PRESS RELEASE

Stockholm, Sweden
November 30, 2021

Innovations from Enea Deliver Traffic Visibility in Encrypted Networks and Enhanced Protection Against Cyberattacks

Enea today announced enhancements to the Enea Qosmos ixEngine® and Enea Qosmos Probe that contribute to smoother network operations and more effective cybersecurity in encrypted network environments.

Encryption plays a vital role ensuring data security and communications privacy, but encryption also limits the visibility IT professionals rely on to both manage networks and detect cyber threats. The two new features announced today help network solution vendors address the challenges.

The first feature is a machine learning-based module for categorizing encrypted traffic, the Enea Qosmos ML Categorizer, which preserves critical visibility in fully encrypted environments. It uses supervised and unsupervised machine learning to categorize traffic flows into application and service categories (for example, video call, streaming video, audio call, etc.). This ensures that essential networking and security functions can continue to operate.

The second new feature detects potential interceptions of secure communications, or “Man-in-the-Middle” attacks. In a MITM attack, threat actors position themselves between two parties who think they are communicating securely over an encrypted connection. The attacker poses as a legitimate destination for encrypted traffic. The attacker then intercepts the traffic, decrypts it, steals or alters it, and then re-encrypts it and sends it on its way to its intended destination.

MITM are extremely difficult to detect and prevent. They are also on the rise as attackers seek new methods to gain access to data that has become harder to reach because of stronger, more pervasive encryption. Enea’s new MITM threat detection capability helps security solution vendors address this formidable threat while preserving encryption for network protection and privacy.

Eric Parizo, Principal Analyst at Omdia, states “Encrypted traffic poses significant visibility challenges for enterprises, so it is critical for solution vendors to develop supplemental or alternative approaches to reduce encrypted traffic risk and widen encrypted traffic visibility – including without the need for decryption. Enea’s new encrypted traffic visibility and MITM threat indication represent precisely the kinds of innovation that are needed to help solution vendors meet this formidable challenge.”

Jean-Philippe Lion, Senior Vice President of the Enterprise Business Unit at Enea says "Encryption plays a critical role in safeguarding online security, that's why our cybersecurity customers rely on us to deliver smart traffic visibility that enables their solutions to protect against sophisticated attacks while retaining privacy."

Links:

For additional information about visibility into encrypted and evasive traffic, see: https://www.qosmos.com/qosmos-for-cybersecurity-visibility-into-encrypted-and-evasive-traffic/

For information about Enea Qosmos ixEngine, see: https://www.qosmos.com/products/deep-packet-inspection-engine/

Contact

Erik Larsson, Senior Vice President of Marketing and Communication
E-mail: erik.larsson@enea.com

About Enea

Enea is one of the world's leading specialists in software for telecommunications and cybersecurity. The company's cloud-native products are used to enable and protect services for mobile subscribers, enterprise customers, and the Internet of Things. More than 3 billion people rely on Enea technologies in their daily lives.

Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

For more information: www.enea.com