

Stockholm, Sweden
November 13, 2023

Enea Evolves Mobile Network Security Portfolio to Improve Resilience Amid Growing Threats

Enea consolidates its suite of network security solutions to serve the unique needs of Mobile Network Operators and CPaaS providers as the volume of messaging and signaling attacks continues to break records and threaten critical infrastructure.

Enea, a leading provider of telecom and cybersecurity solutions, has consolidated its suite of network security solutions to address the mounting challenges of mobile network security and regulatory compliance and addresses two key areas: signaling security and messaging security. The portfolio update emphasizes intelligence-driven adaptability and accuracy and comprises four solutions tailored to the critical and growing demands of Mobile Network Operators (MNOs) and Communication Platform as a Service (CPaaS) providers and aggregators, and a further solution designed for the unique requirements of national security agencies.

The four network security solutions announced today for mobile network operators, CPaaS providers, and aggregators are as follows:

- **Enea Adaptive Signaling Firewall** accurately detects and blocks malicious signaling traffic to protect against threats such as person location tracking, interception of calls and messages, subscriber privacy intrusions, and DoS attacks on mobile networks. It combines the multi-protocol signaling firewall with unified enhanced reporting and signaling threat intelligence, providing a uniquely comprehensive three-point defense against signaling threats to keep attackers in check.
- **Enea Signaling Intelligence Layer** uses aggregated and obfuscated data from a worldwide footprint of signaling firewalls, combined with qualified threat intelligence, to provide insights on global network traffic. It gives mobile network operators unrivaled, up-to-the-minute visibility of the dynamic threat landscape, which can be used to guard against evolving threats on the network.
- MNOs will also benefit from the **Enea Adaptive Messaging Firewall**, which detects, blocks, and protects from rapidly adapting messaging threats such as phishing and spam and protects against revenue leakage to grey routes. Mobile network operators can filter malicious and unmonetized messages using advanced technologies such as tamper-resistant fingerprinting, intelligent message categorization, and URL classification, backed with up-to-the-minute threat intelligence.

- CPaaS providers and aggregators, who transmit A2P messages from brands to mobile networks, will be able to leverage the **Enea Adaptive Messaging Firewall for CPaaS** to filter messages for compliance and use granular controls to prioritize message delivery and guard against rising threats such as Artificial Inflation of Traffic (AIT), which exploit communication platforms for financial gain, often at the cost of the sending brands.

All three firewall solutions are based on Enea's latest cloud-native platform technology, which enables deployment in public or private cloud, on virtual infrastructure, or on bare-metal servers. Granular control for multi-site deployments improves resilience and manages regulatory compliance for cross-border needs. The platform uses flexible configurations, allowing swift upgrades to counter new threats. Mobile network operators typically require both messaging and signaling firewalls and therefore benefit from a unified platform for both solutions.

To ensure optimal protection, all solutions integrate extensive threat intelligence provided through a combination of Enea's expert security analysts, machine learning, and intelligent algorithms. Both signaling and messaging security rely heavily on the actionable insights threat intelligence provides to keep defense up-to-date and ahead of threat actors, fraudsters, and scammers.

The portfolio announced today ensures the needs of different users are comprehensively addressed and separated into discrete solutions. This approach makes it easier for buyers to assess the values offered by the portfolio and will increase the speed at which Enea can bring important innovations to the market and deliver new value to its customers. This agility is vital in the context of a rapidly evolving threat landscape, when signaling-borne and message-based threats are on the rise. As far as messaging is concerned, phishing remains the number one attack vector globally. A recent [survey](#) based on a poll of 8,000 consumers identified a 70% increase in fraudulent messages. As well as the considerable damage cybercrime causes victims, fraudulent messages also erode trust in brands, negatively impacting revenue and churn, making it a growing concern for CPaaS providers and aggregators.

Signaling threats, often posed by nation-state-sponsored threat actors, have come under increased scrutiny by regulators because of their risk to privacy and national security. In a series of recent research publications, Enea has shown how mobile networks in Ukraine have been attacked through the signaling network with the aim of damaging civil and military defenses.

"As is increasingly recognized by both regulators and leading telcos, cybersecurity operations in the telecom sector needs to be increasingly threat-intelligence driven" said Patrick Donegan, Principal Analyst, HardenStance. "It's good to see a mobile network security leader like Enea leading with this as it refreshes and repositions its portfolio."

John Hughes, senior vice president and head of Enea's network security business, commented, "In a zero-trust world, mobile network operators and communications services providers are under near-constant attack. Faced with the pressure to protect their networks and comply with regulations, Enea's suite of intelligence-driven network security solutions give accurate, granular control, simplify and streamline operations, and can scale easily to match modern-day data usage trends."

The Enea Adaptive network security solutions are today deployed in more than 90 service providers worldwide, securing services for 2.4 billion subscribers. In excess of 3 billion messages are handled by Enea's messaging firewalls every day.

To learn more, please visit:

- www.enea.com/solutions/messaging-security/
- www.enea.com/solutions/signaling-security/

Contact

Stephanie Huf, Chief Marketing Officer
E-mail: stephanie.huf@enea.com

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for fixed and mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day.

Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security.

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

For more information: www.enea.com