JOINT SOLUTION BRIEF

Removing the Blind Spot from Encrypted Traffic with AI-Enhanced Protection

mira SECURITY   **DARKTRACE**

Overcoming Security Challenges of Encrypted Traffic

In today's digital landscape, the pervasive use of encryption, while essential for securing data, often creates significant blind spots for security and monitoring tools.

This challenge is compounded by the increasing sophistication of cyber threats that exploit these encrypted channels to evade detection. Consequently, it becomes frustratingly difficult to find effective methods to selectively decrypt potentially malicious traffic while allowing sensitive areas of the network to remain encrypted. The integration between the Darktrace ActiveAI Security Platform and Mira Security's Encrypted Traffic Orchestrator (ETO) addresses these issues by providing high-speed visibility into encrypted traffic without the need for network re-architecting.

Purpose-Built to Deliver Decryption at High Speed

By decrypting traffic once and feeding it to multiple security tools, this integration enhances the speed and effectiveness of existing security measures. Integrated organizations achieve this reliable decryption even inside VLANs or tunnels without terminating. For those worried about TLS, all versions including TLS v1.3 are able to be decrypted.

In a typical feed of Mira ETO to Darktrace, the Mira ETO appliance (virtual or physical) intercepts this encrypted traffic, decrypts it, and then forwards the decrypted data to Darktrace.

Joint Solution Key Benefits

- **No Requirement of Dual Traffic Feeds:** Only one feed of TLS formatted plaintext is required to be sent from Mira to Darktrace, simplifying the processing of traffic.

- **Highly Scalable:** Integrating with Mira allows load balancing across Darktrace and other passive third-party tools.

- **Decrypt Once, Feed to Many:** Ensures decrypted traffic is efficiently distributed to Darktrace and other existing security tools, regardless of whether they are active or passive, thereby optimizing resource usage and enhancing overall security.
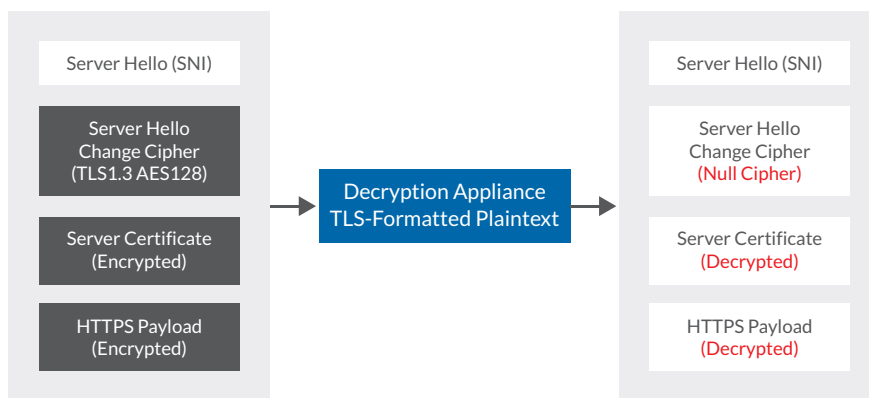
This allows Darktrace to analyze the traffic in its plaintext form, enabling it to effectively detect anomalies that would otherwise be hidden.

By leveraging the integration with Mira ETO, organizations can maintain robust encryption for data security while ensuring that their security tools, like Darktrace, have the visibility needed to effectively monitor and protect their environment. This collaboration not only removes the blind spots, but also optimizes the overall security infrastructure, paving the way for a more secure and effective network environment.

mira SECURITY

MiraSecurity.com   info@mirasecurity.com

Decrypted Traffic

Mira ETO   / Network
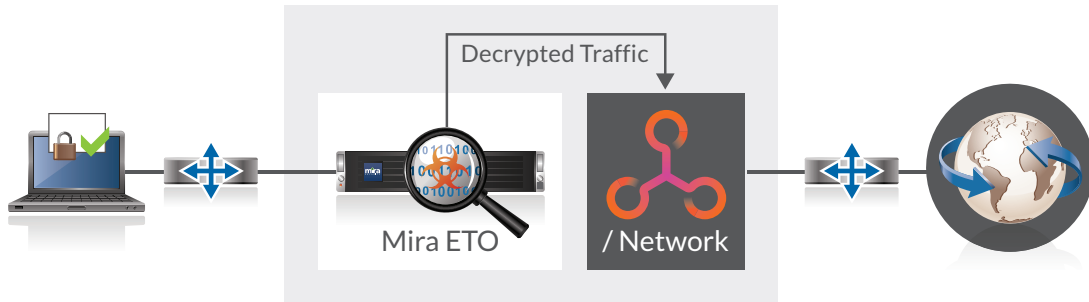
Available Platforms

Like Darktrace, Mira ETO is available in physical hardware or virtual appliance forms, compatible with both private and public cloud settings.

Server Hello (SNI)

Server Hello
Change Cipher
(TLS1.3 AES128)

Server Certificate
(Encrypted)

HTTPS Payload
(Encrypted)

Decryption Appliance
TLS-Formatted Plaintext

Server Hello (SNI)

Server Hello
Change Cipher
(Null Cipher)

Server Certificate
(Decrypted)

HTTPS Payload
(Decrypted)

TSL-formatted Plaintext Benefits:

• Ability to get JA3/JA4 client hash

• Access to TLSv1.3 certificate metadata

• Analysis of TLS behavior within the same feed as decrypted payloads

Use Cases

Selective Decryption
Policy control over which encrypted traffic is made visible allows compliance with industry requirements and enterprise policies on data privacy. Use the Mira ETO's category database to selectively bypass decryption of certain categories of traffic and safeguard sensitive user data.

Public Cloud
Full visibility of all traffic, using gateway load balancers (GWLB) to centrally feed both North-South and East-West traffic into Mira ETO. Minimize upfront investment with the ability to easily and quickly scale up or down to meet demand.

DARKTRACE

About Darktrace
Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally.

To learn more,
visit darktrace.com.

MiraSecurity.com

mira
S E C U R I T Y

info@mirasecurity.com