ENEA

SOLUTION BRIEF

Qosmos Technology for Visibility into Encrypted & Evasive Traffic

Gain Critical Network Traffic Intelligence while Safeguarding Privacy

Key Benefits

Safeguard Essential Traffic Visibility

You can't manage and protect what you can't see. Enea's Qosmos technology preserves the essential visibility you need for traffic management tasks like dynamic service chaining, policy-based traffic steering, advanced monitoring, load balancing and scaling.

It also uses advanced analytics to help you analyze and respond to potential threats:

- **Virtual Private Networks (VPNs)**
  Accurately identify the use of dozens of VPN applications, including those most commonly deployed for malicious activities.
- **Anonymizers**
  Detect anonymous proxy services that may be cloaking harmful activities, including those using multiple layers of encryption.
- **Complex Tunneling**
  Gain visibility into traffic using complex tunneling, with full protocol paths revealed for up to 16 levels of encapsulation.
- **Covert Communication Channels**
  Detect non-standard tunneling activities over legitimate protocols such as DNS or ICMP, which may indicate unauthorized or illegal activities.
- **Domain Fronting**
  Reveal the use of routing schemes in Content Delivery Networks (CDNs) and other services that mask the intended destination of HTTPS traffic (direct or tunneled).
- **Traffic Spoofing**
  Identify apps (e.g., eProxy, HTTP Injector) that combine techniques (such as protocol header customization, proxies, tunneling & domain fronting) to evade detection.
- **File Spoofing**
  Detect inconsistencies such as a false MIME type or a mismatch between the original hash and computed hash.
- **P2P Misuse**
  Classify P2P traffic to support forensics and behavioral modeling of network traffic.

Writer and humorist Mokokoma Mokhonoana once said: "Time is a double-edged sword: while it might heal all wounds, it also kills all the healed."

Like time, anonymity and privacy technologies are at once a blessing and a curse. They can be used by the well-intentioned to safeguard people, data and systems, or by the unscrupulous to cloak cyber attacks.

Defending against such attacks would no doubt be easier if you had 100% visibility into every bit of traffic flowing across your network. But that isn't going to happen. Nor should it, as a rule. But that doesn't mean you have to fight cyber criminals, or steer network traffic, blindfolded.

Enea's Qosmos ixEngine® delivers vital intelligence about the encrypted traffic flowing across a network, while packet content remains private. You can use this data to:

1) Boost the ability of endpoint and perimeter defense systems to detect and respond appropriately to suspicious traffic.

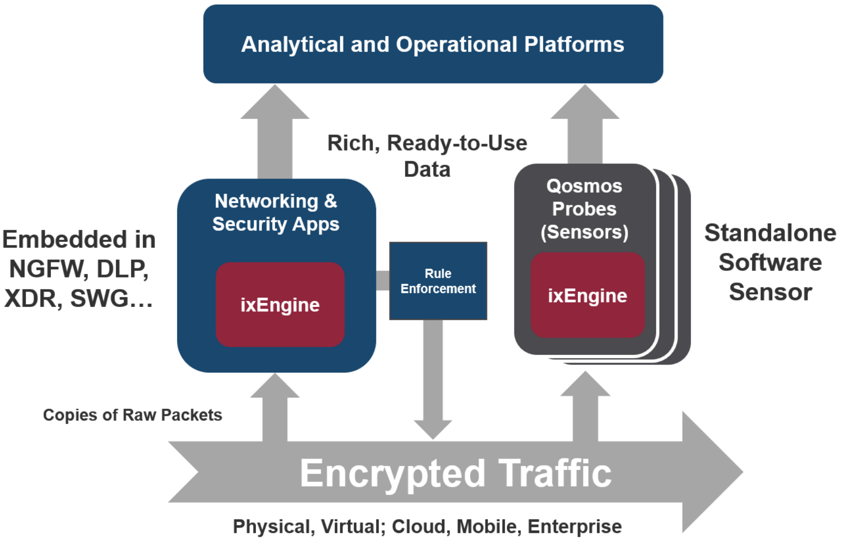
2) Enrich analytics platforms dedicated to detecting and assessing advanced persistent threats that have used evasive techniques to bypass traditional defenses.

3) Enable intelligent, real-time traffic steering and policy enforcement in application-aware environments like SD-WAN and SASE.

And, thanks to Enea Qosmos ixEngine's First Packet Advantage feature, you can accurately classify applications from the first packet in a flow.

For maximum flexibility, the Enea Qosmos ixEngine is available as a Software Development Kit (SDK) in C for embedded use, and as a standalone application for use as a network sensor (the Qosmos Probe). In can also be deployed in physical or virtual environments on-premise or in the cloud.

Enea Qosmos Role in Network Security and Management


Analytical and Operational Platforms
Rich, Ready-to-Use Data
Embedded in NGFW, DLP, XDR, SWG…
Networking & Security Apps
ixEngine
Rule Enforcement
Qosmos Probes (Sensors)
ixEngine
Standalone Software Sensor
Copies of Raw Packets
Encrypted Traffic
Physical, Virtual; Cloud, Mobile, Enterprise

Analytics for Traffic Classification and Anomaly Detection

Below are some of the types of embedded analytics performed to deliver deep, high-quality traffic intelligence. Many of these techniques are combined to produce the most accurate results. A select few are further paired with machine learning to safeguard visibility in environments in which there is a minimal amount of clear data in encrypted flows (for example, where TLS 1.3 and encrypted SSL handshakes are used).

Encrypted Traffic Classification

Techniques for identifying applications and services and generating metadata for encrypted flows include:

Handshake Analysis
Extraction of metadata in handshake messages that precede encrypted packets and which remain clear

Binary Pattern Analysis
Detection & matching of binary patterns against known applications and services

Statistical Analysis
Analysis of packet and flow characteristics using custom models developed by Qosmos R&D

Behavioral Analysis
Analysis of encrypted session behavior versus characteristic protocol behaviors

DNS Cache Analysis with IPDB
First packet analysis via a multi-tier cache and database (IPDB) with 100s of millions of continuously updated, DPI-validated IP address/application matches

Machine Learning
Use of supervised & unsupervised learning to categorize traffic flows in fully encrypted environments

Detection of Suspicious Traffic

Techniques for identifying anomalous traffic (whether encrypted or not) include:

Session Correlation
Regrouping and analysis of flows belonging to the same applications, clients & hosts to detect potentially evasive behavior

Public IP/Port-Based Classification
Identifies anomalies in anticipated behavior for well-known apps/services, FQDNs, ports and publicly routable IP subnets

Deep File Inspection
Packet reassembly, file type detection (280+), MIME type and file extension consistency check, and file hash computation

Cryptocurrency Analysis
Multi-layered analytics to detect and classify cryptocurrencies and mining pools (e.g., Ethereum, Monero, and Ripple)

Man-in-the-Middle Detection
Combines multiple analytic techniques to produce a risk score for MITM attacks

About the Enea Qosmos ixEngine®

The Qosmos ixEngine is the most widely deployed commercial traffic classification engine in cybersecurity, networking and telecommunications. It features the broadest and most accurate protocol and application coverage in the industry. It can be used inline for real-time policy execution, or offline for monitoring and analytics.

Data Quality

The traffic data produced by the Qosmos ixEngine is unmatched for its depth, breadth and accuracy. Qosmos-generated data is:

Accurate
It is based on the most trustworthy source available - telemetry data (not insecure log files), and rigorously validated. It is this reliability that enables Tier 1 vendors to use it with confidence in their planning, decision-making and operations.

Comprehensive
It includes data on *all* network flows provided, and produces highly granular data for these flows. In total, the Qosmos ixEngine provides classification data for 3600+ protocols (including IoT/SCADA & Cloud/SaaS), and delivers 1000s of different types of packet, flow and security metadata.

Relevant
It delivers precise, contextual data via a framework that offers maximum flexibility in selecting the data features most relevant to your analytical or operational needs.

Real-time
It is generated from raw data captured on-the-fly via passive physical or virtual network TAPs that do not affect traffic flow.

Always Up to Date
Updates are continuous and hot-swappable to ensure you will always stay abreast of constantly changing applications and protocols, and benefit from the latest advancements in data classification, especially for encrypted and evasive traffic.

Learn More

For additional information about encrypted and evasive traffic, visit our resource hub at:
https://www.qosmos.com/resources/use-case-hubs/encryption-2/

For detailed product specifications, visit the Products section of our website at: **https://www.qosmos.com/products/**

Find out more!

ENEA

www.enea.com

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. For more information on Enea's Qosmos ixEngine, Qosmos Probe or Qosmos DPI technology: www.qosmos.com.