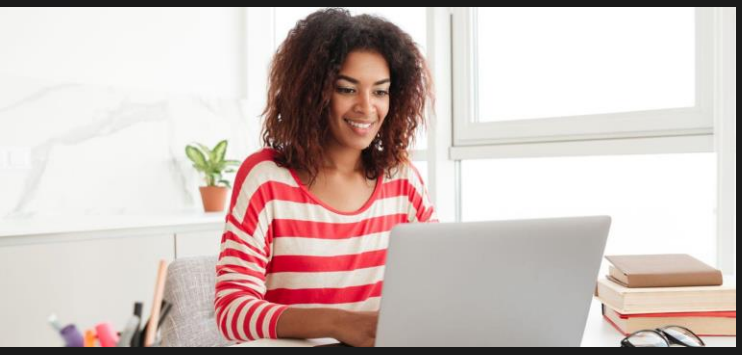
Trellix



Trellix Data Security Suite

As an existing EDR partner, Trellix is pleased to collaborate with the customer on advancing their security maturity journey towards the Trellix Data Security Suite.

The current and future state below explains customer's situation and reason to action

Current State

More Data, Less Control Over It: With data storage growing at an unprecedented rate, ensuring visibility and protecting sensitive data alongside information being produced and transferred becomes increasingly difficult.

Lost, Stolen, and Misplaced Assets: Lost company laptops and other unsecured devices increase risks of security breaches. Management doesn't know if all corporate connected devices are protected.

Compliance Is Burdensome: Companies, especially in highly regulated industries, face ever-changing laws and regulations while governance, risk and compliance tasks are often highly manual, time consuming, resource-intensive, and critical to prevent penalties for non-compliance.

Accidental Insider Data Leaks: Careless information handling and misconfigurations result in accidental data leakage due to a employees sharing potentially sensitive information with unauthorized users.

Future State

Secured Data Across Top Threat Vectors: Manage an expanding information footprint with fewer resources and real-time visibility across common data leakage points.

Centralized Management: Single management console consolidates policy administration over various tools, including BitLocker and FileVault, providing real-time visibility into data events/reporting.

Simplified, Streamlined Compliance: Save countless hours meeting regulatory guidelines with out-of-box classifications, policies, and reporting aligned to global laws and frameworks.

Safeguarding What Matters: Mitigate insider risk by blocking attempts to share sensitive information, request justification and coach users who attempt to violate data sharing policies with minimal impact to business operations.

Trellix brings unparalleled, industry leading Data Security experience with a proven record of excellence to support customer's security maturity journey.

DISCOVER

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

PROTECT

Flexible policies that can be applied based on user risk, status, and role

Encryption at the file level based on integrated DLP policies

RESPOND + REPORT

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

Centralized deployment, policy administration, reporting, and event tracking

Protect Against Insider Risk

- Identify and classify sensitive data
- Monitor and prevent exfiltration
- Coach users with notifications, prompts for justifications and definitions of classifications

Address Compliance Regulations

- Out of the box rules and policy options aligned with regulatory frameworks
- Scanning and capture to support auditing and forensics
- Reporting - regular and ad-hoc (event-based)

Data Visibility & Labeling

- Visibility across the environment and into storage locations with data discovery, identification, and classification
- Label data that needs to be retained and prioritize data protection activities accordingly

Streamlined Management & Event Handling

- Unified management through a central console that simplifies deployment, policy management and reporting
- Automation and workflows to speed up remediation and event handling

Stop Exfiltration in Ransomware Attacks

- Stop exfiltration efforts with policies for blocking extraction of sensitive information
- Integrate with SIEM/ SOAR to ensure streamlined incident management across tools

Why the customer should move to the Trellix Data security Suite now?

Worldwide data storage is expected to increase to 200 zettabytes in 2025.

35% of breaches are driven by internal malicious actors, 80% of them were financially motivated.

68% of data breaches included a human element, with a significant portion driven by accidental user error.

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

The global average cost of a data breach in 2023 was $4.45 million, a 15% increase over 3 years.