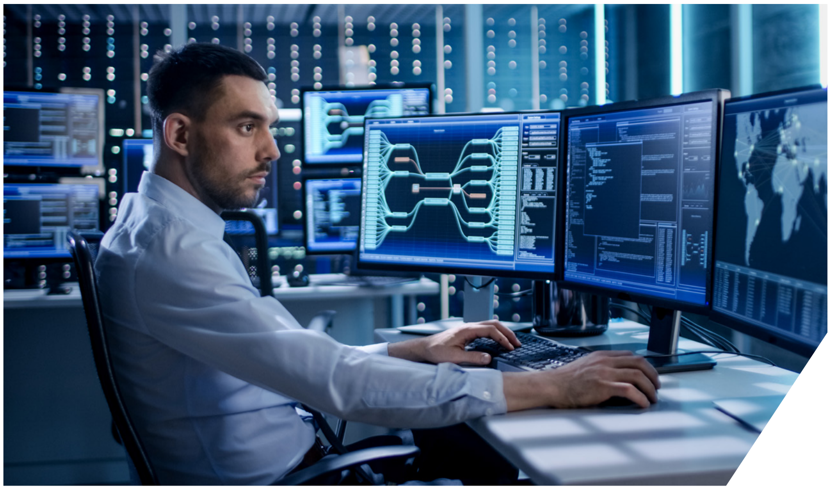
SOLUTION BRIEF

Optimal Security and Visibility: The Trellix and Mira Security Partnership

Introduction

The Trellix security platform is used to protect data across on premise or hybrid cloud ecosystems, while uniquely delivering security management, automation, and orchestration at scale. Mira Security's Encrypted Traffic Orchestrator (ETO), provides industry leading decryption technology that can augment the Trellix platform stack (either as a virtual or physical appliance) providing visibility into encrypted traffic by decrypting TLS/SSL and SSH traffic flows.



The Business Problem

The use of encrypted SSL traffic has been on the rise for many years. It has become the standard that most users and applications expect. Its ease of implementation has allowed organizations of all sizes to utilize it. However, this has also created a blind spot for IT administrators. While protecting data from prying eyes, it can also conceal malicious files from network security tools, allowing them to slip into the network unseen allowing for exfiltration of sensitive company data to go undetected. Security conscious organizations require visibility into encrypted SSL traffic in order to protect their employees, customers and business. While providing visibility into traffic sounds great, it should not be at the expense of performance or security. The end user should not be impacted by the visibility which should be transparent, safe and secure.

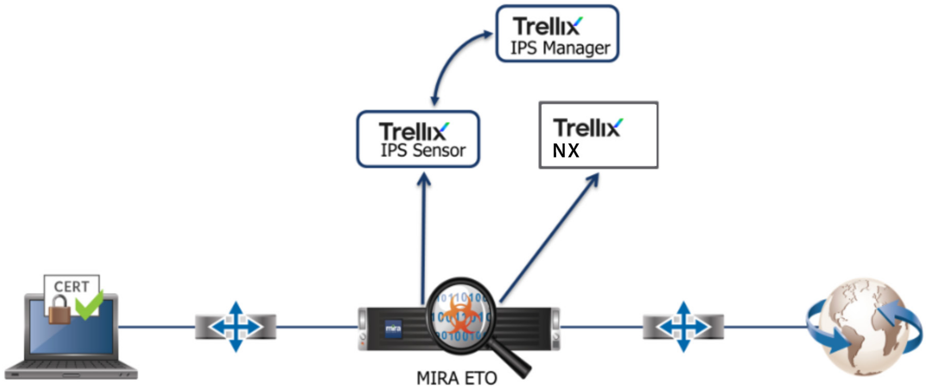
Joint Solution - Trellix Platform and Mira ETO

The Trellix platforms and Mira Security ETO seamlessly work together to provide a powerful solution with scalability and flexibility. Users can choose between inline and passive deployment methods, allowing them to either proactively contain threats or receive timely alerts. Mira Security ETO, positioned between the client and server, decrypts traffic, sends it to the IPS Sensor for analysis, and then re-encrypts it before sending it on to its destination. This strategic process enables Trellix's IPS sensor appliance to identify both recognized and previously elusive threats, going beyond traditional detection methods. The Trellix IPS Manager, a crucial component, offers IT administrators a user-friendly web interface for comprehensive monitoring and management of IPS Sensor activities, enhancing the overall experience.

Trellix Network Security (NX) and Mira Security ETO also work together to seamlessly offer a solution that provides scalability and flexibility. With both inline and passive deployment options, customers can contain a threat before it reaches the destination, or simply alert administrators of its presence. Mira allows full visibility into previously hidden traffic by sitting between the client and server. Decrypting the traffic, sending plaintext to the attached security tool, then re-encrypting the traffic before it is sent onto the destination. This allows Trellix's appliances to detect threats, and with Trellix's Intelligent Virtual Execution (IVX) engine at the core, detection is not relegated to known threats or ones that evade signature and policy based detection. Conventional signature based detection is also included for inline protection functionality.

Inline-Passive Deployment

Network Inline - Appliance Passive: The Mira ETO sits in the middle of the traffic flow. When the SSL/TLS handshake occurs, the ETO actively decrypts the traffic, passes the plaintext data over to the Trellix IPS Sensor and/or NX sensor for inspection, allowing detection of any security threats. It then re-encrypts the data and sends it on to the destination, maintaining the end-to-end connection in an encrypted form. The IPS Sensor will generate alerts and send packet logs to the IPS Manager. If NX is being used it will generate alerts and logs.

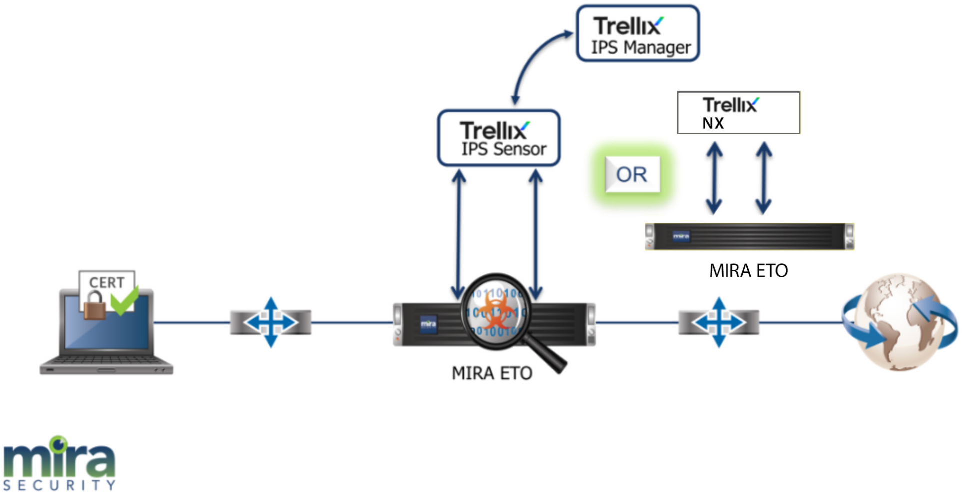


Trellix • mira SECURITY

SOLUTION BRIEF

Inline-Inline Deployment

Network Inline - Appliance Inline: The Mira ETO sits in the middle of the traffic flow. When the SSL/ TLS handshake occurs, the ETO actively decrypts the traffic. It passes this plaintext data over to Trellix IPS sensor or Trellix NX, which then inspects it and blocks any threats before passing the traffic back to the ETO. The ETO then re-encrypts the data and sends it on to the destination. The IPS Sensor will also generate alerts and send packet logs to the IPS Manager. NX will generate alerts and logs.

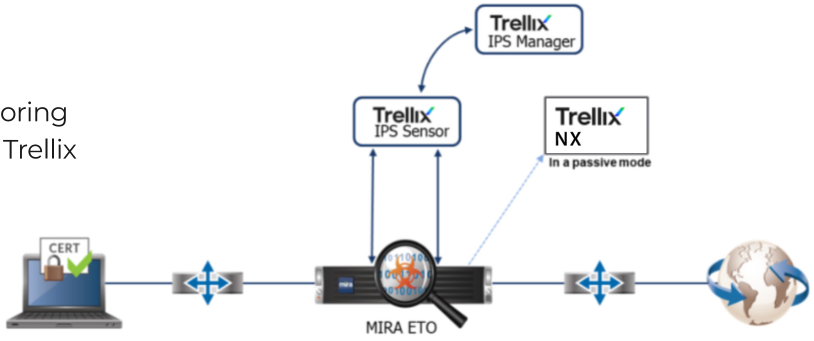


Another Inline-Inline Option: A Defense-in-depth Deployment to reach optimal security levels

Mira's ETO has an important feature that allows it to keep the previous deployment and add an extra layer of defense by activating the mirroring mode. This mode simultaneously sends decrypted traffic to both Trellix's IPS sensor and Trellix's NX, which operates in passive mode and policy-based detection.

Decrypt Once - Feed Many Deployment with Trellix Security Stack

While the ETO is in Inline/Inline mode and mirroring mode is active, decrypted traffic can be sent to Trellix IPS and Trellix NX simultaneity.



Joint Solution Benefits

Visibility: The Mira ETO will remove the SSL/TLS blind spots, allowing the Trellix Platform stack to analyze traffic that might otherwise be hidden by encryption.

Ease of Use & Simplicity: Both the Mira ETO and Trellix Platform solutions are easy to install, configure, and integrate with other elements of your security tech stack.

Flexible Rules & Policies: Use Mira's ETO Category Database to selectively bypass certain categories of traffic and safeguard sensitive user data. In the Trellix Platform, one can detect and prevent many types of attacks, regardless of how it is being delivered.

Scalability & Speed: The Mira ETO is available in speeds from 0.5 to 50Gbps of decrypted traffic supporting high throughput. The Trellix platform stack can handle up to 100 Gbps.

Platform Versatility: Tailoring itself to diverse network requirements, both the Mira ETO and Trellix Platform solutions are available in physical hardware or virtual appliance forms, compatible with both Private and Public Cloud environments.

Efficiency Amplified: Decrypt traffic once and distribute it to attached IPS appliances and passive security tools through app ports and mirror ports. This efficient sharing extends to other passive security devices, such as Trellix NX operating in passive mode.

About Mira

Today, we are an interdependent team with strong backgrounds in cybersecurity and networking. Our mission is to provide visibility into network traffic as our customers transition to higher speeds and new architectures, and to eliminate the compromise between privacy and security along their journey. We build lasting relationships with our valued customers and partners, and deliver innovative encryption software and products.

About Trellix

Trellix is trusted by the world's leading and largest enterprises. More than 40,000 customers, including nearly 80% of the Fortune 500, rely on living security from Trellix. We knew security could be different. Fast enough to keep up with dynamic threats. Intelligent enough to learn from them. Constantly evolving to keep the upper hand. So Trellix brings you a living XDR architecture that adapts at the speed of threat actors and delivers advanced cyber threat intelligence. We're changing what security means and what it can do, giving everyone in your organization the confidence that comes with being more secure, every day.