tbl networks
technology. redefined.

ENCRYPTED THREAT ANALYTICS

Encryption Is Changing the Threat Landscape

Encryption technology has enabled much greater privacy and security for enterprises. However, businesses are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to evade detection and to secure their malicious activities.

WHAT IS ENCRYPTED THREAT ANALYTICS

Encrypted Threat Analytics is a network-based security solution designed to detect and analyze encrypted traffic and threats *without using decryption.*

Enhance Visibility
Gain insight into threats in encrypted traffic, without the need for decryption, using network analytics and machine learning.

Shorten Time to Response
Quickly contain infected devices and users, and secure your network.

Promote Compliance
Know what is and is not encrypted on your network. Promote compliance with cryptographic protocols.

Traditional threat inspection with bulk decryption, analysis, and reencryption is impractical because of the tremendous cost and time overhead. Even when inspection is possible, solutions that decrypt network traffic weaken the privacy of the users and do not work for all types of encryption.

Encrypted Threat Analytics help illuminate the dark corners in encrypted traffic without any decryption by using the types of data elements or telemetry that are independent of protocol details.

Threat Vectors Based On Nature of Encrypted Traffic

Uninspected Encrypted Traffic	Threats
Employees' web browsing	• Malware infection • Covert channel with the command and control server • Data exfiltration
Employees' on internal network connecting securely to network edge (DMZ) servers	• Lateral expansion from infected hosts
Internet users connecting to the enterprise's public servers using encrypted protocols	• Reduced defense-in-depth, with only one protection technology inspecting incoming traffic

FEATURES & BENEFITS

Enhanced visibility

Encrypted Threat Analytics use advanced entity modeling and multilayer machine learning, constantly identifying who is on the network and what they are doing, and can detect anomalous behavior in real time to identify threats. It also uses a global threat map to identify and correlate known global threats to the local environment. This considerably improves the fidelity of malware detection in encrypted traffic, and at the same time provides end-to-end confidentiality and maintains channel integrity because there is no decryption.

Cryptographic assessment

Using the collected enhanced telemetry, **Encrypted Threat Analytics** provide the ability to view and search on parameters such as encryption key exchange, encryption algorithm, key length, TLS/SSL version, etc. to help ensure cryptographic compliance.

Faster time to response

Quickly contain infected devices and users by detecting threats within encrypted traffic in real time without relying on slow, decryption-based methods.

Time and cost savings

Use the network as the foundation for the security posture, capitalizing on security investments in the network.