Trellix

APJ Partner Summit'24

Partnering for a Secure Future

Join us at the APJ Partner Summit

Phuket, Thailand

10-12 JULY 2024

Trellix

Trellix Data Security Solutions

APJ Partner Summit 2024

July 8, 2024

Speakers for Today

Ron Wang
Sr Director, APJ SE

Hidemitsu Sakurai
Sr Director, Japan SE

Manish Sinha
Director, India SE

Carl Thaw
Global Enablement

What are some data security trends you've noticed in your industry over the past year?

Agenda

1) **Why the need for Trellix Data Security solution?**
   Challenges it solves

2) **How does Trellix solve the problem?**
   How we are different

3) **About the Trellix solution**
   Overview & Demo

4) **Personas**
   Who to target

5) **Proof Points**
   Customer Case Study

6) **Product Packaging**
   Product SKUs

7) **Upsell and Cross-Sell**
   Positioning the solution to customers

Trellix

Trellix

Why Trellix Data Security Solutions

The challenges

Today's Biggest Challenges:

Data Security

Insider Risk
Accidental and Malicious Threats

Regulatory Landscape
Complex and Time Consuming Compliance

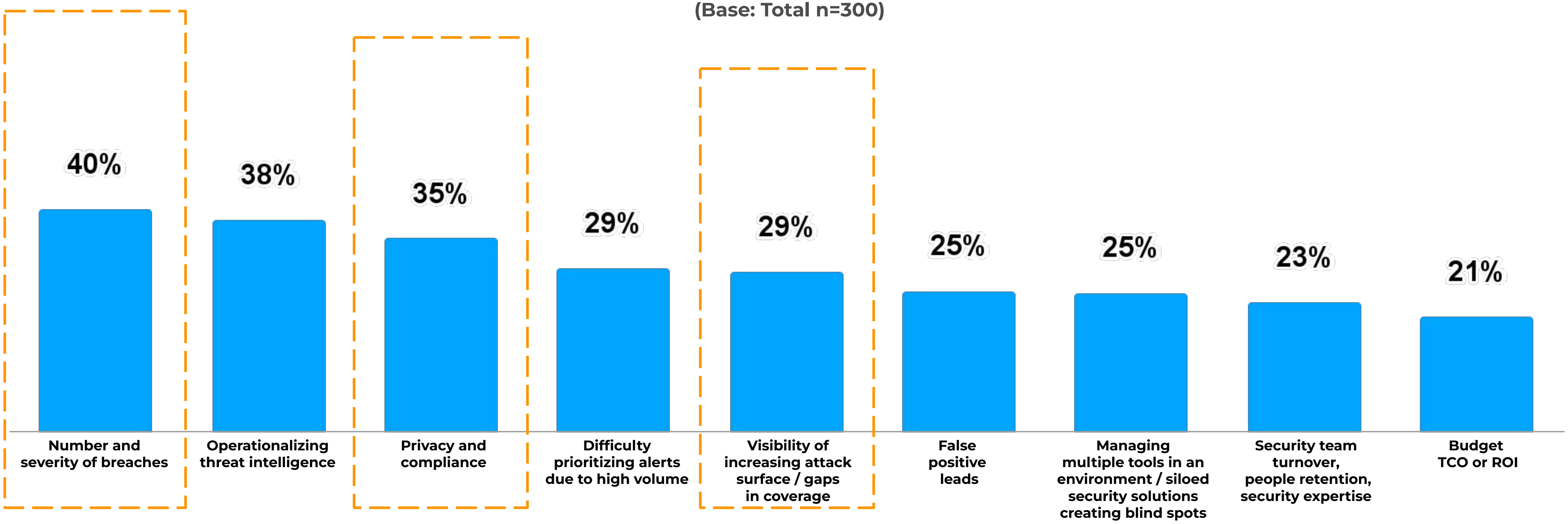
Expanding Information Footprint
Lack of Visibility and Control

Trellix

Top Challenges: Reduce Breaches, Compliance, and Complex Attack Surfaces

Security Challenges Organizations Face

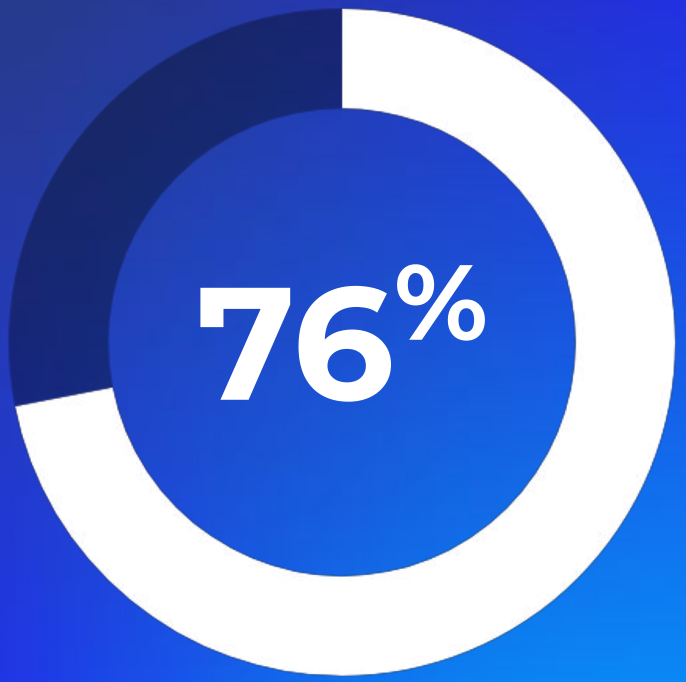
(Base: Total n=300)



Internal Use Only - Esacalent Inc., March 2024

Trellix

Breaches



...of breaches in 2023 were mistakes or malicious intent[1]

According to the 2024 Verizon Data Breach Investigations Report (VDBIR), three-quarters of data breaches could be attributed to a human error or a malicious insider

Today's Data Security Challenges

Malicious Actors

19%

Of breaches were a malicious insider attack[1]

Financially Motivated

80%

Of malicious insiders were financially motivated.[2]

Time to Detect

200 Days

Average time to detect and contain data breaches[2]

[1] - *Verizon DBIR 2023*

[2]- *Averages -IBM, Verizon DBIR*

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

Understanding Market Forces

Compliance is a big concern for our customers

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

Privacy

GDPR

Payment Information

PCI DSS COMPLIANT

Healthcare

HIPAA COMPLIANT

HITRUST

Financial Reporting

SOX

** Trellix - Mind of the CISO Report*

Understanding Market Forces

Sensitive data is expanding, making it harder to protect

Information Storage is Growing

200 ZB

Global data storage expected 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

Required Capabilities to Solve Challenges

The solution should:

Find and Classify

Offer **out-of-the box** options for sensitive data discovery based on common frameworks (personal, health, and payment information, etc.)

Provide customized options to **find the data that matters to the organization** with exact data matching to limit false positives

Protect

Enable options to monitor and **block data exfiltration**, stopping data leaks and combating insider risks while coaching users to improve

Offer **encryption to safeguard the sensitive data** and share only with intended parties

Respond and Report

Detect **data anomalies in real-time**, enabling action, smooth integration with incident management tools and threat intelligence sources

Support centralized management to streamline deployment, reporting, and policy administration **to save time and effort**

What if I don't change - Status Quo?

Increased Risk of Data Breaches

Risk of Penalties, Fines, and Audit Failure

Increased Resource Cost and Team Inefficiency

Trellix

How Trellix Solves it?

How we are different

Trellix Data Security

Protect the data that matters

Value Proposition

Trellix Data Security provides our customers with comprehensive protection for **sensitive and proprietary information** across top threat vectors.

Differentiation

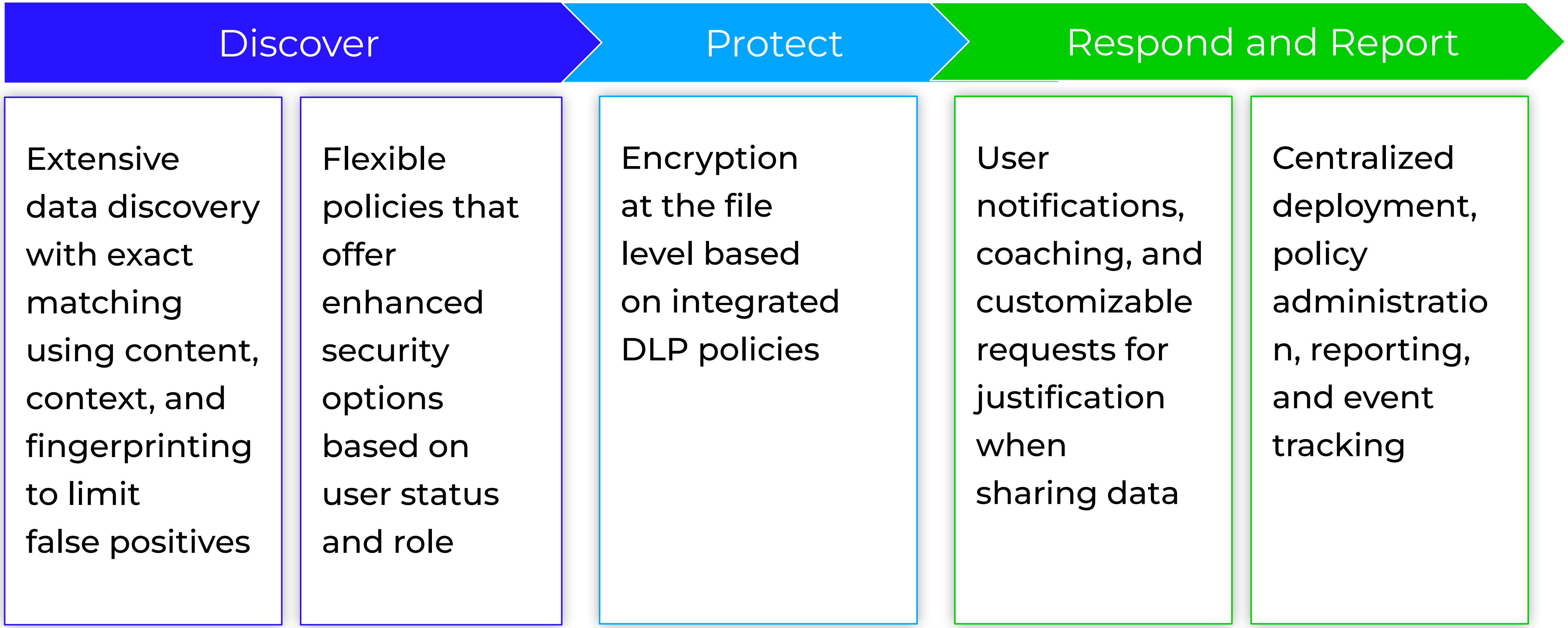
Enterprises of all sizes benefit from the ability to centralize administration, with flexible licensing and delivery, along with the comprehensive visibility and controls to **protect the data that matters** to their organization.

Benefits

Trellix Data Security protects sensitive and proprietary information shared across **endpoints, networks, email, the web, and within databases**, providing encryption protection for devices and data transfers to removable media.

Trellix Differentiators

Why choose Trellix Data Security?



Discover

Extensive data discovery with exact matching using content, context, and fingerprinting to limit false positives

Flexible policies that offer enhanced security options based on user status and role

Protect

Encryption at the file level based on integrated DLP policies

Respond and Report

User notifications, coaching, and customizable requests for justification when sharing data

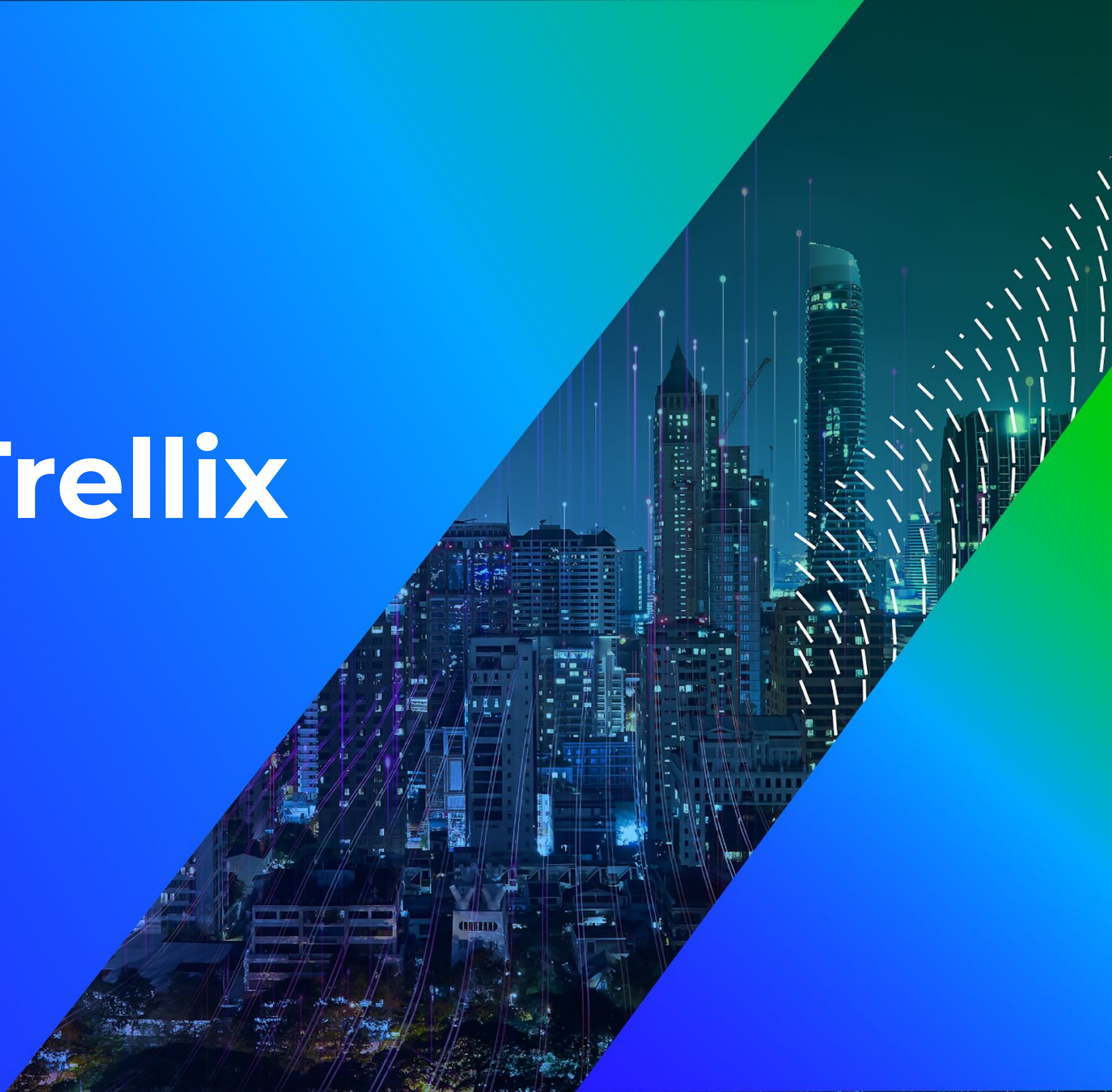
Centralized deployment, policy administratio n, reporting, and event tracking

Trellix

Trellix

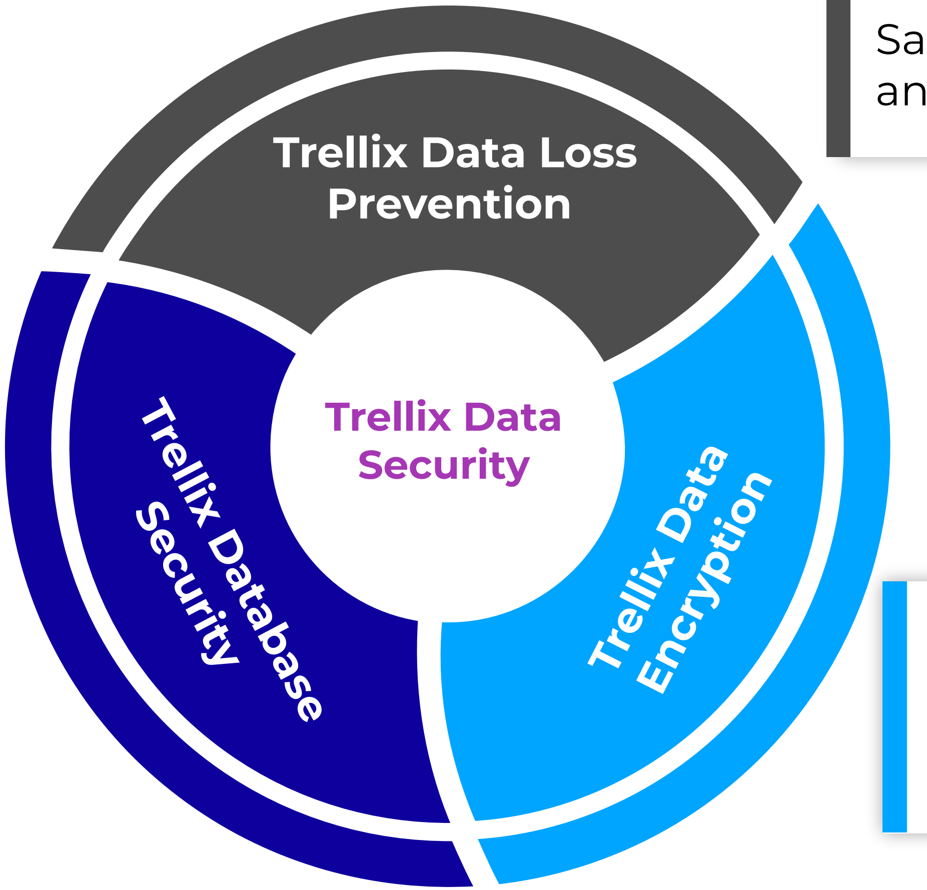
About the Trellix Solution

The challenges



Trellix Data Security

Protect the data that matters



Trellix Data Loss Prevention:

Safeguard against intentional and accidental data leaks

Trellix Database Security:

Find and defend databases and contained information

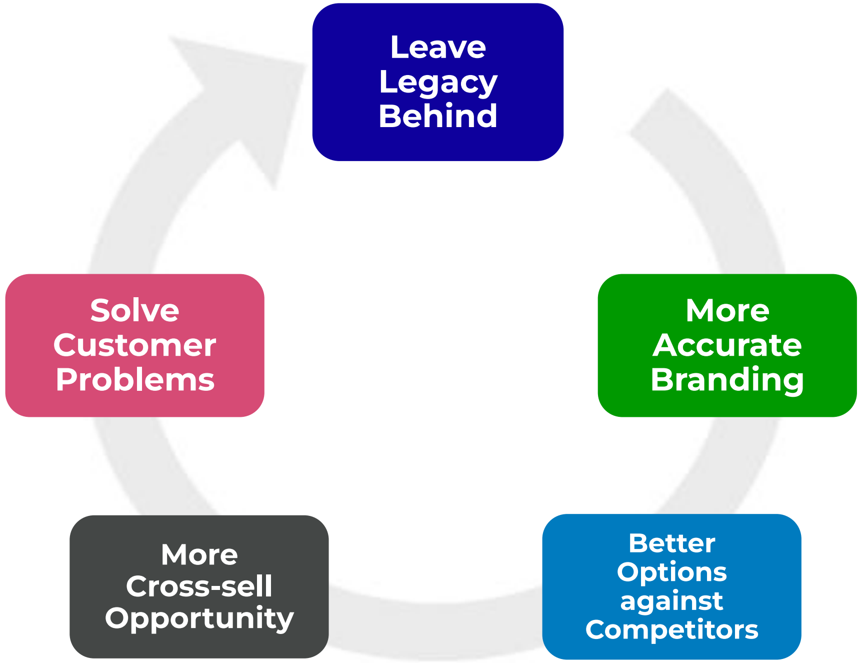
Trellix Data Encryption:

Protect enterprise and removable device data

Trellix

What changed?

Trellix Data Security modernized our offerings



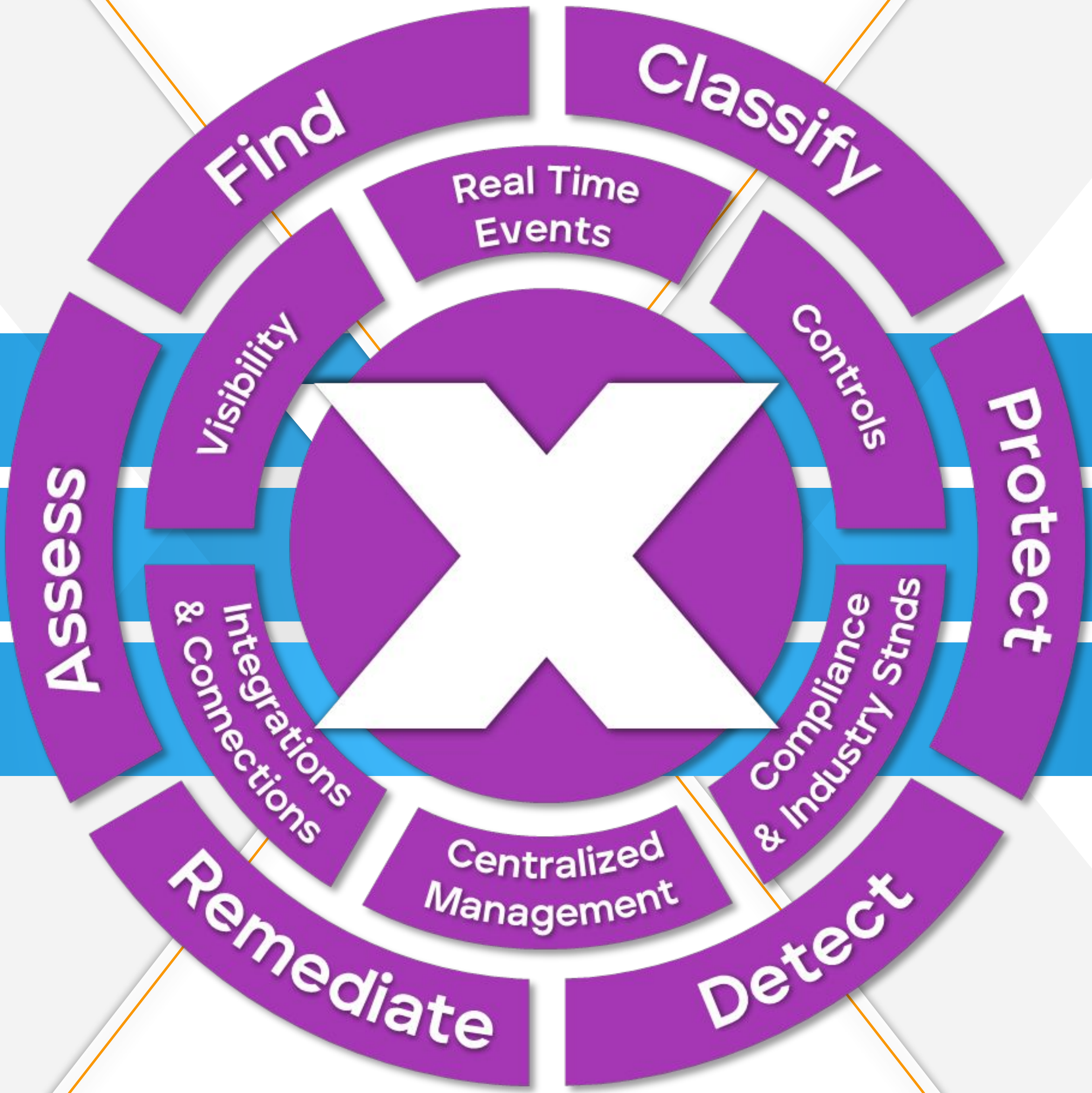
- Trellix Data Protection is now **Trellix Data Security**
- Trellix Data Encryption products are **available individually**
- Trellix Database Security is sold only as a **single offering**
- Some Data Security packages (suites) were **renamed**
  - **SKUs were not changed**
- Minor **product renaming**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

Trellix Data Security

Trellix Data Loss Prevention

Trellix Data Encryption

Trellix Database Security



Trellix

Trellix Data Loss Prevention (DLP) enables organizations to discover, identify, classify, monitor and protect sensitive data from being exposed on endpoints, through email, on the web and across network-storage locations.

Trellix Data Loss Prevention Products

Safeguard against intentional and accidental data leaks

Trellix Data Loss Prevention Endpoint Complete

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

Trellix Device Control

Included in DLP Endpoint Complete

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

Trellix Data Loss Prevention Network Prevent

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

Trellix Data Loss Prevention Network Monitor

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

Trellix Data Loss Prevention Discover

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

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

Trellix Data Encryption (TDE) offers a full range of products to safeguard data and devices from unauthorized access.

Trellix

Trellix Data Encryption Products

Protect enterprise and removable device data

Trellix Drive Encryption (TDE)

- Prevent unauthorized information removal
- Encrypt data prior to transfer to removable media
- Encrypt sensitive email attachments
- Enable separation of duties
- Meets compliance requirements
- Integrates with Active Directory (AD)
- Variety of authentication methods

Trellix Native Drive Encryption (TNE)

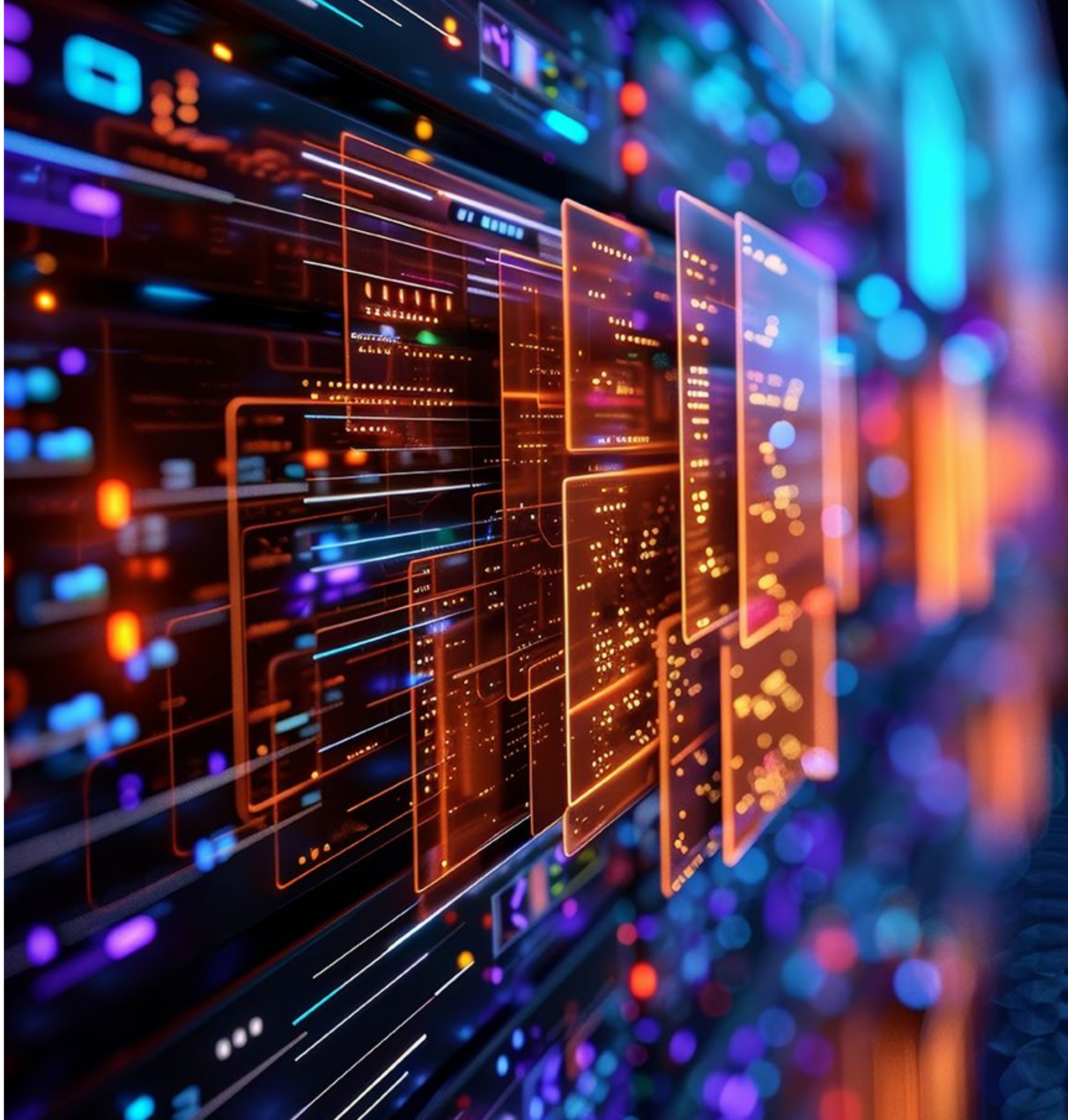
- Full disk encryption
- Supports multiple users
- Integrates with Active Directory (AD)
- Meets compliance requirements
- Seamless login
- Self-service recovery
- Manage users centrally
- FIPS 140-2 standards
- Variety of authentication methods

Trellix File & Removable Media Protection (FRP)

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

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

Trellix Database Security finds and protects sensitive information in databases from accidental leakage or intentional exploitation while maintaining performance and managing user access.



Trellix Database Security

Find and defend databases and the information they contain

Trellix Database Security

Virtual Patching

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

Vulnerability Manager

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

Database Activity Monitoring

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

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

DEMO

Trellix

Personas

Who to target

Data Security Buyers are Diverse

Understanding the buying committee

CISO (Economic Buyer)	Strategic leader, focused on minimizing risk and cost associated with complex environments, preserving reputation, upholding regulatory objectives, value, and efficiency
Security / Technology Leader (Champion)	Secondary buyer, strategic stakeholder, focused on event monitoring, quick remediation, time-saving tools, unified management and ways to simplify for their teams
Risk, Information, and Compliance (Champion)	Could be the technology owner, focused on complex regulatory objectives, breach reporting, auditing, alignment with frameworks, ensuring compliance, privacy, and information governance
User	Administers technology solutions or works with the solutions within a team, collaborates with organization stakeholders to meet business objectives for technology, configuration and reporting
Procurement Vendor Relations	Collaborate with the business to manage the buying process, RFI / RFP, solicit bids and proposals, no role in technology use or administration; critical to new business growth and renewal relationships; often a gatekeeper to business stakeholders

Economic Buyer - CISO

Sample Titles: Chief Information Security Officer (CISO), Chief Security Officer (CSO), Chief Technology Officer (CTO), or Chief Information Officer (CIO)

Challenges and Pain Points:

- Compliance
- Insider Risk / Threats
- Expanding Information Footprint

Key Attributes:

- Strategic leadership
- Understands security goals at the program level
- Conduit to Executives / Board
- Typically an industry expert

Priorities:

- Create a secure, easy-to-manage environment with the best Return on Investment (ROI)
- Deliver value and protect the data ecosystem
- Prevent data theft and data leaks that harm reputation, cost money, and lose customers
- Keep employees focused on strategic priorities and meet business objectives
- Meet regulatory objectives
- Report to Executives and the Board
- Stay up to date on threat intelligence
- Reputation of organization to hire the best people

Champion: Information, Risk, and Compliance

Sample Titles: VP / Director - Governance, Risk and Compliance; Legal, Privacy, Chief Privacy Officer; Director Privacy and Compliance; Director, Governance, Risk, and Compliance; Chief Legal Officer; Director Risk Management; Director / Manager of Information Management; Director of Database Management

Challenges and Pain Points:

- Compliance
- Insider Risk / Threats
- Expanding Information Footprint

Key Attributes:

- Specialty technology owner
- Conducts research, presents options, understands processes
- Manages activities and staff or individual contributor
- Professional / industry expert

Priorities:

- Meet complex regulatory objectives
- Pass audits quickly
- Prevent data theft and data leaks that harm reputation, cost money, and lose customers
- Provide users the information they are entitled
- Align with frameworks like HIPAA and PCI
- AI / ML-powered tools for activities that save time and improve performance
- Audits, reporting, tracking and forensics
- Available expert support; technology solution training
- Align with internal processes / technology tools

User: Technology, Security, and Information

Sample Titles: Information Security Analyst, Security Operations Specialist, Data Security Engineer, Information Security Architect, Information Technology Specialist, SecOps Analyst, Database Administrator, IT Specialist, Technology Services Administrator

Challenges and Pain Points:

- Compliance
- Insider Risk / Threats
- Expanding Information Footprint

Key Attributes:

- Technical skills
- Interacts with organization end-users
- Appreciates efficiency tools, centralization, self-service
- Important influence on buying process

Priorities:

- Prevent data theft and data leaks that harm reputation, cost money, and lose customers
- Maintain operational efficiency
- Complete day to day priorities
- Easy reporting for the leaders to share with executive stakeholders
- Integrate with existing third-party technology and tool orchestration
- Clear informational instructions for end users
- Real-time event data, unified management
- Available expert support and training

Trellix

Pain Point & Discovery Questions

Pain Points	Discovery Questions
Insider Risk \ Threats	● What technologies or processes do you have in place today that protect your organization from insider threats like employee data theft or accidental data leakage? ● How would your current technology spot and stop the exfiltration of sensitive information or intellectual property if your organization was the victim of a ransomware attack? ● How do your current data security technologies instantly coach end users in your organization when they attempt to violate data security sharing guidelines? ● How effective are your current security technologies at blocking attempts to share sensitive information with unauthorized users?

Pain Point & Discovery Questions

Pain Points	Discovery Questions
Ensuring Compliance	● What type of compliance requirements, regulatory standards, or privacy laws impact your organization? ● Do you have any computers / laptops shared by multiple users requiring encryption or the ability to provide detailed reporting on login by authorized users for compliance purposes? ● Do you need solutions to protect data on devices and removable media, including full auditing and compliance capabilities, user-self service recovery and streamlined logins to save administrative resources? ● How do your current technologies handle real-time event monitoring and detailed reporting based on your organization's requirements? ● Do you have databases with sensitive data like PII, PHI, payment card data? How do you ensure only authorized users access that data?

Pain Point & Discovery Questions

Pain Points	Discovery Questions
Expanding Information Footprint	● Do you see the volume of data expanding in storage repositories, on endpoints, and in databases as a concern to your organization? Where is your data expanding most today? ● What type of program do you have in place to identify what data needs to be retained and what can be disposed of? ● How much visibility does your organization have into sensitive data across endpoints, email, the web and network storage? ● How have resource constraints impacted the ability of your organization to develop a program to identify, classify, and protect the data that matters to your stakeholders?

Trellix

Proof Points

Customer Case Studies

Data Security Customer Stories

Services Organization for Large Municipal Agency

Industry: Public Sector - Services

Trellix Products: Trellix Data Encryption Suite (CDB)
Trellix Data Security Endpoint Protection Suite (CDA)

Challenges

- Current policies weren't flexible enough to comply with a variety of use cases
- Challenges demonstrating the separation of duties for access controls
- Constant data expansion made it difficult to properly assess data being uploaded and updated
- Lack of visibility across the data lifecycle

Solutions

- Encryption policies easily deployed at scale through a single management console
- Monitoring of encryption status in real-time with implementation of seamless access controls for users with necessary authentication
- Data discovered and protected across top threat vectors enabling departments and teams to develop custom policies and implement at the file level

Results

- Seamless integration of role-based access control with custom policies by department
- Mixed on-premises and SaaS delivery with centralized deployment and management
- Successfully increased visibility and scaled to handle an average of 10K new files per day

Trellix

Data Security Customer Stories

Energy Sector Agency

Industry: Energy

Trellix Products: Trellix Data Security Suite with OCR
Endpoint Protection Platform (EPP)
Endpoint Detection and Response (EDR)

Challenges

- Experienced failed implementation of previous solution that also proved interoperable with other existing solutions
- Complex government and industry regulations
- Accidental insider risk

Solutions

- Simplified and streamlined compliance activities with out-of-the-box reporting
- Addressed insider-risk threats by instantly coaching end users
- Blocked attempts to share sensitive information with unauthorized contactors
- Integration with the customer's Trellix solutions
- Centralized deployment, administration, event detection and policy management

Results

- Ensured effective compliance with complex government and industry regulations
- Heightened visibility into potential misuse by employees and contractors, whether malicious / accidental
- Single pane of glass for end-to-end security with ePO translated to seamless integration between multiple products

Data Security Customer Stories

Cybersecurity Administrative Agency

Industry: Government / Civil

Trellix Products: Trellix Data Security Suite with OCR*
Thrive Advanced

Challenges

- War in Ukraine causing concerns about targeted attacks
- New privacy laws in effect
- Need to integrate a classification tool
- Need to collaborate with international partners for threat intelligence and data sharing securely

Solutions

- Implementation of integration with Boldon James' (now Fortra) data classification tool
- Apply encryption policies to end-user devices to ensure security in all situations
- Comprehensive compliance policies out of the box to help comply with new privacy law
- Access to threat intelligence and secure data sharing through seamless integrations

Results

- Meet international guidelines for operational readiness
- Closed gaps in security and achieved compliance with privacy law
- Successful integration with third-party tools

*Optical Character Recognition

Trellix

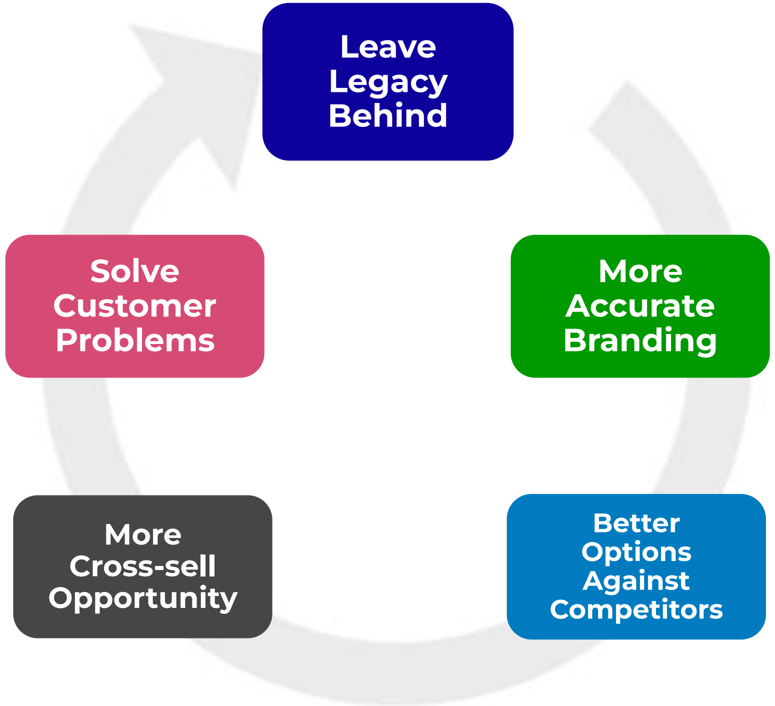
Trellix

Product Packaging

What SKUs

What changed in 2024

Trellix Data Security modernized our offerings



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

Data Security Product Packages

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

Trellix

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

Trellix

Upsell and Cross-Sell

Positioning the solution to customers

Customer Journey

Data Loss Prevention Suite (TDL)

Driver

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

Why Upgrade?

If a customer has Endpoint Protection or Device Control, this adds vast data discovery capabilities, stops data exfiltration across common threat vectors and educates users on data sharing policies. Aligns with regulatory standards for easy compliance.

What is not included

Does not include device encryption, management of native encryption or protect removable media.

Data Security Endpoint Protection Suite (CDA)

Driver

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

Why Upgrade?

If customer has Endpoint Protection, Device Control, or DLPe, this package will increase their ability to protect data on workstations and laptops, as well as removable media. Apply DLP policies to encrypt data at the file level and get self-extracting email encryption protection for attachments.

What is not included

This package does not include Network Discover, Capture, or offer the OCR add-in for forensics.

Database Security (DCD)

Driver

Unprotected databases and the sensitive information they contain

Why Upgrade?

If a customer manually manages their database security, add this to their Trellix protection. If they have activity monitoring from another vendor, our product is more comprehensive with DAM, vulnerability manager and virtual patching. This tool helps with several global compliance mandates automate manual tasks.

To consider:

DCD can be sold as a stand alone to new customers, but this is best offered to clients with other Trellix tools as part of renewals or new deals.

Data Security Suite + Database Security Add-on (DATA | DATA-DB)

Driver

Protect the data that matters

Why Upgrade?

Customers will get comprehensive discovery, visibility and control across the top threat vectors for the entire data lifecycle. Protect sensitive and proprietary data across endpoints, email, web and network storage, as well as safeguard device and file data. Get centralized management, robust compliance reporting and user coaching. Database add-on available at a discounted price.

To consider:

For organizations that want solutions that extend into the Cloud consider adding products from Skyhigh Security.

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

Existing Customer Opportunities

Targeted Paths to Revenue

Path	Why These Opportunities?	Upsell / Cross-sell Them
Cross-Sell Data Security into Endpoint Customers **Targeted SKUS:** - Endpoint Bundles with **(MV 1, 2, 4, 5, 6, 7, TRX1)**	- Existing Endpoint and Device Control customers are often unaware of the full capabilities of Data Security products, especially DLP Endpoint - Given that these customers already have a vested interest in securing information on workstations and laptops, we're looking for those customers to convert into adopting one of our Data Security offerings	Data Security Endpoint Protection Suite **(CDA)** -OR- Data Loss Prevention Suite **(TDL)** -OR- Data Security Suite **(DATA)** In Addition: Add-on Database Security **(DCD or DATA-DB)** if applicable
Upsell Existing Data Security Customers **Targeted SKUS:** - Device Control **(DEC)** - DLP only SKUs **(DLP, DDS, DPO, DPV)** - All Data Security Bundle SKUs **(TDL, CDA, CDB, NDLP)**	- Existing DLP customers are often not aware of the full suite of capabilities we offer in our full Data Security Portfolio and the more comprehensive protection they'd receive. - Data Security Suite (SKU: DATA and DATA-S) is a new SKU. We want to sell into it to increase deal size and deliver comprehensive coverage. - Database Security is an add-on available for our our suite DATA (only on-premises) and as a standalone that we're re-launching in Q2 2024 supported by new developers with a robust roadmap	Data Loss Prevention Suite **(TDL)** -OR- Data Security Endpoint Protection Suite **(CDA)** -OR- Data Security Suite **(DATA)** In Addition: Add-on Database Security **(DCD or DATA-DB)** if applicable
Database Security As a stand-alone or as an add-on. - All targeted SKUs	- Database Security is now available as a standalone that we're re-launching in Q2 2024 supported by new developers with a robust roadmap - We should promote this product to any existing customer with databases even if they don't purchase one of our other packages.	Database Security **(DCD)**

Cross-Sell Data Security into Endpoint

Selling TDL, CDA, or DATA (Add-on DCD | DATA-DB)

- Increases customer's endpoint protection to add robust data discovery, stops data exfiltration and options like OCR and Capture, delivers added options for auditing and forensics across the top data leak vectors (TDL, DATA)
- Customers that want encryption and to stop data exfiltration from endpoints will benefit from this product (CDA, DATA)
- The TDE and TNE products provide significant flexibility for workstation and device encryption - CDA (CDA, DATA)
- FRP is a great add on to stop exfiltration and enhance endpoint use cases (CDA, DATA)

Benefits for Sales

- Increase total customer spend
- Place Trellix as the comprehensive solution to protect data
- Expand ePO stickiness as a foundation for Trellix products
- Leverage vendor consolidation desires of the customer

Sales Path Opportunity Cheat Card

Value Messaging

- Visibility and control across top data threat vectors
- Data discovery, classification
- Out-of-the-box compliance policies, reporting
- Supports remote work
- Flexible for organizations with mixed environments
- Centralized administration, events, reporting in ePO
- Safeguard device and file data

Customer Positive Outcomes

- Save money by avoiding financially motivated malicious insider attacks / accidental data leakage
- Speed up and simplify compliance activities
- Avoid reputational damage, penalties, and fines
- Speed up and simplify compliance
- Manage expanding information footprint with fewer resources

Discovery Questions

- Have you experienced a data breach? (TDL, CDA, DATA)
- How do you currently montor and stop the exfiltration of sensitive data? (TDL, CDA, DATA)
- What compliance requirements or regulatory standards apply to your organization? (TDL, CDA, DATA)
- What type of sensitive information does your organization store or process? (TDL, CDA, DATA)
- What third-party tools do you integrate with for incident management, data classification, etc..? (TDL, DATA)
- How does your organization address the need for multiple users to address workstations and laptops? (CDA, DATA)
- What types of encryption protection do you apply today and at what level of your data is it enabled? (CDA, DATA)
- Do you have databases and what types? How do you ensure your database protection is up to date? (DCD, DATA- DB)

- We also recommend **Thrive Advanced** or **Thrive Elite** be added so customers can work with professional services to assess and enhance data governance programs
- To extend DLP coverage from the **Keyboard to the Cloud**, combine **Trellix DLP products and Skyhigh Security SSE**
- For customers that consider our suites too expensive or who don't need all the features, consider just **DLP Endpoint Complete.**

Additional Notes

Upsell Existing Data Security Customers

Selling TDL, CDA, or DATA (Add-on DCD | DATA-DB)

- The full DLP suite provides more comprehensive protection. ((TDL)
- Any DLP policies in ePO can be extended to all DLP products (TDL, DATA)
- Customers that want encryption and to stop data exfiltration from endpoints will benefit (TDL, CDA, DATA)
- DLP policies in ePO combined with FRP to encrypt at file level (CDA, DATA)
- FRP is a great add on to stop exfiltration and enhance endpoint use cases (CDA, DATA)
- Leverage the new DATA bundle for 2024 that includes all the DLP and Encryption products (DATA)

Benefits for Sales

- Increase total customer spend
- Place Trellix as the comprehensive solution to protect data
- Expand ePO stickiness as a foundation for Trellix products
- Leverage vendor consolidation desires of the customer

Sales Path Opportunity Cheat Card

Value Messaging

- 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
- Safeguard device and file data

Customer Positive Outcomes

- Stop data leaks and insider threats
- Users prevented from removing sensitive or proprietary data
- Users are better educated
- Understand device status across environment
- Smoothly integrate with other Trellix tools, add Skyhigh for cloud coverage, seamless API integrations with third-parties like Chrome

- We also recommend **Thrive Advanced** or **Thrive Elite** be added so customers can work with professional services to assess and enhance data governance programs.
- To extend DLP coverage from the **Keyboard to the Cloud**, combine **Trellix DLP products and Skyhigh Security SSE**
- For customers that consider our suites too expensive or who don't need all the features, consider just **DLP Endpoint Complete**

Discovery Questions

- Have you experienced a data breach? (TDL, CDA, DATA)
- How do you currently montor and stop the exfiltration of sensitive data? (TDL, CDA, DATA)
- How are you using notifications to coach users and request justification to share sensitive data? (TDL, CDA, DATA)
- What compliance requirements or regulatory standards apply to your organization? (TDL, CDA, DATA)
- What type of sensitive information does your organization store or process? (TDL, CDA, DATA)
- How does your organization address the need for multiple users to address workstations and laptops? (CDA, DATA)
- What types of encryption protection do you apply today and at what level of your data is it enabled? (CDA, DATA)
- Do you have databases with sensitive or proprietary information? How do you ensure that vulnerabilities are addressed and that only authorized users can access the information they are entitled to? (DCD, DATA- DB)

Additional Notes

Database Security for Existing Customers

Selling DCD | DATA-DB

- Database Security from Trellix is a great way to expand our presence in a current account that has databases they are managing configurations for on their own, with patches that are out of date, that contain sensitive information and / or that may not be cataloged within the environment
- Cross-selling into this product as we relaunch is a good strategy because the product will be enhanced in the next year

Benefits for Sales

- Increase deal size
- Enhance relationship with Trellix products
- Position Trellix as the comprehensive solution to protect data

Sales Path Opportunity Cheat Card

Value Messaging

- Compliance with mandates for data activity monitoring
- Protect organization’s most sensitive data
- Save time and resources with scan / patching

Customer Positive Outcomes

- Meet compliance guidelines
- Stop unauthorized access to sensitive data
- Automate current manual tasks and protect databases that no longer receive manufacturer’s patches

Discovery Questions

- What compliance laws and regulations impact your organization? (DCD, DATA-DB)
- What type of sensitive information does your organization store or process in databases? (DCD, DATA-DB)
- How are you protecting and optimizing your databases? (DCD, DATA-DB)
- Do you know what databases and where are in your environment? (DCD, DATA-DB)
- Do you have any legacy applications with out of support databases that you’re responsible for protecting? (DCD, DATA-DB)
- How do you ensure your databases are protected when a zero-day vulnerability is announced until a vendor patch is created? (DCD, DATA-DB)
- How do you know if all of your databases are running the latest security patches? (DCD, DATA-DB)

Additional Notes

- We also recommend **Thrive Advanced** or **Thrive Elite** be added so customers can work with professional services to assess and enhance data governance programs.
- DBSec is priced per instance, so please work with your SE team to understand impacts to your quotes
- Supported database types and licensing can be complex, engage the SE team or Product Management with questions - especially during the early stages of the relaunch in 2024

Organizational Profiles

Ideal Targets for Both New and Existing Customers

Organizational Size

Large and complex environments

Multi-location organizations

Trellix Segments:
Major and Enterprise

Information and IT Environment

Medium to high information governance maturity

On-premises

Hybrid

Industries or Verticals

Government / Civic - International, National, and Regional / Local (SLED*)

Financial / Banking

Healthcare

Infrastructure / Energy

Manufacturing / Industrial

Science and Technology

*State, Local and Education (SLED)

Trellix