Trellix

3-6 November 2025

Data Security Workshop

Agenda

- Data Security Challenges, Solutions, Latest Innovations & Roadmap
- Architecture & Best Practices
- Key Uses Cases & Demonstrations
- Licensing & Packages
- Trellix Differentiators & Key Competitors

Trellix

Trellix

Data Security Challenges

Today's Biggest Challenges:
Data Security

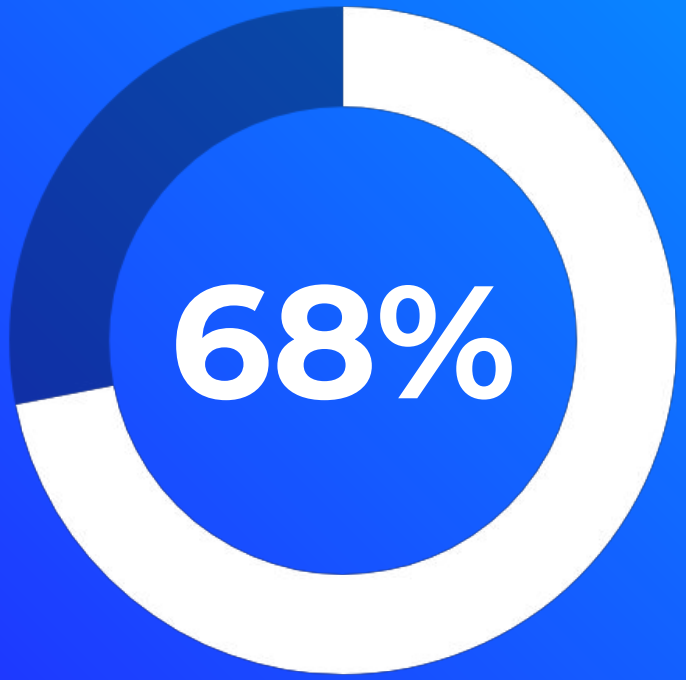
Insider Risk
Accidental and Malicious Threats

Regulatory Landscape
Complex and Time Consuming Compliance

Expanding Information Footprint
Lack of Visibility and Control

Trellix

Breaches Caused by Insider Risk



Of breaches in 2023 included a human element[1]

According to the Verizon Data Breach Investigations Report (VDBIR), more than two-thirds of data breaches could be attributed to some human element in the chain of events.

Trellix

1 - Verizon DBIR 2024

Today's Data Security Challenges

Malicious Actors

35%

Of breaches were a malicious insider attack1

Financially Motivated

90%

Of malicious insiders were financially motivated.[1]

Time to Detect

200 Days

Average time to detect and contain data breaches.2

1 - Verizon DBIR 2024
2- Averages -IBM, Verizon DBIR

The majority of insider data leaks
are the result of **unintentional or accidental** information sharing.

Understanding Market Forces

Sensitive Data is Expanding - Making it Harder to Protect

Information Storage is Growing

200 ZB

Global data storage to reach 200 zettabytes in 2025[1].

Users Do More Online

2030

The year Gartner estimates that enterprise browsers will be the core platform for workplace productivity applications

1- cybercrime magazine

Trellix

Trellix

Current Solutions Overview

Integrating Data Security within the Trellix Platform

Cloud

On-prem

Hybrid

Air-gapped

Partner Managed

Single Security Operations Console

Threat Hunting	Dashboarding & Case Management	Policy and Configuration

Engine

Detection & Prioritization	Multi-vector Correlation	Context & Enrichment
Automation & Orchestration	Guided Response	Threat Hunting & Forensics
Data Parsing & Normalization	Data Lake	Open API Framework

Security Controls

Endpoint

Network

Data

Collaboration

Cloud

3rd Party

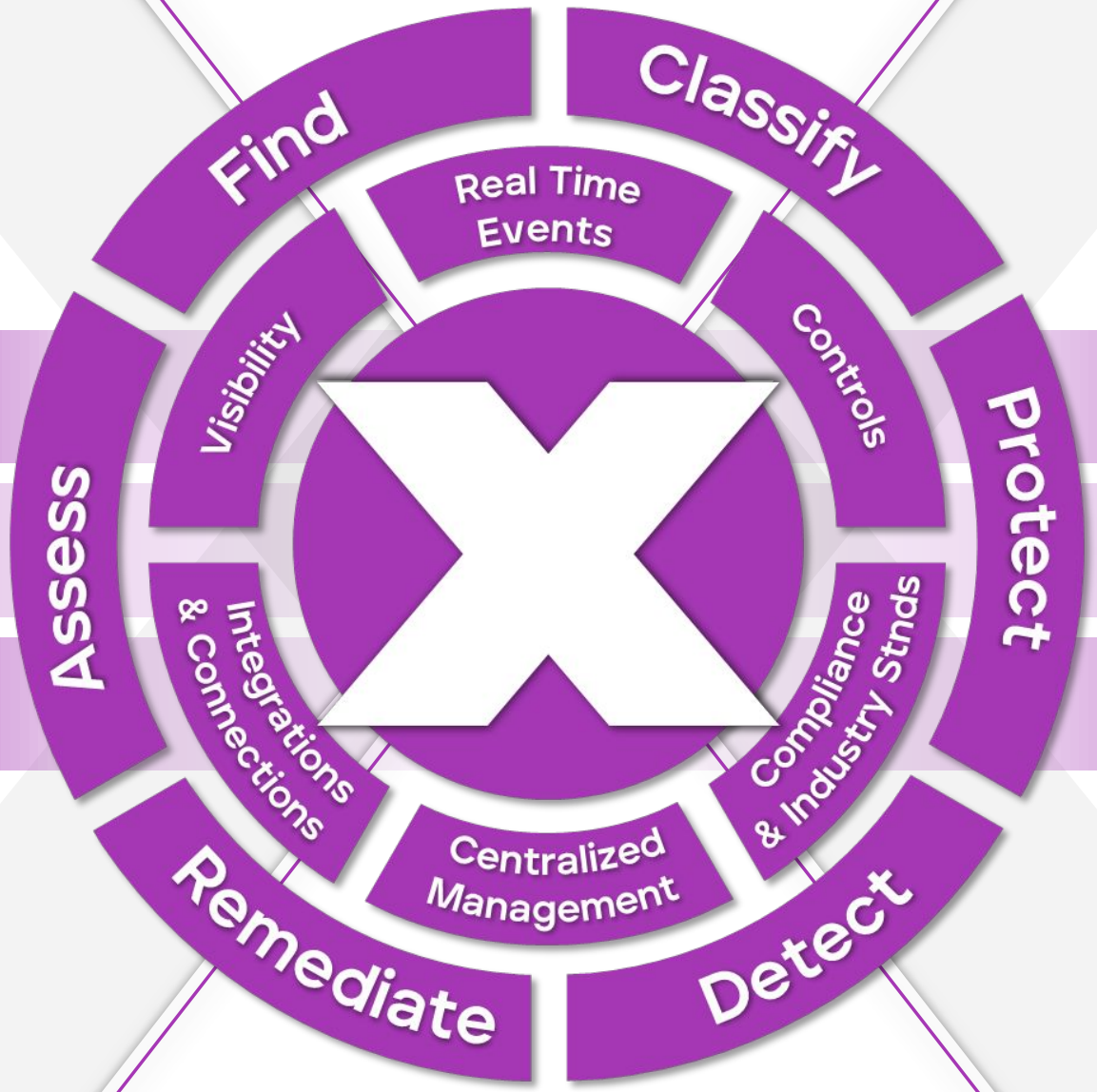
Trellix

Trellix Data Security

Trellix Data Loss Prevention

Trellix Data Encryption

Trellix Database Security



Trellix

Centralized Platform - Trellix ePolicy Orchestrator

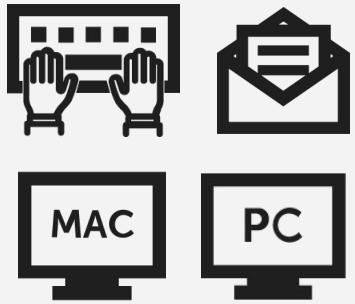
Centralized Management, Protection Across Top Threat Vectors

ePolicy Orchestrator

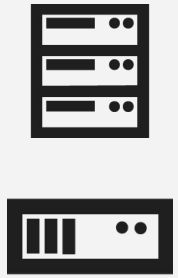
Deploy protection, administer policies, manage events, generate reports

Trellix Data Encryption

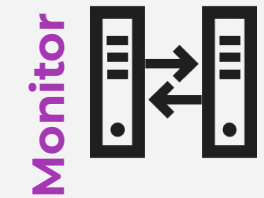
Trellix DLP Endpoint Complete



Trellix DLP Discover



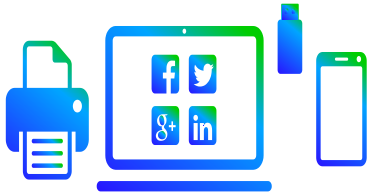
Trellix DLP Network



Seamless Integration with **Skyhigh Security** for additional cloud application protection.

Trellix

Trellix Data Security



Data on the Endpoints

Data in the Network

Data in the Database

Data in the Cloud

Discover

- More than 300 content types
- Self-remediation scan option
- On-premise and in the cloud
- OCR

Classify

- Manual
- Automated
- 3rd party integrations
- Visual Labeling

Protect

- Unified Console
- Out-of-the-box templates
- Customizable reports
- Monitor or Block
- Encrypt disks, files and USBs

Align your data protection classifications and controls needs to your Trellix Data Protection Solutions

Trellix

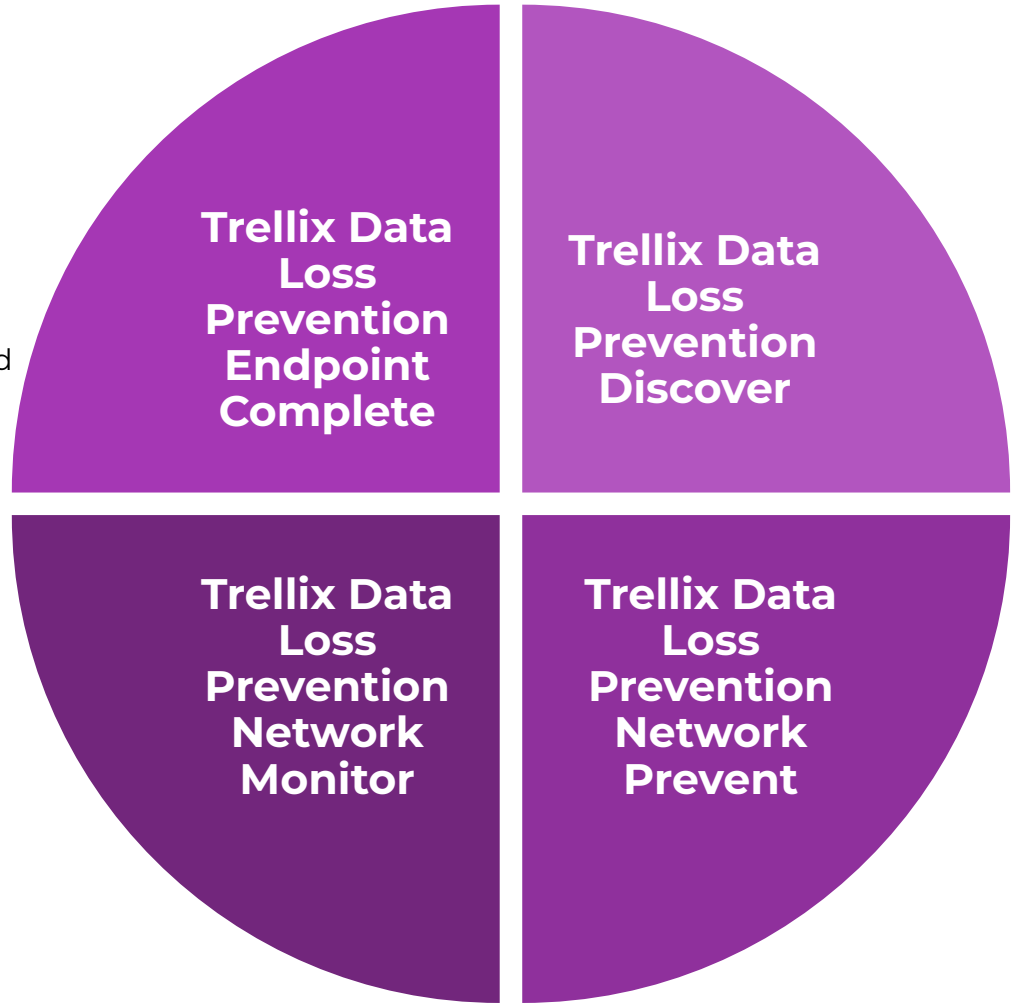
Trellix

Data Loss Prevention

Trellix Data Loss Prevention - Solutions

DLP Endpoint Complete

- Workstations and servers (Win and macOS)
- Data discovery and classification
- Compliance & reporting
- Prevents data leaks from: storage, email, web, and print controls
- User notifications & exception requests
- Device Control – content filtering, monitoring & blocking, stops unauthorized device installs



DLP Discover

- Comprehensive data inventory
- Exact data matching (EDM) – content, context & fingerprinting (400+ content types)
- Auto classification & labeling
- Integrations with 3rd party tools
- Copy. move, manage sensitive files
- Apply rights management
- Optical Character Recognition (add-on)
- Compliance & reporting

DLP Network Monitor

- Analyze network traffic in real time
- Monitors network-connected applications and storage
- Identifies data anomalies with EDM
- Capture data events in a trackable record
- OCR add-on
- Compliance & reporting

DLP Network Prevent

- Integrations with web proxies, email gateways and cloud email
- Block sensitive data exfiltration
- User notifications & exception requests
- Capture data events in a trackable record
- OCR add-on
- Compliance & reporting

Trellix

Trellix DLP products deployed on-premises or SaaS via ePO. Centralized policy administration, event management, and reporting.

OCR on Endpoint, Text Upload Blocking (Limited Availability) & Visual Labeling

OCR on Endpoint

Protect sensitive information in non-text file formats, extending capability across our entire ecosystem

- **Enhanced Visibility** - Extracts text from images, screenshots, PDF, and scanned documents
- **Multiple Language Support** - Supports most Western & Asian languages*
- **Improved Productivity** - Reduce analyst overhead in manually verifying non-text documents
- **Increase Efficiency** - Discover sensitive data stored on endpoints in non-text file formats
- **Seamless Protection** - Use existing or new content protection rules
- **Included with Data Security Suite** - Available add-on for Network DLP (today), add-on for Endpoint DLP, add-on for full DLP, and included in our top tier Data Security Suite package

Text Upload Blocking*

Protect upload of sensitive text from being uploaded

- **Enhanced Protection** - Block texts manually typed into text boxes, web forms, chat window, comments, & GenAI prompts
- **Multiple Language Support** - Supports all languages currently supported by Trellix DLP Engine
- **Reduce Risk of Social Engineering** - Blocking prevents end users from unintentionally sharing sensitive information via malicious chats, chatbots or deceptive webforms
- **Flexible Policy Enforcement** - Allow upload of PII, PCI & PHI Information only on authorized websites
- **Prevention of Unintended use by AI Models** - Avoid inadvertent IP thrift or unauthorized data utilization by AI models

**This feature is under feedback evaluation based on limited availability for testing purposes.*

Visual Labeling

Enforce document classification and promote user awareness

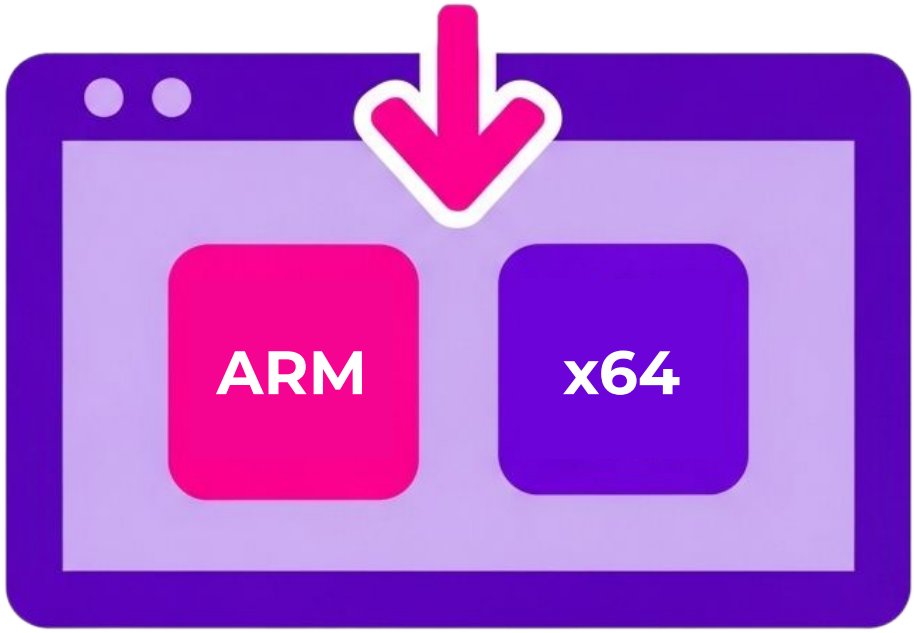
- **Strengthened Data Protection:** Enforce Single Label selection to avoid misclassification helping DLP trigger appropriate controls based on the identified sensitivity.
- **Improved User Awareness:** Clearly communicate document sensitivity through customizable and color-coding visual labels
- **Reduced End-User Error:** Minimize accidental data sharing by making sensitivity classifications immediately visible to all users.
- **Enhanced Compliance Adherence:** Facilitate compliance with data handling regulations by ensuring documents are clearly marked according to their sensitivity level.

Trellix

Trellix DLP Endpoint

Feature Overview - 11.12.1 Windows OS

- **Single installer:** A single installer package will support both ARM compatible and x64 processor architectures, simplifying deployment across an organization's computing devices.
- **Streamlined deployment:** The correct software version for the processor is automatically delivered to the endpoint, saving time and resources.
- **Comprehensive functionality:** ARM users benefit from all features of Trellix DLP Endpoint Complete, (Windows) including advancements like Optical Character Recognition (OCR), enhanced visual labeling, and expanded support for UAS drives in removable storage rules.



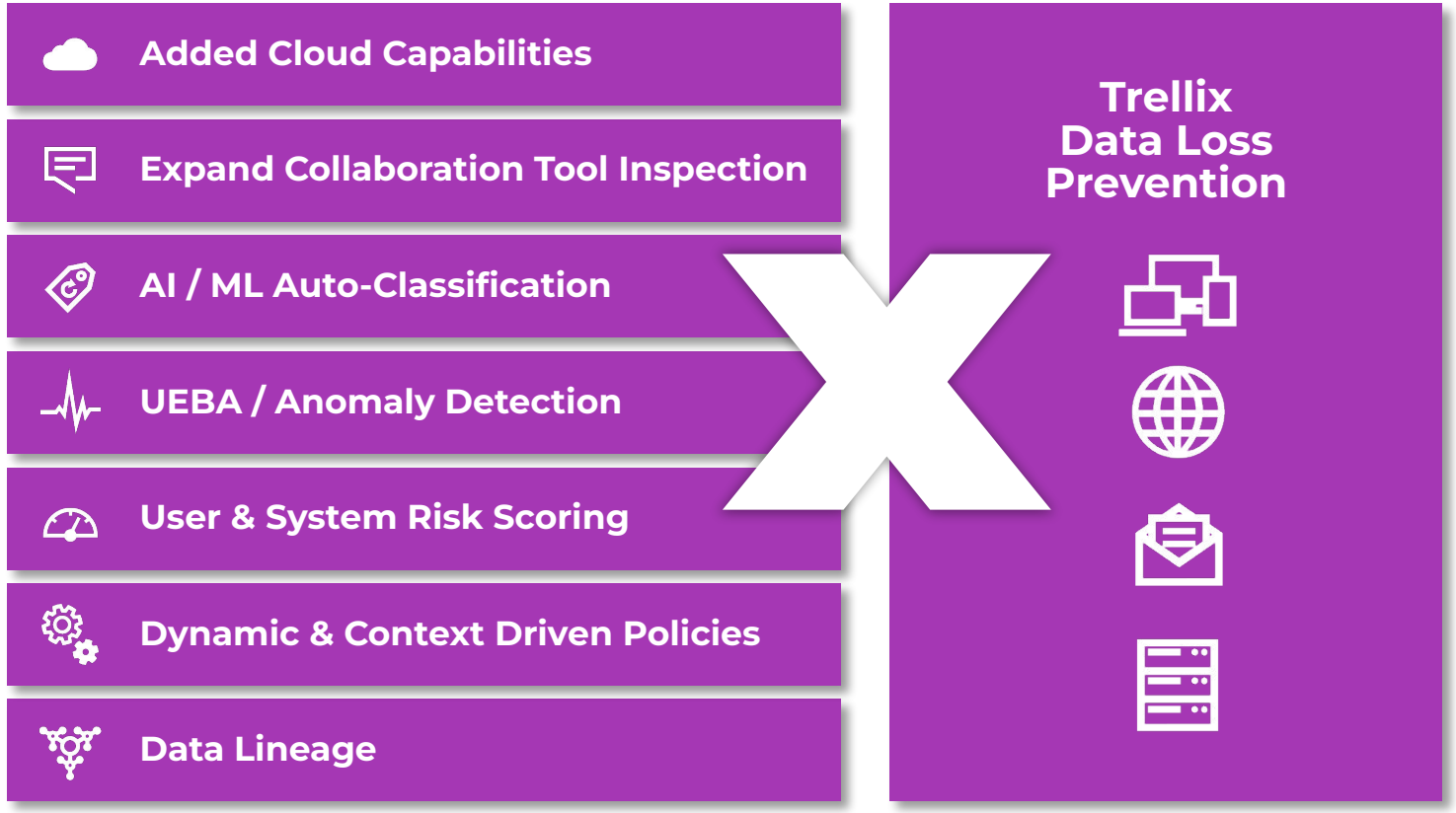
ARM support is included with DLP Endpoint Complete - no separate license or SKU is required.

Trellix

Intelligent Data Loss Prevention

Looking Ahead in the DLP Roadmap

- Data expansion in cloud storage
- Data is created and interacted with in new ways
- Find the data that matters
- Make creating and updating policies easier
- Risk based prioritization
- Better investigative tools



Trellix

Trellix

Data Encryption

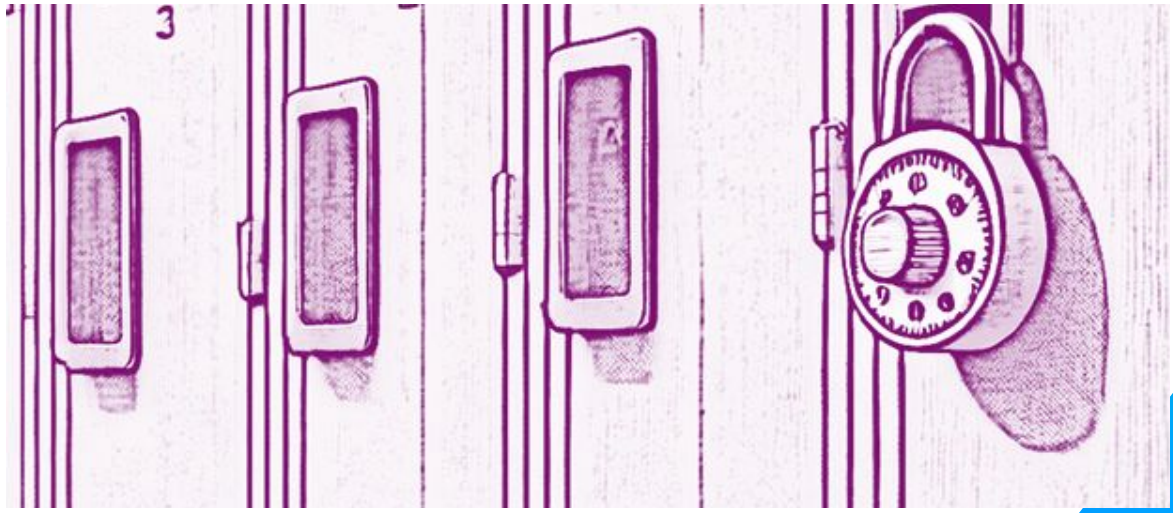
Trellix Full Disk Encryption (FDE) Options

Trellix Drive Encryption

- Integrated with Active Directory
- User authentication
- Access control
- Authenticate multiple users to the same device
- User self-service recovery
- Multi-factor authentication (MFA)
- Compliance features
- FIPS 140-2 compliant

Trellix Native Drive Encryption

- Simplify management of Bitlocker & FileVault
- Bring devices into compliance & monitor for gaps
- Report on BYOD systems
- Automatically provision new systems
- Report on compliance
- User recovery
- Re-apply encryption if disabled
- Rotate recovery keys when used or expired
- Maintenance mode for unattended patching
- Compliance reporting for lost or stolen devices

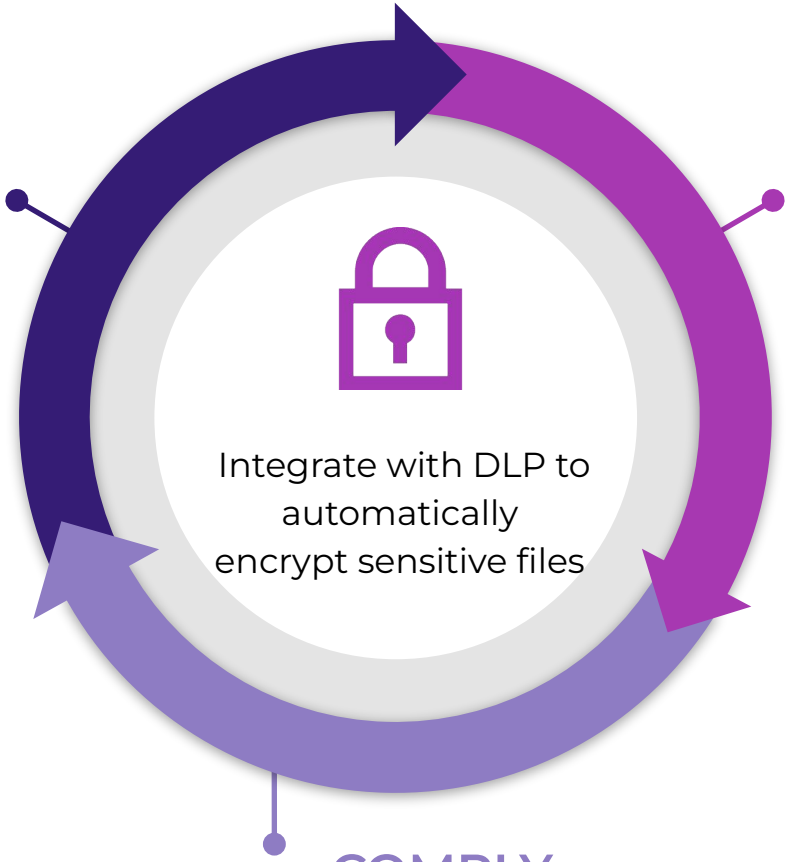


Trellix

File & Removable Media Protection

MANAGE

- Compatible with Windows and macOS, manage via ePO
- Integrate with Active Directory
- Variety of authentication methods (MFA, smart card, etc)



PROTECT

- Data from unauthorized transfer to external media
- Encrypt data prior to transfer to removal media
- Self extracting encrypted email attachments

COMPLY

- Enable separation of duties (role-based access and file sharing)
- Auditing and compliance reporting

Trellix

Looking Ahead at Data Encryption

Drive Encryption SaaS (December 2024)

Cryptographic transitions for NIS2, FIPS-140-3 and CNSA 2.0 (post-quantum)

Cloud-native IDP support (Entra, Okta)

Trellix

Circa H2 2024. Subject to change.

Trellix

Database Security

Trellix Database Security

Find and defend databases and the information they contain

ONE COMPREHENSIVE OFFERING!

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

Trellix Database Security

Vulnerability Manager

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

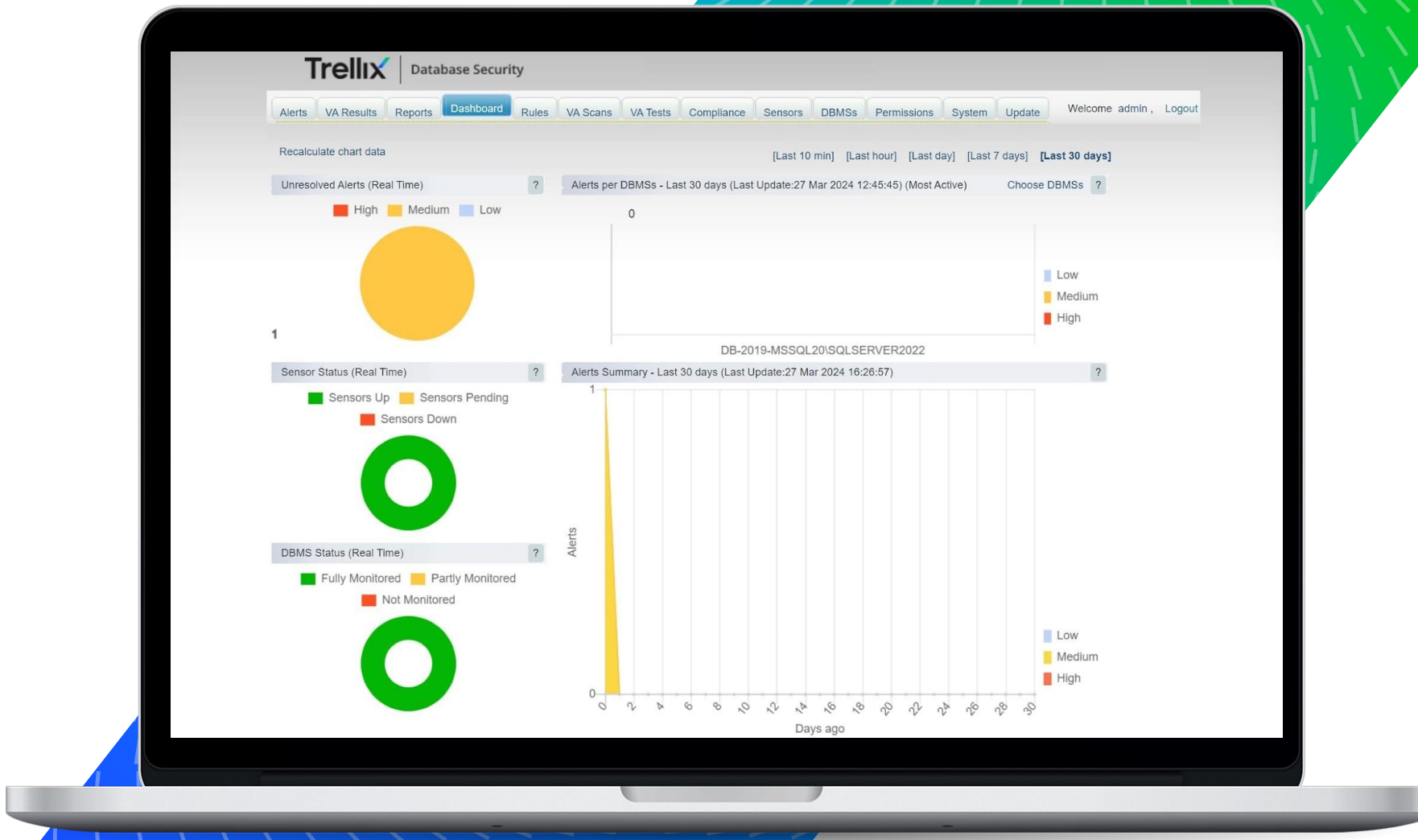
Database Activity Monitoring

- 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 Database Security v10.2 New Features

- **AWS RDS (plug-in based) DB Support**
  - MySQL
  - Maria DB
  - PostgreSQL
- **New Databases Supported**
  - Oracle 19.24, 19.25
  - MySQL (8.0.37 to 8.0.40)
  - Mongo DB 7.0
  - Maria DB 11.3.2, 11.4.2 and 11.5.2
  - PostgreSQL - 16.0 to 16.4 and 15.7, 15.8
  - PostgreSQL Enterprise Edition - 14.3, 13.16, 16.0 to 16.4
- **Performance Improvement!**
  - 2K ➜ 12K Queries Per Second
- **Monthly vPatch Content Updates**
- **Quarterly Vulnerability Assessment Content Release**
  - v206 - for Oracle v19.x



Amazon RDS Support

Secure your cloud-native databases on AWS with enterprise-grade controls

- Purpose-built protection for your managed MS SQL and Oracle databases
- Security that scales automatically with your RDS database growth and demands.
- Faster onboarding with minimal performance impact
- Improves cloud database adoption by mitigating operational risks
- Gain visibility and control over your Amazon RDS Databases
- Comply with regulatory and internal security requirements

Trellix

Trellix

Data Security Suites

Data Security Product Packages

Package	What it Includes	IRT	GRC	EIF
Trellix Data Loss Prevention Suite	All Data Loss Prevention Products	✔	✔	✔
Trellix Data Encryption Suite	All Data Encryption Products	✔	✔	
Trellix Data Security Endpoint Protection Suite	Data Loss Prevention Endpoint Complete and Data Encryption Products	✔	✔	
Trellix Data Security Network Suite	Trellix DLP Network Prevent, Trellix DLP Network Monitor, and Trellix DLP Discover	✔	✔	✔
Trellix Database Security	One comprehensive Database Security offering with all critical features	✔	✔	✔
Trellix Data Security Suite	All DLP and Encryption Products	✔	✔	✔
Trellix Database Security for Data Security Suite	Add-on for Database Security to Data Security Suite with *discounted* rate	✔	✔	✔

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

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.

Less Complex, Less Regulated → **More Complex, More Regulated**

Data Encryption Suite

Available on prem, hybrid, or via Saas

Value
Protect enterprise and removable data from attacks

- Safeguard device and file data
- Secure devices for remote use
- Stop data exfiltration to removable media and establish separation of duties for file sharing
- Flexible for organizations with mixed environments (Win/MacOS)
- Centralized administration, events, reporting in ePO

Data Loss Prevention Suite

Available on prem, hybrid, or via Saas

Value
Extend protection for data on endpoints, across network storage and shared over web browsers

- Visibility and control across top data threat vectors
- Flexible policies, scale to your environment
- User coaching and notifications
- Data discovery, classification
- Out of the box compliance policies, reporting
- Flexible for organizations with mixed environments (Win/MacOS)
- Protection for devices connected to the endpoint

Data Security Endpoint Protection Suite

Available on prem and hybrid

Value
Defend endpoint data, stop data exfiltration, safeguard device and file data

- Visibility and control across top data threat vectors
- Data discovery, classification
- Out of the box compliance policies, reporting
- Secure devices for remote use, stop data exfiltration to removable media and establish separation of duties for file sharing
- Flexible for organizations with mixed environments (Win/MacOS)
- Centralized administration, events, reporting in ePO
- Safeguard device and file data

Database Security

Available on prem
Add on for DATA and standalone

Value
Protect databases and the sensitive information they contain

- Compliance with mandates for data activity monitoring
- Protect organization's most sensitive data
- Find databases and sensitive information
- Save time and resources with scan/patching
- Meet compliance guidelines
- Stop unauthorized users from accessing sensitive data
- Automate currently manual tasks and protect databases that no longer receive manufacturer patches

Data Security Suite

Available on prem, hybrid, or via Saas

Value
Protect the data that matters throughout the entire lifecycle

- Visibility and control across top data threat vectors
- Data discovery, classification
- Out of the box compliance policies, reporting
- Secure devices for remote use, stop data exfiltration to removable media and establish separation of duties
- Flexible for organizations with mixed environments
- Centralized administration, events, reporting in ePO
- Safeguard device and file data
- Avoid financially motivated malicious insider attacks and accidental data leakage
- Speed up and simplify compliance activities

Trellix

DLP Endpoint & Network Additional New Features

DLP Endpoint

- Optical Character Recognition
- Browser Text Upload Protection
- Enhanced Visual Labeling
- Plug and Play Rules Support for UAS Device
- Block Data Copy to Network Shares
- Universal Windows App Support
  - Snipping Tool
  - Screen Recorder
- ARM Support
- Webdav Support for Evidence Transmission and Storage (MAC)
- Clipboard Support (MAC)
- Airdrop (MAC)
- Quality, Performance & Security Improvements (MAC)

DLP Network

- DLP Network is now powered by Alma Linux
- Supports new validators
- Confidence Threshold
- AD Authentication
- Admin Password Complexity

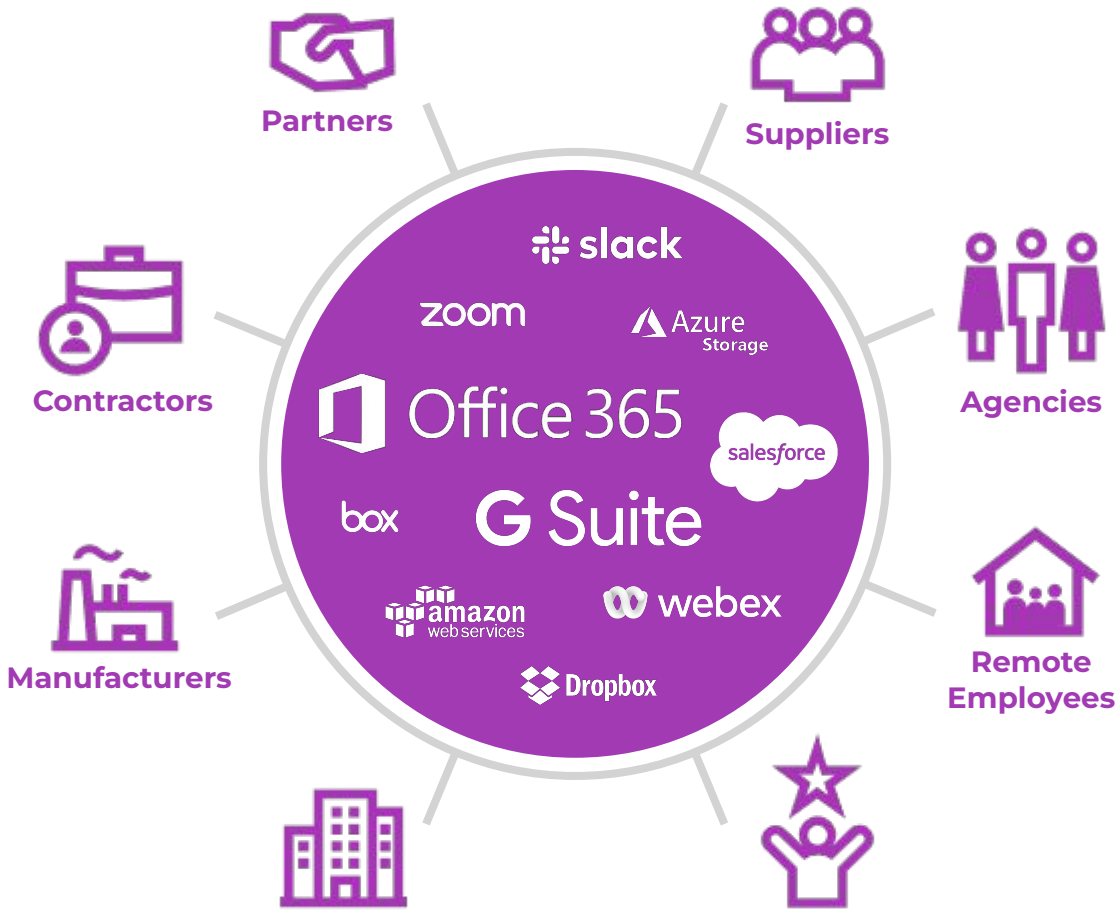
DLP SaaS Extension

- Support for new incident fields
- Custom Queries & Reports
- Persistent Incident Manager Views
- Performance Improvements
- Microsoft Entra ID Integration for DLP Policies
- S3 Bucket Configuration optional for Device Control only deployments
- New built-in custom validators

Trellix

Deeper Integration with Trellix ETP & IVX for Collaboration Security

- Additional enhancements to support more options for resolution
- Coverage for more cloud applications
- Visual Labeling
- Native integration with DLP SaaS (Data Security Engine - No appliance needed)



Currently Supported Cloud Apps:

- Slack
- Slack Enterprise
- Box
- Amazon S3
- Microsoft Teams
- Microsoft Sharepoint
- Microsoft OneDrive
- Microsoft Azure Blob Storage
- Dropbox

- Slack
- Slack Enterprise
- Box
- Amazon S3
- Microsoft Teams
- Microsoft Sharepoint
- Microsoft OneDrive
- Microsoft Azure Blob Storage
- Dropbox

Trellix

Trellix Database Security

ONE COMPREHENSIVE OFFERING!

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

Trellix Database Security Supported Databases:

On-premises: Oracle, Microsoft SQL Server, MySQL, PostgreSQL MariaDB, Sybase, DB2, SAP HANA, Percona, Teradata

On AWS RDS: MariaDB, MySQL, PostgreSQL

Supported Operating Systems: Windows, Linux, Solaris, AIX, HPUX

Trellix

Trellix Data Security - What's Next?

	1H 25	2H 25	NEXT
ENTERPRISE READY	**Hybrid Security** • **Encryption SaaS migration** • **Cloud Native Database Security** • **Enhanced Visual labeling**	**Future Readiness** • ARM Native Support • IPv6 Support • DBS support for Azure IaaS • **Azure/Entra ID integration**	**Seamless Security** • Post-Quantum Cryptography • Apple SSO/Enterprise Connect • Native Browser Integrations: Edge, Firefox, and Island • DBS support for GCP Cloud SQL
INTELLIGENT DATA SECURITY	**Data Insights** • **OCR Expansion to Endpoint** • **UAS Device Handling**	**Risk Management & Visibility** • AI Data Risk Dashboard • Helix Integration with Wise Events • Relaunch DBS Insights & Analytics Hub	**Intelligent Efficiency** • AI Data Classification • AI Policy Builder
DATA SECURITY ENGINE	**Streamlined Operations** • **Integration ready APIs** • **Content inspection tools & health check**	**Expanded Detection** • DLP native integration with email and collaboration security	**Comprehensive Control** • DLP integration with endpoint and network security • DLP as a service integration

Trellix

Trellix Data Security Engine (DSE)

We're consolidating and re-architecting our DLP engine to bring you:

- **Smarter, Faster Data Protection**: Experience enhanced DLP capabilities integrated across your security controls, with new features like AI, delivered quicker across deployment types.

- **Simpler Solutions, Broader Reach**: Enjoy an improved user experience, streamlined integrations, and expanded coverage for new use cases.

Trellix

Trellix AI Capabilities in Development

Trellix Wise for DLP

Customer **design partners** are currently providing feedback to refine product requirements and user experience, prior to participating in early adopter/beta testing.

Intelligent Data Classification Powered by Wise

- Accelerate data discovery with intelligent content analysis and enhanced matching
- AI-driven technology identifies and tags sensitive content while adapting to the organization's unique classifications over time
- Reduce false positives while finding more sensitive data

Intelligent Policy Building Powered by Wise

- Converts simple queries into actionable DLP policies through an intuitive interface
- Walk admins through policy configuration with user-friendly prompts and recommendations
- Create effective enterprise-grade security controls, based on organizational requirements

Guided Event Resolution Powered by Wise

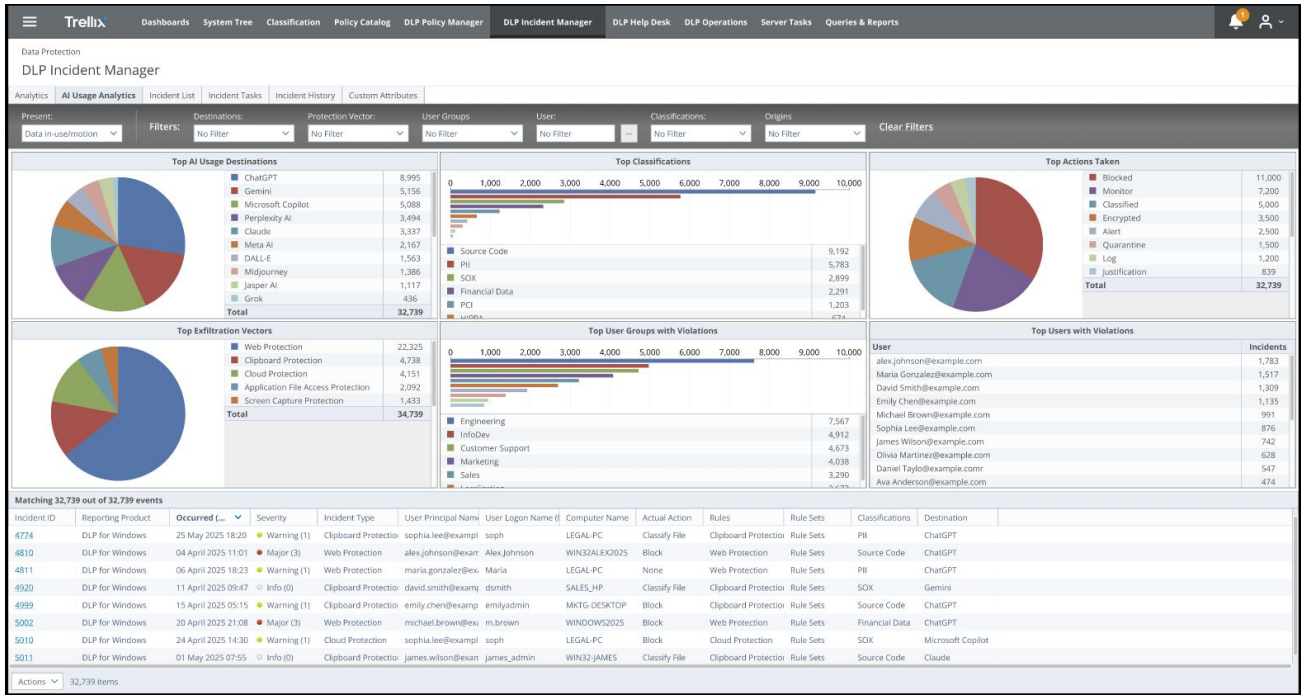
- Correlate related events, assess severity, and provide rich insights about potential data breach risks
- Offer step-by-step guidance for swift incident resolution and risk mitigation.
- Enable a quick focus on critical incidents requiring immediate attention

Trellix

Trellix DLP AI Data Risk Dashboard

One View is All You Need

- **Shadow AI** is an emerging use case that organizations are eager to identify and track - this new dashboard can help.
- Organizations need **visibility** into how and where users are sharing sensitive information with AI tools.
- Trellix DLP Endpoint monitors file application rules, web activity, and top sensitive data loss vectors (copy/paste, file upload) that can **find data leakage through AI tools.**
- Teams can **review and take action on incidents** directly from the dashboard.



Coming in December to DLP Endpoint Complete - look for the **demo environment** in November!

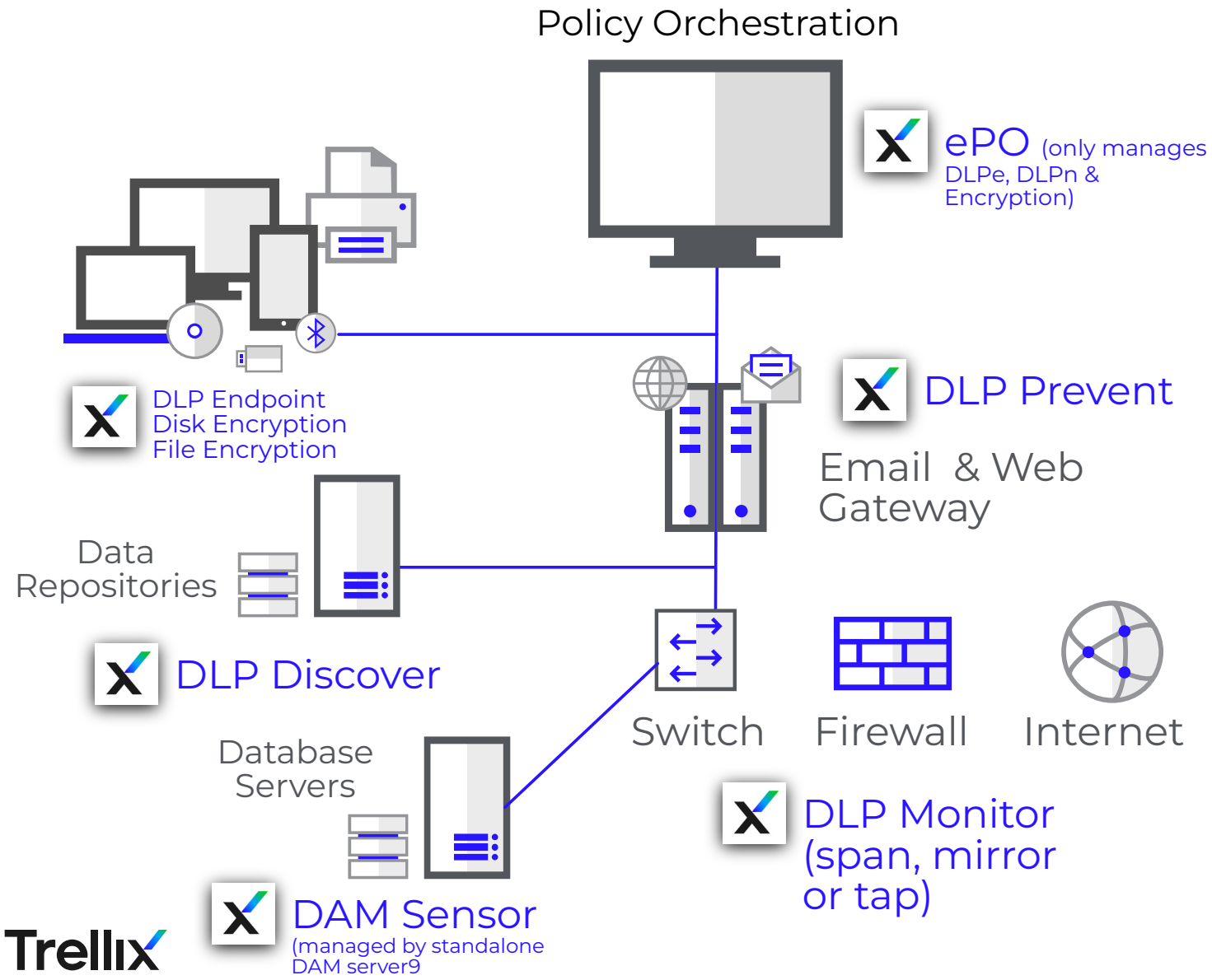
Trellix

Trellix

Architecture & Best Practices

General Architecture

Simplified endpoint & network with full set of product suite

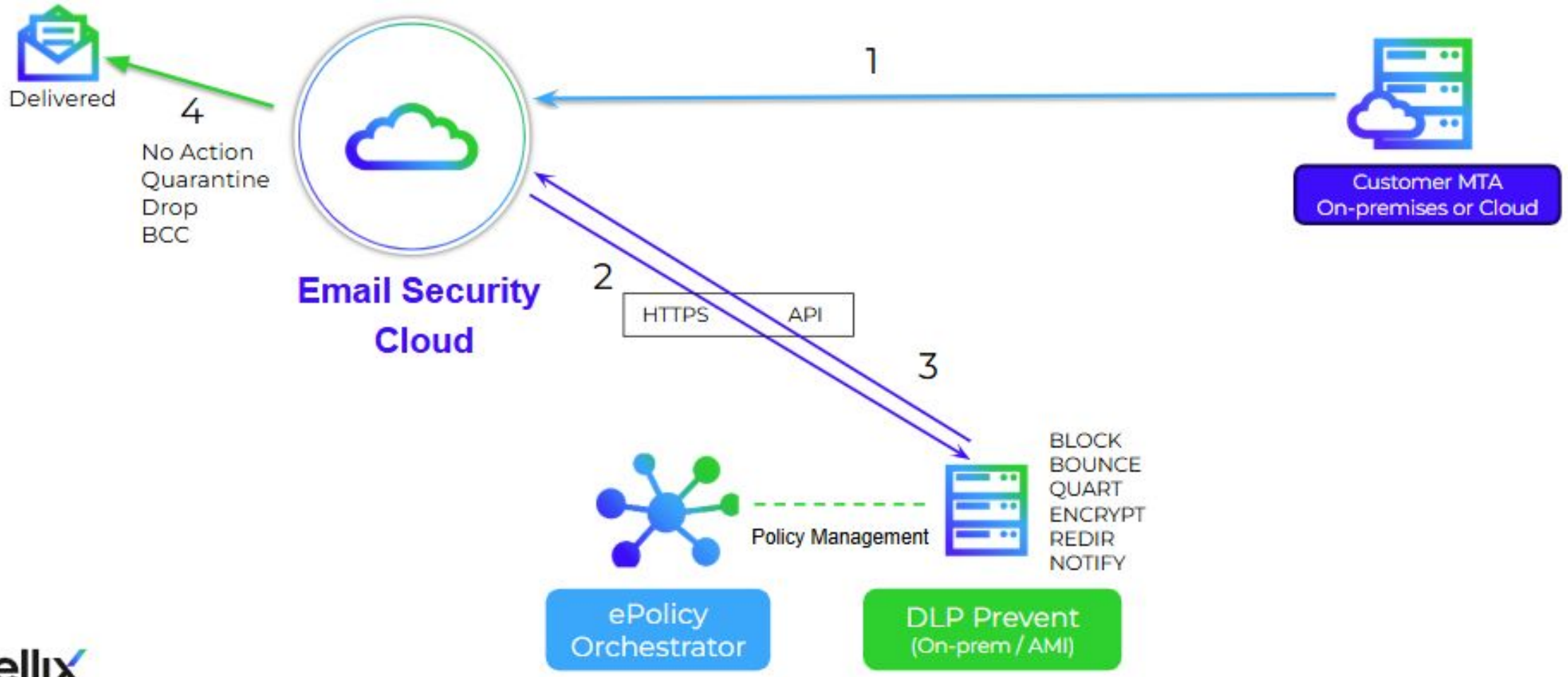


- **Trellix ePO** performs policy configuration and incident management for all Trellix DLP products
- **Trellix DLPe and Trellix Device Control** monitor and restrict user data use. Trellix DLPe also scans endpoint file systems and email
- **Trellix DLP Discover** scans files from local or cloud repositories 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
- **Trellix Database Security** actively monitors databases and generates incidents, detect vulnerabilities and take actions based on custom or predefined policies

Trellix

Email Security and DLP Architecture

API Integration: No Complex Mail Routing. No Impact to Mail Flow



Trellix

Best Practice: Choose the correct Disk Encryption Solution

Job to be done	Notes	BitLocker	FileVault	TNE	TDE
Protect the OS & data from unauthorized access	To apply encryption, some form of *authentication* is required at the pre-boot authentication screen. There should be some human element to the process of *authorizing* (or unauthorizing) a user's access to that data.	x	✓	x	✓
Simplify management of the solution by using a single intuitive console	Trellix architecture enables all governance workflows to occur within a single ePO console for all security needs. In contrast, Microsoft solutions often involve multiple separate management interfaces.	x	x	✓	✓
Bring devices into compliance quickly	BitLocker's reliance on GPO for configuration delays enforcement via InTune. Trellix ePO on the other hand has fine-grained control of policy enforcement intervals, allowing quick time-to-compliance of full disk encryption policies.	x	?	✓	✓
Grant or revoke access to specific users	This requires the notion of *identity*, and is a recommendation of NIST SP 800-111. Trellix Drive Encryption provides full access management, including workflows for revoking access of users to any/all devices.	x	?	x	✓
Increase security using MFA	Smartcard multi-factor authentication is required for phishing-resistant authentication (recommended by NIST SP 800-63B), or to eliminate the use of passwords. Note that TPM and BitLocker USB startup keys are not tied to user identities.	x	x	x	✓ (G)
Minimize user authentication prompts	A user can perform a single sign-on, and be taken straight to their Windows desktop.	x	x	x	✓
Provide a seamless localized user experience	Locale and keyboard layout support helps to avoid the pitfalls that BitLocker experiences, where an enhanced PIN may be set in one keyboard layout, but pre-boot will default to En-US.	x	✓	x	✓
Allow users to reset forgotten credentials without helpdesk support	InTune provides self-recovery for BitLocker but does not help the user to reset their credentials. Trellix Drive Encryption has multiple self-recovery options that include credential reset.	x	?	x	✓
Use FIPS cryptography without forcing OS into full FIPS mode	BitLocker supports FIPS mode, but requires the entire OS to use FIPS cryptography. This generates compatibility issues with user applications that use Windows cryptography.	x	✓	x	✓
Ensure encryption remains applied	Local administrators of the device can force BitLocker and FileVault to decrypt, against the needs of the organization. With Trellix Drive Encryption it is not possible for any local users to remove the encryption.	x	?	x	✓
Provide access control evidence for compliance purposes	When tasked with meeting regulations such as GDPR, PCI-DSS, HIPAA etc, certain evidences may be required during the auditing process. Trellix Drive Encryption does the heavy lifting, ensuring the latest state of encryption and access control is reported accurately, and an audit log to show the last-known access control activity on a lost/stolen device.	x	x	x	✓
Automatically unlock volumes on trusted networks (good for headless / server instances)	BitLocker supports full OS and data (✓✓) volume network unlock, but requires a Windows Deployment Services server, DHCP configuration, and certificates. Native Drive Encryption only supports data (✓) volume network unlock (OS volume remains unprotected), but everything is managed within ePO, and there is no requirements to stand up servers.	✓	x	✓ (onprem)	x

? - Depends on chosen MDM capabilities

G - SaaS parity gap - not being delivered in first release of TDE SaaS

Trellix

Best Practice: Leverage Key Seismic Resources

For further help you in your DLP Sales and Demo, we have key elements in Seismic (main site here):

- Trellix DLP Intellectual Property Web - Presentation
- Trellix DLP Discover (Network) Classify US PII
- Trellix DLP and FRP Intellectual Property - Removable Media - Presentation
- Trellix DLPe and NDLP PII - Web
- Trellix DLP and FRP PII Demo - Removable media - Presentation
- Trellix DLP and FRP PII Use - Removable Media
- Trellix DLP and FRP Intellectual Property - Removable Media
- Trellix DLP Discover Intellectual Property - Presentation
- Trellix DLP Discover Intellectual Property
- Trellix DLP Intellectual Property - Web
- Trellix DLP Discover (Network) Classify US PII - Presentation
- Trellix DLPe and NDLP PII Web - Presentation
- Trellix Data Security
- Demos

Trellix

Trellix

Key Use Cases & Demonstration

Find & Classify Your Sensitive Data

Data Loss Prevention

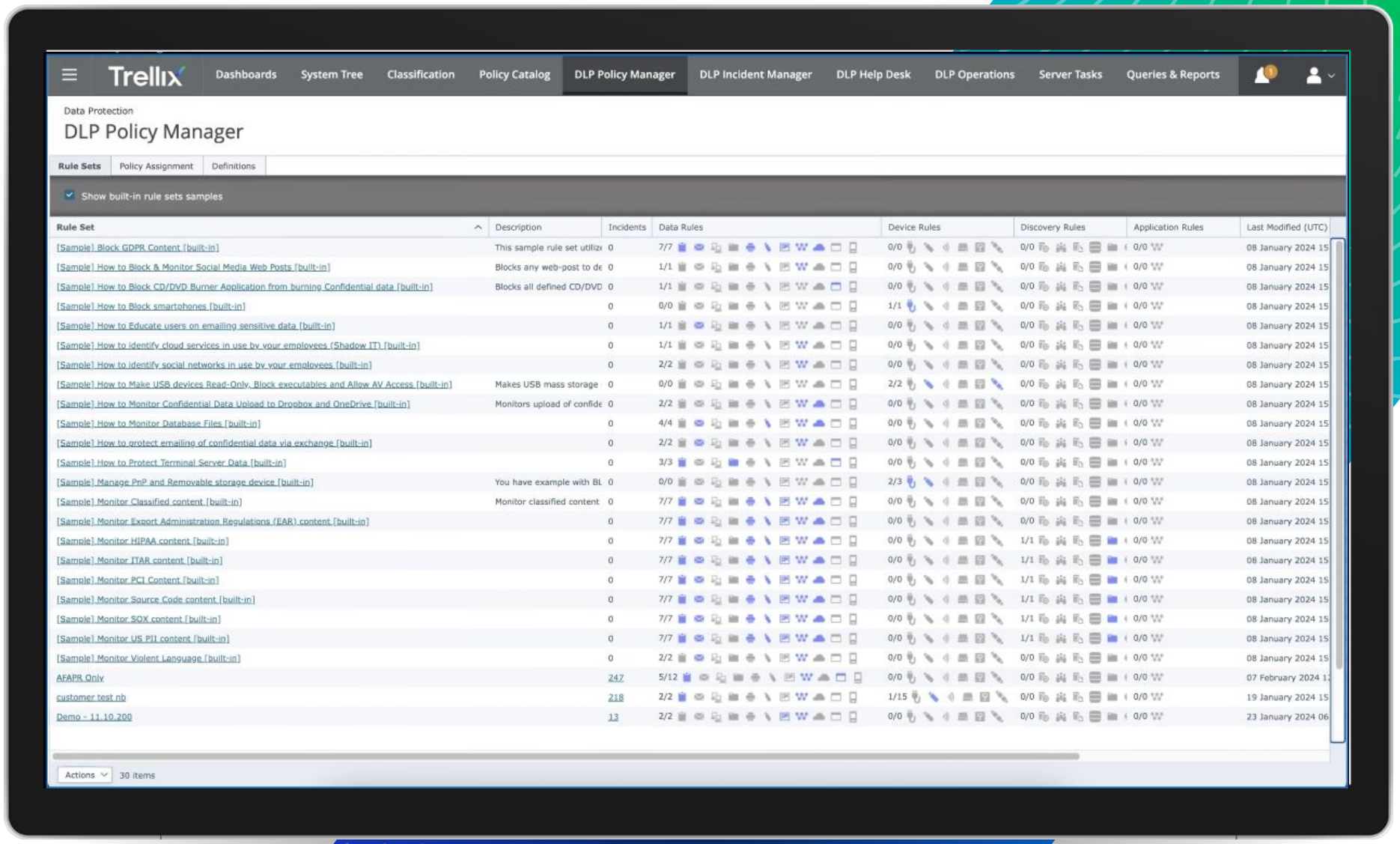
- 400+ file formats
- Out-of-the-box rules for PII, PHI, PCI, etc.
- Visibility across the top threat vectors
- Exact Data Matching (EDM) limits false positives

Trellix Data Loss Prevention Endpoint Complete

Trellix Data Loss Prevention Discover

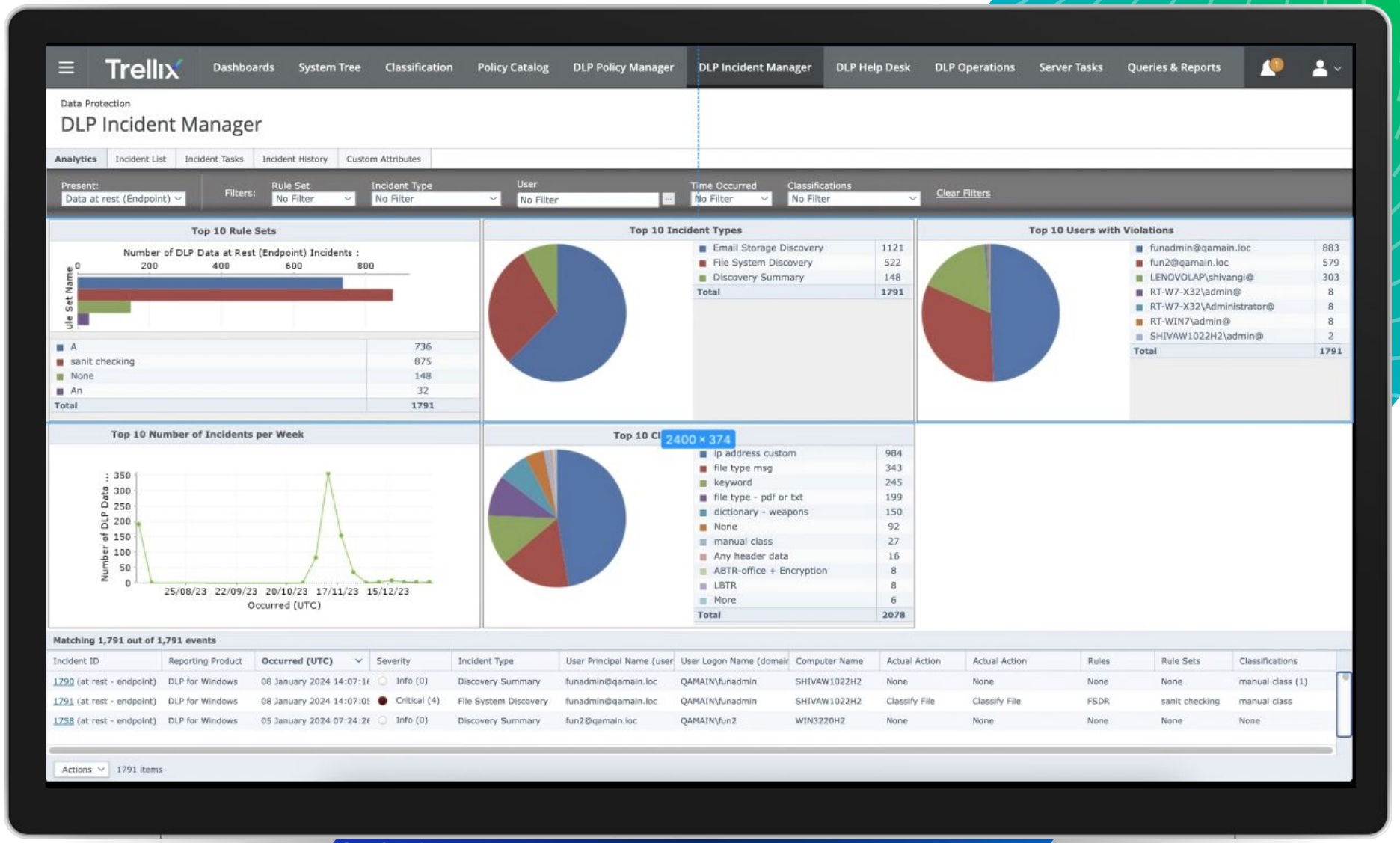
Trellix

Out of the box policies



Trellix

Easy to Use Dashboards and Reports



Trellix

Protecting Sensitive Information on Web Browsers

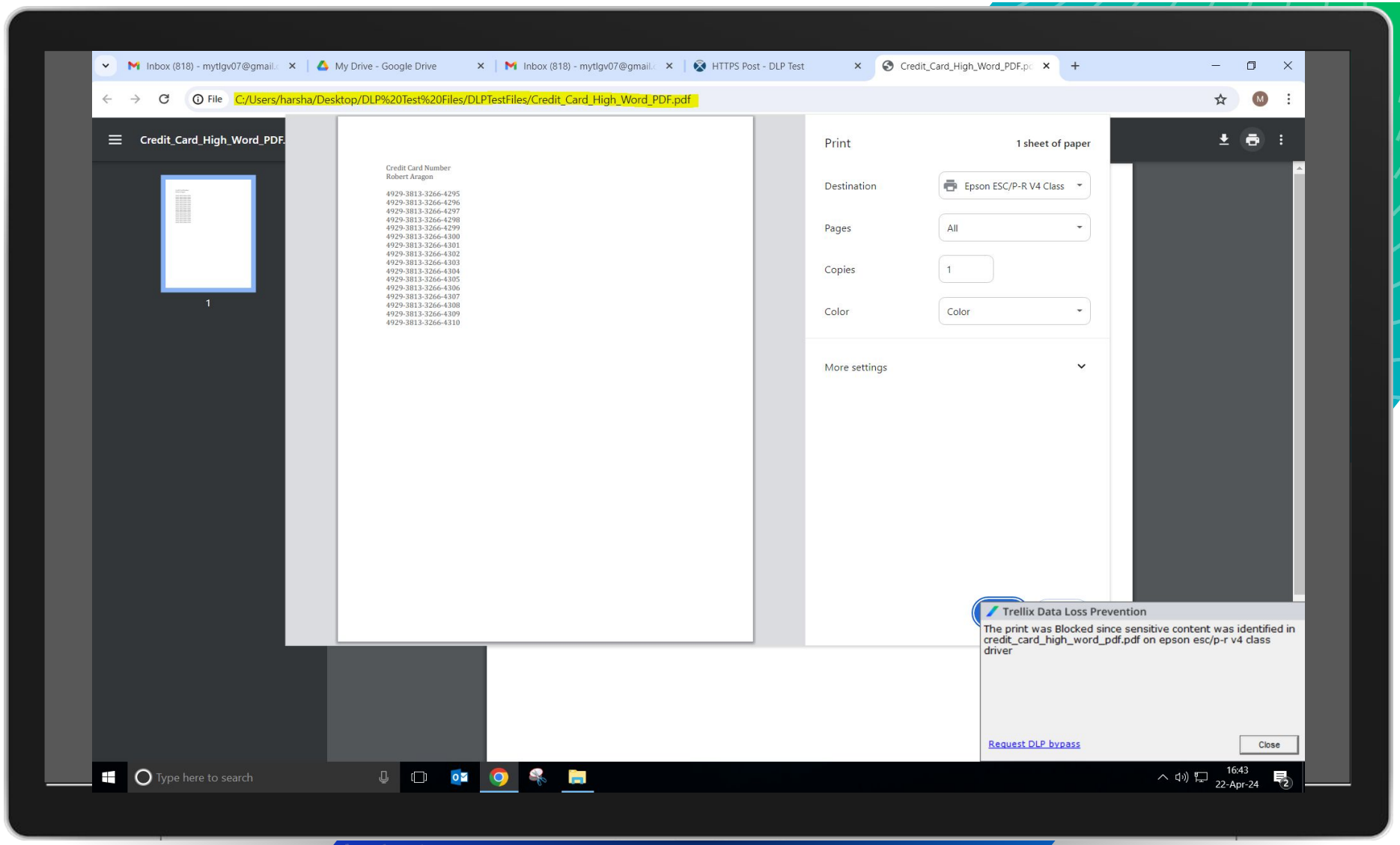
Data Loss Prevention Endpoint

- Extend DLP policies to protect information shared over browsers
- Extension-based protection for Windows/macOS endpoints
  - Chrome, Edge, Safari, and Firefox
  - File upload protection, copy/paste protection, print controls, URL filtering
- Seamless API integration for Chrome Enterprise
  - File upload protection, copy/paste protection, print controls

Trellix Data Loss Prevention Endpoint Complete

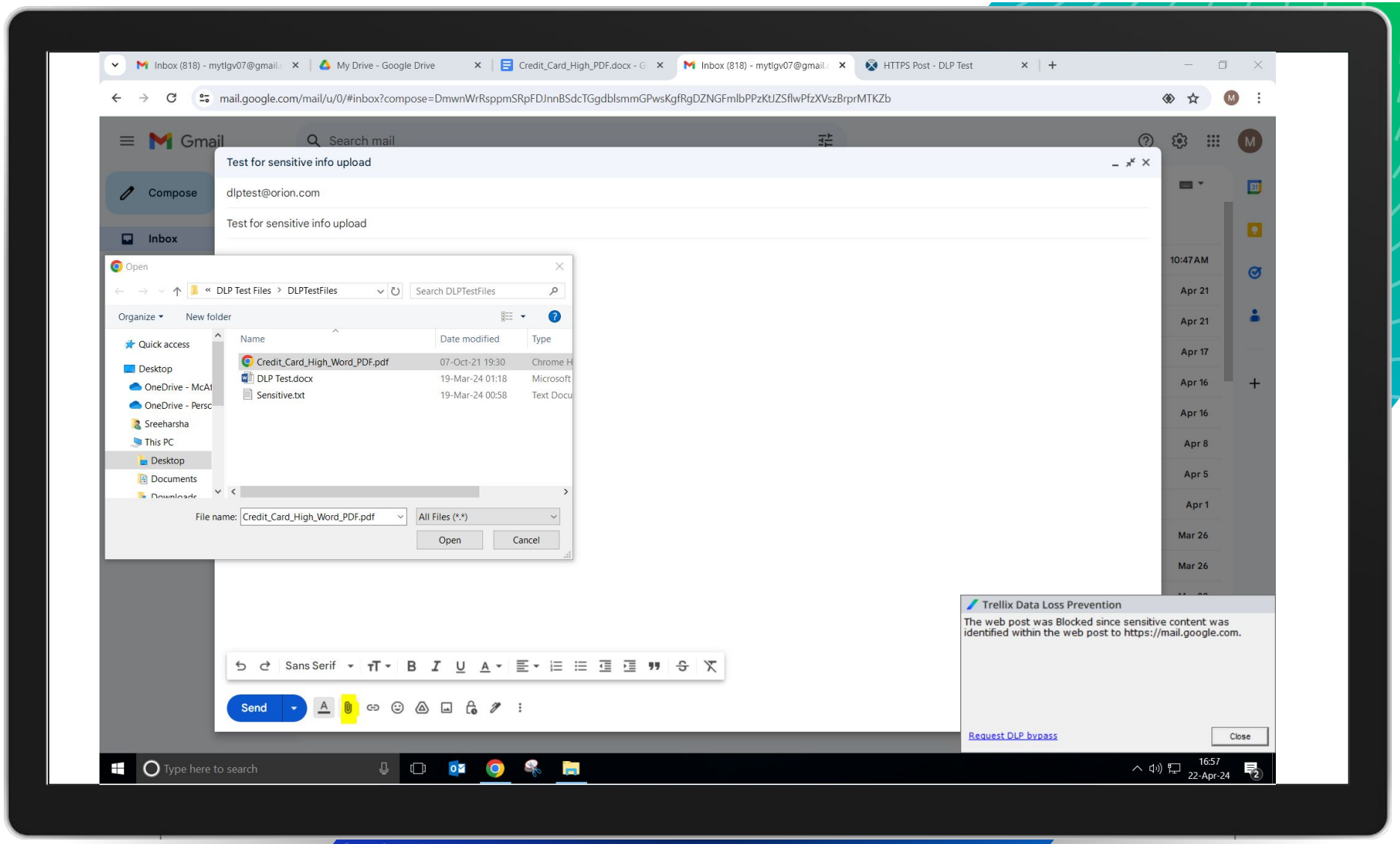
Trellix

Protect Sensitive Data Shared via Browsers



Trellix

Protect Sensitive Data Shared via Browsers



Trellix

Securing Device Data

Trellix Data Encryption

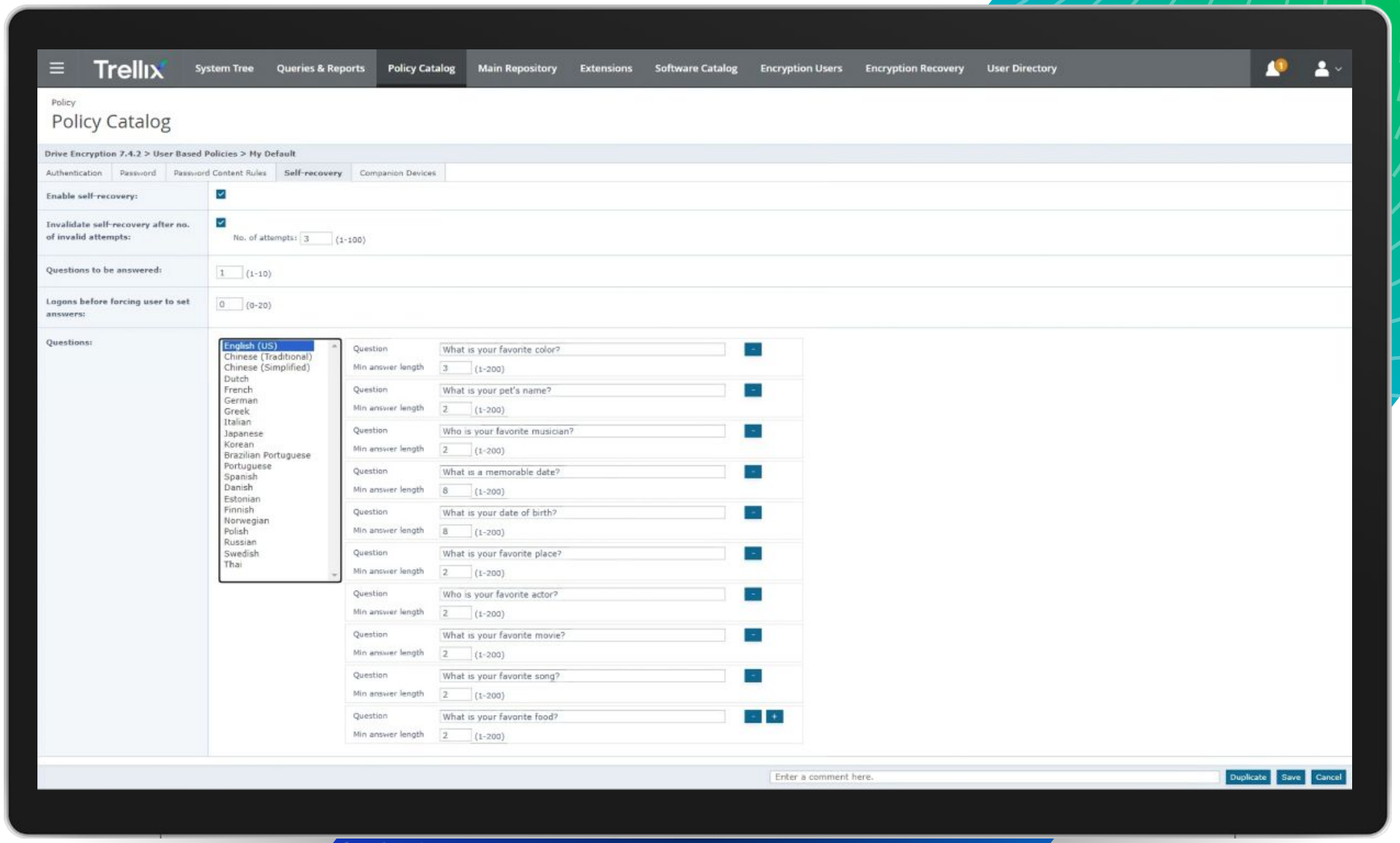
- Protect data on devices that are lost or stolen
- Full disk protection, multi-user authentication, and self-service user recovery options
- Deploy and manage native Windows or MacOS device encryption from a single console
- Understand device status in your ecosystem and report on compliance

Trellix Drive Encryption

Trellix Native Drive Encryption

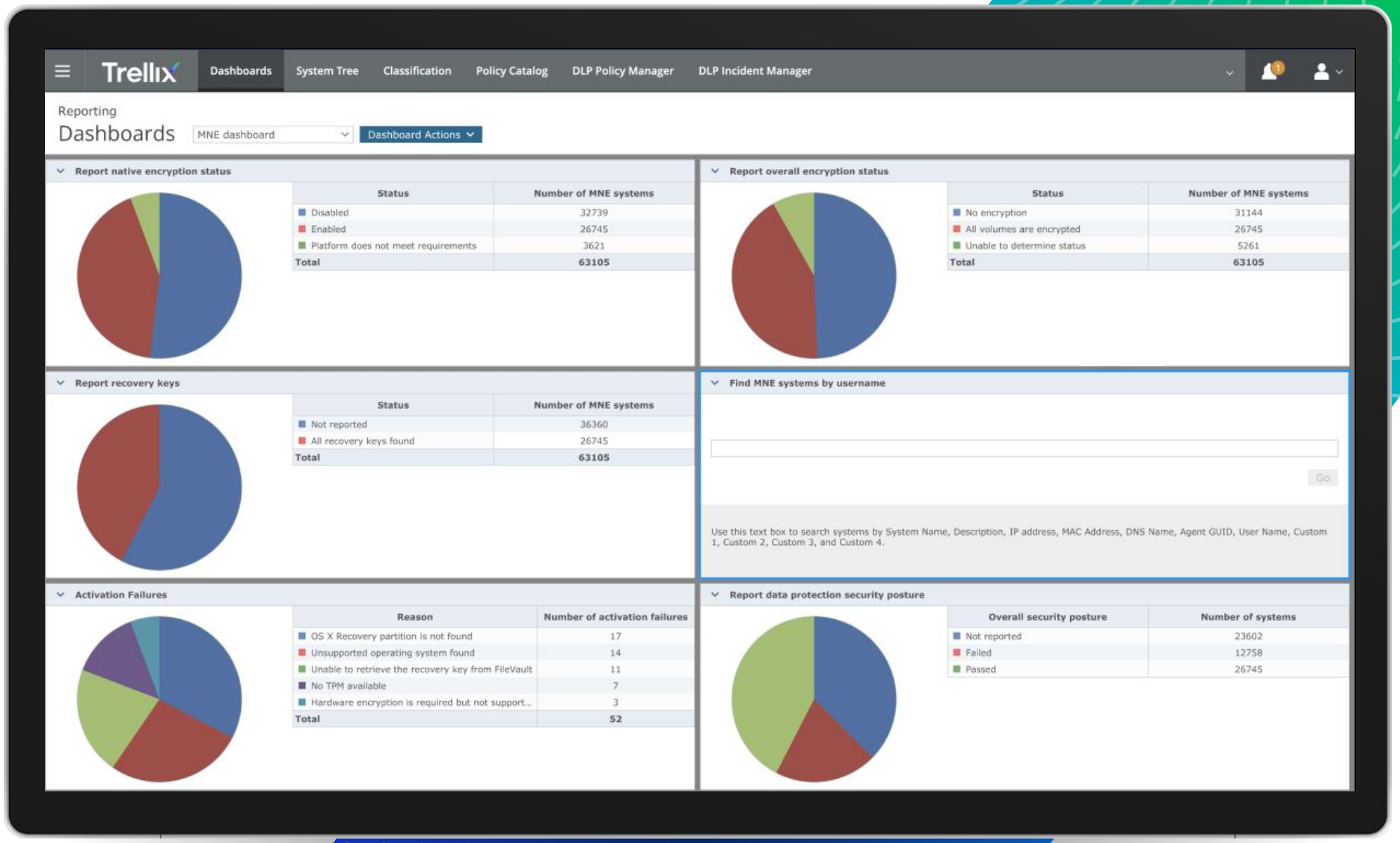
Trellix

Authentication, Password, and Recovery Options



Trellix

Status of Devices in Your Ecosystem



Trellix

Policy-based File Encryption for Sensitive Data

Trellix Data Security

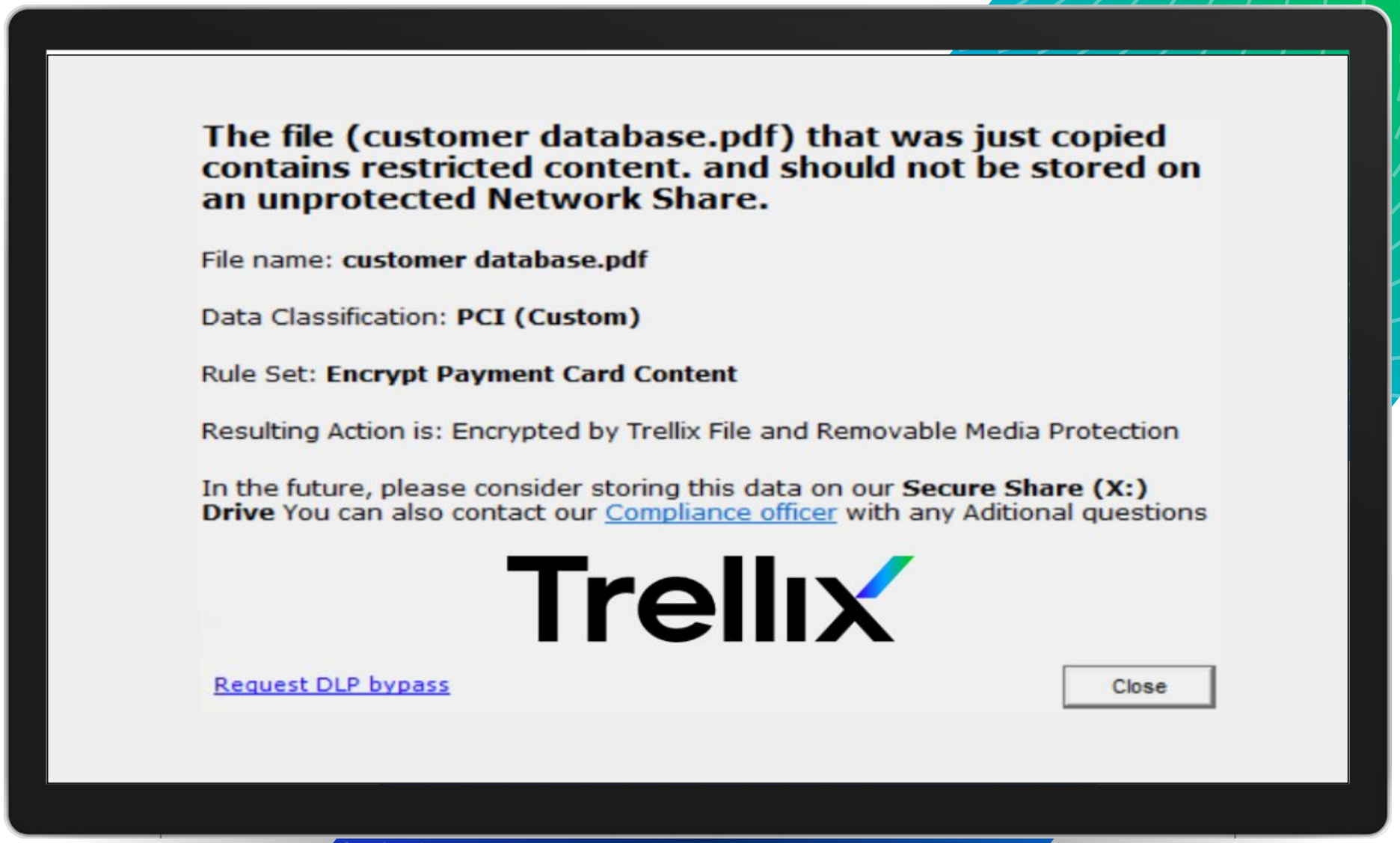
- Apply Data Loss Prevention policies to encrypt sensitive or proprietary data at the file level
- Create extra protection for sensitive data without extra work for security or information governance teams

Trellix Data Loss Prevention Endpoint

Trellix File & Removable Media

Trellix

Encrypt Sensitive Data at File Level



Trellix

Event Monitoring and Management

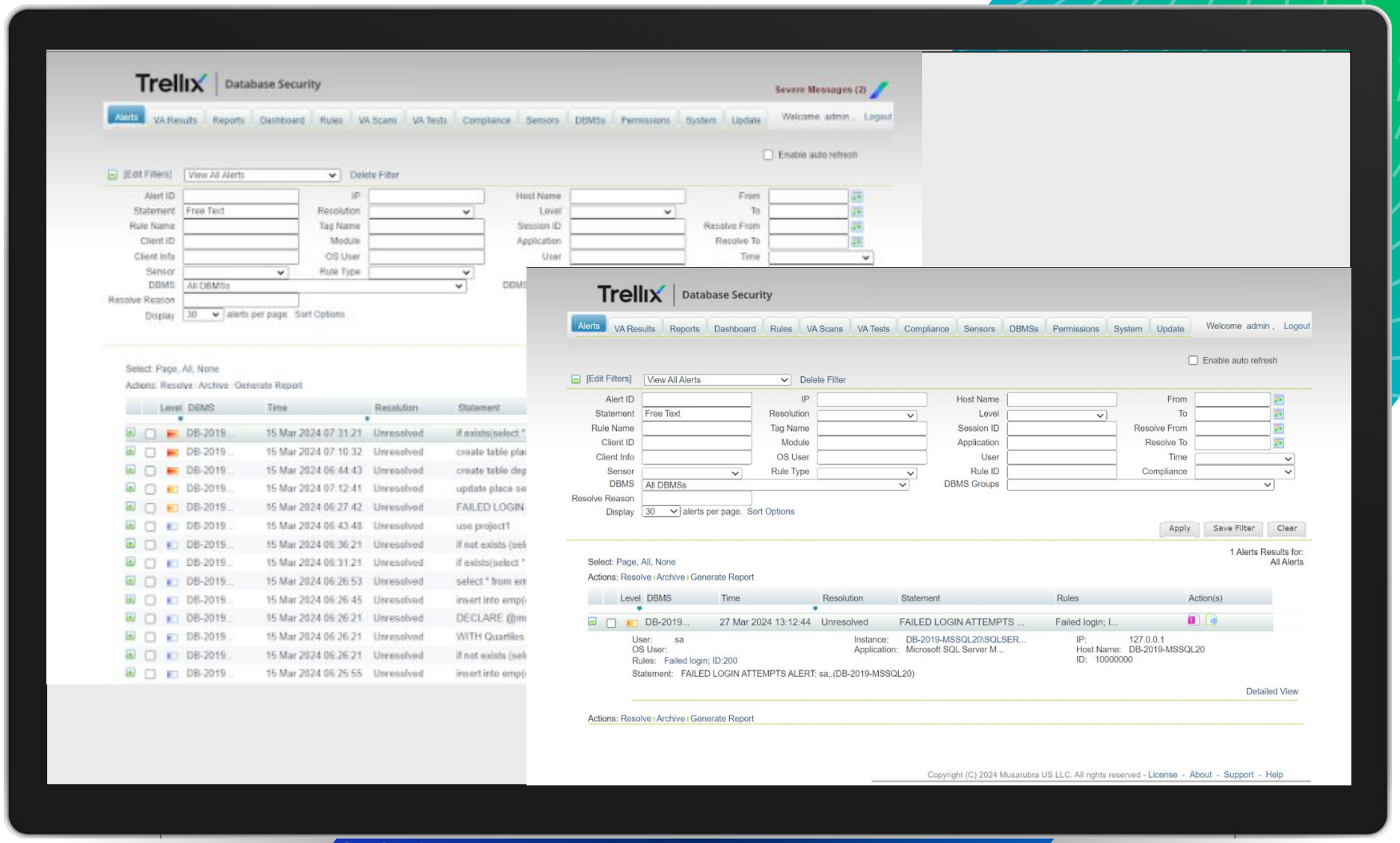
Trellix Data Security

- Get detailed information about data events
- Take action to address incidents in our tools like Trellix Database Security
- Generate reports and track event resolution

Trellix Database Security

Trellix

Data Alerts with Detailed Information



Trellix

Trellix

Licensing & Packages

Data Security Product Packages

Package	What it Includes	IRT	GRC	EIF
Trellix Data Loss Prevention Suite	All Data Loss Prevention Products	✔	✔	✔
Trellix Data Encryption Suite	All Data Encryption Products	✔	✔	
Trellix Data Security Endpoint Protection Suite	Data Loss Prevention Endpoint Complete and Data Encryption Products	✔	✔	
Trellix Data Security Network Suite	Trellix DLP Network Prevent, Trellix DLP Network Monitor, and Trellix DLP Discover	✔	✔	✔
Trellix Database Security	One comprehensive Database Security offering with all critical features	✔	✔	✔
Trellix Data Security Suite	All DLP and Encryption Products (and OCR)	✔	✔	✔
Trellix Database Security for Data Security Suite	Add-on for Database Security to Data Security Suite with *discounted* rate	✔	✔	✔

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

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

Less Complex, Less Regulated → More Complex, More Regulated

Data Encryption Suite

Available on prem, hybrid, or via Saas

Value
Protect enterprise and removable data from attacks

- Safeguard device and file data
- Secure devices for remote use
- Stop data exfiltration to removable media and establish separation of duties for file sharing
- Flexible for organizations with mixed environments (Win/MacOS)
- Centralized administration, events, reporting in ePO

Data Loss Prevention Suite

Available on prem, hybrid, or via Saas

Value
Extend protection for data on endpoints, across network storage and shared over web browsers

- Visibility and control across top data threat vectors
- Flexible policies, scale to your environment
- User coaching and notifications
- Data discovery, classification
- Out of the box compliance policies, reporting
- Flexible for organizations with mixed environments (Win/MacOS)
- Protection for devices connected to the endpoint

Data Security Endpoint Protection Suite

Available on prem and hybrid

Value
Defend endpoint data, stop data exfiltration, safeguard device and file data

- Visibility and control across top data threat vectors
- Data discovery, classification
- Out of the box compliance policies, reporting
- Secure devices for remote use, stop data exfiltration to removable media and establish separation of duties for file sharing
- Flexible for organizations with mixed environments (Win/MacOS)
- Centralized administration, events, reporting in ePO
- Safeguard device and file data

Database Security

Available on prem
Add on for DATA and standalone

Value
Protect databases and the sensitive information they contain

- Compliance with mandates for data activity monitoring
- Protect organization's most sensitive data
- Find databases and sensitive information
- Save time and resources with scan/patching
- Meet compliance guidelines
- Stop unauthorized users from accessing sensitive data
- Automate currently manual tasks and protect databases that no longer receive manufacturer patches

Data Security Suite

Available on prem, hybrid, or via Saas

Value
Protect the data that matters throughout the entire lifecycle

- Visibility and control across top data threat vectors
- Data discovery, classification
- Out of the box compliance policies, reporting
- Secure devices for remote use, stop data exfiltration to removable media and establish separation of duties
- Flexible for organizations with mixed environments
- Centralized administration, events, reporting in ePO
- Safeguard device and file data
- Avoid financially motivated malicious insider attacks and accidental data leakage
- Speed up and simplify compliance activities

Trellix

Trellix

Trellix Differentiators & Key Competitors

Why Choose Trellix Data Security?

Discover	Protect	Respond and Report		
Extensive data discovery with exact matching using content, context, and fingerprinting to limit false positives	Flexible policies that offer enhanced security options for organizations' with custom requirements	Encryption at the file level based on integrated DLP policies	Dedicated database security protection with activity monitoring, vulnerability management, and automated patching	Centralized deployment, policy administration, reporting, and incident response

Trellix

Trellix Differentiator - What's the Pitch?

We Can Get Ahead of the Market on Key Use Cases

- **Address Shadow AI:** Identify and manage security risks from unapproved AI tools.
- **Centralize AI Risk Tracking:** The new Trellix AI Data Risk Dashboard provides granular visibility into how and where sensitive data is shared with AI tools.
- **Stop Data Leaks:** Monitor application and web activity to find and block sensitive data leaks.
- **Prevent AI Access to Data:** Enforce encryption on sensitive content, making the data unreadable to anyone—including an AI model—without the correct decryption key.
- **Protect Databases:** Protect critical data and block attacks like SQL injection.

Featured Products & Packages:

- Data Loss Prevention Endpoint Complete (DLP)
- Database Security (DCD)
- Data Security Endpoint Protection Suite (CDA)
- Data Security Suite (Data)
- Data Security Suite (Data) + DCD Add-on

Get the OCR Suite included with this package to enhance data detection!

Trellix

Trellix Differentiator - 3 Easy Paths to Success

Pick the option that works best for you!

Customer Scenario	Door Opener	Who to Talk To?
The customer currently has **DLP Endpoint Complete** (including packages TDL, CDA & Data) - and will be renewing or is at risk	**Option 1 -** Turn your existing DLP investment into an immediate AI Governance control center with a free dashboard upgrade.	Champion: CIO, Compliance, Information Management Teams, Data Governance / DLP Analyst Buyer: CISOs, CTOs, C-suite executives
The customer has **any Data Security product** (DLP, Encryption, Database Security) but **not the full Data Security Suite**, and there is an upsell opportunity.	**Option 2 -** Stop leaks to Shadow AI and future-proof AI data risk protection with advanced capabilities like OCR and Database Security.	Buyer: CIO, Compliance, CISOs, CTOs Champions: Information Management Teams, Data Governance / DLP Analyst
The customer has **flex credits**, or there is an opportunity to attach T**hrive Advanced or Elite** to a deal. And needs help optimizing or implementing policies or wants to fine-tune their implementation of any of the Data Security products or packages. This helps with renew, upsell, or just staying sticky.	**Option 3-** Leverage our experts to help develop or implement your AI Acceptable Use Policy, and ensure your rules are working as intended to address AI data risks.	Buyer: CIO, Compliance, CISOs, CTOs Champions: Information Management Teams, Data Governance / DLP Analyst

For **talking points and discovery questions** to support each option see this asset on Seismic.

Trellix

Meet our Competitors

DLP

Microsoft
CROWDSTRIKE
Symantec
CHECK POINT
CISCO
VARONIS
paloalto NETWORKS
FORTRA
netskope

Encryption

Symantec
Microsoft
FORTRA
TREND MICRO
CHECK POINT
SOPHOS
THALES

Database

IBM
imperva
Microsoft
ManageEngine
dynatrace

Trellix

Trellix vs Microsoft

DLP | Encryption | Database

Overview

+ Broad security portfolio
+ C-Level Access
+ Industry Recognition
+ Native insider risk module
+ Web content protection
- Limited data security functionality and detection outside the Microsoft ecosystem
- Limited user coaching
- Partial user insight and context around how data is being used
- Insufficient regulatory data compliance with less common regulations
- Lack full network DLP
- File access blocking is limited
- Less robust integrated threat intelligence to inform data events

Trellix Strengths

- On-premises and hybrid deployment
- Options for Windows and macOS
- Extensive out-of-the-box policy options, flexibility
- Extensive data discovery and classification across endpoint, email, web and network storage
- Full disk encryption
- Easily manage BitLocker and FileVault in single console
- Encrypt at the file level based on DLP policy
- Comprehensive database security
- Integrated threat intelligence

Countermeasures

- Trellix reduces insider risk and better addresses compliance through more comprehensive visibility and control throughout the data lifecycle.
- Trellix customers get simple and clear licensing, as well as delivery and centralized management through our proven single console for DLP and Encryption.
- Protect sensitive data in leading database types, including legacy databases, from advanced threats while supporting compliance initiatives.

WATCH FOR: **Microsoft C-Level access may bypass security Champions, positioning security in productivity bundles as being lower cost.**

Trellix

Trellix Data Security vs Microsoft

Category	Requirement	Trellix	Microsoft	How We Win
Management and Administration	Centralized User and Policy Management Console	🟢	🟡	**Trellix** - Centralized EPO console streamlines policy deployment, user management, event tracking, and reporting. **Microsoft** - Fragmented tools (Intune, GPO, Defender); macOS deployment is manual and complex; Endpoint DLP centralized management is in early stages.
	Screen Capture Protection Rules	🟢	🟢	**Trellix** - Blocks screen capture with contextual protection for sensitive data. **Microsoft** - Requires Active Directory; OCR service needed; limited to specific Windows OS versions; includes watermarking.
	Policy Update Confirmation via EPO	🟢	🔴	**Trellix** - EPO system tree allows confirmation of policy updates. **Microsoft** - Tracking lacks cohesion, split between Intune and Azure Update Manager.
	Policy Update Confirmation via Purview	🟢	🟡	**Trellix** - EPO ensures real-time, granular policy push tracking. **Microsoft** - Tracking fragmented; updates rely on device check-ins; Azure Update Manager required for scale.
	Instant Policy Updates	🟢	🟡	**Trellix** - Policies deployed globally in minutes with ePO's wake-up agent capability. **Microsoft** - Compliance Center changes take up to an hour; authorized group updates may take 24 hours.
	Centralized Management Console	🟢	🟡	**Trellix** - Mature ePO console for managing all policies and administrative tasks. **Microsoft** - Fragmented management across Intune, Purview Compliance, and Defender portals.
Web Protection	Web Content Protection	🟢	🟢	**Trellix** - Comprehensive capabilities: Clipboard and web upload restrictions; supports Chrome, Edge, Firefox, Island, Safari. **Microsoft** - Strong policy support; prevents data pasting/uploads; primarily works with Edge; Purview extensions for Chrome/Firefox.
Email Protection	Email Content Protection	🟢	🟡	**Trellix** - Broad compatibility: Endpoint and Network-level rules (e.g., blocking sensitive email attachments). **Microsoft** - Narrow scope: Primarily within M365; requires additional solutions for broader platform compatibility.
Network Protection	Network Port Rules	🟢	🔴	**Trellix** - Comprehensive coverage: Network communication protection rules to monitor, block, or enforce policy-based actions. **Microsoft** - DLP not designed for network-level protection or creating network communication protection rules.
Evidence Collection & Investigations	Forensic and Record Collection	🟢	🟡	**Trellix** - DLP products preserve and highlight sensitive content for investigations and forensics. **Microsoft** - Partial capabilities; enables evidence collection for file activities on Windows devices; supports eDiscovery; copies stored in Azure.
Discovery & Classification	Data Classification with Fingerprinting	🟢	🟡	**Trellix** - Advanced features: Combines content/context with easy GUI; supports document fingerprinting and ML-based keyword searches. **Microsoft** - Complex UI: Policy-based fingerprinting with hash value storage in Active Directory; no storage for original documents.
Incident Management	Short Match String Visibility	🟢	🔴	**Trellix** - Granular detection: Trellix DLP enables short match string visibility in the incident manager. **Microsoft** - Limited functionality: Microsoft Endpoint DLP does not support short match string visibility.
	Event Data Preview	🟢	🔴	**Trellix** - Unique feature: Trellix provides sensitive data previews for faster incident resolution. **Microsoft** - Missing functionality: Microsoft lacks data preview capabilities.
File Access Management	Blocking Unknown Processes	🟢	🔴	**Trellix** - Threat intelligence integration: Blocks unknown/low-reputation processes from accessing classified files. **Microsoft** - Limited blocking; preventative measures rely on machine-learning classifiers.
Data Identification and Tracking	Document Fingerprinting	🟢	🟡	**Trellix** - Simplified GUI: One-click options for fingerprinting; saves original files. **Microsoft** - Complex policy rules; converts patterns into hashes; stores only hash values in Active Directory.

Trellix vs Symantec (Broadcom)

DLP | Encryption

Overview

+ Feature rich DLP solution
+ Comprehensive coverage a nd protection of sensitive data movement, with on-premises capabilities
+ Single console for deployment and policy management across multiple channels
  - User notification, coaching, exception tracking, policy development and file-based encryption limitations
  - Limited compliance capabilities
  - Limited data at rest coverage
  - Service quality / support after purchase

Trellix Strengths

- Flexible deployment and licensing
- Comprehensive data discovery and classification
- Robust compliance policies and reporting
- Open architecture and extensive third-party integrations
- Full disk encryption
- Easily manage BitLocker and FileVault in single console
- Encrypt at the file level based on DLP policy
- Comprehensive database security
- Integrated threat intelligence

Countermeasures

- Many customers come to us after failed implementations with other tools that previously beat us on price.
- Our products are backed 24/7 by a Support team of global professionals
- Position our expert Professional Services team with data governance specialists who can design a program to help optimize our customers' tools to reach time to value faster. Mention Thrive packages with Flex credits where the customers decide which services they want to take advantage of to increase their security posture.

WATCH FOR: Attempts to beat us on pricing.

Trellix

Trellix Data Security vs Symantec

Feature Capability	Trellix	Symantec	Customer Benefit
Endpoint DLP (Windows)	🟢	🟢	**Trellix** - Same maturity; flexible deployment (SaaS or on-prem); integrated Device Control. **Symantec** - Mature capabilities; strong policy granularity.
MacOS DLP Coverage	🟢	🟡	**Trellix** - Supports latest MacOS; better tuning, fewer false positives. **Symantec** - Weak support, frequent false positives.
Network DLP (Monitor/Prevent)	🟢	🟢	**Trellix** - Full coverage (Monitor/Prevent), with SaaS/virtual appliance flexibility. **Symantec** - Robust but requires standalone appliances and Oracle.
Cloud DLP (SaaS Apps, O365, GDrive)	🟢	🟢	**Trellix** - Native via SaaS DLP or integrated with Skyhigh CASB (Gartner MQ Leader). **Symantec** - Supported via DLP Cloud + CloudSOC CASB; requires add-ons, separate licensing.
DLP for Collaboration (Teams, Slack, etc.)	🟢	🟡	**Trellix** - Coverage via Trellix IVX for enterprise platforms; DLP policies extend across channels. **Symantec** - Requires CloudSOC Gateway + manual tuning.
Data Classification Integration	🟢	🟢	**Trellix** - Native integrations with Titus/Bolden James; real-time classification. **Symantec** - Also supports Titus/Bolden James.
OCR (Optical Character Recognition)	🟢	🟡	**Trellix** - Available as an add-on, included in Data Security Suite top tier. **Symantec** - Available but requires dedicated server install.
Email DLP (Gateway, O365, Gmail)	🟢	🟡	**Trellix** - Integrated via Trellix Email Security Cloud & DLP Prevent. **Symantec** - Covered via separate DLP for Email product.
Insider Risk Controls (Browser DLP, USB)	🟢	🟡	**Trellix** - Browser DLP for Chrome Enterprise + USB controls + separation of duties (via encryption integration). **Symantec** - Basic device controls, risk scoring via UEBA.
Reporting & Analytics	🟢	🟡	**Trellix** - Centralized via ePO, enhanced by Thrive onboarding + templated reports. **Symantec** - Powerful engine, but dated UI, limited customization.
Policy Tuning & Templates	🟢	🟡	**Trellix** - Pre-built policies, guided setup, Thrive-enabled optimization. **Symantec** - Requires skilled staff, frequent manual tuning.
UEBA & Behavioral Analytics	🟡	🟡	**Trellix** - Trellix Wise and ongoing ML/behavior analytics investments. **Symantec** - Risk scores, late-stage addition; not deeply integrated.
Data Discovery (at rest)	🟢	🟢	**Trellix** - Included in all suites; SaaS or on-prem delivery. **Symantec** - Strong scan performance; separate deployment path.
Data Encryption Integration	🟢	🟡	**Trellix** - Native, Data Security Suite includes endpoint encryption + removable media control. **Symantec** - Requires separate products or partners.
Database Security	🟢	🔴	**Trellix** - Add-on to Data Security Suite or standalone **Symantec** - Not bundled; separate Broadcom product
Cloud-native Deployment (SaaS)	🟢	🟡	**Trellix** - Fully supported; also available as Amazon Machine Image (AMI). **Symantec** - Available via Symantec DLP Cloud, but often feels like a separate product.
Support, Onboarding, Training	🟢	🟡	**Trellix** - Backed by Trellix Thrive – flex credits, adoption plans, PS architects. **Symantec** - Limited unless you're a top 250 account.
Licensing Simplicity & TCO	🟢	🟡	**Trellix** - Flexible licensing (SaaS/hybrid), bundled SKUs, lower infra requirements (no Oracle <10K users). **Symantec** - Complex bundles, forced lock-ins, separate SKUs for Cloud, OCR, CASB, etc.
Analyst Sentiment (2024–2025)	🟢	🟡	**Trellix** - Customer favorite in Forrester Wave, strong support/manageability scores, GigaOm & Info-Tech Leaders. **Symantec** - Scores declining (Forrester, Info-Tech); IDC notes complexity, slow innovation.

Trellix Data Security vs Crowdstrike

DLP | Encryption

Overview

+ Broad security portfolio that utilizes a solid amount of user telemetry from their endpoint protection platform
+ Acquisition of Flow Security enables expansion of data security posture management (DSPM) capabilities
+ Various data source integrations
  - Limited DLP capabilities (no email DLP capabilities and very limited network DLP)
  - Limited compliance/regulatory focused functionality
  - Limited Encryption capabilities
  - File access blocking is limited to known and common processes only due to lack of integrated threat intelligence
  - Absent data at rest controls

Trellix Strengths

- Comprehensive data discovery and classification
- Mature Endpoint and Network DLP offerings
- Robust compliance policies / reporting
- Open architecture and extensive third-party integrations
- Full disk encryption
- Easily manage BitLocker and FileVault in single console
- Encrypt at the file level based on DLP policy
- Comprehensive database security
- Integrated threat intelligence

Countermeasures

- Trellix better combats the expanding information footprint and simplifies compliance tasks with comprehensive offerings that protect sensitive information across the top threat vectors from endpoints to email, the web and in network storage.

- Proven DLP combined with mature encryption and database security solutions protect the data that matters to organizations.

WATCH FOR: CrowdStrike claiming that Trellix is legacy.

Trellix

Trellix Data Security vs Varonis

DLP

Overview

+ Partnership with Microsoft on E5 and Co-pilot
+ Solid classification engine and capabilities
+ Detailed visibility into user interaction with sensitive data
+ Additional modules for user risk management
  - Enhanced capabilities are contingent upon using their native ecosystem, integration with Microsoft E5, a plethora of data to process, and add-on modules that all prove costly
  - Management complexity
  - Data storage volumes
  - Unproven protection

Trellix Strengths

- Event detection and response
- Monitoring and blocking to stop data exfiltration
- Encryption protection at the file level
- Applying FRP to create separation of duties
- Database security
- Single management console for DLP and Encryption
- Third-party integrations including classifiers like Boldon James and Titus (Forta)
- Flexible deployment / licensing options

Countermeasures

- Trellix Data Loss Prevention is deployed from a single console where events are tracked in real-time, policies are applied and reports are easily generated.

- We discover more than 400 file types and can apply controls like alerting, blocking, and file-level encryption from a single-pane-of-glass making Trellix a one-stop-shop solution for full data loss prevention.

WATCH FOR: Pretending to be a DLP solution or teaming up with Microsoft to take us on.

Trellix

Trellix Data Security vs Forcepoint

Capability	Trellix	Forcepoint	Seller Notes / Additional Context
False-positive rate & "explainability"	🟢	🔴	**Trellix**: MVX + ML show rule-match, hash, confidence & decoded payload in one pane; tuning wizard auto-suppresses low-entropy hits. **Forcepoint**: A major, recurring theme in user reviews. Customers consistently report that Forcepoint generates "too many alerts" and a high rate of "false positives," requiring significant "manual tuning" and creating alert fatigue.
Unified dashboards & drill-down	🟢	🟡	**Trellix**: ePO SaaS "Data Security Overview" widget stacks endpoint, network, cloud, database events; 4-click journey from fleet view → event → decrypted payload. Export JSON directly to Splunk/Elastic. **Forcepoint**: The "single dashboard" is a marketing claim that masks an architectural reality. The platform is split between the on-prem Forcepoint Security Manager (FSM) and the Forcepoint ONE cloud portal. The ultimate proof is the DLPCONSSE add-on, a paid SKU required just to connect their own products
OCR on endpoint & network	🟢	🟡 (parity on email, still lag on endpoint)	**Trellix**: Windows OS (v11.12) offers Optical Character Recognition support, reading 17 Western & Asian scripts; Network also offers server-side OCR. No extra license for OCR if in the Data Security Suite. Add-on in other packages. **Forcepoint**: OCR available via Image Analysis add-on ($8 user/yr - many customers decline due to cost/latency.) This is a known gap highlighted by their own users, who have explicitly requested that Forcepoint "align OCR with endpoints," calling it a "highly demanded technology".
Cross-vector policy reuse	🟢	🟡/🔴	**Trellix**: Single DLP rule set lives in ePO DB. Admin marks which channels (Endpoint, ICAP, Discover) it applies to; inheritance cascade by AD group/Tag. **Forcepoint**: Fundamentally broken due to their fragmented architecture. Policies created in the on-prem FSM are separate from those in the Forcepoint ONE portal.
Exact data / doc matching scale	🟢	🟡	**Trellix**: Fingerprint sharding; lab ingest of 250 M customer records (1 TB CSV) finished in 52 min, detection latency < 100 ms. Supports incremental sync via SFTP. **Forcepoint**: EDM index stored in Oracle; tuning guide warns at 50M rows performance may degrade. SME saw daily index runs spilling into business hours, forcing split jobs. Their PreciseID fingerprinting is a mature technology, but users have reported issues.
Mac & Linux endpoint parity	🟢	🔴	**Trellix**: ARM-Mac support, Snipping-Tool and screen-recorder block, FRP file encryption parity; Linux agent monitors exfil to SCP/NFS and USB operations. **Forcepoint**: Mac agent lags two versions; no clipboard or print monitoring. Linux DLP only covers email channel via ICAP, not local actions. This is a well-documented and persistent weakness.
ARM Windows endpoints	🟢	🔴	**Trellix**: Compiled filter driver for Windows-on-ARM (Qualcomm) since agent 11.12; validated on Lenovo X13s with 3% CPU overhead during copy-to-USB block tests. **Forcepoint**: Roadmap slide says "under investigation"; no agents, no ETA, no current support. Their own documentation and release notes show no available agent or stated support for Windows-on-ARM devices, creating a coverage gap for modern hardware.

Trellix

Trellix Data Security vs Forcepoint (Cont.)

Capability	Trellix	Forcepoint	Seller Notes / Additional Context
User coaching & justification	🟢	🟡	**Trellix**: Inline toast shows rule hit, masked PII and offers Justify/Encrypt/Cancel; user rationale captured in incident. Localised in 14 languages. Works for email, USB, network copy, cloud logins. **Forcepoint**: Endpoint shows blocking bubble only. “Justification” offered by sending a follow-up notification email which re-triggers policy, adds "round-trip" latency and user confusion. FP official docs mention "DLP coaching dialog," but the capability is less dynamic and integrated than ours.
Visual file-label enforcement	🟢	🟡	**Trellix**: Office ribbon label, metadata tag, watermark PDF/JPEG; policy can deny send if label missing. Labels stored in AES-256 header, readable by MSFT Information Protection. **Forcepoint**: No native labelling engine. Their strategy relies on the acquisition of Getvisibility, which is sold as a separate, paid add-on (CLASSIFY at ~$30/user/yr) with its own console. This adds cost, complexity, and another console to manage.
Incident triage click-count	🟢	🔴	**Trellix**: In SaaS console, analyst clicks Alert → Details → Payload → PCAP screen (4 clicks), remains in one tab. Ticket export to ServiceNow via webhook burns 15s. **Forcepoint**: Fragmented console experience directly impacts triage efficiency - Admins must jump between the FSM and Forcepoint ONE portals to get a full picture. Requires Incident Manager, Log Viewer, Dashboard; we timed 15 clicks to reach payload. FIT screen replay triggers separate browser; analysts complained of “console spaghetti” during POV.
Cloud SaaS API coverage	🟢	🟡	**Trellix**: Covers Microsoft 365, Google Workspace, Box, Salesforce today; GitHub/Confluence slated Q4-25. Pricing is per-tenant seat with no per-app license. **Forcepoint**: API scanning is sold in restrictive and costly “3-App packs” (ONECAP13). Each additional trio of apps costs extra, creating a TCO snowball for customers with diverse SaaS environments like GitHub, Jira, and Slack. Each extra trio costs $25 user/yr.
Inline TLS break-and-inspect @ 10Gb	🟡	🟢	**Trellix**: VE sensors 2Gb, H-Series hardware 8Gb; roadmap 10Gb VE slated FY26. Bypass NIC auto-bridges on failure. **Forcepoint**: Achieves this with their high-end V-Series appliances (V10KG4R2, V20KG1) but it requires the full Forcepoint stack (SWG & appliance license). This is a valid checkbox win for them if a customer mandates 10Gb inline everywhere and already owns the necessary hardware (list ≈ $42K per appliance)
Adaptive DLP + UEBA risk score	🟡	🟢	**Trellix**: Endpoint risk tag feeds DLP block/coach; full UEBA in Helix (separate SKU) integrates via REST. On-prem customers must forward logs to an XDR/NG-SIEM stack. **Forcepoint**: This is their flagship "Risk-Adaptive Protection," but it's a costly, multi-product bundle. It requires purchasing Insider Threat (ITRMX) or UEBA (UEBASTDX), plus the RAP add-on (ONEDSRAP), and it mandates the top-tier Enterprise Support (a 28% uplift on the entire deal). It's solid but prohibitively expensive.
Post-delivery remediation (M365)	🟢	🔴	**Trellix**: Graph API purge & Teams file zap under 30s; can quarantine OneDrive file, replace with tombstone HTML. Helps SOC clean 0-days without waiting for user click reports. **Forcepoint**: Lacks deep, post-delivery remediation capabilities for modern collaboration tools. Their actions are primarily preventative (block/allow) at the gateway or endpoint, with limited ability to retract or remediate data once it has been delivered to a cloud service like Teams. “Mark suspicious message” adds banner but keeps mail in inbox.

Trellix Data Security vs Forcepoint (Cont.)

Capability	Trellix	Forcepoint	Seller Notes / Additional Context
Removable-media encryption tie-in	🟢	🔴	**Trellix**: DLP rule can auto-move file to FRP AES container on copy; decryption self-extract on authorized machine; supports device serial whitelists. **Forcepoint**: No native capability. This is a major portfolio gap. Their own competitive chart falsely claims they have "Native encryption of files moving to removable media," but their product line and price list show no such product. They advise using BitLocker or 3rd-party tools, which are not integrated with their DLP policies.
Classification engine / MIP parity	🟢	🟡	**Trellix**: Built-in engine + REST SDK; writes both internal tag and MIP label if Microsoft Information Protection present. Full auto-class on-prem requires SaaS classifier micro-service. **Forcepoint**: Relies on the acquired Getvisibility technology, sold as a separate, paid add-on (CLASSIFY at ~$30/user/yr) with its own console. While it can read MIP labels, its native classification is not a core part of the DLP platform, adding cost and complexity.
Database discovery & vPatch	🟢	🔴	**Trellix**: DB Security 10.2 scans Oracle, MS-SQL, Mongo, MariaDB, patch shielding with inline filter; supports AWS RDS auto-scaling. **Forcepoint**: No native Database Activity Monitoring (DAM) or virtual patching. This is a critical portfolio gap that leaves structured data stores completely unprotected from direct threats.
Deployment models	🟢	🟡	**Trellix**: Full SaaS or hybrid; legacy on-prem ePO still supported but lacks new widgets. Air-gap requires on-prem Network + Endpoint agents. **Forcepoint**: Their "cloud" deployment is a heavyweight IaaS model, not true SaaS, requiring customers to manage Forcepoint servers in their own AWS/Azure environment. Their on-prem solutions are sunsetting in 2027, creating a risky future for air-gapped customers, which must stay on legacy branch; aka no new features.
SLA & support cost	🟢	🟡	**Trellix**: 24×7 Sev-1 within 30 minutes included in subscription; no list uplift. Dedicated TAM optional via Thrive. **Forcepoint**: This is a massive commercial vulnerability. Support is not included and must be purchased as a separate, mandatory SKU. The tiers are expensive: Essential = 15% ERP list; Enhanced = 21% or $13K min floor; Enterprise = 28% or $78K min floor.
Tuning transparency	🟢	🔴	**Trellix**: Policy tester shows regex hits, matched context, and sample redaction. Click Promote to add test string to allow-list; change effective in < 1 min. **Forcepoint**: No test-bench. This ties directly to the "false positive" problem. Users complain that reducing noise requires significant "manual tuning" and ongoing effort.
Incident forensics depth	🟡	🟢	**Trellix**: Capture add-on grabs PCAP + screenshot, but no keystroke. Not licensed in base Suite. **Forcepoint**: Insider Threat (FIT) agent provides solid forensic capabilities, including full video recording and keystroke logging. However, this is an extremely expensive proposition: the FIT license (ITRMX) is ~$130/user/yr and mandates the purchase of the top-tier Enterprise Support (a 28% uplift on the entire deal). It's a powerful but prohibitively costly option for most.
Multi-tenant MSP console	🟡	🟡	**Trellix**: ePO SaaS Tenant Manager handles delegated auth, but on-prem ePO lacks MSP overlay. **Forcepoint**: No true multi-tenant management. Each tenant requires a separate instance. Their new "Forcepoint Cloud Dash" overlay is in preview and only aggregates alerts, not policy management, failing to meet core MSP requirements.
False-positive tuning tooling	🟢	🟡 (with heavy scripting)	**Trellix**: Noise-Reducer clusters similar incidents, auto-suggests rule-mask and provides hit distribution graph; one click to publish suppress rule. 2× faster “steady-state tuning". **Forcepoint**: Lacks sophisticated, UI-driven tuning tools. Admins must manually edit regex or thresholds and redeploy. .

Trellix Data Security vs Imperva

Capability	Feature Description	Trellix	Imperva
Database discovery	Find databases across the environment and identify the sensitive information they contain.	🟢	🟢
Compliance rules	Implement data protection rules aligned to common regulatory frameworks (PII, PCI, PHI, etc).	🟢	🟢
Custom rules	Create custom rules as determined by the organization's information governance program.	🟢	🟢
Access Controls	Ensure that only authorized users can access sensitive database information.	🟢	🟢
Data Masking	Protect sensitive information in databases through masking capabilities.	🟢	🟢
Vulnerability scanning	Identify security gaps, issues with configuration, and known vulnerabilities.	🟢	🟢
Database patching	Automate patching known vulnerabilities for databases and implement security rules for unpatched vulnerabilities without impacting users or database performance.	🟢	🔴
Auditing capabilities	Access to detailed information on database access, update history, and user activity.	🟢	🟢
Incident management	Real-time alerts for suspicious activity, actions to address potential threats.	🟢	🟢
On-premises databases	Protect the most common database types and versions for on-premises databases.	🟢	🟢
Cloud databases	Protect cloud-based databases such as Amazon RDS , Google Cloud, Azure SQL Database.	🟡	🟢
Alerts and Notifications	Detailed alerts with actionable intelligence that can be immediately converted into updated rules.	🟢	🟡
SaaS Management	Manage database protection activities from a SaaS console.	Coming Soon!	🟢
Database Support	Support for relational (SQL) and non-relational databases (MongoDB).	🟢	🔴

Trellix

Trellix

Questions?

Thank You