Detect. Decrypt. Deter.

JOINT SOLUTION BRIEF

Mira Security Partners with Trellix to Reach New Optimal Levels of Security and Visibility into Encrypted Traffic

Intro

Trellix's 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 SSL/TLS and SSH traffic flows.

The Business Problem

The use of encrypted SSL/TLS 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 enabled 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 and allowing exfiltration of sensitive company data to go undetected. Security-conscious organizations require visibility into encrypted SSL/TLS 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.

Joint Solution Benefits

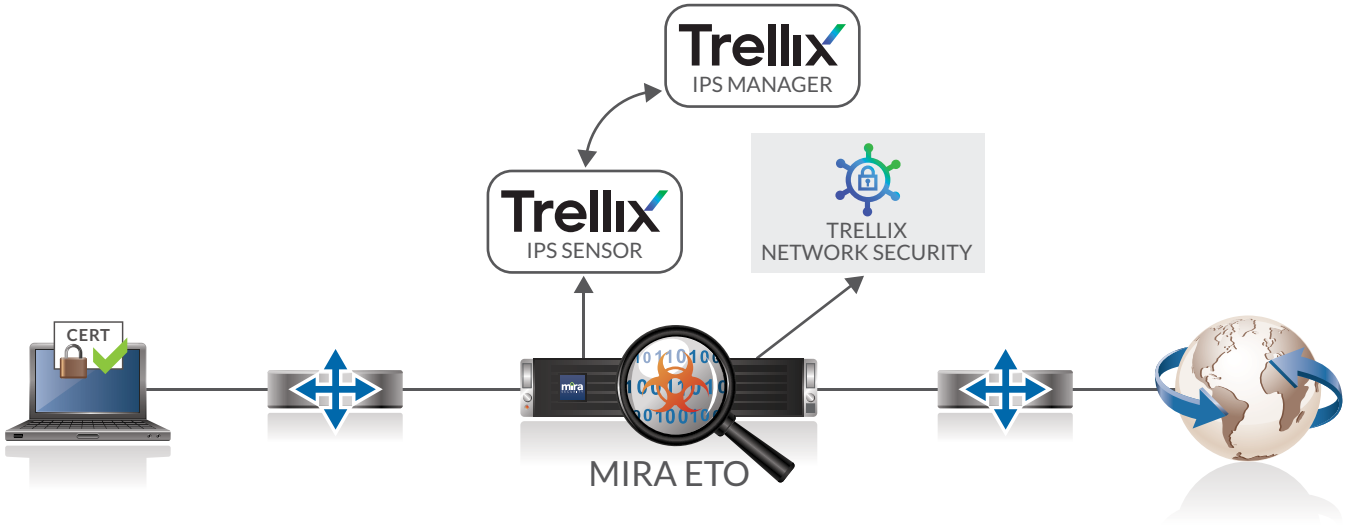
- **Visibility.** The Mira ETO will remove the SSL/TLS blind spots, allowing the Trellix platform stack to analyze traffic that might otherwise be hidden by encryption.
- **Ease of Use & Simplicity.** Both the Mira ETO and Trellix platform solutions are easy to install, configure, and integrate with 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 they are 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 10Gbps.
- **Platform Versatility.** Tailoring itself to diverse network requirements, both the Mira ETO and Trellix platform 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.

Mira ETO and Trellix Platform Joint Solution

Mira's ETO and Trellix's Intrusion Prevention System (IPS) work together seamlessly, providing 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. The 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 appliances 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.

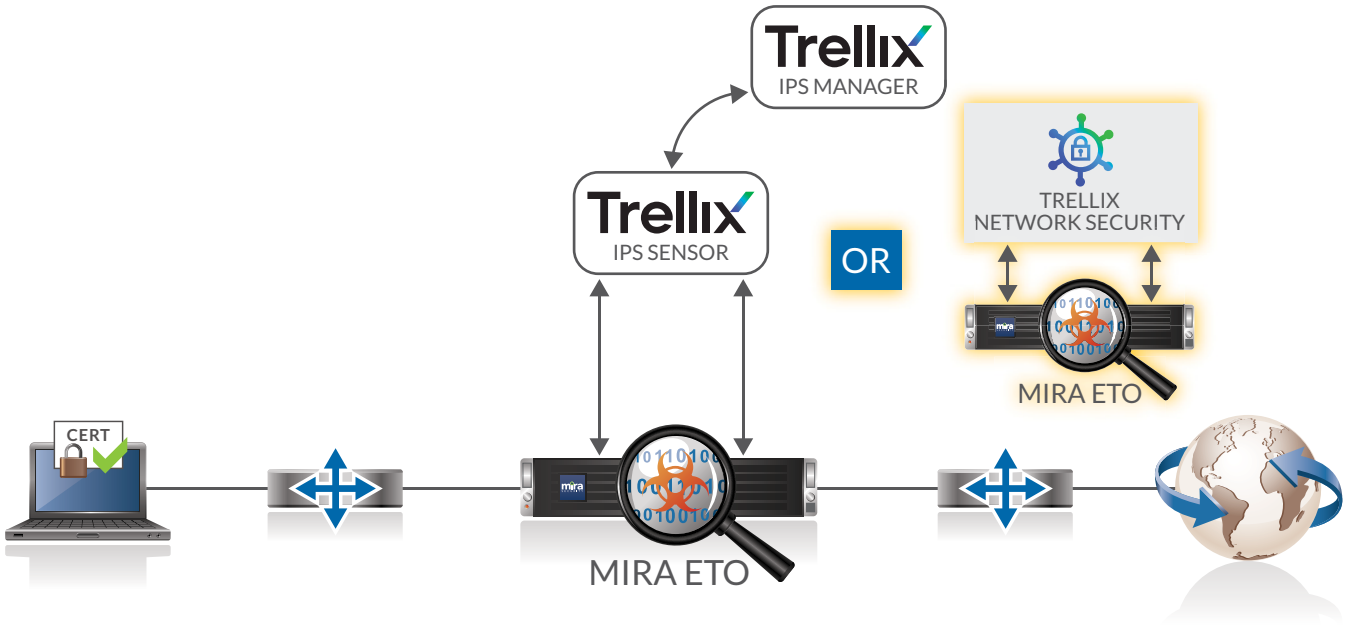
Mira's ETO and Trellix's Network Security NX also work together seamlessly to offer a solution that provides scalability and flexibility. With both inline and passive deployment options, customers can either contain a threat before it reaches the destination, or simply alert administrators of its presence. The Mira ETO allows full visibility into previously hidden traffic by sitting between the client and server decrypting the traffic, sending plaintext to the attached security tool, and then re-encrypting the traffic before it is sent onto the destination. This allows Trellix's appliances to detect threats and, with Trellix's (Multi-Vector Virtual Execution) MVX 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.

Typical Deployment Topologies



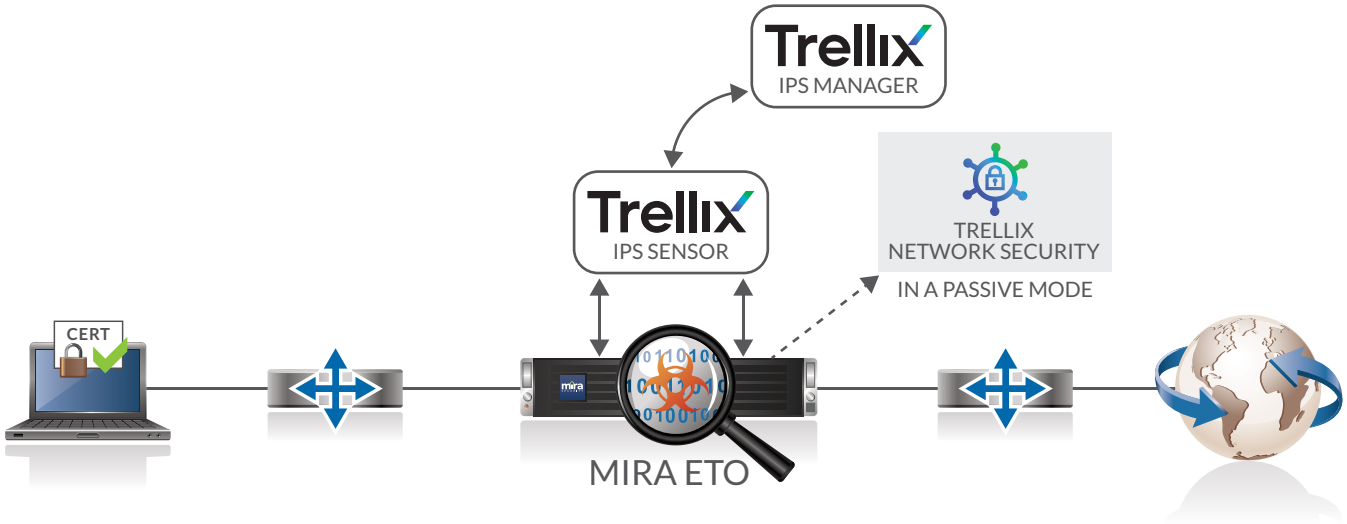
Network Inline – Appliance Passive

The Mira ETO sits in the middle of the traffic flow. When the SSL/TLS handshake occurs, the ETO actively decrypts the traffic and 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 the Trellix Network Security (NX) is being used, it will generate alerts and logs.



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

As an important feature, Mira's ETO can maintain the previous deployment and add an extra layer of defense by activating the mirroring mode which will be sending decrypted traffic simultaneously to both Trellix's IPS sensor and Trellix's NX running in a passive mode.

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.

Visit https://www.trellix.com to learn more.

MiraSecurity.com

info@mirasecurity.com

Mira Security
330 Perry Highway, Suite A
Harmony, PA 16037
Phone: +1 (412) 533-7830

Email: info@mirasecurity.com
mirasecurity.com

MIRA-TRELLIX-8/24