Detect. Decrypt. Deter.

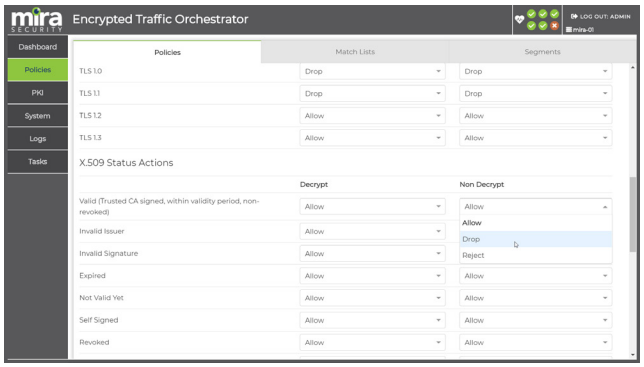
Encrypted Traffic Orchestration

Encrypted traffic has become ubiquitous in networks today, delivering privacy and protecting users' data. However, encrypting data also creates a new set of security issues for enterprises, as existing security mechanisms are "blind" to any threats carried by encrypted connections. The Mira ETO software enables an enterprise to remove this "blind spot" by providing visibility into the unencrypted connection for the full range of security and analytic tools being used.

Encryption Orchestration without Compromise

Mira Encrypted Traffic Orchestration (ETO) software provides safe and secure visibility into encrypted traffic allowing the tools used by enterprise security teams to function effectively, even when all the important traffic is encrypted. Enabling the enterprise security stack to detect and mitigate threats while providing features to enable privacy and ensure compliance requirements can be met is central to Mira ETO software.

- Automatically detect all SSL/TLS and SSH traffic in the network, no matter what ports are being used
- Capable of decrypting SSL v3, TLS 1.0, 1.1, 1.2 and 1.3, as well as SSHv2
- Transparent to the higher-level protocols being carried on top of the encrypted layer providing decrypted flows to security tools for any existing or future protocols
- Seamless integration with existing security tools protects existing security investments
- Policy control over which encrypted traffic is made visible allows compliance with industry requirements and enterprise policies on data privacy



Configure whether to allow or deny traffic based on the SSL/TLS version or certificate status.

- Policy control over which encryption mechanisms are allowed in the enterprise network to prevent weak or obsolete methods from being used
- Comprehensive logging enables the enterprise to analyze encrypted traffic within the network and derive actionable changes to operational policy
- Scaling from a sub 1G for branch offices and micro edge locations to nearly 100G allows for growth and supports the collapsing of data centers.

MiraSecurity.com

mira SECURITY

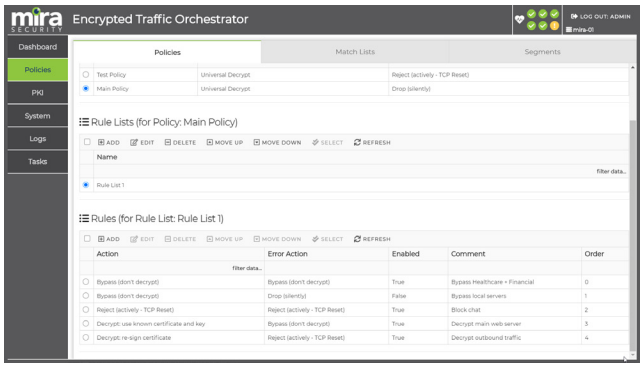
info@mirasecurity.com

Encrypted traffic has become ubiquitous in networks today, delivering privacy and protecting users' data. However, encrypting data also creates a new set of security issues for enterprises, as existing security mechanisms are "blind" to any threats carried by encrypted connections. The Mira ETO software enables an enterprise to remove this "blind spot" by providing visibility into the unencrypted connection for the full range of security and analytic tools being used.

Mira ETO automatically detects SSL, TLS and SSH traffic and can decrypt this traffic in order to send the unencrypted data to one or more security tools. Port numbers are not used during detection of encrypted traffic, so all traffic will be discovered irrespective of the port number being used. Decrypted data is sent to security tools with the same packet header details as the original encrypted flow. Optionally, the decrypted flow can be marked allowing the tool to determine that the flow was originally encrypted.

Flexible policy control features of Mira ETO allow enterprises to enforce policy on what encryption mechanisms are allowed in order to ensure a secure environment. For example, policy can be used to prevent any traffic from using obsolete encryption versions such as SSLv3 or TLS 1.0 and TLS 1.1. For encrypted traffic that is allowed, there are fine-grained policies that allow control over which encrypted flows are decrypted and made visible to security tools. Policy controls can optionally make use of the Mira category database and/or a locally created category database to determine which types of traffic are decrypted. Enterprises need to balance security risks of not decrypting traffic with the privacy implications of doing so, and Mira ETO provides the flexible policy controls to ensure that balance is achieved.

Increasing network traffic is causing a shift from 10 Gbps links to 40 Gbps and 100 Gbps links in enterprise networks with essentially all traffic being encrypted. This means that scalable solutions to provide visibility into traffic are required. Mira ETO software is designed for high-performance decryption and can work with link speeds of 1, 10, 25, 40 and soon 100 Gbps, providing decryption for anywhere from < 1 Gbps of encrypted traffic up to >100 Gbps. In addition to industry-leading decryption capacity, Mira ETO software supports high rates of new TLS handshakes per second, ensuring that there is no performance impact when deployed in an enterprise network. The software is architected to allow the use of external hardware PKI engines if these are available, allowing



Configure whether and how to decrypt traffic using match/action rules.

both decryption performance and new handshake performance to be scaled even higher, if required.

Mira ETO software decrypts traffic and feeds it to one or more security tools that actually detect and mitigate any threats that may be present. No special interfaces or software changes are required to the security tools; they simply receive traffic from Mira ETO as if it was traffic directly from the network. This means the existing security stacks can regain their effectiveness, diminished by the increase in encrypted traffic, simply by deploying Mira ETO to feed them.

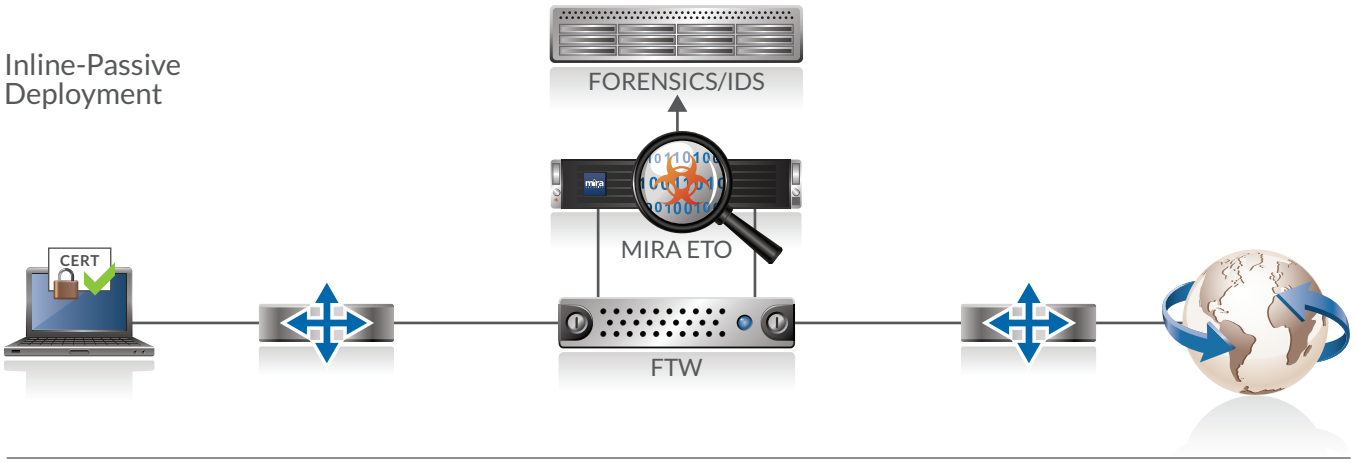
Multiple decryption mechanisms are supported by Mira ETO software and the system allows for the appropriate mechanism to be used on a per-flow basis. The three primary mechanisms are:

- Known server key mode. This can be used for TLS and SSH traffic and requires that the server private key is available to the Mira ETO software. This is used by enterprises to inspect encrypted traffic to servers under their control.
- Certificate re-sign mode. This can be used for TLS traffic and relies on the Mira ETO software acting as a Certificate Authority that enterprise clients trust.
- Self-signed mode. This can be used for TLS traffic to servers that have a self-signed certificate.

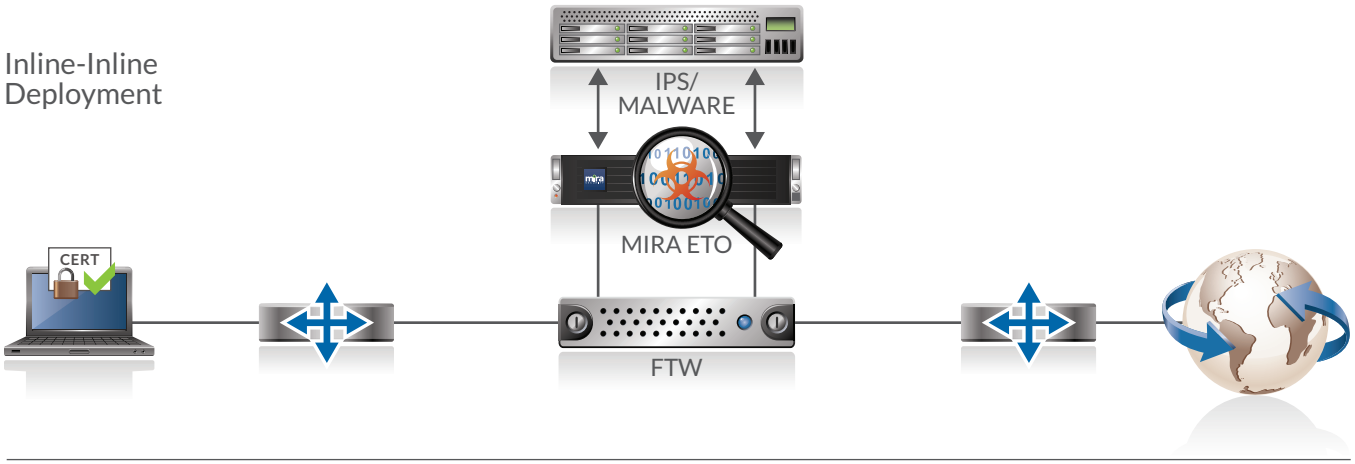
Depending on the decryption mechanisms being used, the Mira ETO software needs to be located either in-line as a "bump in the wire" or attached to a network tap, so that it receives copies of packets. Deployments where Mira ETO is attached to a network tap can only be used to provide visibility into traffic when known server key mode is being used and when the TLS handshake is using RSA key exchange. TLS 1.3 does not support the use of RSA key exchange, so this mode cannot be used for TLS 1.3 traffic. This passive-passive deployment is used by a limited number of enterprises.

Typical Deployment Topologies

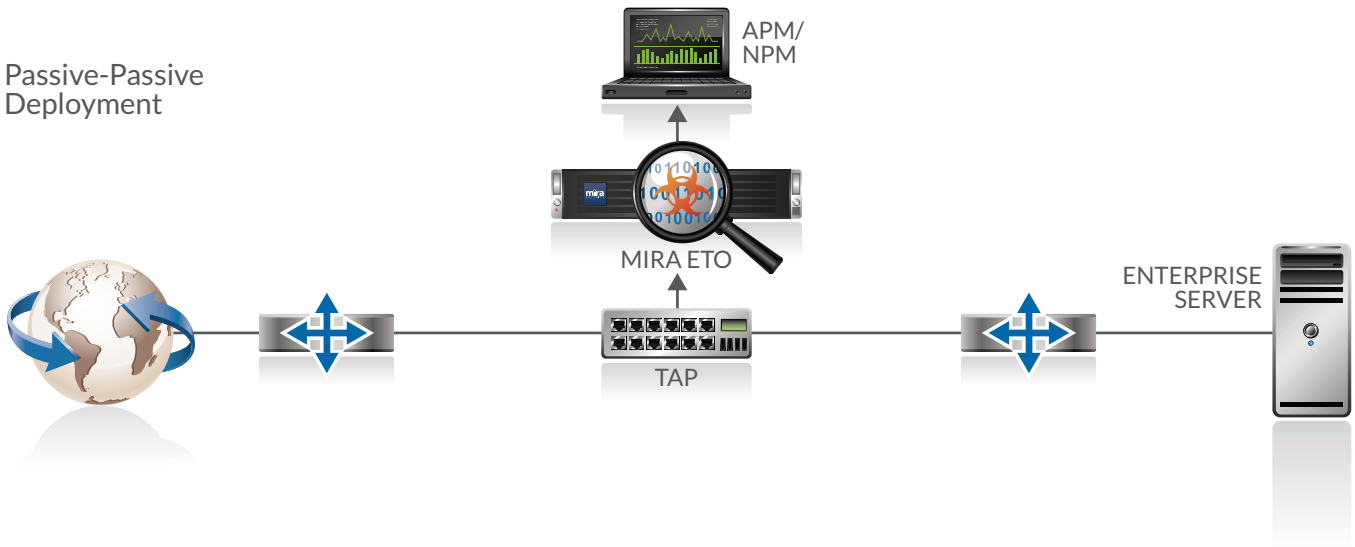
Inline-Passive Deployment



Inline-Inline Deployment



Passive-Passive Deployment



The majority of deployments rely on in-line deployment modes that allow for all decryption mechanisms to be used and TLS 1.3 traffic to be handled.

The Mira ETO software operates transparently at Layer 2, so there is no requirement to assign IP addresses to interfaces and no need to re-engineer the enterprise network addressing. Decrypted traffic sent to attached security tools retains the original packet header information, allowing these to be used as part of the threat detection and mitigation mechanisms used by the tool. Encrypted traffic within tunnels, such as GRE or VXLAN, can be detected and decrypted without requiring the tunnel to be terminated and re-originated.

Mira ETO software is managed by a web user interface and implements role-based access controls (RBAC), allowing enterprises to ensure that network and security team staff have appropriate access. A REST API is supported, allowing programmatic access to all of the features that are accessible via the web UI. Details of encrypted sessions are captured in a session log capable of holding 300M entries. Session log details can be sent to remote syslog servers, allowing analysis and monitoring using existing enterprise tools, such as Splunk. Mira ETO can be used to prevent the use of QUIC, thus forcing the use of TLS.

Software Subscription License

Mira ETO software is licensed as a subscription model. Subscriptions can be for 12 months or 36 months and can be upgraded during the subscription period. The license purchased determines the amount of encrypted traffic that can be decrypted to provide visibility for security tools.

ETO Software Subscription Options for physical appliances

ETO License SKU	ETO-DL-1	ETO-DL-2.5	ETO-DL-5	ETO-DL-10	ETO-DL-15	ETO-DL-20	ETO-DL-30	ETO-DL-40	ETO-DL-50
Licensed Decrypt Gbps	1	2.5	5	10	15	20	30	40	50
Max Full TLS Sessions/s EC256	2,000	5,000	10,000	15,000	17,000	22,000	30,000	40,000	50,000
Max Full TLS Sessions/s RSA 2048	2,000	5,000	7,000	12,000	14,000	18,000	25,000	30,000	35,000

License Compatibility

A license can be used on either a virtual appliance or on one of the hardware appliances available from Mira Security. The following matrix shows which licenses can be used on specific hardware appliance models:

Appliance Model Capabilities

Appliance Model SKU	Interfaces / Speeds	Max Segments	Max SSL Flows/ Segment	Max SSL Flows	Max Session Log Entries	Licensed Capacity Options (Gbps)
HN-3-0610	6 / 1, 10 Gbps	1	4M	4M	300M	1, 2.5, 5, 10, 15
HN-3-1010	10 / 1, 10 Gbps	2	2M	4M	300M	1, 2.5, 5, 10, 15
HN-5-1025	10 / 1, 10, 25 Gbps	2	5M	10M	300M	5, 10, 15, 20,30
HN-7-1240	12 / 40 Gbps or 24 / 10 Gbps (Breakout)	3* (Breakout)	5M	20M	300M	15, 20, 30, 40, 50

** Six (6) breakout segments planned for future software release.*

Physical Appliance Details

Model Family	3xxx	5xxx	7xxx
Dimensions	1U rack mount (WxHxD) 17.25 x 1.72 x 25.58 in. (438.4 x 43.6 x 649.9 mm)	1U rack mount (WxHxD) 17.2 x 1.7 x 29 in. (437 x 43 x 737 mm)	2U rack mount (WxHxD) 17.2 x 3.5 x 28.5 in. (437 x 89 x 723 mm)
Power Supplies	2 x 500W redundant 100V to 240V auto sense 50 to 60 Hz	2 x 1000W redundant 100V to 240V auto sense 50 to 60 Hz	2 x 1600W redundant 100V to 240V auto sense 50 to 60 Hz
Operating Temp.	5° to 35° C (41° to 95° F)	10° to 35° C (50° to 95° F)	10° to 35° C (50° to 95° F)
Non-operating Temp.	-40° to 60° C (-40° to 140° F)	-40° to 70° C (-40° to 158° F)	-40° to 60° C (-40° to 140° F)
Operating Relative Humidity	8% to 90% (non-condensing)	8% to 90% (non-condensing)	8% to 90% (non-condensing)
Non-operating Relative Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)	5% to 95% (non-condensing)
Regulatory Compliance	Electromagnetic Emissions: FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3, CISPR 32 Class A Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe) Other: VCCI-CISPR 32 and AS/NZS CISPR 32 Environmental: Directive 2011/65/EU and Directive 2012/19/EU	Electromagnetic Emissions: FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3, CISPR 32 Class A Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) Other: VCCI-CISPR 32 and AS/NZS CISPR 32 Environmental: Directive 2011/65/EU and Delegated Directive (EU) 2015/863 and Directive 2012/19/EU Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)	Electromagnetic Emissions: FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3, CISPR 22 Class A Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)

MiraSecurity.com

info@mirasecurity.com

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

Email: info@mirasecurity.com
mirasecurity.com

MIRA-SW-V2-06-25