ENEA

SOLUTION BRIEF

Qosmos for Cybersecurity: Visibility into Encrypted & Evasive Traffic

Gain Critical Network Traffic Intelligence while Safeguarding Privacy

Key Benefits

Shine a Light on Hidden Threats

You can't neutralize what you can't see. Qosmos technology delivers the visibility you need to detect, analyze & respond to threats masked by:

- **Encryption**
  Get maximum visibility into all encrypted traffic to support triage for decryption, advanced analytics for anomaly detection, and forensics.
- **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 blindfolded.

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

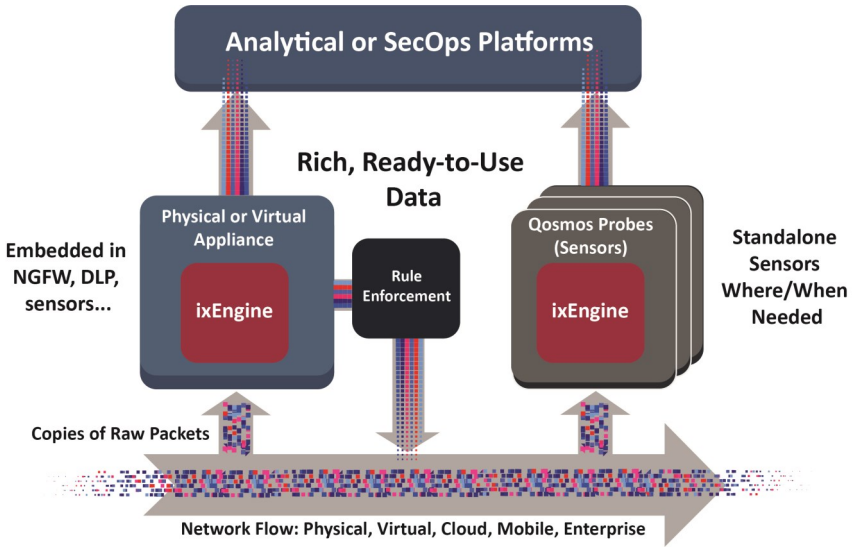
1) Boost the ability of endpoint and perimeter defense systems to detect and respond appropriately to evasive traffic, or

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

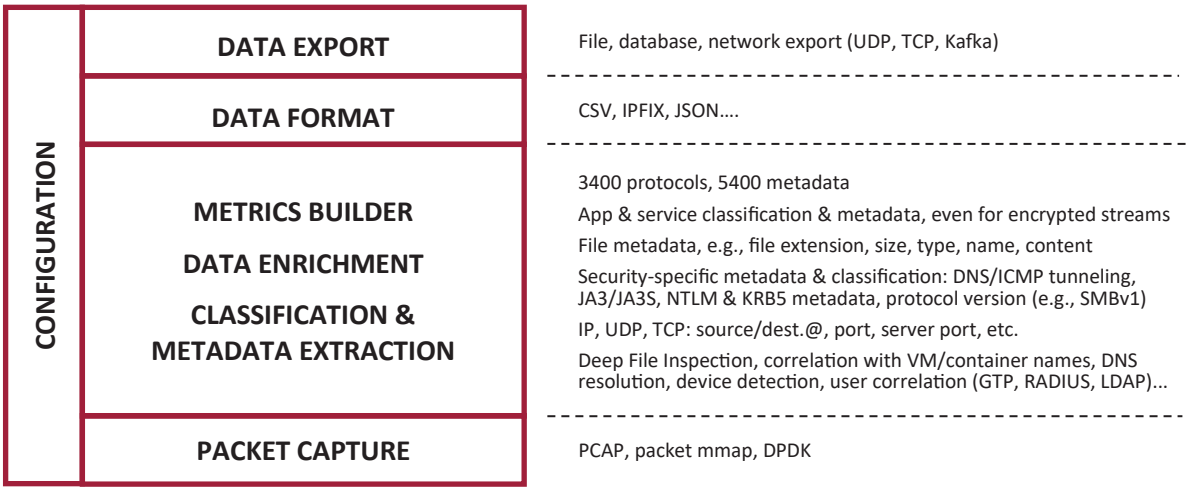
Available as a Software Development Kit (SDK) in C for embedded use, and as a standalone application for use as a network sensor (the Qosmos Probe), the Qosmos ixEngine uses advanced analytics to extract detailed and highly-accurate information on network traffic that is using evasive techniques including:

- Encryption
- VPNs
- Anonymizers
- Tunneling
- Domain fronting
- Traffic spoofing
- File spoofing, and more

Qosmos Role in Cybersecurity



Qosmos ixEngine & Probe Functional Architecture



Classification & Metadata Generation Techniques

Qosmos uses embedded analytics to deliver deep, high-quality traffic data. Below are some of the types of analysis performed, most of which are executed in tandem to produce the most accurate results.

Encrypted Traffic

To maximize visibility into encrypted traffic, Qosmos ixEngine uses techniques including:

- **Handshake Analysis**
  Extract 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**
  Analysis to identify mismatches in what the cache indicates an application should be and what its final resolution reveals

Evasive Traffic

To produce highly-accurate classification and metadata generation for evasive traffic (encrypted or not), Qosmos uses tools including:

- **Session Correlation**
  Regroup and analyze flows belonging to the same applications, clients & hosts to detect potentially evasive behavior
- **Public IP/Port-Based Classification**
  Identify discrepancies between traffic behavior and well-known apps/services, FQDNs, ports & 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)

About the Qosmos ixEngine®

The Qosmos ixEngine is the most widely deployed commercial traffic classification engine in cybersecurity and telecommunications. It features the broadest protocol and application coverage in the industry, and excels at transforming raw packet and flow data into a richly-detailed data stream for operational and analytical security components and platforms.

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 3400 protocols (including IoT/SCADA & cryptocurrencies), and produces 5400 different types of packet and flow metadata—the broadest coverage in the industry
- **Relevant**
  It is precise, contextual data delivered 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 a world-leading supplier of innovative software components for telecommunications and cybersecurity. Focus areas are cloud-native, 5G-ready products for mobile core, network virtualization, and traffic intelligence. 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