Solution Brief

Mira Encrypted Traffic Orchestrator (ETO) and Stamus Security Platform (SSP) Solution Offers Visibility into TLS Traffic

The ability to detect threats in an encrypted environment is critical. Nearly all Internet traffic today is encrypted. And according to a 2020 SANS Institute network visibility report, 82% of respondents encrypt 25% or more of their internal network traffic. This poses a serious visibility challenge for monitoring the perimeter and is beginning to wreak havoc on systems inspecting internal traffic as well.

Innovative network security companies have responded by developing techniques to identify malicious activity in encrypted traffic without having to decrypt the flows. These techniques include heuristics around JA3 and anomaly detection using machine learning. But even with these techniques in place, the network-based threat detection systems will miss some threats.

This paper describes the powerful combination of network decryption from Mira Security and network detection and response from Stamus Networks.

USING THE NETWORK TO SECURE THE ENTERPRISE

The network holds the ground truth for an enterprise's security posture. Even as more organizations shift to cloud-based workflows, encrypted transmission, and remote workforces, nearly all cyber threats generate communications that can be observed on the network.

As such, mature enterprises tap into the inherent power of network traffic to uncover critical threats to their organizations. Network detection and response (NDR) systems use a combination of multiple detection technologies, such as signatures and machine learning-based anomaly detection, to uncover serious and urgent threats and help security teams respond sooner.

Unlike endpoint solutions, an NDR does not require installing agents on every system, does not consume valuable resources on each host, cannot be bypassed by attackers, and can provide exceptional visibility into user activity in environments with high concentrations of BYOD or guest systems. Fundamentally, an NDR can be deployed rapidly and without disrupting users.

The Business Problem

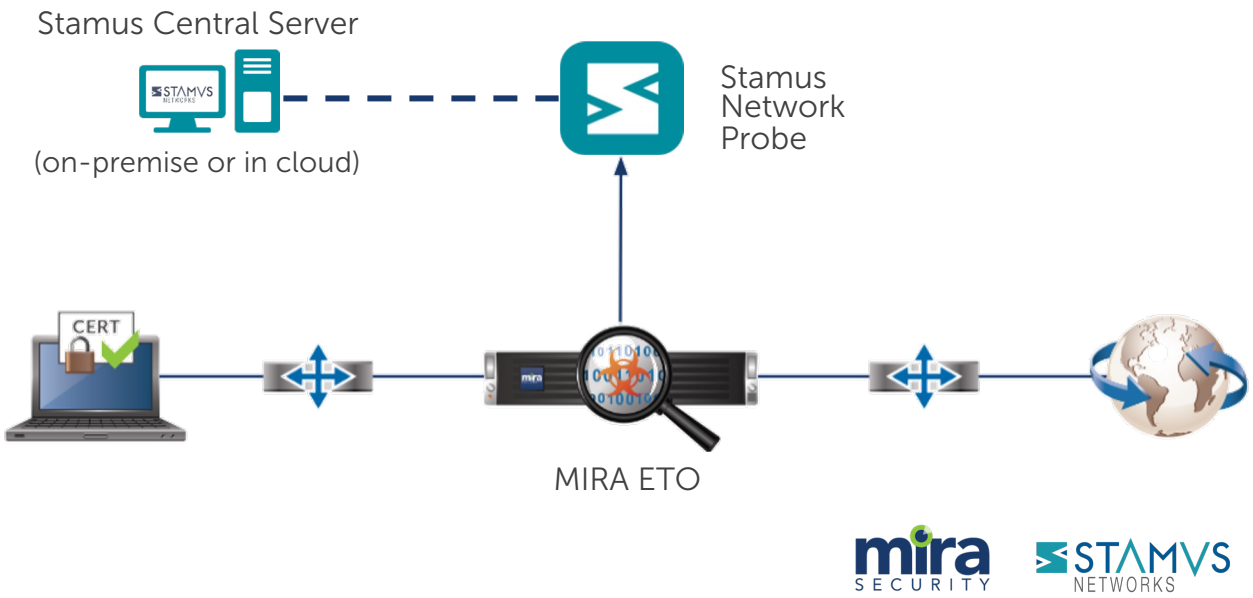
Nearly all network traffic is encrypted today, making the job of security tools significantly more difficult as threats are hidden inside the encrypted traffic flow. While encryption offers enhanced security and privacy to the end user, it raises serious issues for enterprise security teams tasked with protecting the organization and ensuring that relevant legal and regulatory requirements are met. Striking the correct balance between security and privacy in the enterprise is challenging, which – in most cases – requires visibility into at least some portion of the encrypted traffic.

Technical Challenges

Encrypted network traffic is ubiquitous in enterprise networks today, over 90% of north/south traffic is encrypted and over 65% of east/west traffic is typical. While SSL/TLS standards have evolved over the years only TLS 1.2 and TLS 1.3 are recommended today but earlier versions are still encountered in legacy devices. TLS 1.3 differs from TLS 1.2 in many ways that improve the security provided but reduces the visibility for security devices that do not decrypt traffic

MIRA SECURITY AND STAMUS NETWORKS SOLUTION

Mira Security's powerful ETO decrypts all relevant SSL/TLS traffic and sends the decrypted flows to the enterprise network-based threat detection and response from Stamus Networks. Stamus Networks' SSP delivers broad-spectrum threat detection in an open system, providing defenders with response-ready and high-fidelity notifications from machine learning, stateful logic and signatures. The partnership of ETO and SSP offers a complete solution to a historically difficult problem and provides enterprise security teams with unprecedented visibility into threats facing their organization.



In a "network inline - appliance passive" configuration, the ETO sits in the middle of the traffic flow – between the client and the server. When the SSL/TLS handshake occurs, the ETO actively participates in the handshake to insert itself in the TLS flow, it then decrypts the flow and passes the plaintext data over to the Stamus Network Probe for analysis. Then it re-encrypts the data and sends it on to the destination, maintaining the end-to-end connection in an encrypted form.

JOINT SOLUTION BENEFITS

- **Visibility -** The Mira ETO will remove the SSL/TLS blind spots allowing the Stamus Security Platform to analyze traffic that might otherwise be hidden by encryption.
- **Ease of Use -** Both the Mira ETO and the Stamus Security Platform are easy to install, configure and integrate with other elements of your security tech stack.
- **Flexible Rules and Policies -** Use the ETO's Category Database to bypass certain categories of traffic and protect sensitive user data. With SSP, you can leverage integrated detection algorithms, third-party threat intelligence and rulesets; and easily transform a threat hunt into custom detection logic.

JOINT SOLUTION BENEFITS (continued)

- **Connectivity -** The Mira ETO and Stamus Network appliances are available with 1G, 10G, 25G and 40G interfaces.
- **Scalability -** The Mira ETO offers decrypt licenses from 500 Mbps up to 50 Gbps. The Stamus Security Platform offers probe licenses from 100 Mbps up to 40 Gbps line rates.
- **Support for different Platforms -** The Mira ETO and SSP are both available as physical hardware or virtual appliances to fit the needs of various networks.

ABOUT MIRA SECURITY

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 will build lasting relationships with our valued customers and partners to deliver innovative encryption software and products.

Visit MiraSecurity.com to learn more

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

