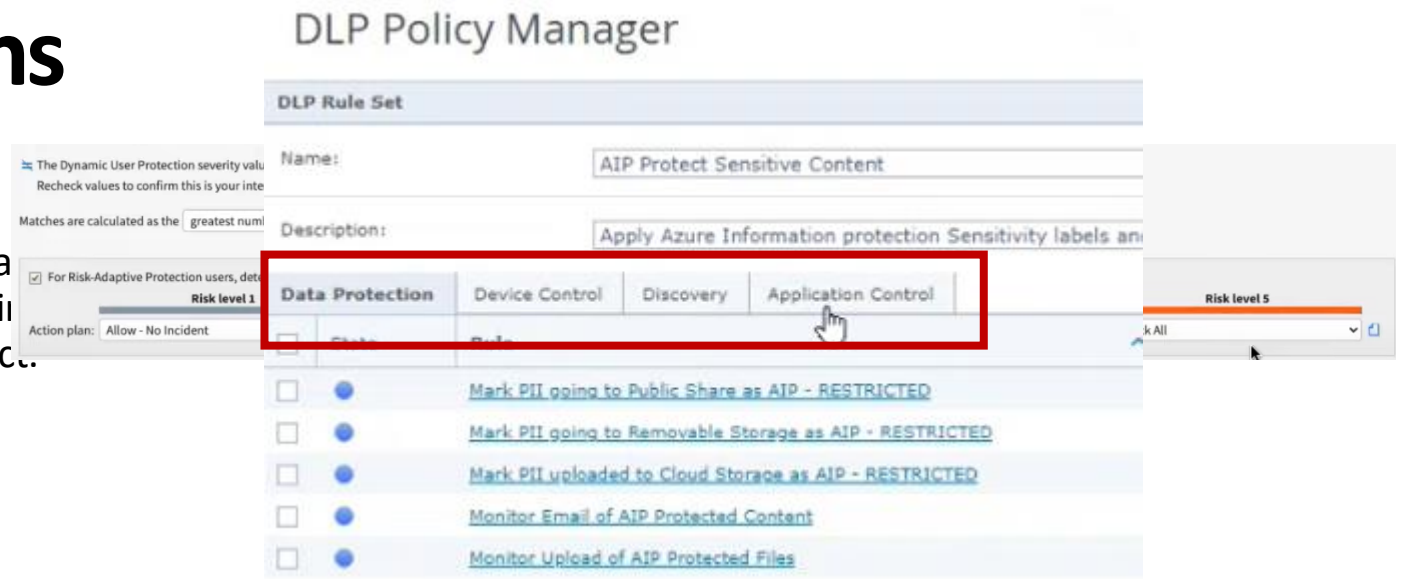
DLP in the SOC
Policy Configurations

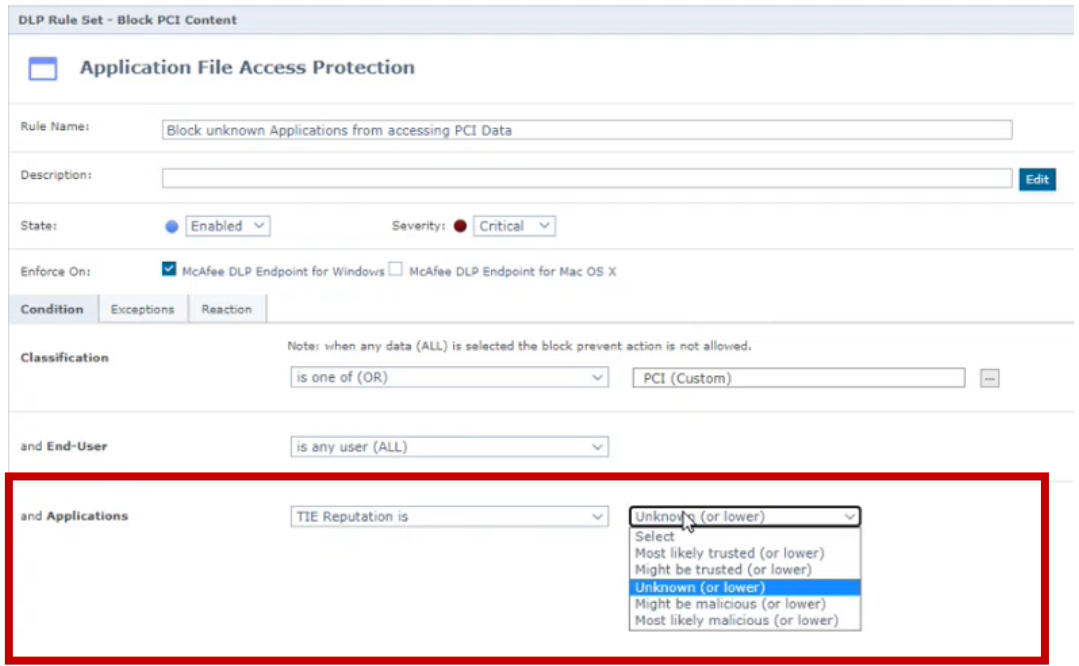
•How they do it:

- Forcepoint can leverage ML, user behavior a risk based policy. However it is still challengi to tune policies while minimizing user impac
- Also Forcepoint has limited device control capability that isn't fully integrated in their solution.

•How we do it better:

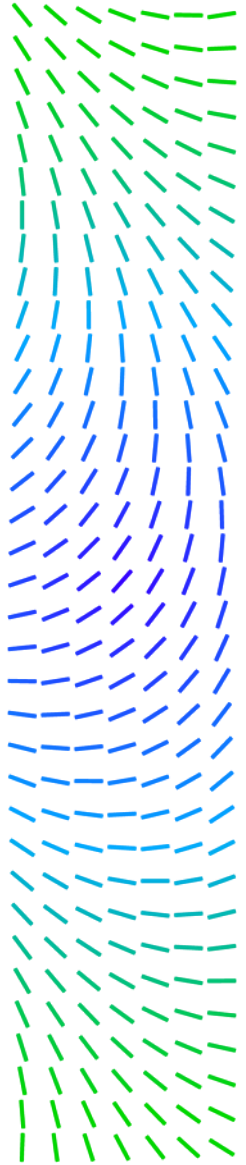
- Trellix has integrated device control within the DLP console to prevent insider risk.
- Also integrates with TIE to prevent untrusted processes from accessing sensitive data.





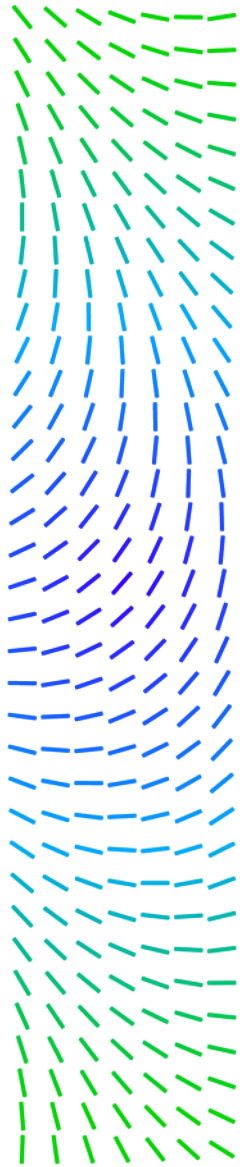
Forcepoint Takeaways

Forcepoint has good out-of-box policies	• Trellix DLP also has broad out of box policies and a more integrated approach across channels including device control
Forcepoint risk adaptive approach is a strength	• Trellix DLP leverages threat protection integration with TIE to block apps with bad reputation from accessing sensitive data
Forcepoint serves mid-market to enterprise	• Trellix DLP is suitable for mid-market to enterprise for threat protection AND DLP portfolios with shared ePO managment



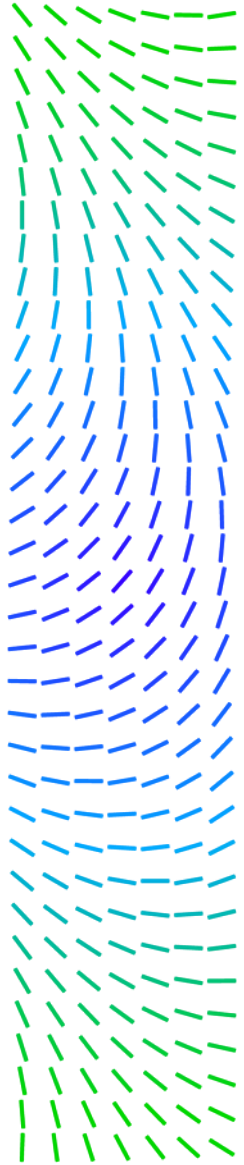
Trellix

Summary Takeaways



Trellix DLP Takeaways

Microsoft is built-into the platform and seems “free”	• Trellix DLP has a stronger and more efficient management and reporting with ePO
Symantec DLP has the most powerful DLP capabilities	• Trellix DLP has comparable capabilities and native reporting in ePO for simpler management
Forcepoint Risk Adaptive approach simplifies policy tuning	• Trellix DLP has a more integrated approach across channels, like device control, for ease of management



Trellix

Trellix

Q&A

Data Security

Thank You

Trellix