Trellix • STELLAR CYBER®

SOLUTION BRIEF

Enhanced Threat Detection and Response Across the Entire Attack Surface

Trellix and Stellar Cyber Working Together to Make Security Operations Simpler for Everyone

Challenges

- The complexity of managing security tools
- Evolving attacks
- Lack of skilled resources

Trellix Compatible Solution

- Stellar Cyber SecOps Platform
- Trellix Endpoint Security

Trellix Solution

- Reduces SecOps complexity
- Built-in automation
- Speedy investigation and mitigation

Results

- Gain visibility and SecOps efficiency with enriched analytics and investigation.
- Integrate and correlate critical data across multiple attack vectors.
- Accelerate threat investigations and threat hunting through automated response.

Security teams need their security products to work together to eliminate blind spots and reduce manual processes that severely impact their ability to deliver consistent, continuous security outcomes.

Trellix and Stellar Cyber are integrating to deliver a solution to help organizations protect their on-premises, cloud, and hybrid environments by using the latest advancements in cybersecurity technologies. Stellar Cyber provides a security operations platform that automates the identification of advanced threats by correlating disparate threat signals from various data sources, providing security analysts with the information needed to mitigate threats quickly. As a result, customers using the combined offering will see improvements in detecting and responding to threats, decreasing the risk of a significant breach.

Stellar Cyber automatically incorporates rich threat intelligence from Trellix, enabling real-time threat protection and providing analytics for comprehensive security insights. Individual alerts automatically correlate into a context-rich incident to reconstruct the attack end-to-end. The added visibility of Trellix detections enriches data in Stellar Cyber, providing additional context for threat detection and investigation. By combining Trellix and Stellar Cyber, SecOps outcomes are improved dramatically, eliminating the ability for threat actors to take advantage of blind spots.

The Business Problem

Security teams are inundated with data, hampering their ability to quickly identify and investigate threats that could impact their environment most. To keep pace with the continuous flow of attacks, security teams need products that:

- Replace time-consuming manual tasks with automated processes
- Automate data ingestion and event correlation
- Deliver investigation-ready cases that require no manual intervention
- Makes responding to threats fast with pre-built integrations
- Are backed by backed by a company invested in their team's success.

SOLUTION BRIEF

About Stellar Cyber

Stellar Cyber delivers a flexible, easy-to-use, affordable security operations platform, empowering lean security teams to take control of their security operations. With NG-SIEM, NDR, UEBA, TIP, FIM, IDS, and intelligent automation, Stellar Cyber streamlines investigation workflows, driving down attacker dwell time while increasing security analyst productivity.

About Trellix

Trellix is redefining the future of cybersecurity with its open and native extended detection and response (XDR) platform, helping organizations to gain confidence in the protection and resilience of their operations. Trellix and its partner ecosystem, accelerates innovation through machine learning and automation, empowering over 40,000 customers with living security.

Learn More

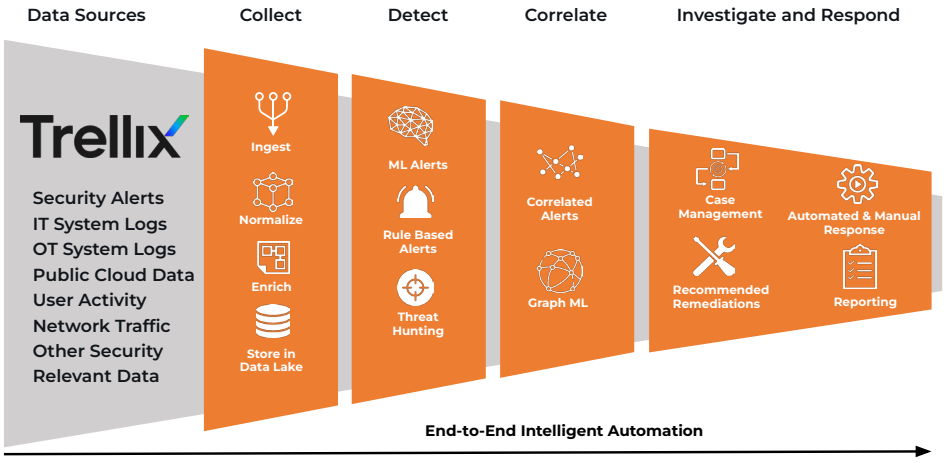
Contact your Trellix representative or channel partner for more information, or visit www.trellix.com.

Trellix and Stellar Cyber Joint Solution

In today's dynamic cybersecurity landscape, organizations face increasingly sophisticated threats that require advanced tools and strategies for detection, response, and mitigation. By combining Trellix endpoint security mutual customers can see real- time correlation for endpoint data with network events, enhancing the ability to detect sophisticated threats and anomalies. When HX data is sent to the Stellar Cyber platform, Stellar Cyber can centralize, correlate and enrich the data enabling analysts to prioritize threats based on severity and relevance. Security analysts can leverage Trellix's forensic capabilities and Stellar Cyber's advanced analytics to investigate security incidents thoroughly.

This is precisely what the Stellar Cyber SecOps Platform delivers. With Stellar Cyber, you can ingest data from any data source into the platform where automated normalization, processing, and threat correlation occur automatically.

Stellar Cyber SecOps Platform



Joint Benefits include:

- Enhanced Visibility: Expands "line of sight" visibility across the entire attack surface from endpoint to cloud workloads.
- Intelligent Automation: AI-driven threat detection with automated investigation allows SOC analysts to combat threats effectively.
- Ease of Use: The combined solution means security analysts of any expertise, from beginner to seasoned experts, can deliver consistent security outcomes.