Detect. Decrypt. Deter.

JOINT SOLUTION BRIEF

# Trellix partners with Mira Security Encrypted Traffic Orchestrator (ETO) to give you optimal security and visibility.

mira SECURITY Trellix

## Intro

Trellix Network Security is used to protect data across your hybrid cloud ecosystem, all while uniquely delivering security management, automation, and orchestration at scale. Mira Security's ETO is a leading decryption technology that can augment the Trellix platform (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 now. 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. It has become clear that 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.

## Trellix and Mira Joint Solution

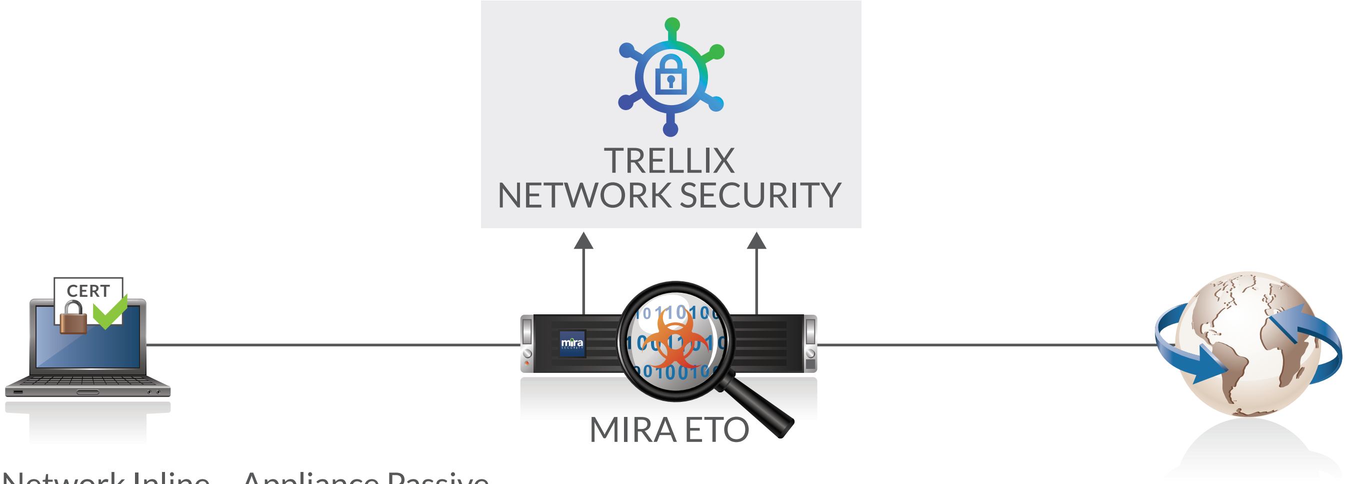
In combination, Trellix's Network Security and Mira's ETO offer an excellent solution that provides scalability

## Joint Solution Benefits

- **Visibility.** The ETO will remove the SSL/TLS blind spots allowing Trellix Network Security to analyze traffic that might otherwise be hidden by encryption.
- **Ease of Use.** Both the ETO and Trellix Network Security solutions are easy to install, configure, and integrate with other elements of your security tech stack.
- **Flexible Rules & Policies.** Use the ETO's Category Database to bypass certain categories of traffic and protect sensitive user data. In the Trellis Network Security, many types of attacks can be detected and prevented regardless of how it is being delivered.
- **Scalability & Speed.** The ETO is capable of decrypting traffic at speeds from 0.5 to 50 Gbps and allows for high throughput. Trellix Network Security is able to detect up to 10 Gbps.
- **Support for Different Platforms.** The ETO and Trellix Network Security are both available as physical hardware or virtual appliances to fit the needs of various networks.
- **Efficiency.** Decrypt traffic once and distribute it to attached Trellix Network Security appliances through app ports and mirror ports.

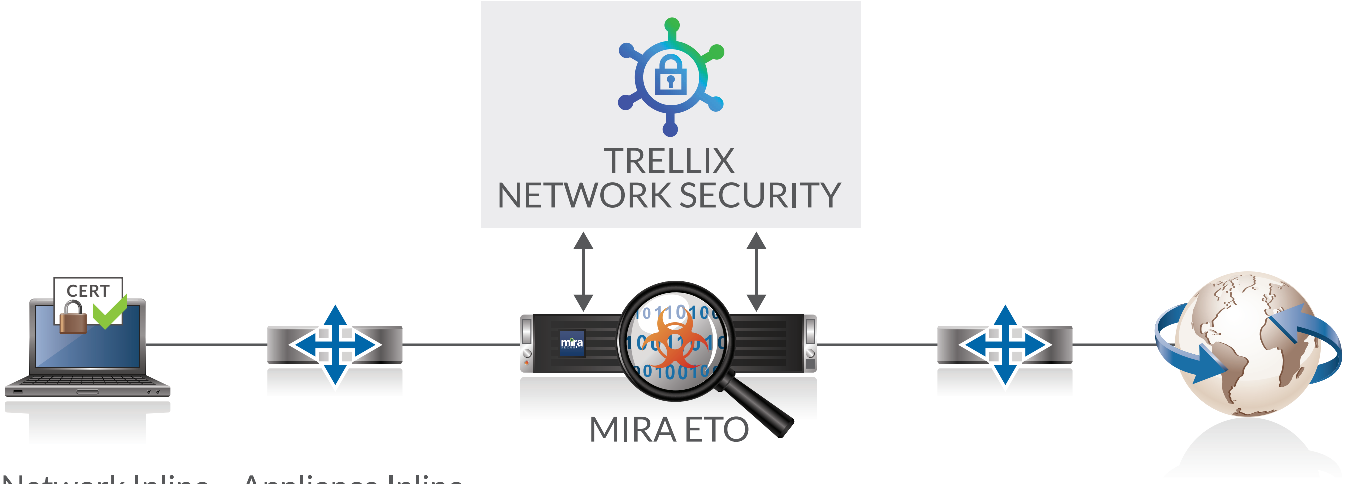
and flexibility. With both inline and passive deployment options, customers can either contain a threat before it reaches the destination, or simply alert administrators of its presence. Mira Security allows full visibility into previously hidden traffic by sitting between the client and server, decrypting the traffic, sending plaintext to the attached security tool, and then re-encrypting the traffic before it is sent onto the destination. Trellix Network Security is powered by the Trellix MVX detection engine, giving defenders the industry's most complete signature-based and signature-less detection to identify known and emerging threats. 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 appliance to analyze it and detect any security threats. Then it re-encrypts the data and sends it on to the destination, maintaining the end-to-end connection in an encrypted form.



### Network Inline – Appliance Inline

The Mira ETO sits in the middle of the traffic flow. When the SSL handshake occurs, the ETO actively decrypts the traffic. It passes this plaintext data over to Trellix appliance which then analyzes it and removes any threats it detects before passing the traffic back to the ETO. The ETO then re-encrypts the data and sends it on to the destination.

## 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
3159 Unionville Road, Suite 100
Cranberry Township, PA 16066
Phone: +1 (412) 533-7830

Email: info@mirasecurity.com
mirasecurity.com