Trellix

23-26 OCTOBER 2023

Trellix EMEA Partner Tech Summit 2023

Rome, Italy

Trellix

Collaboration

Security

Fabrizio Rega

EMEA Solution Engineer
November 10, 2023

Agenda

Email and Collaboration Security

- **Introduction**
- **Trellix Email Security**

  Product line pitching and new features

- **IVX Enterprise Cloud**

  Product line pitching and new features

- **Demonstration**

  Use case #1 Complex Phishing Pattern

  Use case #2 Move laterally using M365

- **Partner Resources**
- **Questions**

Introduction

Email and Collaboration Security

Digital transformation has introduced a new threat vector

Extended Enterprise

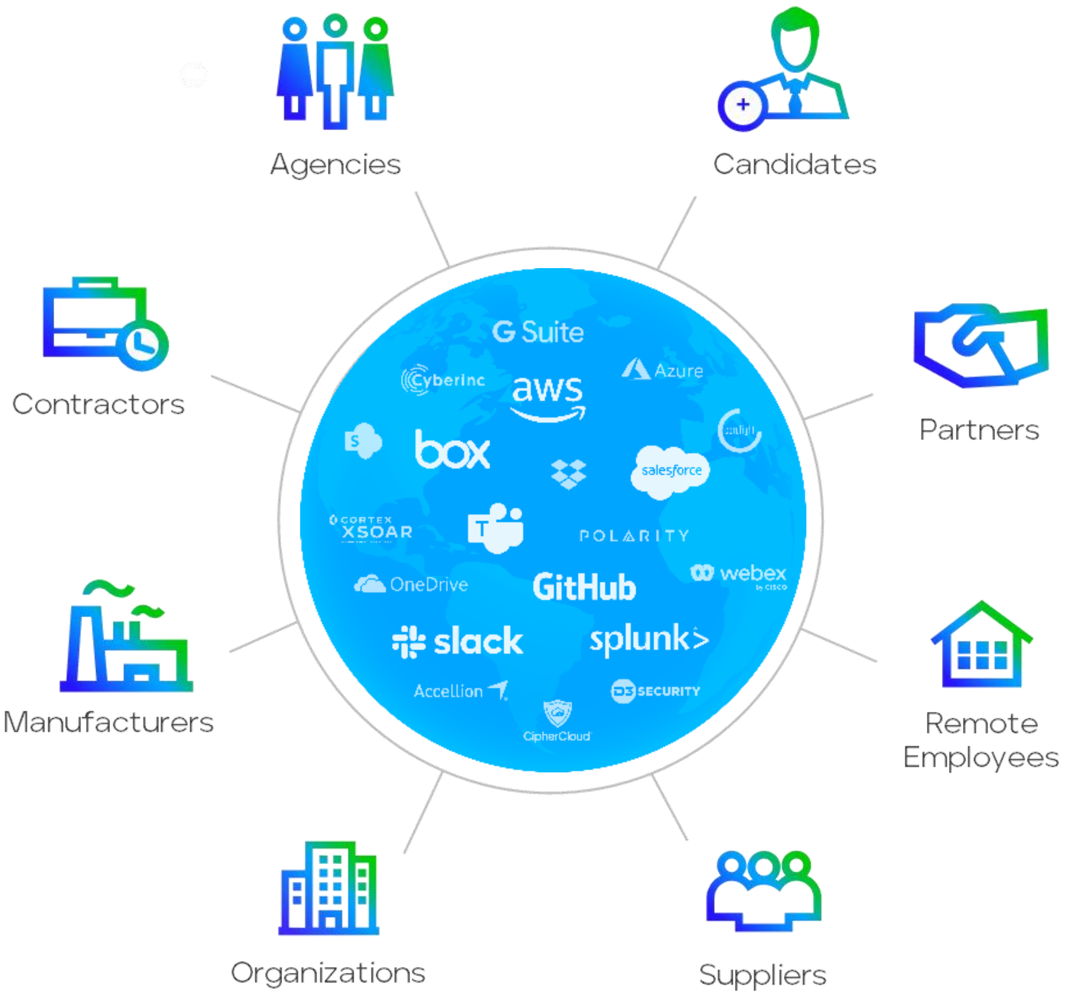
Business agility and innovation require third-party relationships to extend enterprise capabilities

Digital Transformation

Digitally-enabled partner ecosystem creates significant risk exposure

SaaS Insecurity

Vendors secure their platform but don’t worry that they provide an open door to your environment



Trellix

The nature and velocity of collaboration has changed

Creating three main fronts to defend

Email

Still the primary attack vector. Over 90 % of cyberattacks begin with phishing.

Collaboration Platforms

Allow us to freely share information, but do not ensure the integrity of what is being shared

Enterprise Applications

Digital transformation initiatives grant access to suppliers, vendors, customers – and threat actors

What’s top of mind for you?

Challenges with securing the extended enterprise

I don’t know what security risks my partner ecosystem creates for my organization

Paper-based security assessments provide little insight into a potential partner’s true security posture

Just one security incident can end the mutual trust between partners

The velocity and volume of file sharing makes manual submission infeasible

Application variety and complexity make consistent inspection challenging

Trellix

> “What I found personally to be true was that it’s easier to manipulate people rather than technology”

Kevin Mitnick

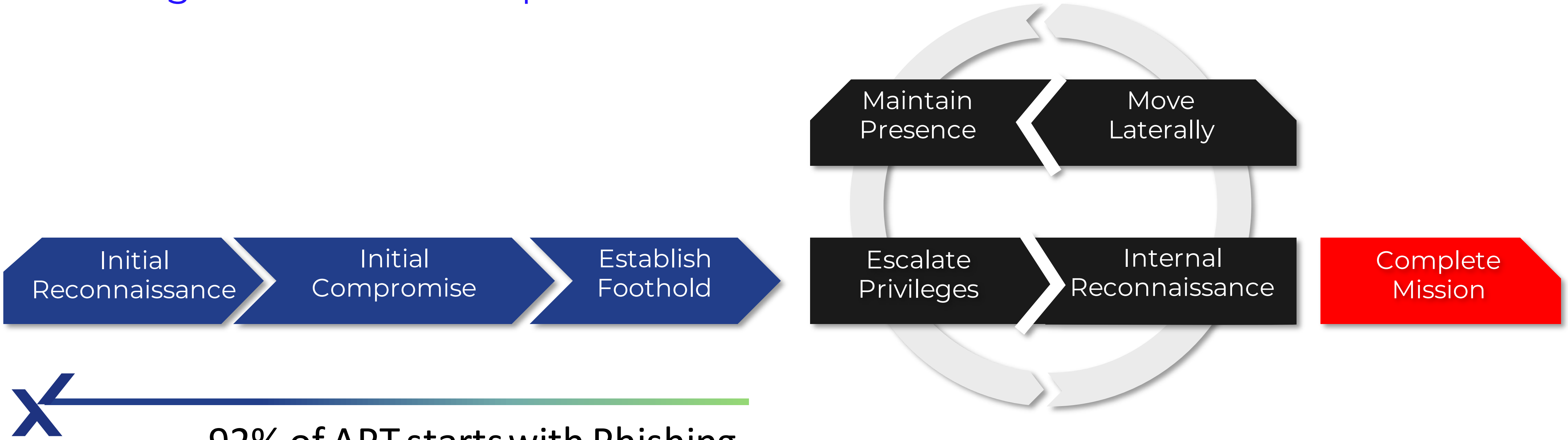
Email Security

Product line pitching and new features

Trellix

Kill Chain

Phishing for the inital compromise



92% of APT starts with Phishing

Intelligence-led security

Trellix Advanced Research Center

Global Visibility

Persistent data collection from customer, technology partner, and service provider networks around the world

Detection Innovation

Intelligence-led detection continually powers Trellix products
to prevent, detect, and respond to the most sophisticated threats

Research & Expertise

Elite intel analysts actively track vulnerabilities and malware campaigns—and the nation-states and malicious actors behind them

Advanced Techniques

Catch me if you can

- Weaponization
- Packed Malware
- Encrypted Malware
- Content Injection
- Search Engines Phishing
- Image as Text
- Impersonation
- Website Forgery
- QR Coding

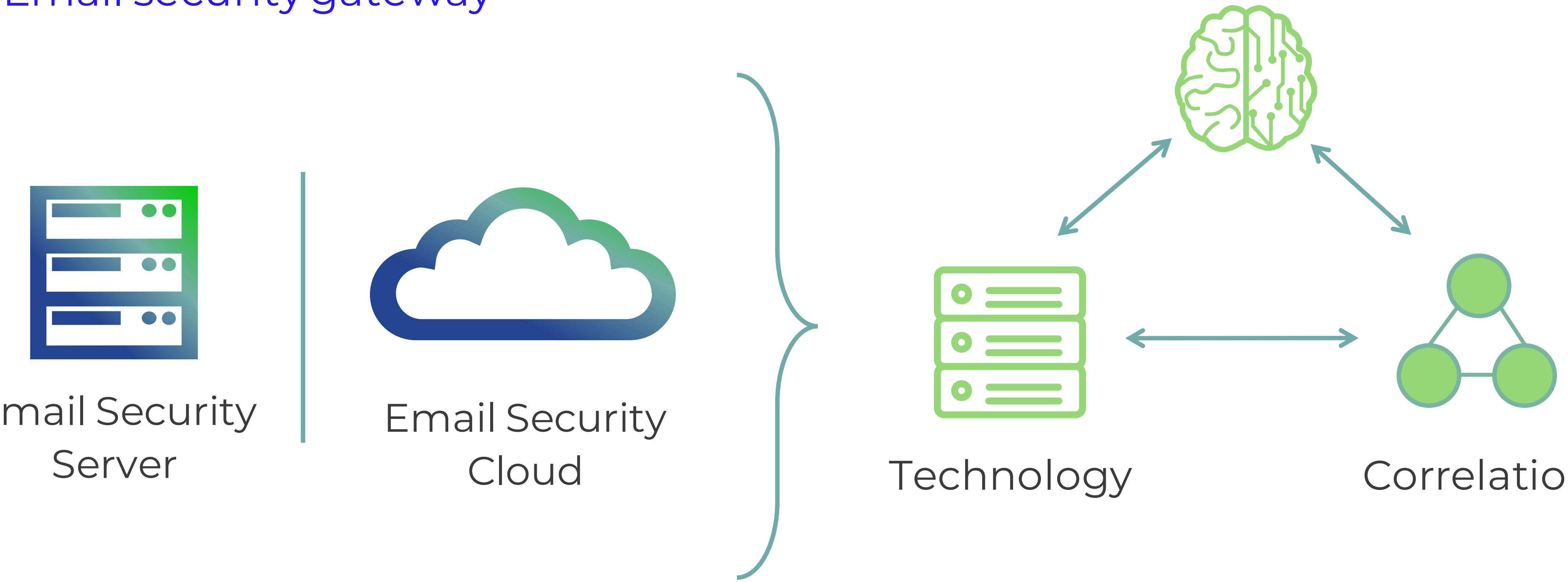
Countermeasures

How we catch them

- Dynamic Analysis
- Machine Learning
- Deep Learning
- Threat Intelligence
- Continuous Monitoring
- Password Extraction
- Retroactive Remediation
- QR Decoding
- OCR Scanning

Trellix Email Security

Email security gateway



Email Security Server

Email Security Cloud

Intelligence

Technology

Correlation

Superior efficacy in detecting and stopping advanced email-borne threats.

Intelligent Virtual Execution

The sandbox

Trellix Hardened Hypervisor

- Custom hypervisor with built-in countermeasures
- Designed for threat analysis

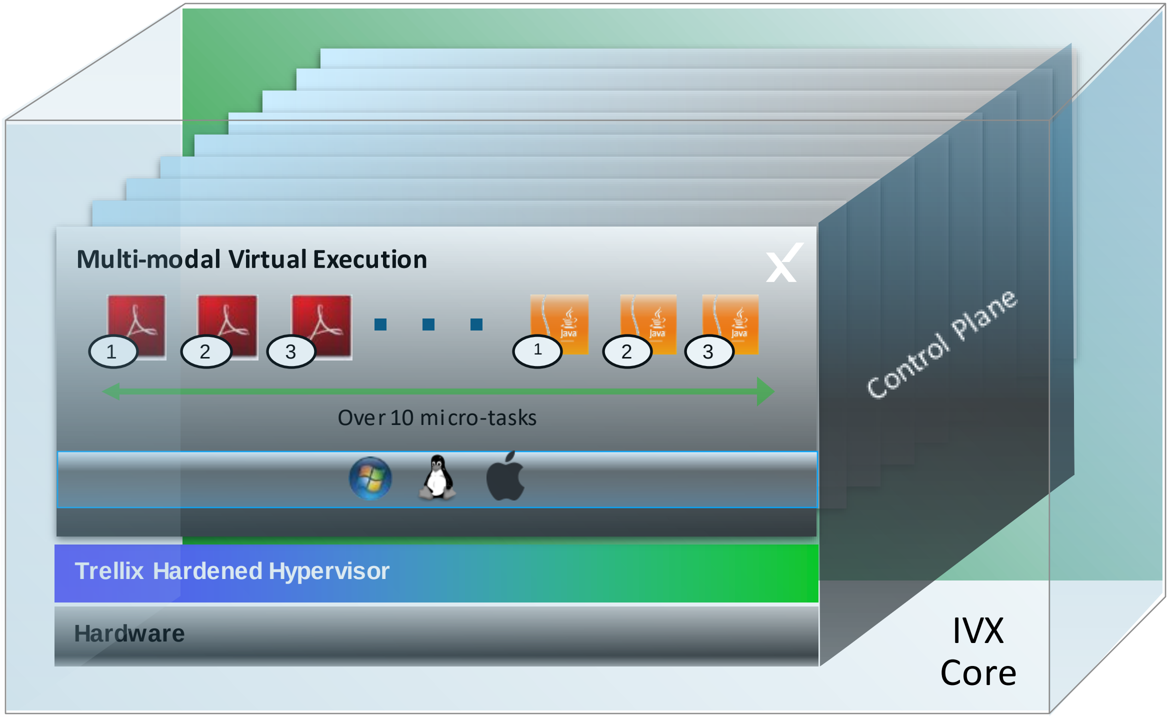
Multi-modal Virtual Execution

- Multiple operating systems
- Multiple service packs
- Multiple applications
- Multiple file-types

Threat Protection at Scale

- Over 2000 simultaneous executions
- Multi-stage analysis

Nearly 200 execution environments



Trellix Detection Technology

The Industry's Best Detection, Bar None

IVX

High-fidelity detection of
advanced & zero-day threats

Hardened Hypervisor
Multi-vector, Multi-flow detection
Huge Attack Surface
High Performance
Intel sharing
Rapid 6 week Engine Updates

+

AUDE 3.0

Intelligence- and heuristic-based analysis of URLs

Malware Guard

Machine Learning Engine to detect malicious objects

ML Analytics

New techniques to find Data Exfil, Beaconing and malicious SSL traffic

Expert Knowledge, Codified

Translating what we know
into our products via
SmartVision, rules, IOCs, analytics

IVX password protected file analysis

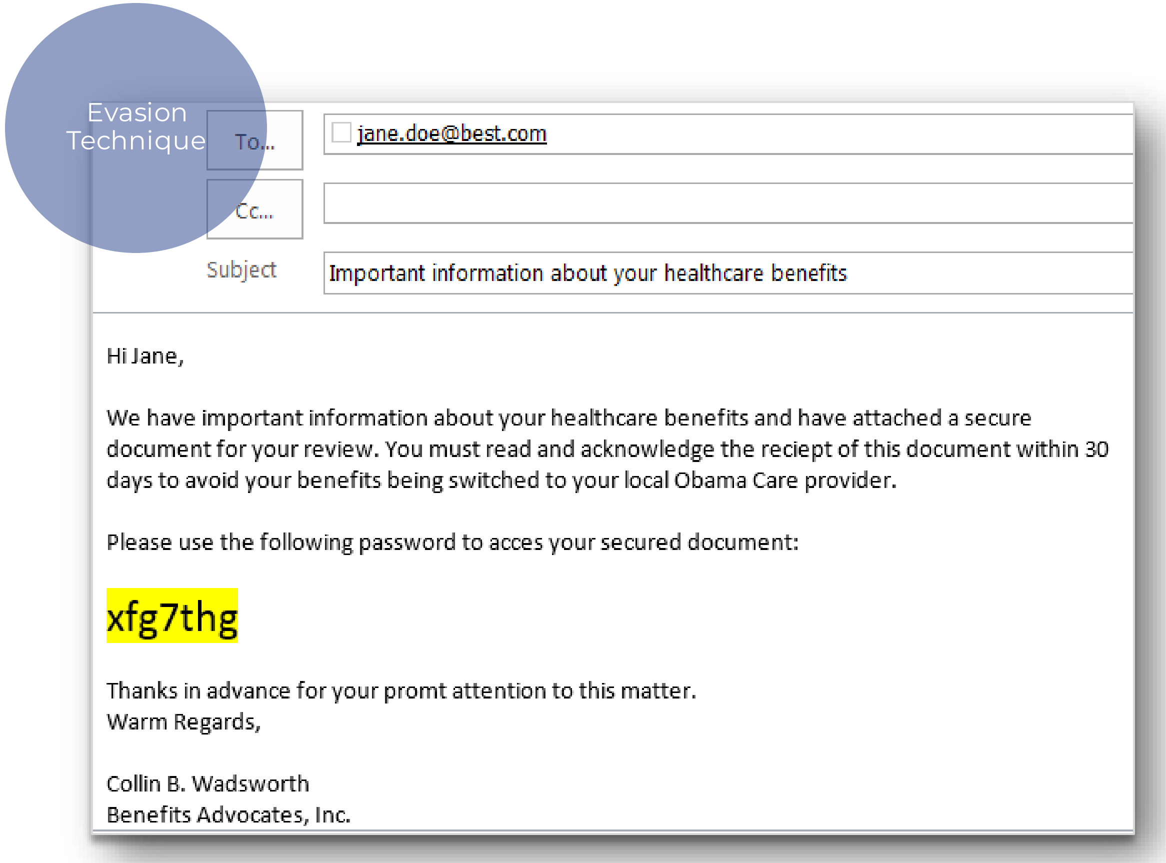
Evasion techniques in phishing attacks

Protects against common evasion technique of password-protecting PDF and MS Office files in email attachments

Identifies potential password candidates within email body

Determines password based on PDF and password candidates

Supports detection of Latin, Cyrillic, and 2-byte language passwords



□ jane.doe@best.com

Important information about your healthcare benefits

Hi Jane,

We have important information about your healthcare benefits and have attached a secure document for your review. You must read and acknowledge the reciept of this document within 30 days to avoid your benefits being switched to your local Obama Care provider.

Please use the following password to acces your secured document:

xfg7thg

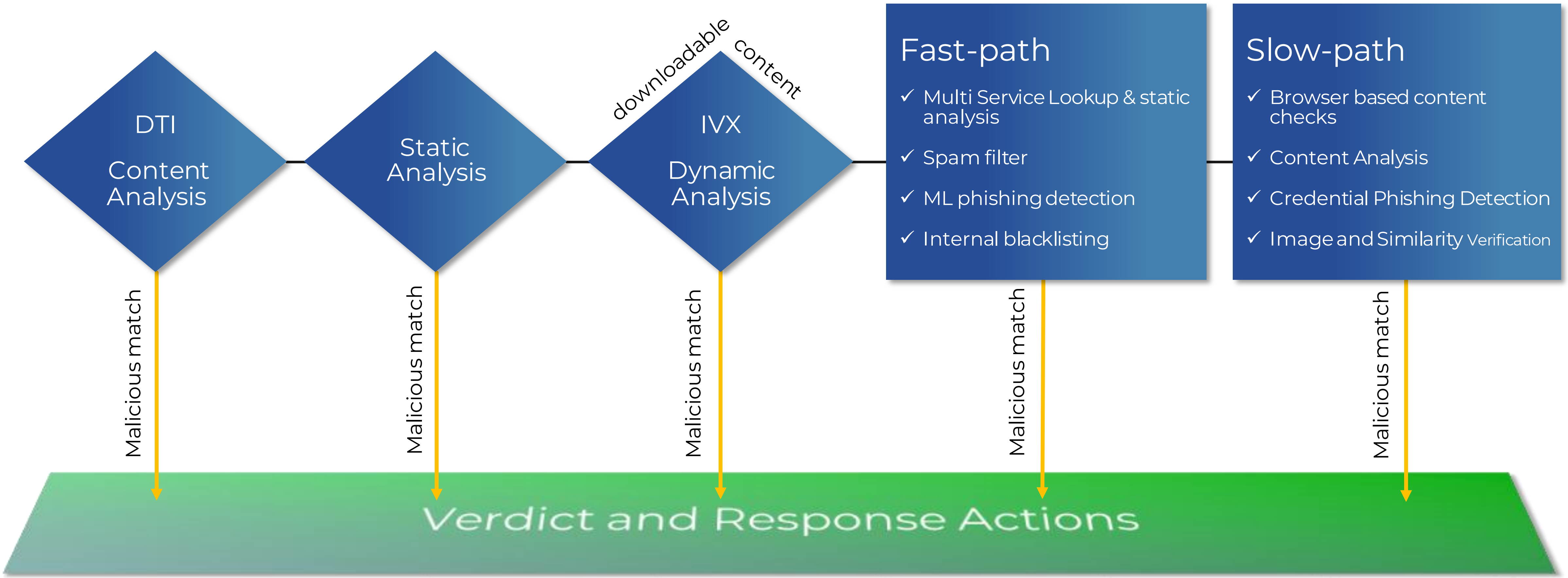
Thanks in advance for your promt attention to this matter.
Warm Regards,

Collin B. Wadsworth
Benefits Advocates, Inc.

Trellix

Advanced URL Defense

Fast-path versus slow-path analysis



Fast-path

- ✓ Multi Service Lookup & static analysis
- ✓ Spam filter
- ✓ ML phishing detection
- ✓ Internal blacklisting

Slow-path

- ✓ Browser based content checks
- ✓ Content Analysis
- ✓ Credential Phishing Detection
- ✓ Image and Similarity Verification

Trellix

Image Similarity Detection

Deep learning phishing detection

Advanced URL Defense plug in

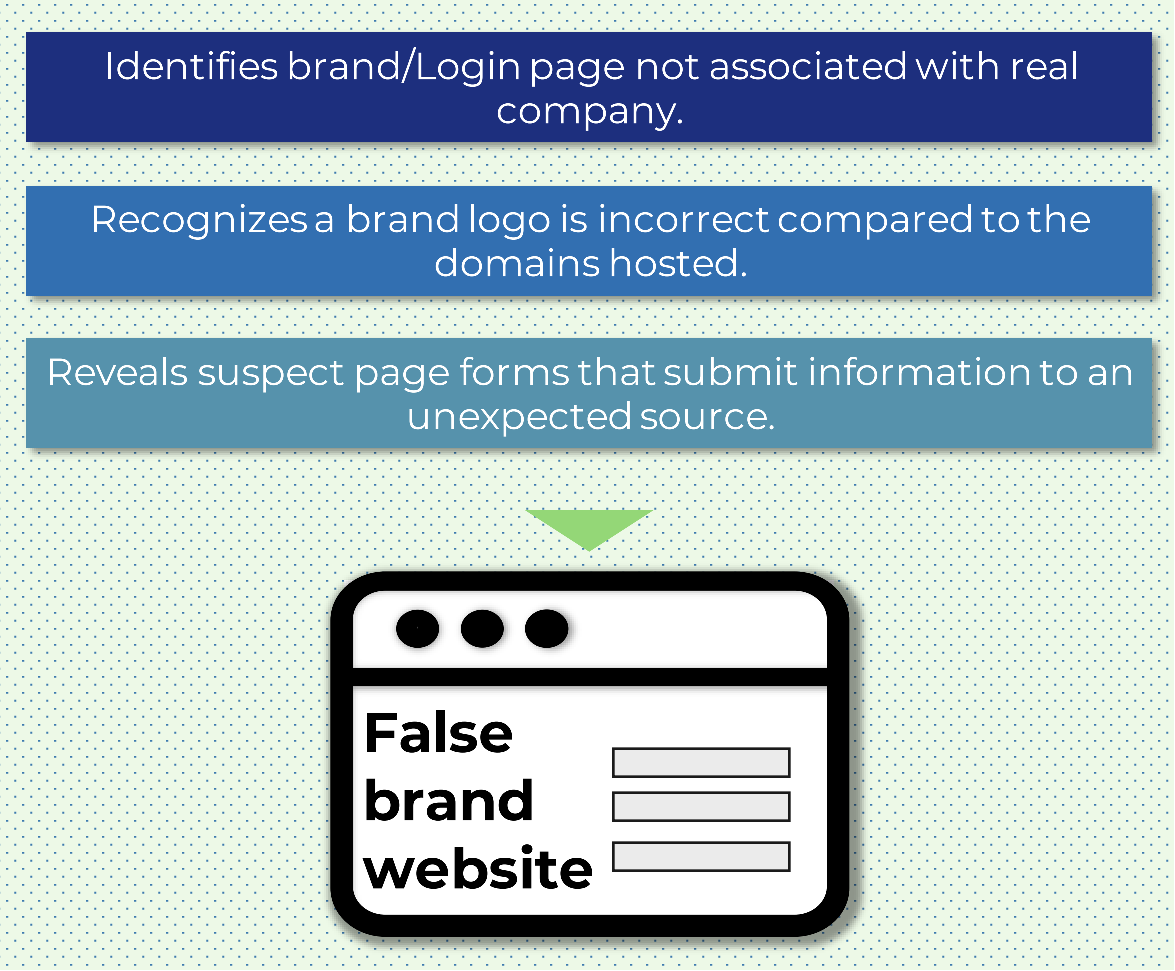
Image classification engine

- Uses deep learning
- Compiles/compares screenshots of commonly targeted brands against URLs in an email

Provides brand targeting insight

Reduces false negatives

https://acct.login.com



Identifies brand/Login page not associated with real company.

Recognizes a brand logo is incorrect compared to the domains hosted.

Reveals suspect page forms that submit information to an unexpected source.

Trellix

QR Decoding

New feature!

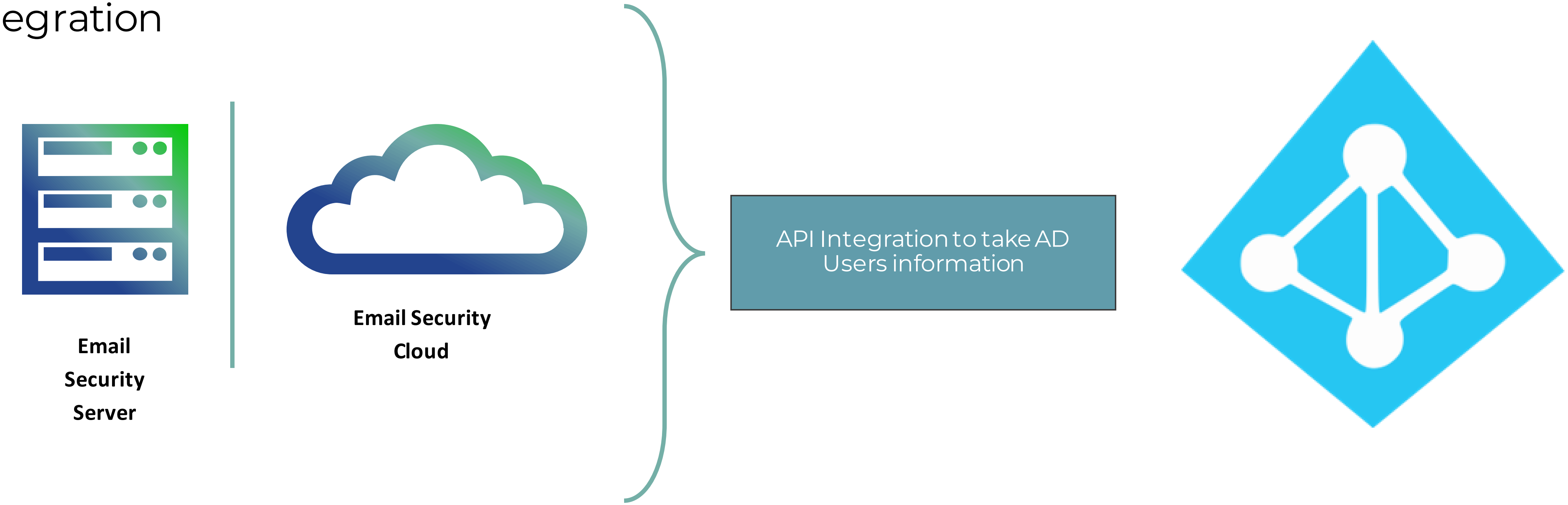
Use of QR codes for phishing is not new, but there is more to these campaigns. Analysis of these campaigns revealed that malicious actors not only used QR code as a primary means of defence, but also layered evasion tactics to make these campaigns hard to detect.

Trellix Email Security Cloud supports QR Code detection within email body, images within email body and pdf files. The QR Code to URL conversion plugin is now deployed and tested

Impersonation Detection

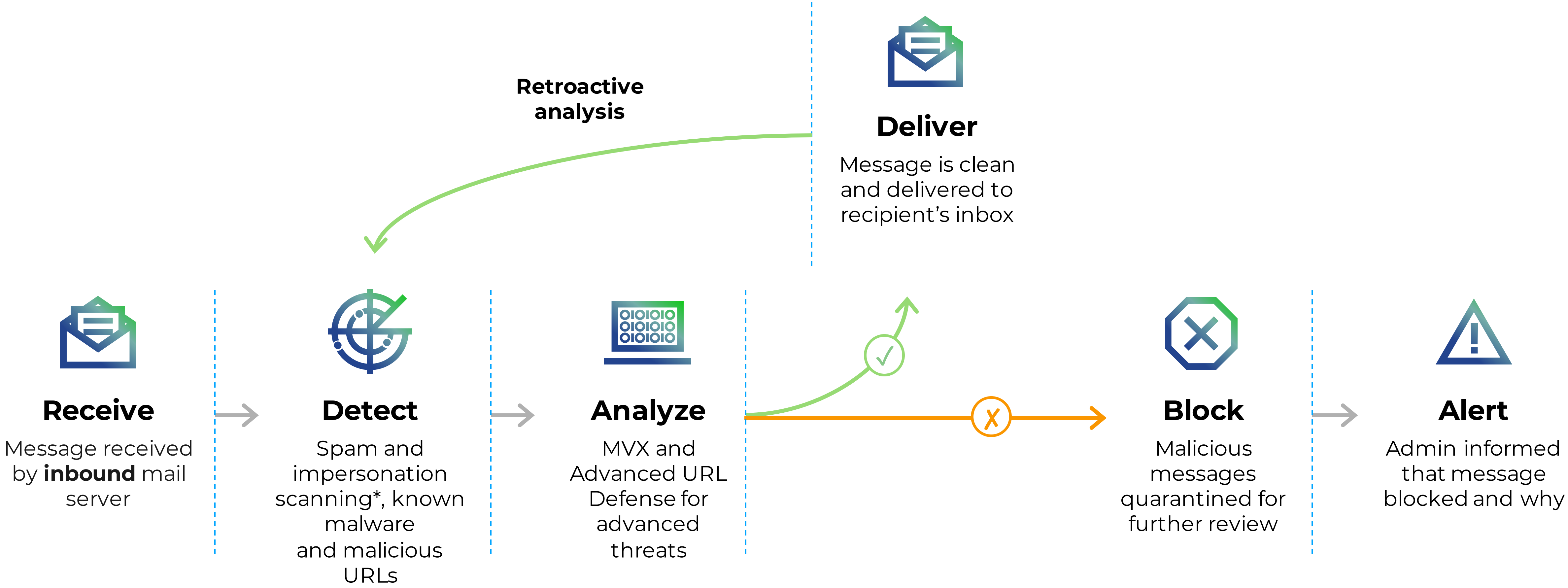
Evil in the mirror

Protects against common impersonation attacks using semantic analysis and Azure Active Directory Integration



Email Security in Action

Inbound and Outbound Protection



Retroactive analysis

Deliver

Message is clean and delivered to recipient’s inbox

Receive

Message received by **inbound** mail server

Detect

Spam and impersonation scanning*, known malware and malicious URLs

Analyze

MVX and Advanced URL Defense for advanced threats

Block

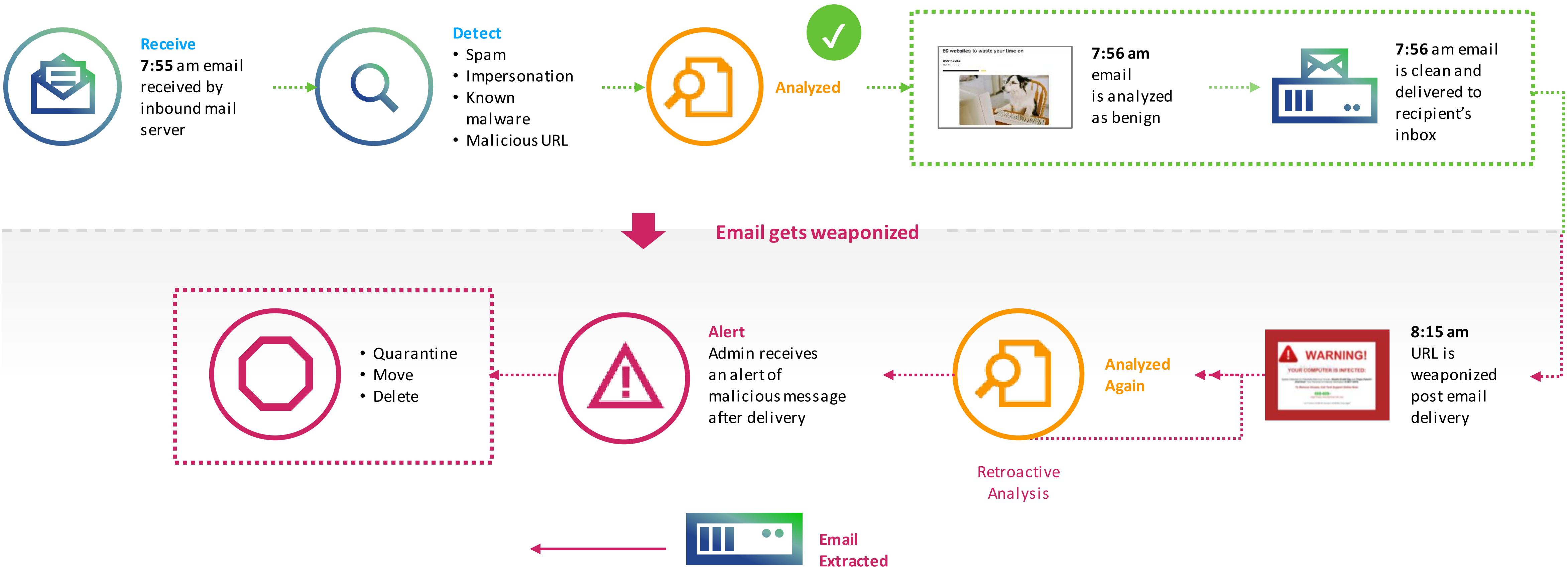
Malicious messages quarantined for further review

Alert

Admin informed that message blocked and why

Trellix

Automated Threat Remediation MS365 and Google Workspace



Receive
7:55 am email received by inbound mail server

Detect
- Spam
- Impersonation
- Known malware
- Malicious URL

Analyzed

7:56 am email is analyzed as benign

7:56 am email is clean and delivered to recipient's inbox

Email gets weaponized

8:15 am URL is weaponized post email delivery

Analyzed Again

Retroactive Analysis

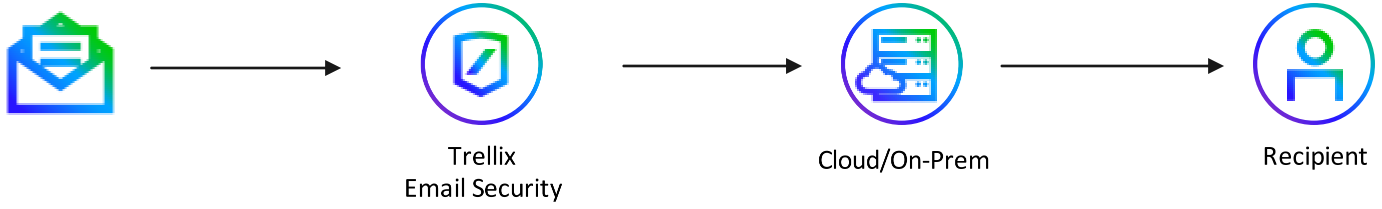
Alert
Admin receives an alert of malicious message after delivery

- Quarantine
- Move
- Delete

Email Extracted

Deployment Options – Cloud Email

1. **Primary SEG with Full Hygiene.**

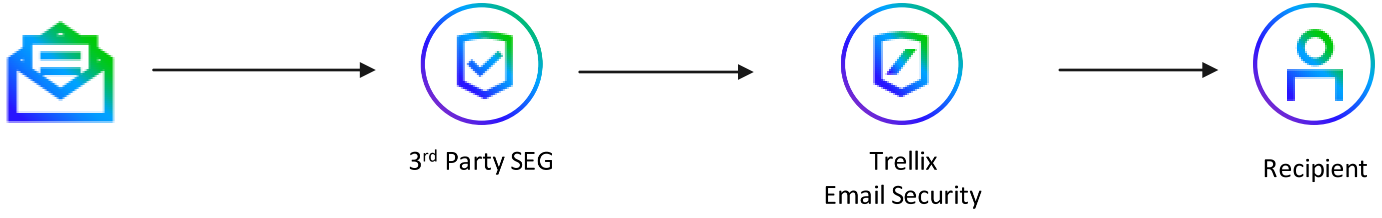


Trellix
Email Security

Cloud/On-Prem

Recipient

2. **Full Hygiene inline, second hop, behind a 3rd party SEG.**

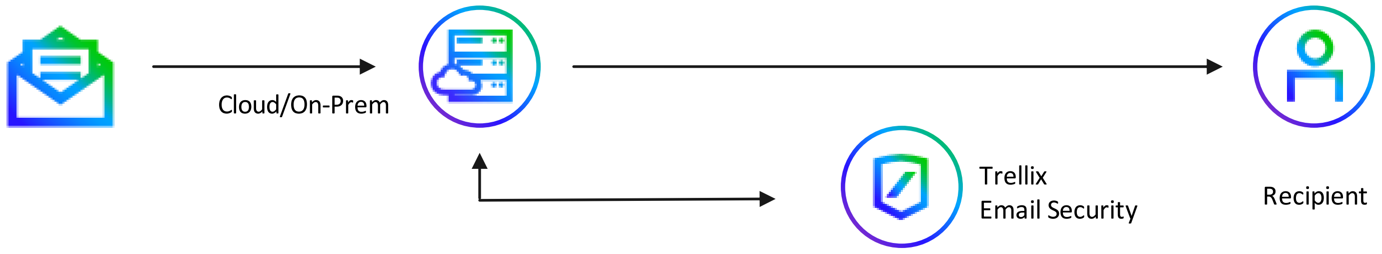


3rd Party SEG

Trellix
Email Security

Recipient

3. **Full Hygiene in BCC mode and sends alerts.**



Cloud/On-Prem

Trellix
Email Security

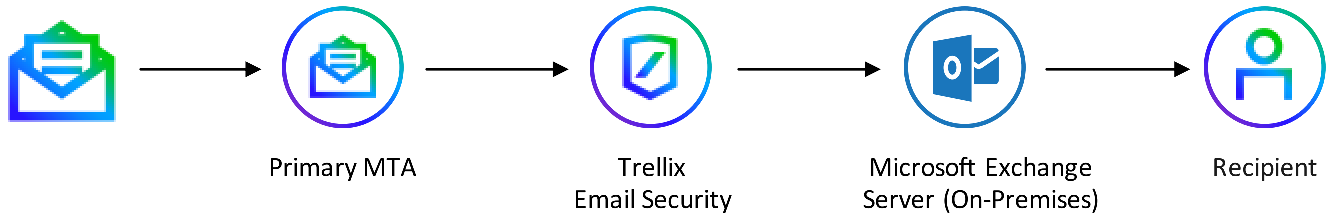
Recipient

4. **MS365/Google Workspace Native API Integration**

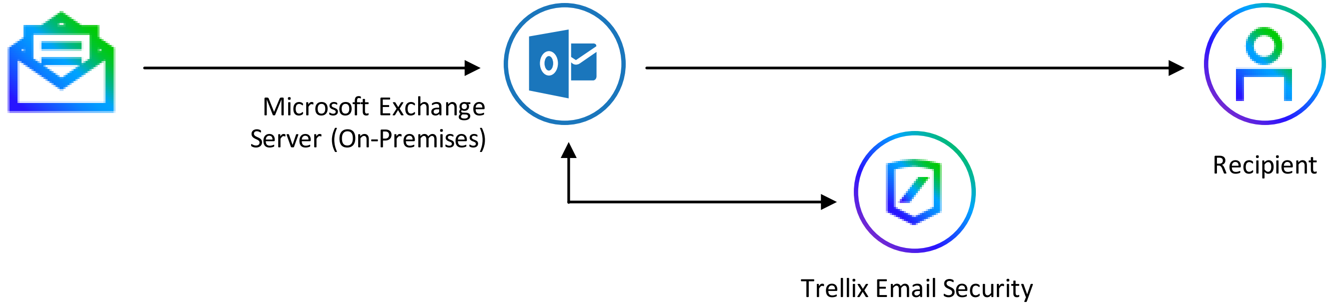
Google Workspace   Microsoft 365

Deployment Options – Server Email

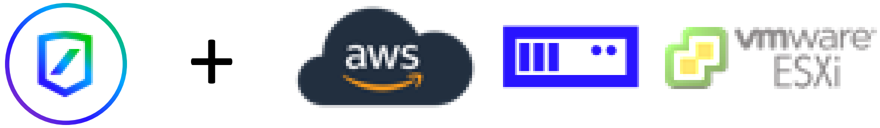
1. **On prem Inline mode**



2. **On prem in BCC/Monitor modes**



3. **Appliance deployments (Form factors)**



IVX Cloud

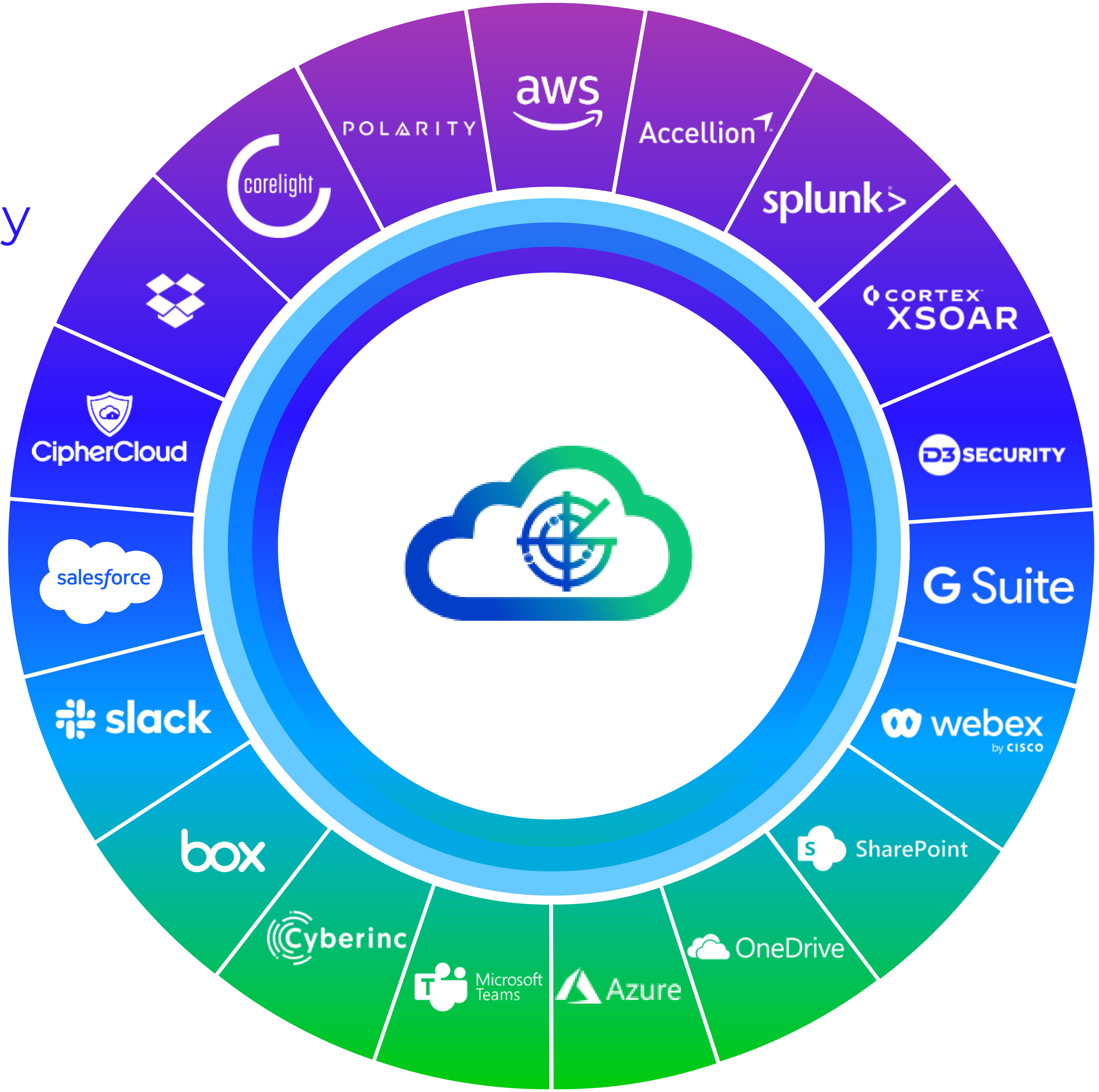
Product Pitching

Trellix

A new playground

The importance of collaboration security

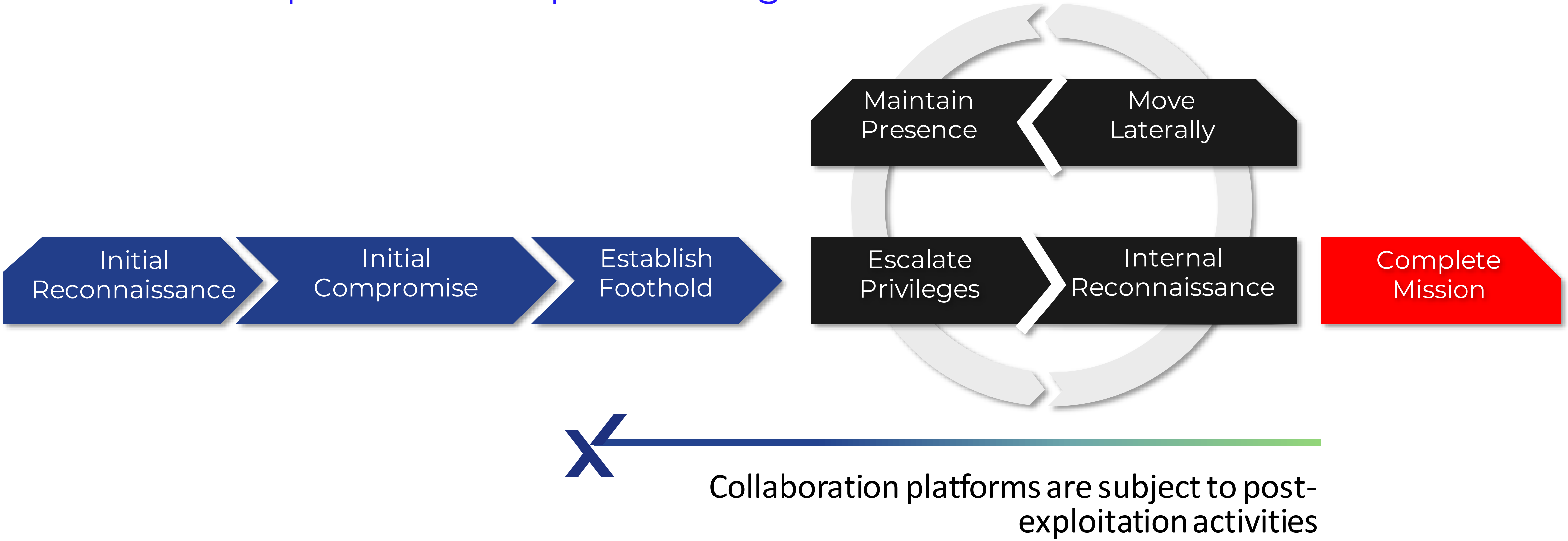
- Protect your workflow
- Defence in Depth
- Detect Anywhere



Trellix

Kill Chain

Collaboration platforms are part of the game



Collaboration platforms are subject to post-exploitation activities

A new playground

Techniques and tactics

Links in chat tabs

Malicious URLs

Weaponizing Meetings

Evil in Cloud Storage

Embedded website in Sharepoint

Weaponizing Links in chat

C3 via Cloud Storage

internal Phishing

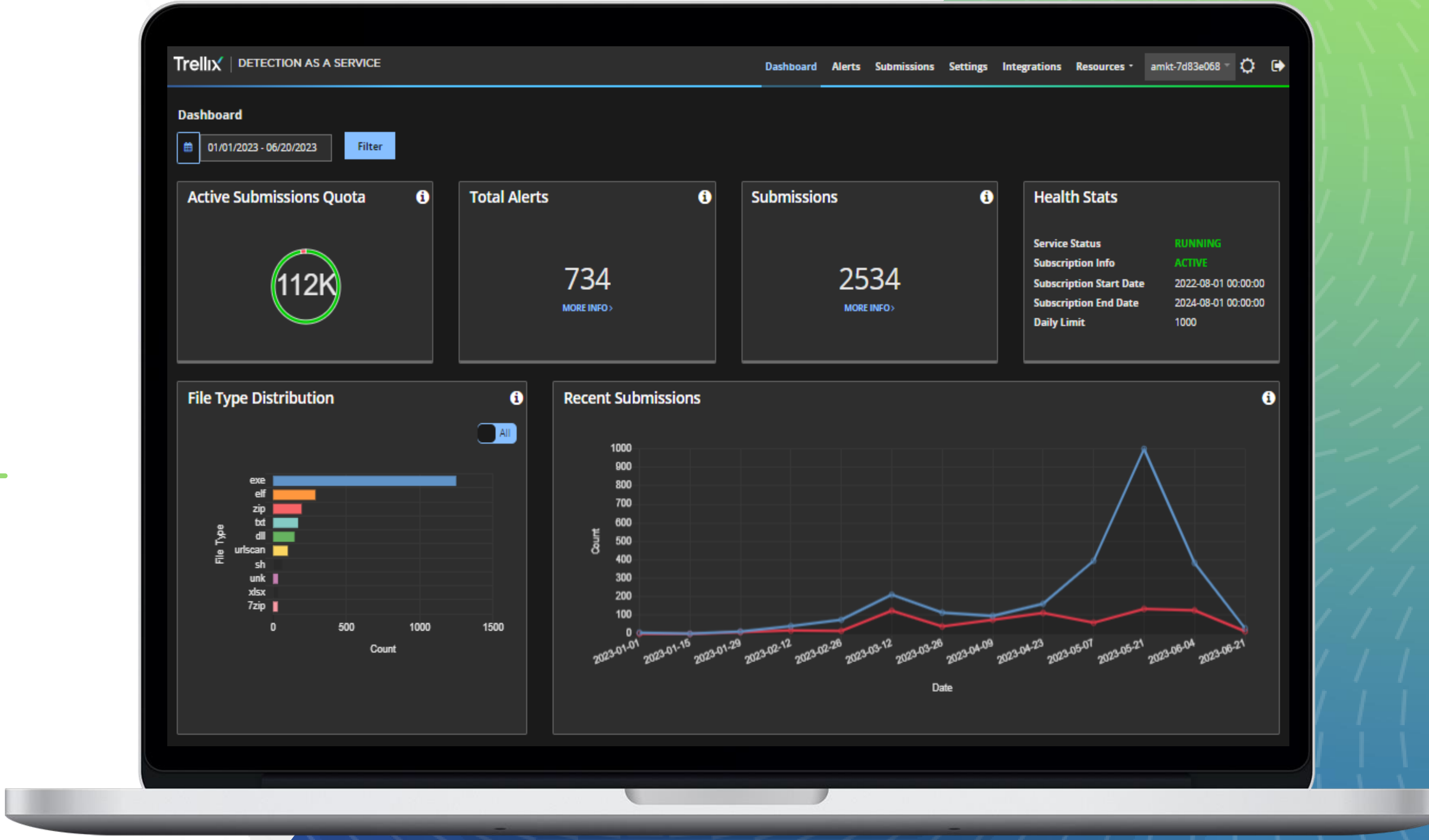
Federation

Trellix

IVX Enterprise Cloud

More than a Sandbox

A cloud-native service, Trellix IVX Cloud rapidly scans submitted content to identify malware.



Dashboard

01/01/2023 - 06/20/2023

Active Submissions Quota: 112K

Total Alerts: 734 MORE INFO ›

Submissions: 2534 MORE INFO ›

Health Stats

Service Status	RUNNING
Subscription Info	ACTIVE
Subscription Start Date	2022-08-01 00:00:00
Subscription End Date	2024-08-01 00:00:00
Daily Limit	1000

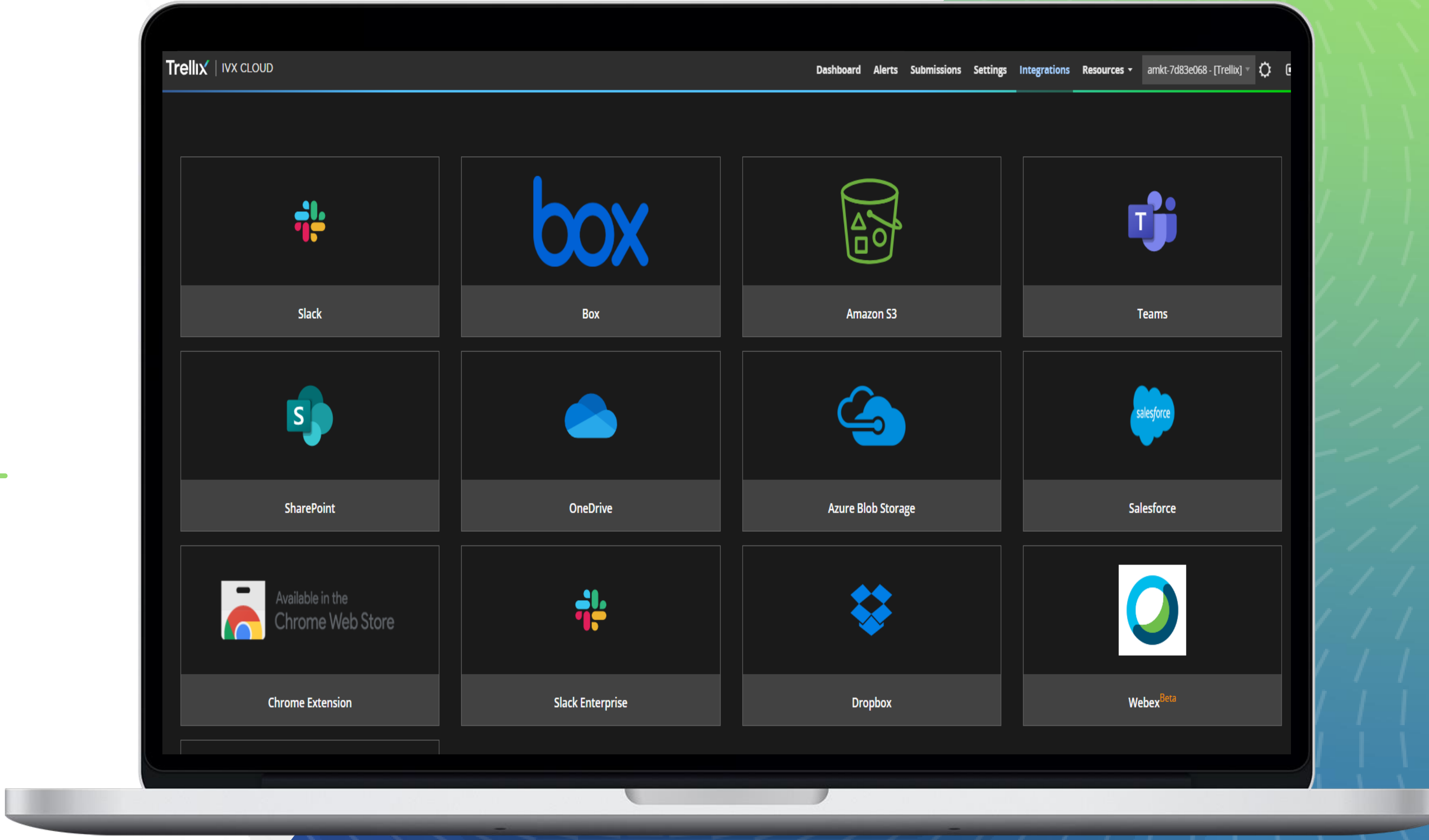
File Type Distribution

Recent Submissions

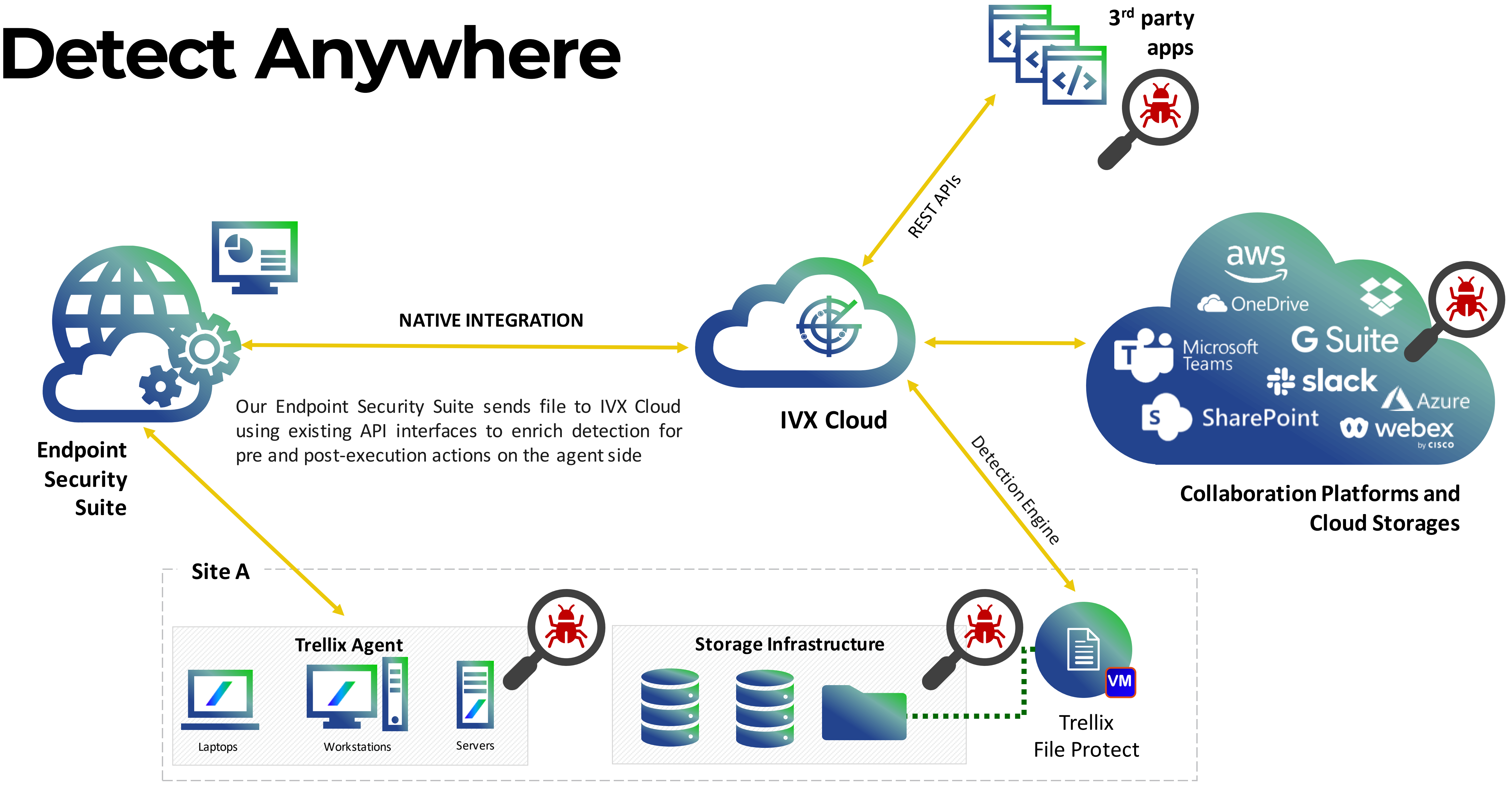
OOTB Integrations

Plus API ready

A cloud-native service, Trellix IVX Cloud rapidly scans submitted content to identify malware.



Detect Anywhere



Our Endpoint Security Suite sends file to IVX Cloud using existing API interfaces to enrich detection for pre and post-execution actions on the agent side

Trellix

Journey of a file

IVX Cloud

Submission

File or URL submission using different sources.

Supports 200+ file types

Fast Lookup

Dynanic Threat Intelligence and Global Cache lookup

Pre Filter

Quick actions defined by pre-filters: allow or blacklist, Riskware Rules

Analysis

Analysis process that includes Static Analysis, Machine Learning and Dynamic Analysis

Post Processing

Result Correlation and post processing

Verdict

⊗ MALICIOUS

⚠ QUARANTINE*

✓ CLEAN

DEMO

Use Cases

Trellix

#1 Complex phishing pattern

Email Security Cloud

A Phishing Email

Incoming phishing email from a valid source with a non-spammy reputation

Containing a PDF

The email contains an attachment in PDF format

With a QR Code in it

The PDF contains a QR code that refers to a malicious URL

To download a zip file

The malicious URL download an archive file in 7zip format

Password Protected

The 7zip is password protect and the password is written into the PDF attached document

That drops a Malware

The extracted malware refers to a Hancitor Trojan to download a Cobaltstrike agent and a Stealer

#2 Lateral movement in 365

IVX Enterprise Cloud

A Teams message

A compromised account sends you a message on Microsoft Teams

From a Social Engineer

The account is controlled from a malicious actor that uses social engineering techniques to deceive the User

Trying to push Malware

The goal is to spread a Malware on the User's machine

Via File

Using a malicious file transmitted via Microsoft

Or URL

The actor also paste a URL into the chat to download the same malware

To deploy a backdoor

Result Correlation and post processing

Resources

Partner SE Technical Bookmarks

Product Technical Documentation Portal

- Product Documentation:
- https://docs.trellix.com/

- Administratorion Guides
- Deployment Guides
- System Security Guides
- Release Notes
- Hardware Guides
- Reference Guides

Cloud Labs

- CrossFire (ASH):
- https://login.trellix.com/

- MDemo:
- https://trellix-mdemo.skytap-portal.com/

- Consolidation in progress...

Communication

Partner Care Team

- partnercareemea@trellix.com

- MSP Partner Care Team
- msppartnercare@trellix.com

Expert Center

Knowledge Base

Forum

- Trellix-F Community:
- https://community.fireeye.com/
- Trellix-M Community:
- https://communitym.trellix.com/
  Consolidation in progress...

Questions

Trellix

Trellix

Data Security

Leon Matthasen

Senior Solutions Engineer
November 10, 2023

Use the following WIFI:
SID:
Password:

Before We Begin

Please pay attention to the following items...

Silence Your Devices

Please mute or turn off your smartphones and other electronic devices to minimize distractions during the presentation.

Restrooms

Restrooms are located [Specify location, e.g., down the hall to your left].

Emergency Exits

Familiarize yourself with the nearest emergency exits, located at [Specify locations, e.g., front and rear of the room].
In case of an emergency, follow the exit signs and proceed calmly to the nearest exit.

Q&A

We will have a Q&A session at the end of the presentation. Please save your questions until then.

Session Schedule

The session is expected to last approximately 3 hours with no breaks.

Welcome

EMEA Partner Tech Summit 2023

Trellix

Introduction

Data Protection Speaker

Leon Matthasen

Senior Solutions Engineer

Trellix

Agenda

Data Security

- Welcome
- Latest Updates and Product Line Pitching
- Use cases and Demonstration Guidance
- SE Resources – How to Access
- POV Guideline and Process
- Trellix Differentiators
- Point of Contacts

Trellix

Product Line Pitching

Data Protection

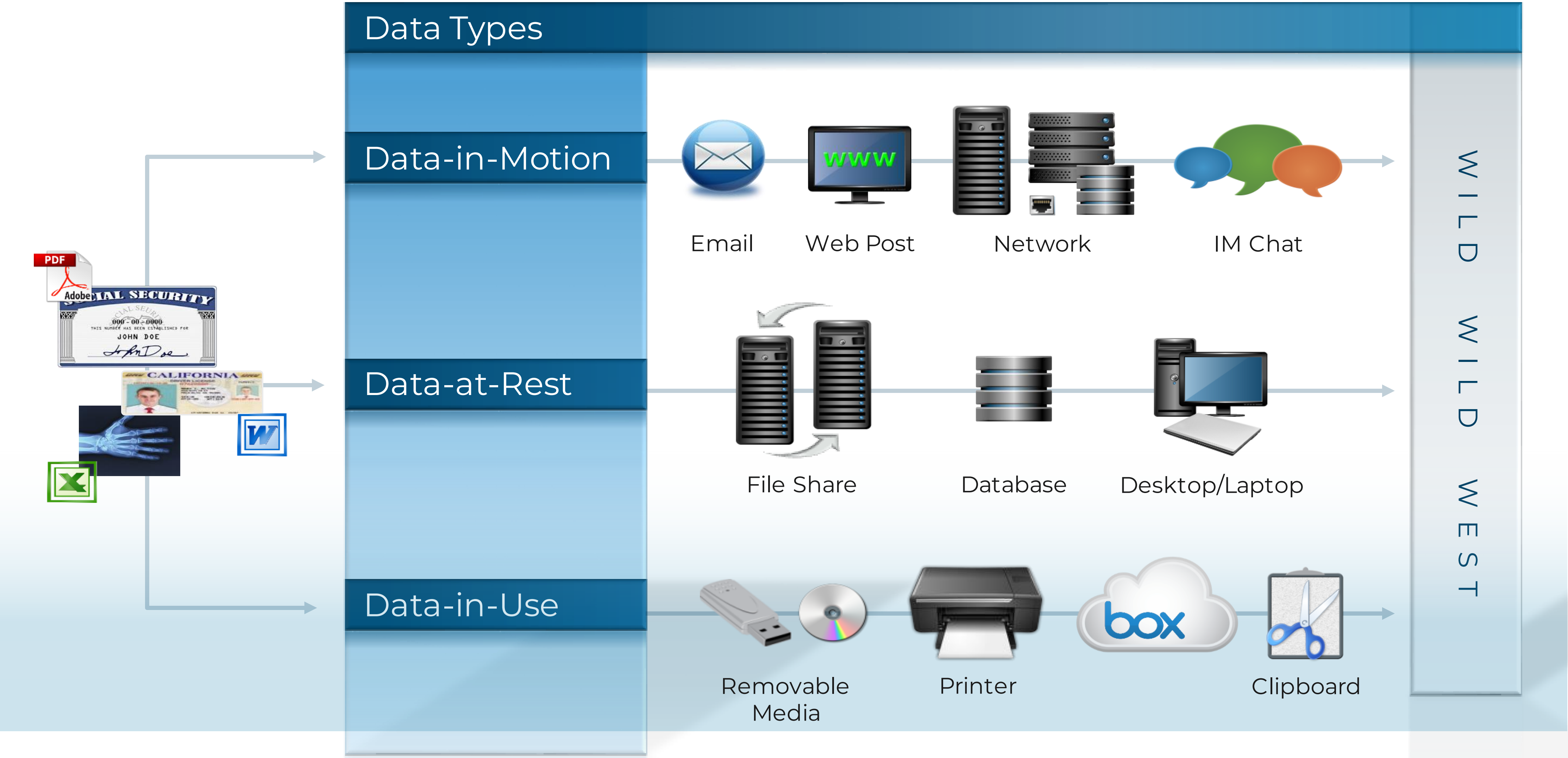
Trellix

Do you know where your data is?

Do you know what data is sensitive?

How do you protect your sensitive data?

The Sources of Data Loss



Top Data Protection Challenges

Rising success rate of malware intrusions

Keeping up with regulatory compliance

Lack of visibility and control of data

Both a technical problem and a business problem to overcome

A Sampling Of Big Breaches

T-Mobile
80M Customers

Facebook
530M Customers

Solarwinds
>18,000 Customers

Corporations Bear The Brunt Of Data Loss

Lots of reasons to be worried about Data Security

$888M

The largest single data protection fine levied against a company

$100Bn

Yearly cost of Healthcare fraud.

35%

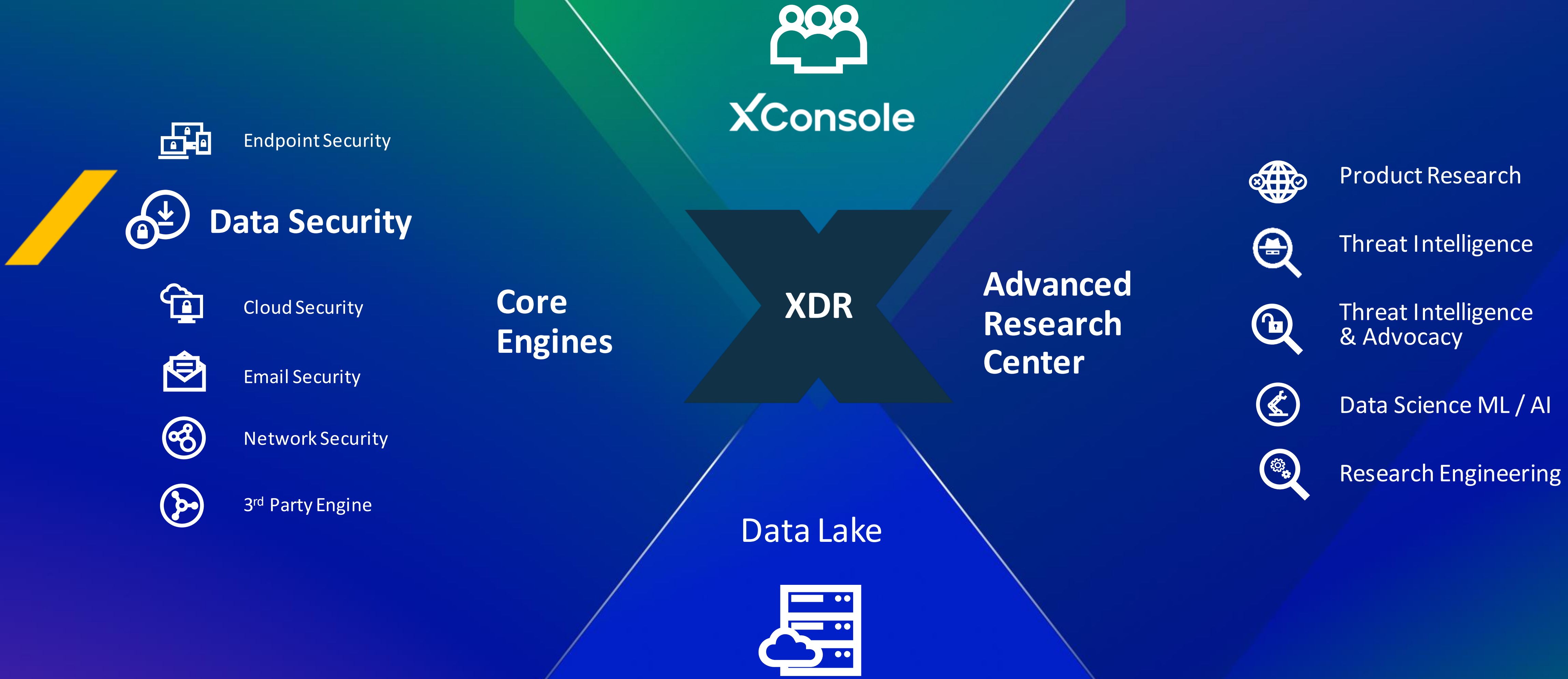
More than 35% of all DLP implementations fail

$43B

Cost of business email compromise attacks

Trellix

Trellix Platform



Endpoint Security

Data Security

Cloud Security

Email Security

Network Security

3rd Party Engine

Core Engines

XConsole

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
- Phishing
- DDoS
- Exploits
- DNS Attack
- Social Engineering
- Ransomware
- Man in the Middle
- SQL Injection
- APTs

XDR Is Not Complete Without Data Security

Objectives

Endzone Defense Around the Attacker's Ultimate Objective...

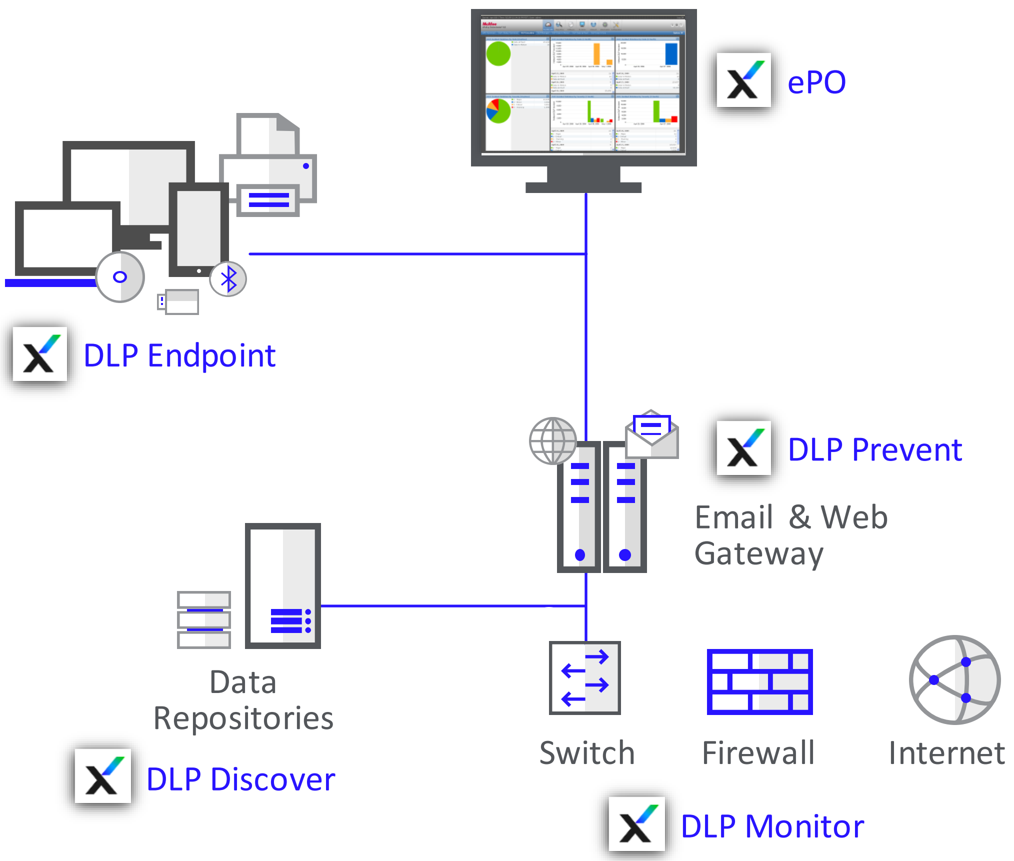
Your Data

Trellix

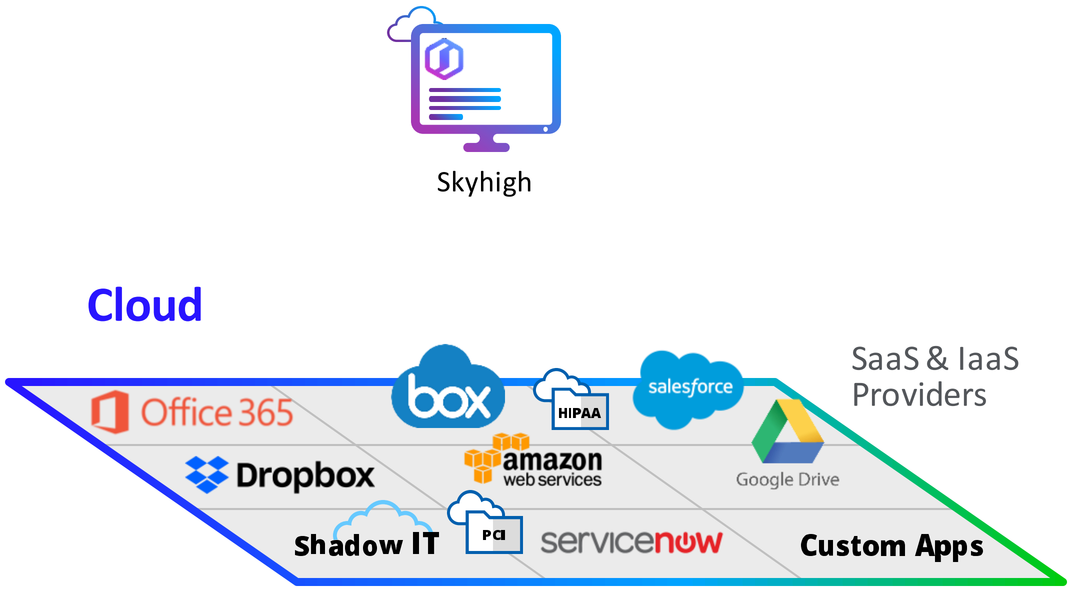
Protect Data Wherever it Resides

Native Capabilities

Policy Orchestration



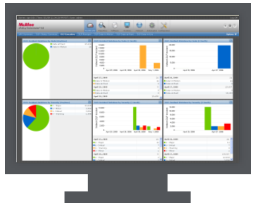
Partner Integration



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

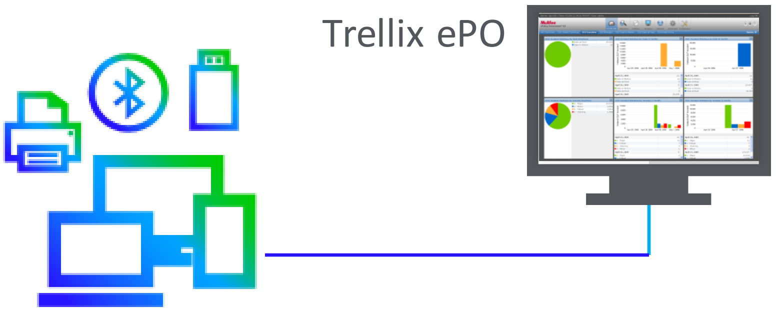
Trellix DLP Classification

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 DLP solution

Cover Endpoints, Networks, and Cloud Environments


Trellix ePO

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 DLP Endpoint

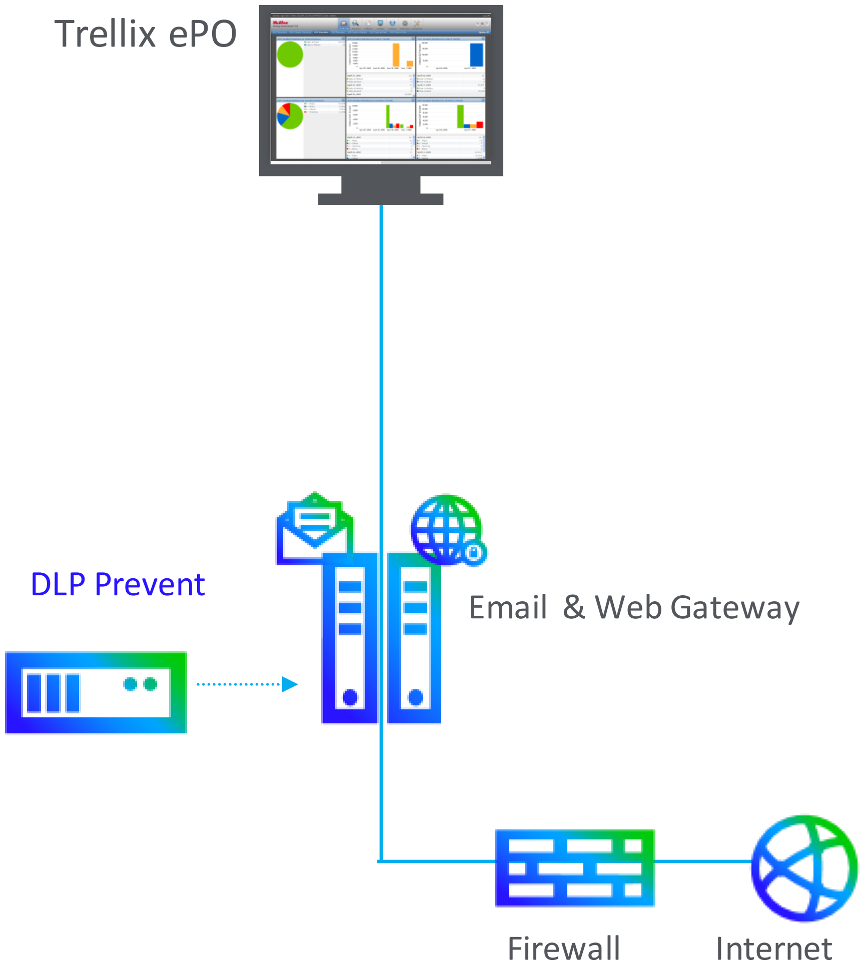
Extend Your Data Security to the Endpoint

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 DLP Prevent

Enforce Network Policies

Web

Email

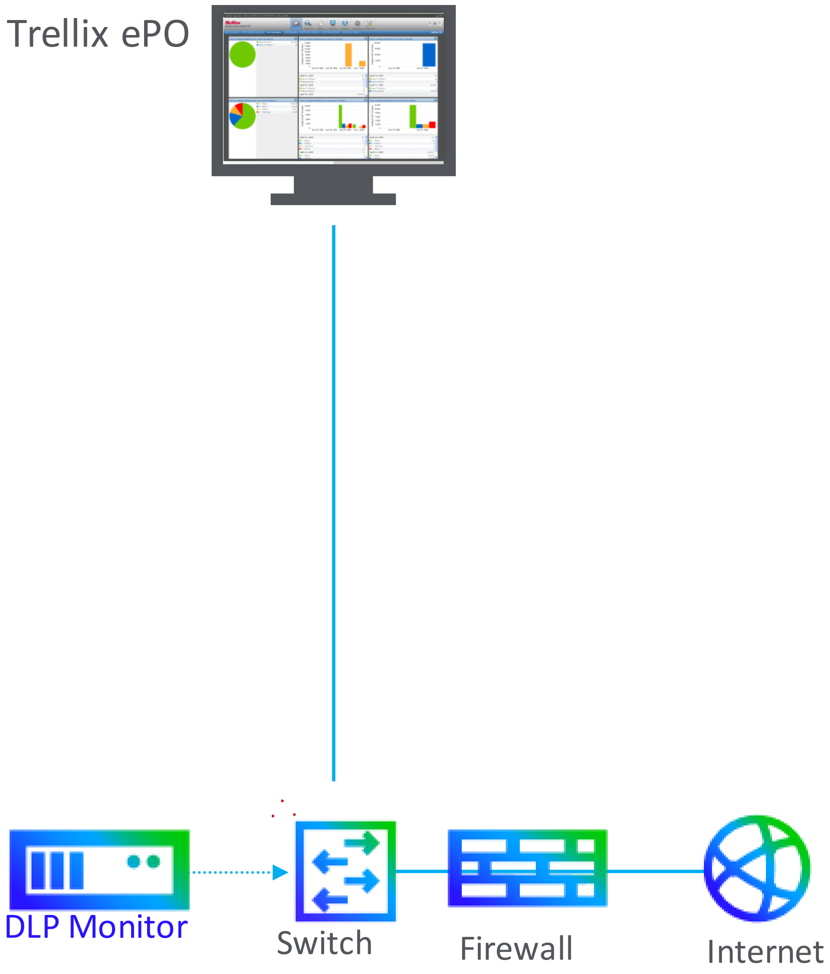
Prevent the movement of sensitive data

- 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 DLP Monitor

Safeguard vital data

Email

Web

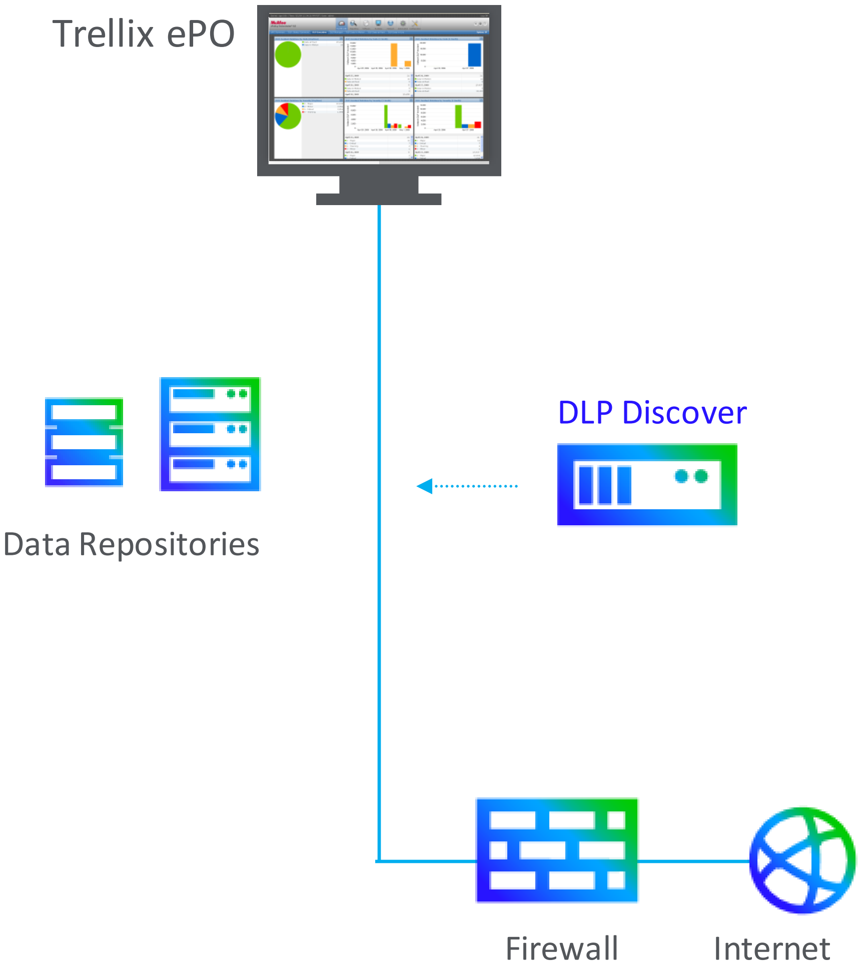
Network

- 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 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

Database Security Suite

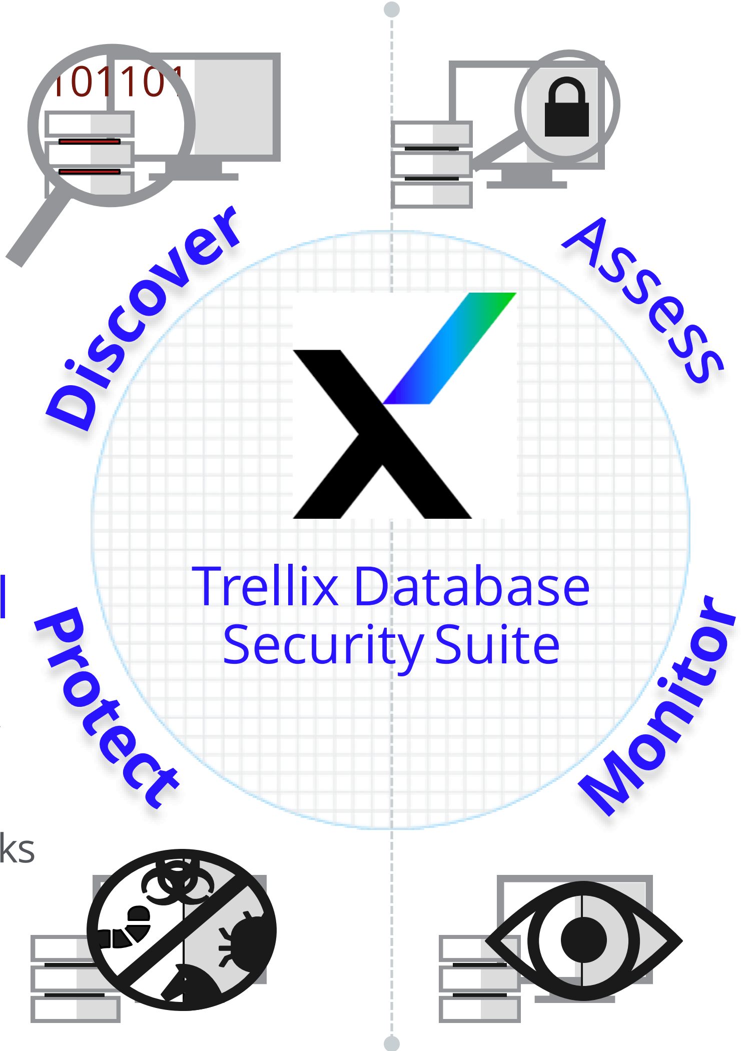
Why Trellix Database Security?

Database Discovery & Data Classification

- Database Discovery
- Sensitive Data Discovery
- User Rights Management
- GDPR, BSI, CIS Specific

Security Assessment

- Vulnerabilities
- Misconfiguration
- Missing Patches
- Vulnerable Code
- More than 6000 Checks



Protection and Virtual Patching

- Identification and Prevention of Exploitation Attempts
- Protection Against Known Attacks
- Generic Pattern
- Abnormal Activity

Activity Monitoring

- Real-Time Monitoring
- Policy Enforcement
- Audit, Alert or Block Activity

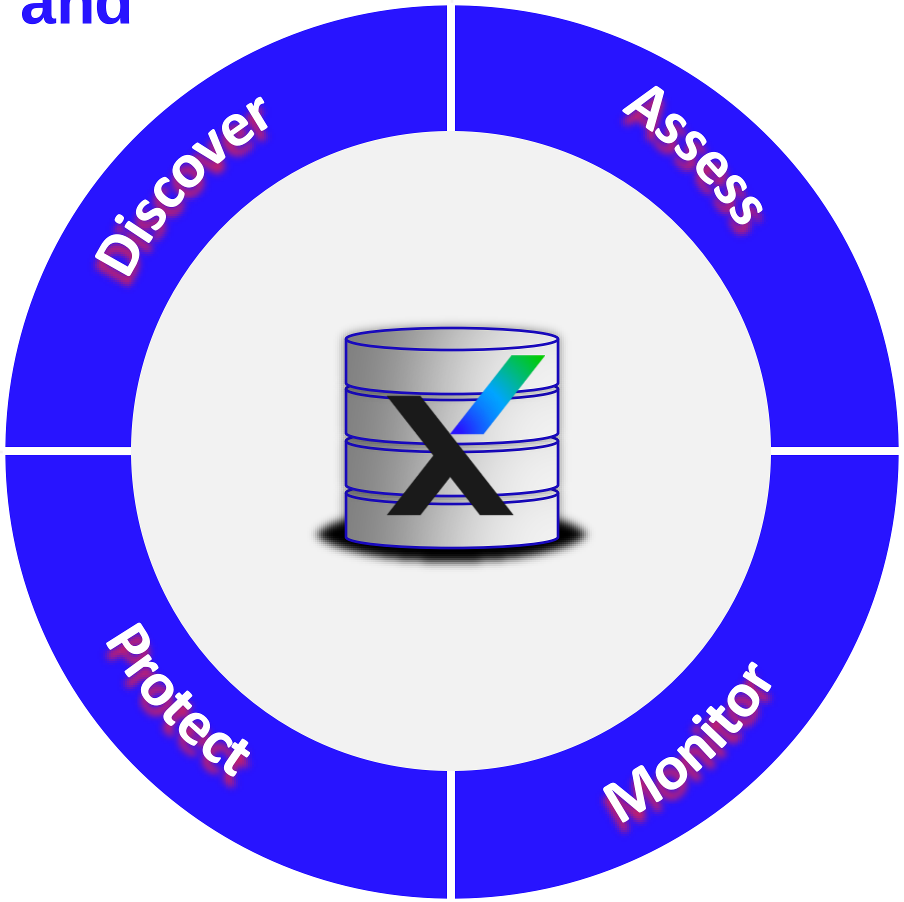
Static Disposition of the Database

Database Vulnerability Manager (DVM)

Trellix Database Vulnerability Manager

Database Discovery and Data Classification

- ✓ Database Discovery
- ✓ Sensitive Data Discovery
- ✓ User Rights Management



Log certain types access to the database

- Enterprise-class database vulnerability assessment and data discovery engine
- DB & sensitive data discovery

Most comprehensive security scanning library

- Over 6,800 checks, Continuously updated by McAfee Labs

Non-intrusive and light-weight scanning

Detailed **remediation** advice

Trellix Database Vulnerability Manager Test Categories

Auditing

Backdoor Detection

CIS & STIG Benchmarks

DB Configuration checks

Custom checks

Data Discovery

Default Password Checks

GDPR

OS Tests

PCI DSS Checks

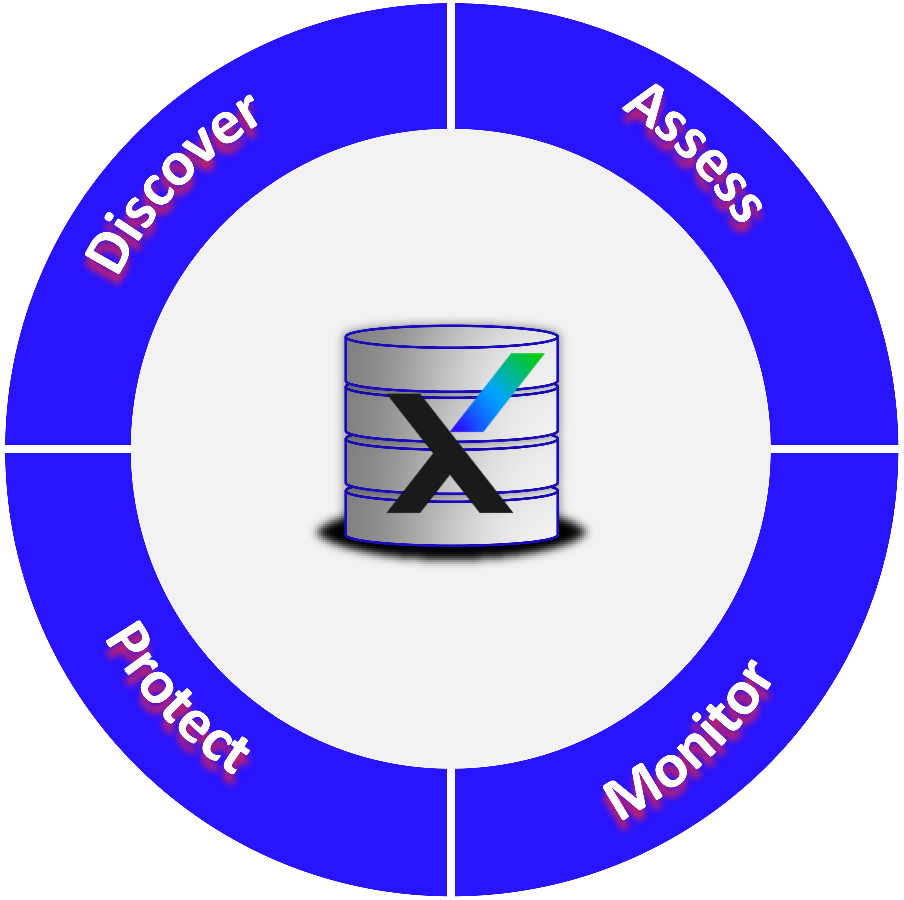
Patch Checks

Unused Features

Known Vulnerabilities

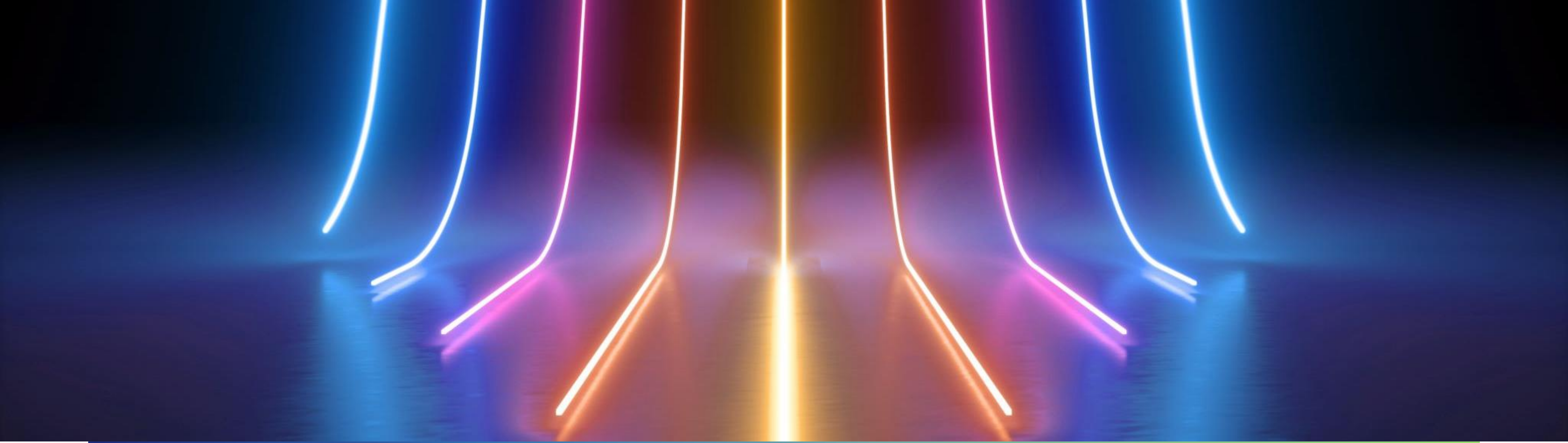
Vulnerable Code

Weak Passwords



Security Assessment

✓Vulnerabilities
✓Misconfiguration
✓Missing Patches
✓Vulnerable code
✓Over 6,800 checks



Creating Greater Visibility Into Your Environment

Database Activity Monitoring (DAM)

Trellix

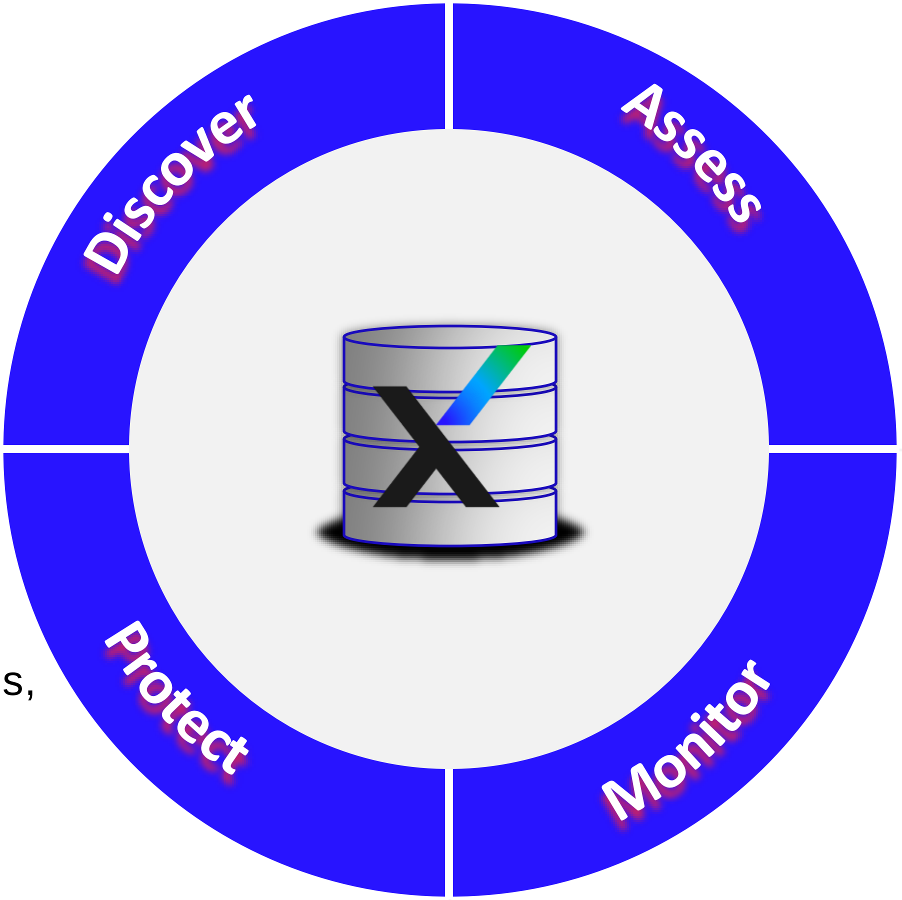
Trellix Database Activity Monitoring

Log certain types access to the database
Log all access by certain users
 (DBAs, sys-admins, contractors).
Log all direct-access to sensitive tables

Alert in real-time on suspicious
/unauthorized access to the DB,
Access from an application
not approved to touch the DB.
Failed login attempts

Prevent suspicious/un-authorized access
to the database unauthorized
TABLE DROP in production
databases. Unauthorized change to
the database (users, permissions/privileges,
table definitions etc.)

Quarantine



✓Real-time Monitoring
✓Enforcing Policy
✓Audit, Alert or Block activity

Activity Monitoring

Trellix

Advance Memory Monitoring

Unique and Advanced memory monitoring technology – non intrusive and zero-risk

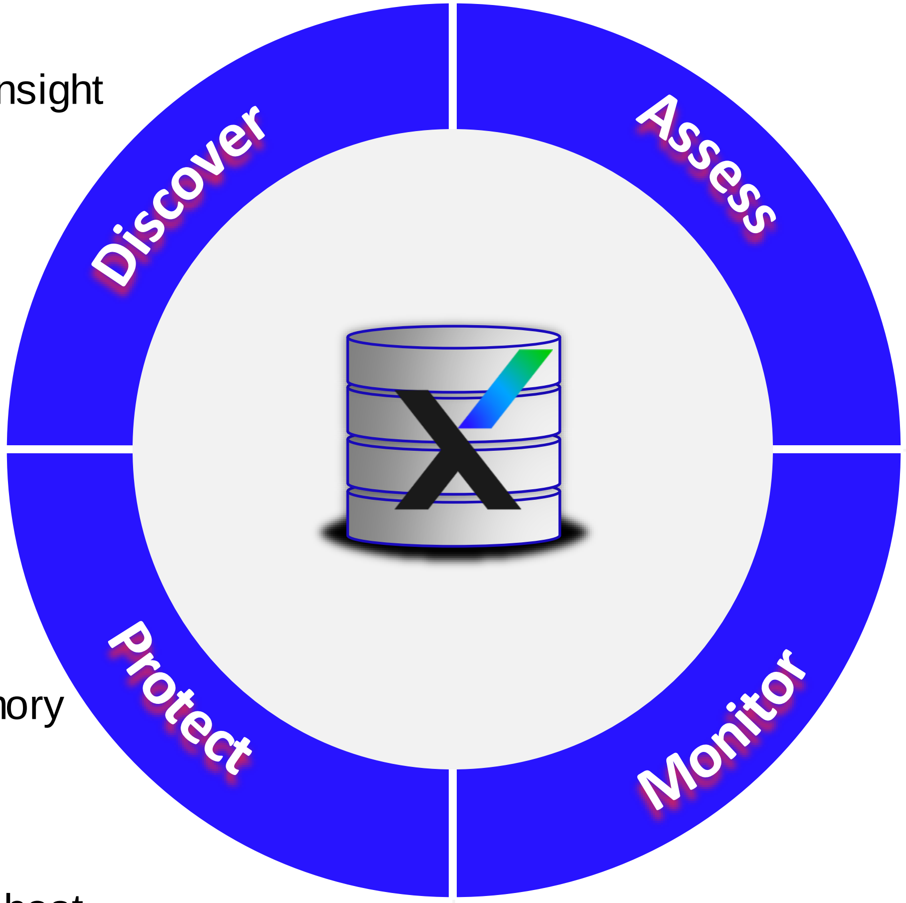
Shared Memory analysis enables deep insight into the database transactions to view:

Actual accessed objects (real ones, not parsed or guessed!)

Internal transactions including Stored procedures, Triggers, Views, Dynamic SQL and Inflow Statements

Memory Analytics is done in **real time** by analyzing the database shared memory

No snapshots or duplication of memory areas – thus no impact on performance or IO of the database host



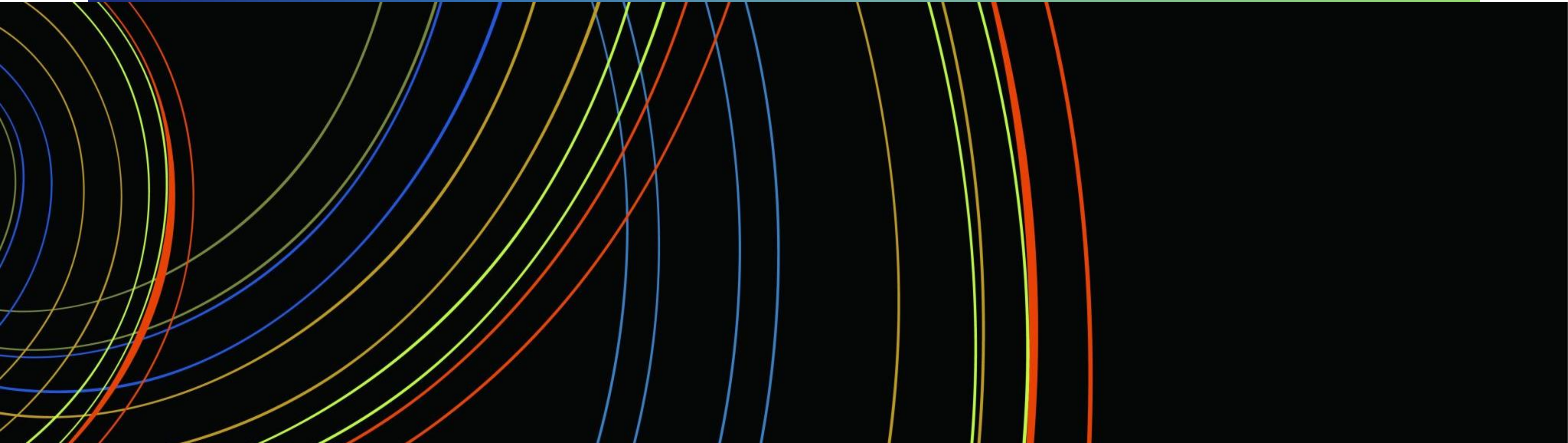
- ✓Real-time Monitoring
- ✓Enforcing Policy
- ✓Audit, Alert or Block activity

Activity Monitoring

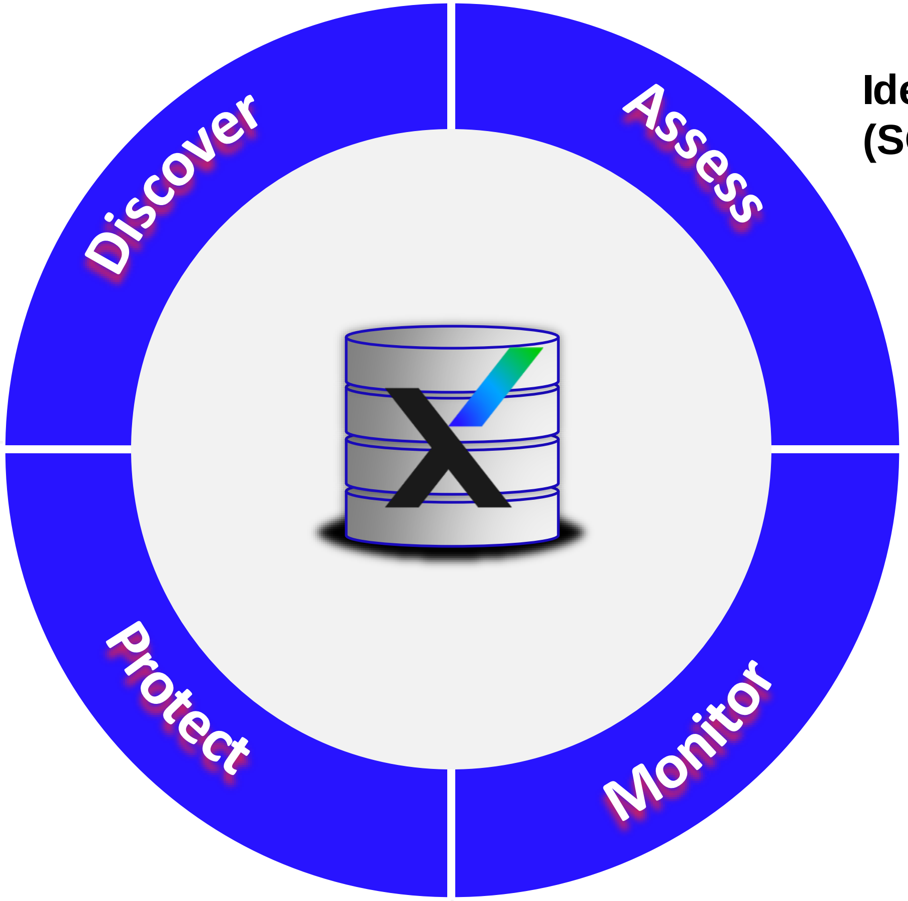
Trellix

Compensating Controls

Protection and Virtual Patching (vPatch)



Trellix Virtual Patching (vPatch)



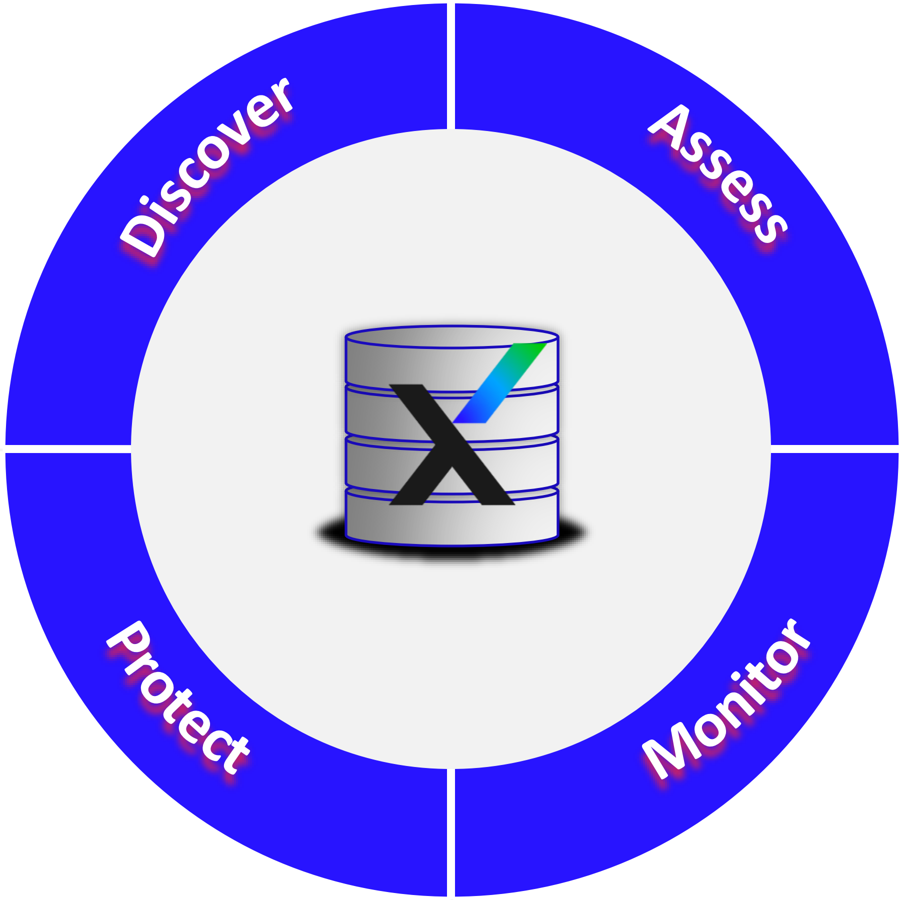
Identifies and prevents known exploits (SQL injection, buffer overflow, etc).

- Protection from known and some zero-day attacks
- **> 700** vPatch protections (continuously updated)
- **vPatch** update released within 48-72 hours from vendor patch or after zero-day attack disclosure
- **vPatch** updates automatically deployed from central management console to the relevant databases

✓ Identify and prevent exploitation attempts
✓ Known attacks
✓ Generic patterns
✓ Abnormal activity

Protection and Virtual Patching

Trellix Virtual Patching



- ✓ Identify and prevent exploitation attempts
- ✓ Known attacks
- ✓ Generic patterns
- ✓ Abnormal activity

Protection and Virtual Patching

Detects and protects the databases from various attack vectors and types

Known Vulnerabilities

Public CVEs, Internal researched vulnerabilities, Zero-Days, etc.

Behavioral Vulnerabilities

Generic SQL Injection protection, evasion attempts (i.e. obfuscation), privilege escalations, etc.

Suspicious Activity

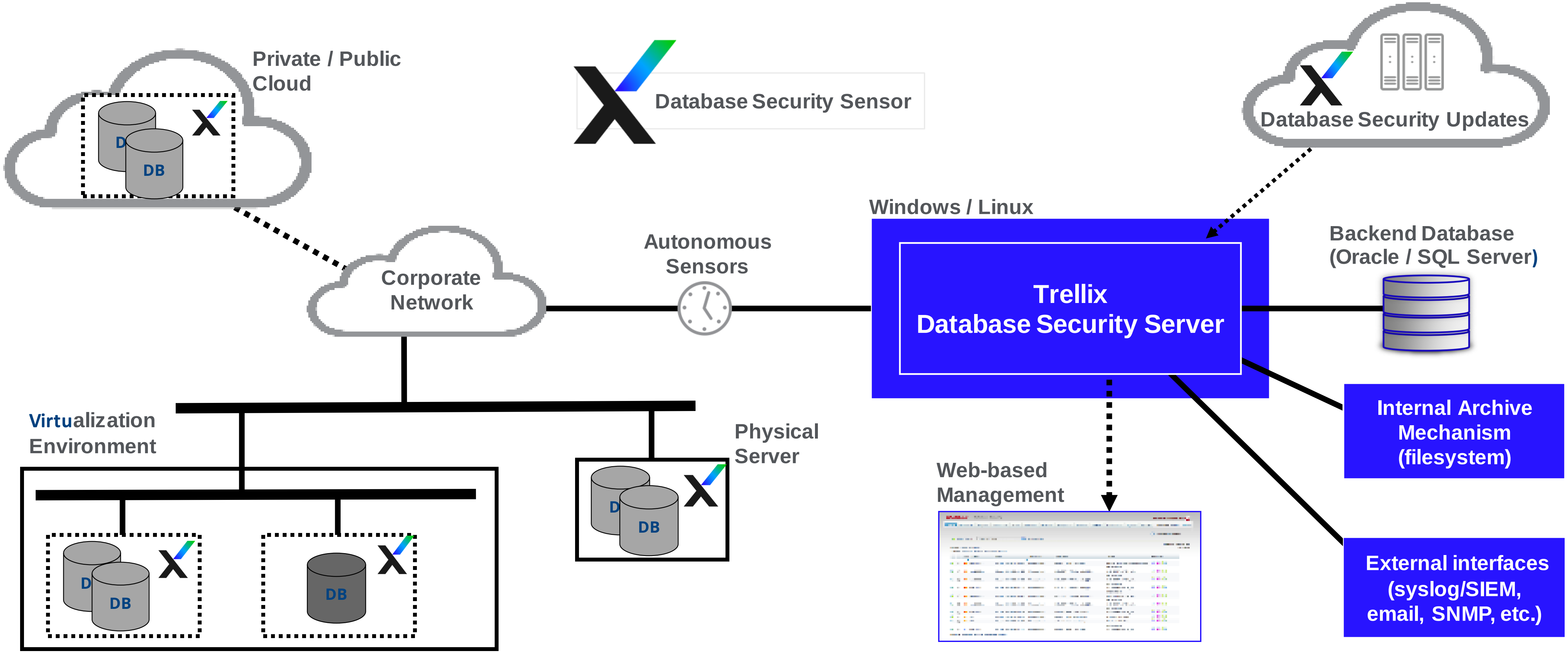
Usage of default accounts, Usage of scanning/ hacking tools, Usage of suspicious procedures, etc.

Trellix

Architecture

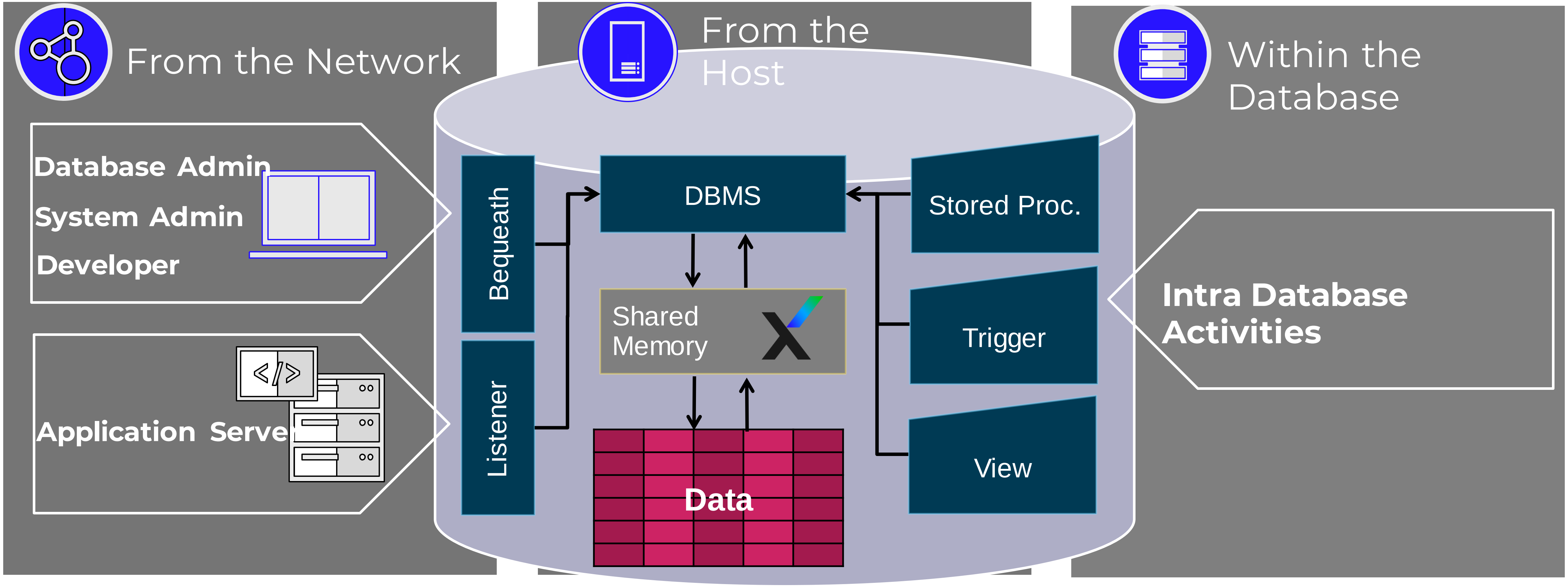
DB Security

Architecture Overview


Private / Public Cloud
DB
DB
Database Security Sensor
Database Security Updates
Windows / Linux
Autonomous Sensors
Corporate Network
Trellix Database Security Server
Backend Database (Oracle / SQL Server)
Virtualization Environment
DB
DB
DB
Physical Server
DB
DB
Web-based Management
Internal Archive Mechanism (filesystem)
External interfaces (syslog/SIEM, email, SNMP, etc.)

Sensor Architecture

Databases can be accessed in three ways:



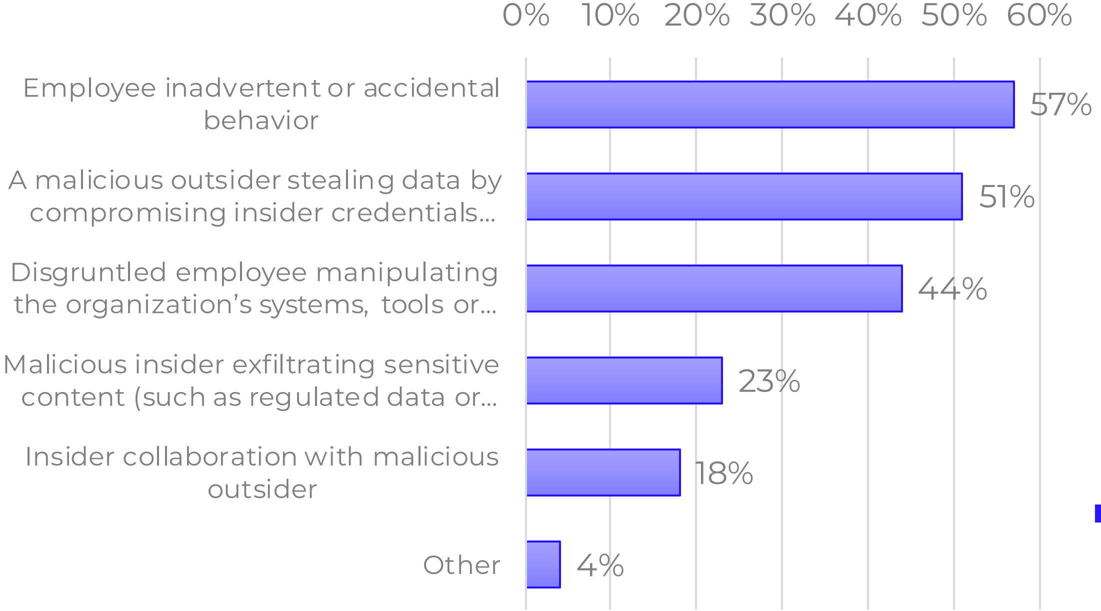
Trellix

Use Cases

Data Protection

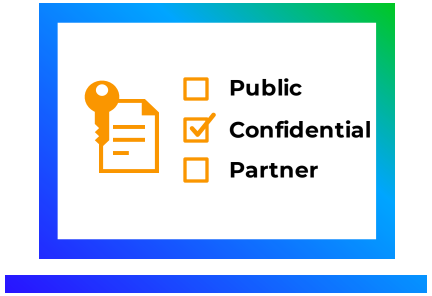
Insider Threat

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



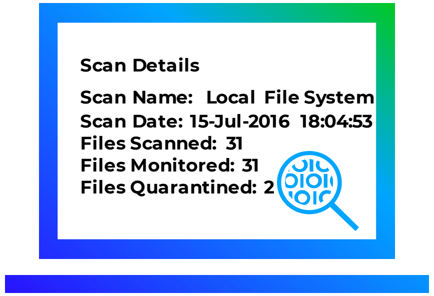
Trellix allows administrators to coach and monitor end-user Behavior

Manual **Classification**



□ Public
☑ Confidential
□ Partner

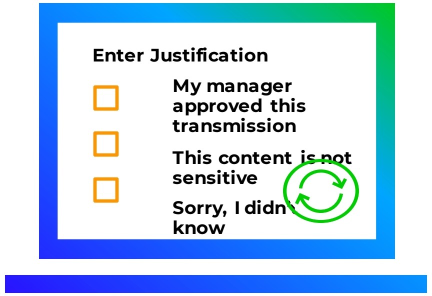
Self Remediation



Scan Details

Scan Name: Local File System
Scan Date: 15-Jul-2016 18:04:53
Files Scanned: 31
Files Monitored: 31
Files Quarantined: 2

Real-time **Feedback**



Enter Justification

□ My manager approved this transmission
□ This content is not sensitive
□ Sorry, I didn't know

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

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

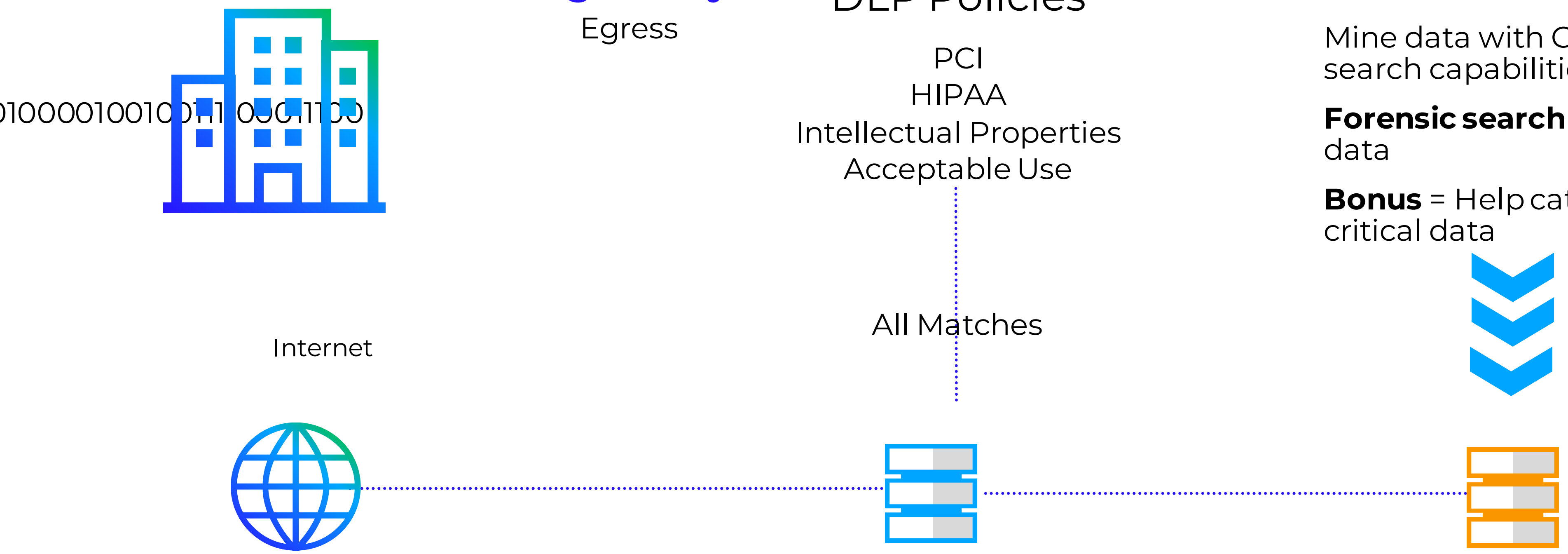
Discover and monitor across multiple data loss vectors

Unified console for management, dashboard and reporting

Trellix

Forensics Capabilities

Forensic and learning ability



Egress

010000100100111100011100

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

Demo

Data Protection Capabilities

Demonstration Guidance

Data Protection

Trellix

Access to Mdemo

https://trellix-mdemo.skytap-portal.com/

SE Resources How to Access

Data Protection

Trellix

Partner Care Team here to help with:

partnercareemea@trellix.com

msppartnercare@trellix.com

Partner Care

- **Partner Portal & Service Portal**
- **Product/Licensing queries**
- Profitability programs
- Partner Registration
- Partner Update/Certification
- **NFR Depot**
- Reports
- **Training/Partner Onboarding**
- **Lab Access**

MSP Partner Care

- **iAsset access**
- **Partner training: iAsset, PBC, MSP program, Download center**
- Partner Business center (PBC), Reporting
- Product & Licensing
- BPS Portal
- Billing
- Tenant
- Name and address updation on MSP accounts

Partner SE Technical Bookmarks

Product Technical Documentation Portal

- Product Documentation:
- https://docs.trellix.com/

- Administratorion Guides
- Deployment Guides
- System Security Guides
- Release Notes
- Hardware Guides

Cloud Lab

- CrossFire (ASH):
- https://login.trellix.com/

- MDemo:
- https://trellix-mdemo.skytap-portal.com/

- Consolidation in progress…

Communication

Partner Care Team

- partnercareemea@trellix.com

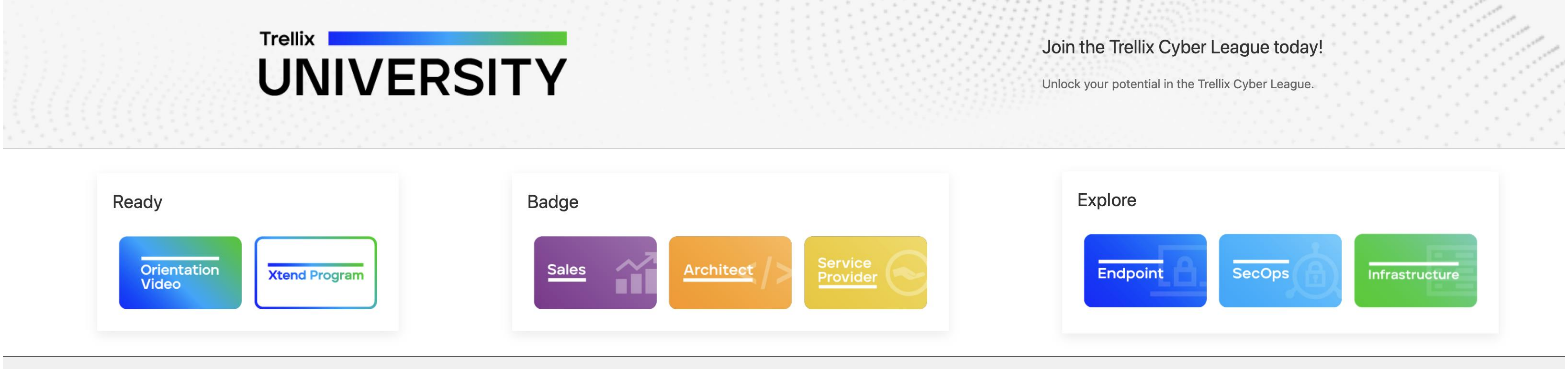
- MSP Partner Care Team
- **mspartnercare@trellix.com**

Expert Center

Knowledge Base

Forum

- Trellix-F Community:
- https://community.fireeye.com/
- Trellix-M Community:
- https://communitym.trellix.com/
  Consolidation in progress…



Join the Trellix Cyber League today!

Unlock your potential in the Trellix Cyber League.

Trellix University – Training Portal

https://training.Trellix.com

Role Based Certification Program

12 Major Products Certification Tracks

103 On-Demand Courses

Available to Partner Community at no cost!

Trellix

Partner Portal

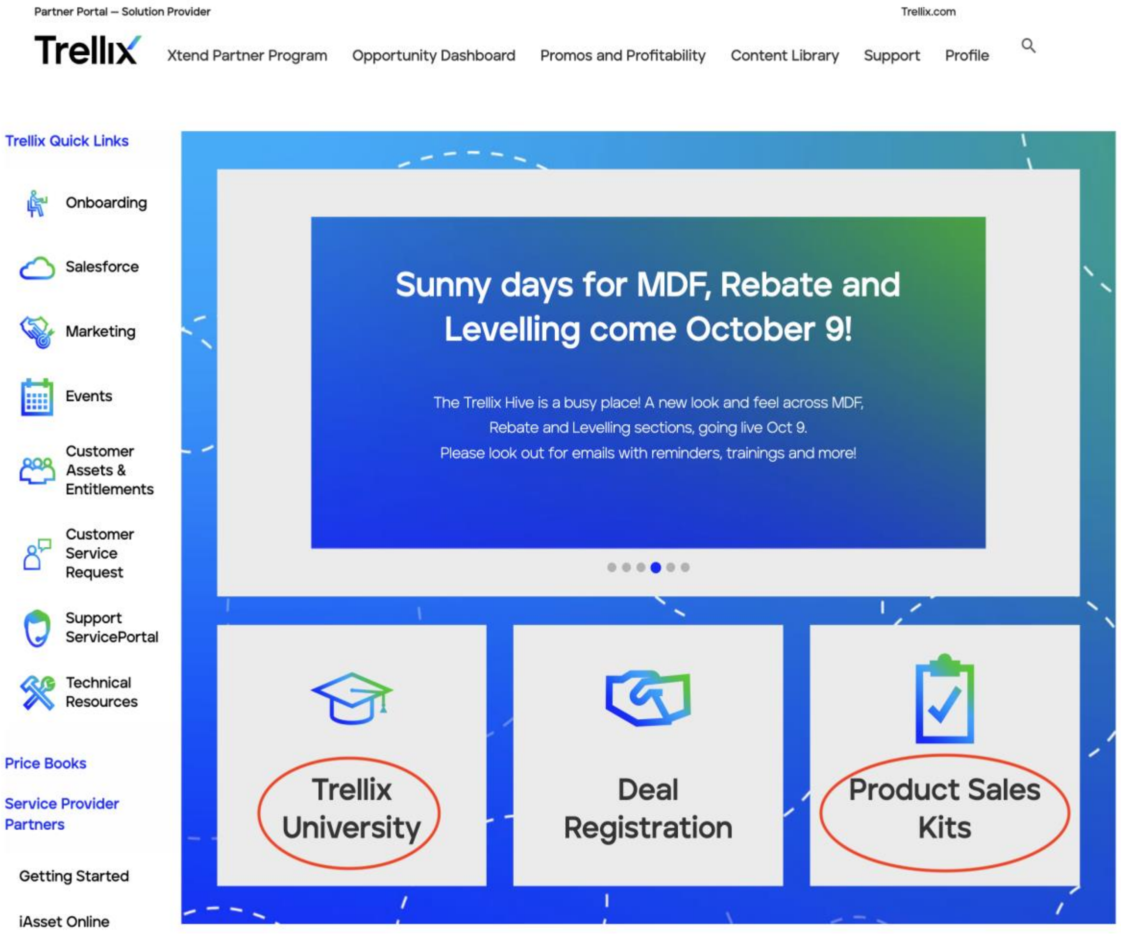
https://partners.trellix.com

- Xtend Partner Program
  - Overview
  - Program Guide
  - Newsletter
- Opportunity Dashboard
  - Registration
  - Management
- Promos and Profitability
  - Deal Registration
  - Renewals
  - Global Sales Plays
  - Rebates Guideline and Portal
  - MDF
- Content Library
  - Trellix Platform
  - Sales Resources
  - Resource Library
- Sales Tools
  - Competitive Battle Cards
  - Corporate Strategy
  - Product Solution Guides
  - Sales Plays
  - Trellix Market Place
  - 3rd Party Research
- Ordering
  - Quote and Ordering Policies
  - End User Purchase Policy
  - Price Books
  - NFR Ordering
  - Quoting Product Requirements
- Technical Documentation Portals
  - Cloud Lab Access
  - Expert Center
- Technical Support & Services
  - Customer Success Plans
  - Consulting Services

Partner Portal – Sales Kits

https://partners.trellix.com/partner/en-us/solution-provider/product-sales-kits.html

Product Sales Kits will be updated frequently



Partner Portal — Solution Provider

Trellix.com

Xtend Partner Program | Opportunity Dashboard | Promos and Profitability | Content Library | Support | Profile

Trellix Quick Links

- Onboarding
- Salesforce
- Marketing
- Events
- Customer Assets & Entitlements
- Customer Service Request
- Support ServicePortal
- Technical Resources

Price Books

Service Provider Partners

Getting Started

iAsset Online

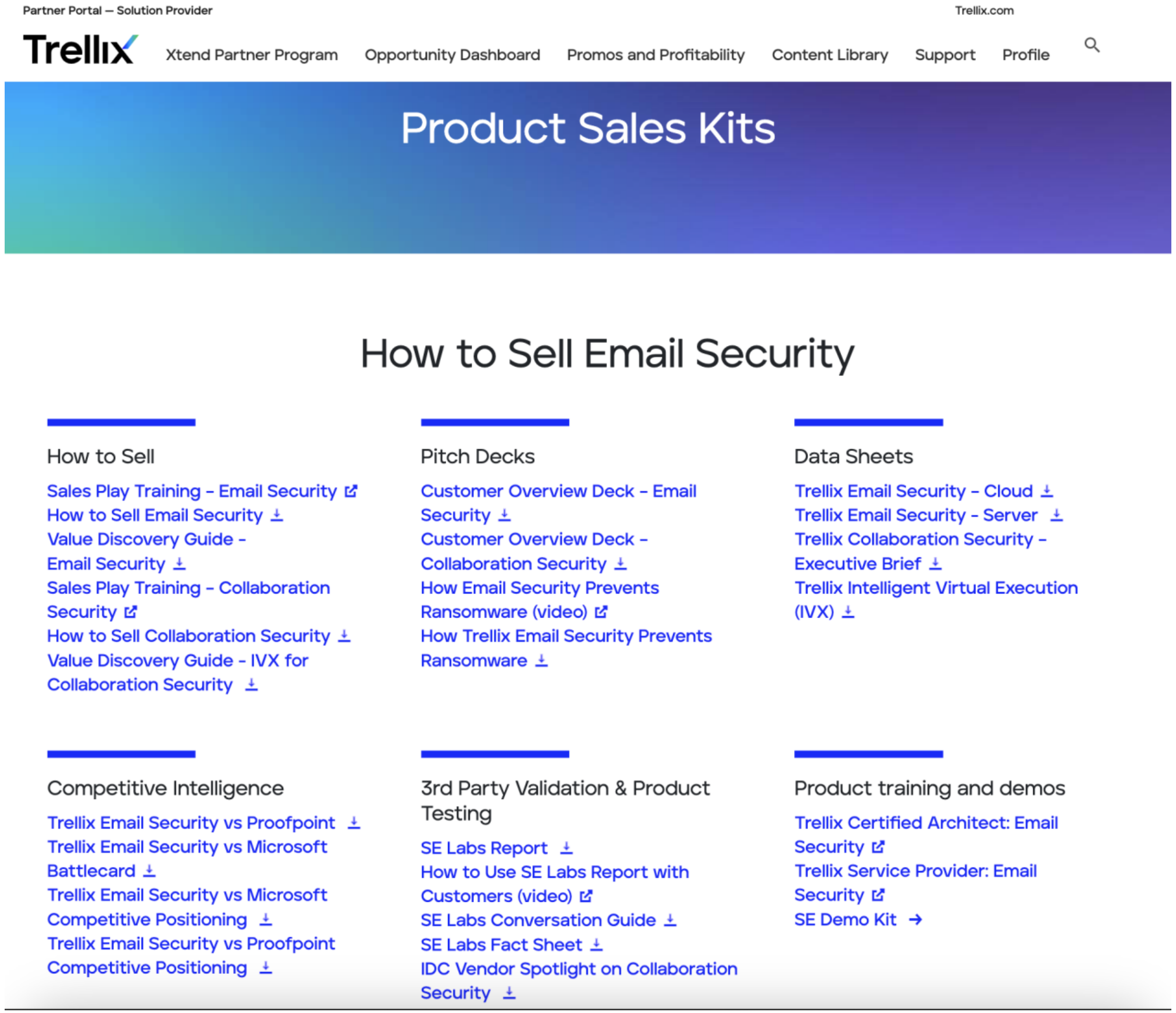
Sunny days for MDF, Rebate and Levelling come October 9!

The Trellix Hive is a busy place! A new look and feel across MDF, Rebate and Levelling sections, going live Oct 9.
Please look out for emails with reminders, trainings and more!

Trellix University

Deal Registration

Product Sales Kits



Partner Portal — Solution Provider

Trellix.com

Xtend Partner Program | Opportunity Dashboard | Promos and Profitability | Content Library | Support | Profile

Product Sales Kits

How to Sell Email Security

How to Sell

- Sales Play Training – Email Security
- How to Sell Email Security
- Value Discovery Guide - Email Security
- Sales Play Training – Collaboration Security
- How to Sell Collaboration Security
- Value Discovery Guide - IVX for Collaboration Security

Pitch Decks

- Customer Overview Deck – Email Security
- Customer Overview Deck - Collaboration Security
- How Email Security Prevents Ransomware (video)
- How Trellix Email Security Prevents Ransomware

Data Sheets

- Trellix Email Security – Cloud
- Trellix Email Security - Server
- Trellix Collaboration Security - Executive Brief
- Trellix Intelligent Virtual Execution (IVX)

Competitive Intelligence

- Trellix Email Security vs Proofpoint
- Trellix Email Security vs Microsoft Battlecard
- Trellix Email Security vs Microsoft Competitive Positioning
- Trellix Email Security vs Proofpoint Competitive Positioning

3rd Party Validation & Product Testing

- SE Labs Report
- How to Use SE Labs Report with Customers (video)
- SE Labs Conversation Guide
- SE Labs Fact Sheet
- IDC Vendor Spotlight on Collaboration Security

Product training and demos

- Trellix Certified Architect: Email Security
- Trellix Service Provider: Email Security
- SE Demo Kit →

Differentiators

Data Protection

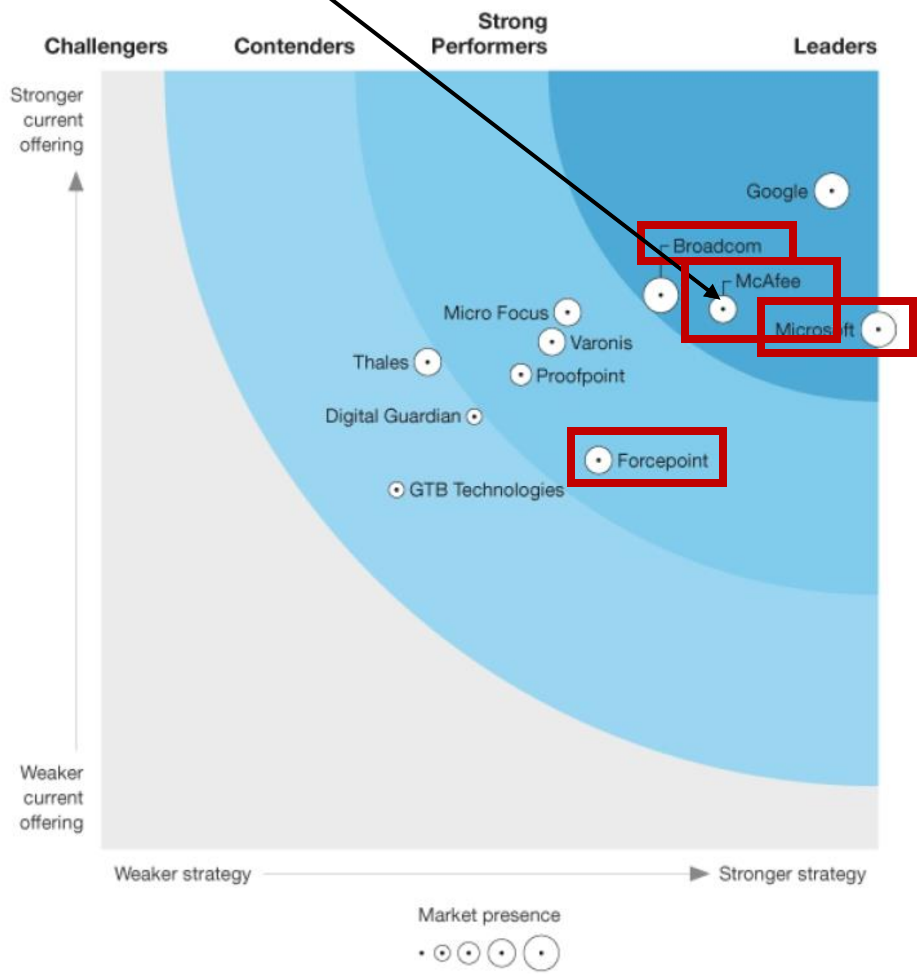
Top Competitors

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.



THE FORRESTER WAVE™
Unstructured Data Security Platforms
Q2 2021

Microsoft

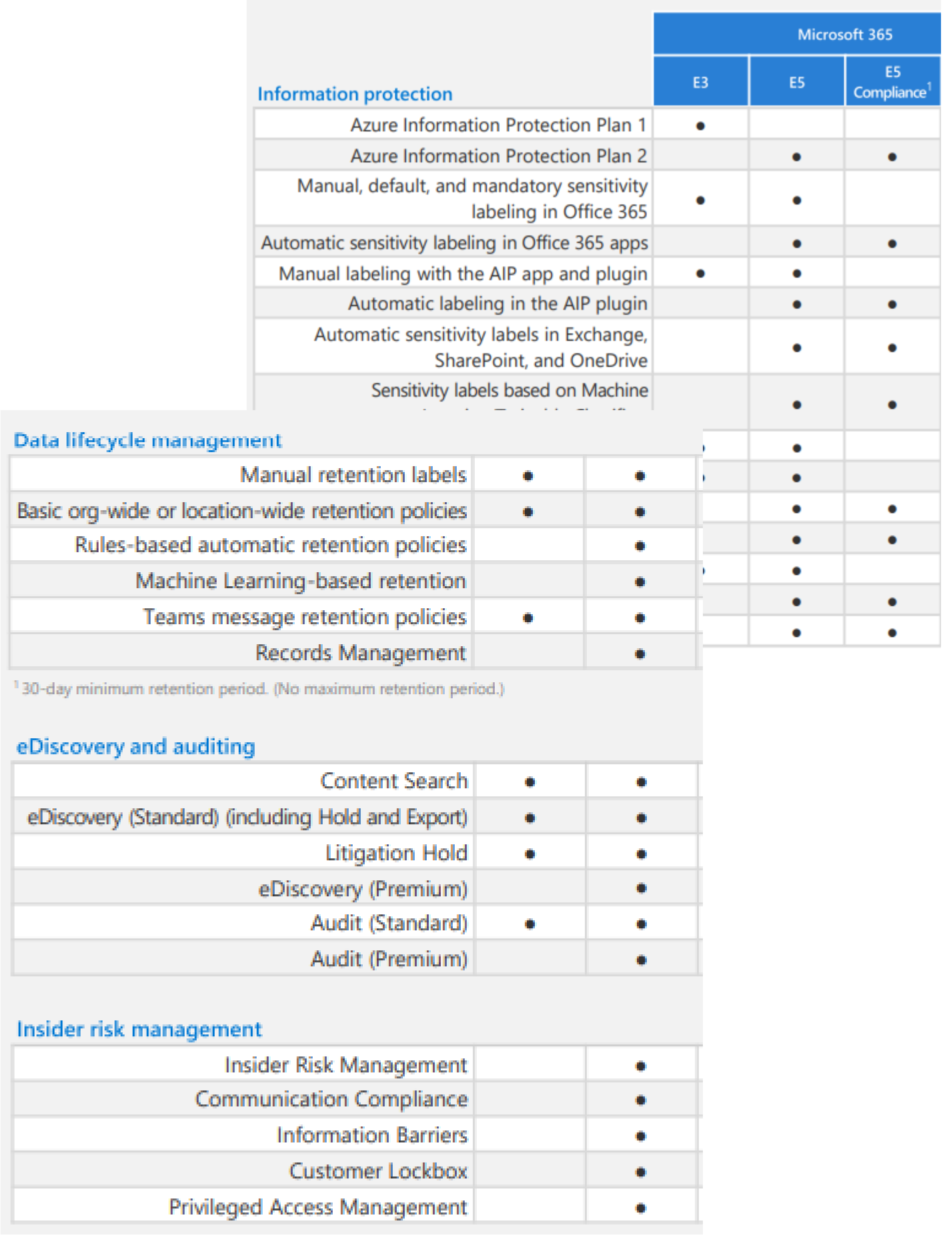
Trellix

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	E5	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

Symantec™

A Division of Broadcom

Trellix

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

Forcepoint

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

Summary Takeaways

Trellix

Microsoft

Symantec.™
A Division of Broadcom

Forcepoint

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

Point of Contacts

Data Protection

Contact us

Email

partnercareemea@trellix.com

Trellix

Thank You!