ENEA

Solution Brief

Suricata + Enea Traffic Intelligence

Improve Suricata's Ability to Detect Threats in Evolving Networks

Suricata is the most widely deployed Intrusion Detection and Prevention System (IDS/IPS) in cybersecurity. Enea Qosmos ixEngine® *is the most widely deployed carrier-grade L2-L7 traffic classification and deep packet inspection (DPI) engine in the networking, telecom and cybersecurity industries. Integrating these two best-of-breed technologies allows you to better adapt Suricata rules to new environments (like multi-cloud networks and hybrid IT/IoT networks), to develop white- and blacklists with the applications most pertinent to your network (including custom and legacy applications), to more effectively identify anomalous and evasive traffic (even in encrypted traffic), and to speed threat analysis and forensics with meaningful contextual data.*

Boost Suricata Threat Detection Capabilities with Enea Qosmos Technology

Suricata is the most trusted IDS/IPS available today, and serves as a cornerstone technology in many leading commercial cybersecurity solutions. The Enea Qosmos ixEngine leads the market for DPI and related traffic intelligence software, with coverage for more than 3600 protocols and applications, and the ability to generate thousands of types of security and networking metadata, including threat indicators for encrypted and evasive traffic.

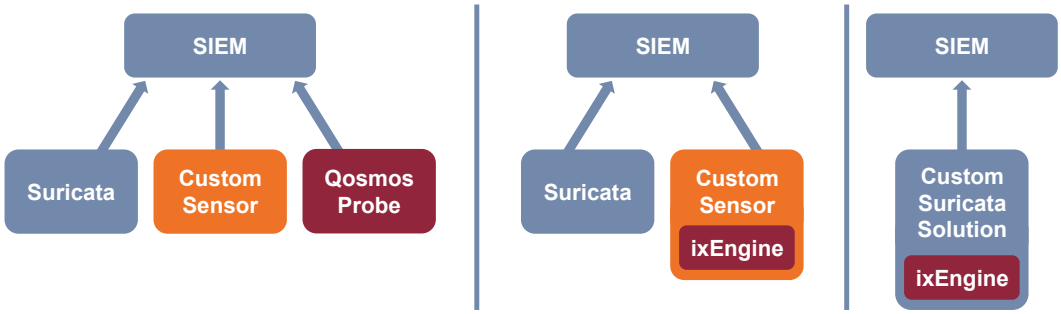
When Qosmos ixEngine is integrated with Suricata, it extends and enhances Suricata's general threat detection capabilities, and enables Suricata rules to be tailored more effectively to unique network environments. This combined value is used to enhance a wide variety of security products, including Cloud Firewalls (FWaaS), Secure Web Gateways (SWG), Next Generation Firewalls (NGFW), Network Detection and Response (NDR) and Extended Threat Detection and Response (XDR) platforms.

In these products, Qosmos ixEngine enhances Suricata by:

- Enabling rapid development of whitelists and blacklists that leverage Qosmos ixEngine's expanded protocol coverage (particularly for Cloud, SaaS, IoT and OT applications and protocols plus custom and legacy applications)
- Significantly improving Suricata's ability to detect anomalous and evasive traffic
- Safeguarding the visibility Suricata requires even in fully encrypted environments
- Making threat analysis and forensics faster and easier through high-value contextual metadata (while simultaneously reducing the need for full packet capture)

Integration Options

Integration options are flexible, supporting active use cases like firewalling, or passive use cases like threat hunting and forensics, in both virtual and physical environments. Qosmos ixEngine is available in two form factors: an SDK in C or embedded in a standalone software sensor (Qosmos Probe). VNF and CNF form factors are available as well, as is a physical appliance option for the Qosmos Probe.



Qosmos Probe deployed alongside Suricata, or Suricata plus a custom sensor (probe)

Qosmos ixEngine embedded in a custom sensor (probe) or a custom Suricata instance

Rapidly Produce White- and Blacklists that Are Right for Your Network

Suricata's protocol coverage is well-suited to traditional IP networks, but there are some protocol visibility gaps in important application categories like Cloud and SaaS, instant messaging, business collaboration, and Internet of Things communications.

With signatures covering over 3600 protocols and applications, integrating Enea Qosmos technology with Suricata enables you to fill these gaps. As a result, you can improve security and your user experience by rapidly generating whitelists and blacklists that are right for your network.

Extend Suricata Coverage to 3600+ Protocols and Applications

- **Cloud and SaaS Applications**
  Amazon AWS, MS Azure, Google App Engine, Okta, Atlassian, Salesforce, Zendesk, Tencent Meeting, Skype, Dropbox, HubSpot, etc.
- **ICS/SCADA & IoT Protocols**
  Modbus, DNP3, ENIP, GOOSE, OPC, S7 Communication, MQTT, PCCC, HDLC over IP, Proficy, Moxa, iWareHouse, BR Automation, Alexa, etc.
- **Communication and Collaboration Applications**
  WhatsApp, Douyin, WeChat, DingTalk, MS Stream, Mango TV, Youtube TV, Tencent Video, Kuaishou, Philo, etc.
- **Business and Productivity Applications**
  MS Teams, Slack, Yammer, Sharepoint, Adobe Connect, Ctrip, Fliggy, Office 365 (categorized from the first packet), etc.

Create Custom Signatures for Your Proprietary or Legacy Applications

The latest ready-to-use commercial and open source software meets most – but not all – business needs. Nearly every organization has unique requirements they feel are best met using custom or legacy applications: a cloud service provider using proprietary applications to automate network operations, a government agency using custom applications for security reasons and legacy applications for budgetary reasons, an industrial network relying on long-proven, proprietary machine-to-machine protocols... Whatever type of proprietary or legacy applications you may use, you can use the Enea Qosmos Custom Signature Module (CSM) to automatically generate signatures for these applications, which can then be used to enrich the application logs and policy capabilities.

Identify Suspicious Traffic Based on What is Not Normal for Your Network

This expanded protocol coverage is just one of the ways Enea Qosmos technology can improve Suricata performance. Another critical advantage is boosting the behavioral anomaly detection capabilities of Suricata.

Suricata is primarily known for defending networks against known threats, but it can also detect some anomalies in traffic behavior that could indicate the presence of an unknown theat. For example, Suricata can recognize if there is a mismatch between a port being used by one of the protocols it recognizes and the port normally assigned to that protocol (for instance, HTTP traffic not

using TCP port 80 or 8080 as expected), or Suricata may detect if a flow doesn't match the physical characteristics typical for a given protocol (e.g., deviations in the number or size of the packets).

But, because Suricata is based on common rules, it can't learn what is normal or abnormal for an individual network. This is where Qosmos ixEngine provides value. It can be used to create a profile of what is normal for *your* network, including protocols, applications, services, connected devices, users, transaction types, files, connection patterns, and much more.

Armed with this information, you can tailor Suricata rules to more effectively detect deviations which may indicate a hidden threat. This baselining also reduces false positive alerts on behavior that Suricata would otherwise see as 'abnormal' even though it is normal for your particular network.

Example

Detecting Command & Control (C2C) Attacks Hiding Behind Common Protocols

To remain under the radar of IDS/IPS systems like Suricata, some C2C attacks encapsulate commands inside common protocols communicating via standard assigned ports. This way, they blend in with normal traffic.

This is one of the tactics identified in the MITRE ATT&CK framework of known adversary techniques (Technique ID T1071, Application Layer Protocol). The framework suggests several means of detecting such a covert C2C attack. In each instance, Suricata complemented by Qosmos ixEngine is far more effective at detecting this type of attack.

MITRE T1071: Indicators of Potential Malware	**Suricata** Anomaly Detection Capability	**Qosmos ixEngine** Anomaly Detection Capability
Uncommon data flow	**Medium** Mainly detects uncommon flows based on packets, count, size, TCP flags (L2/L4 rules). Generic rules generating lots of false positives.	**High** Detects uncommon flows at L7 level (Domain Fronting, Anonymizer…). Reduces false positives by being more permissive on well-known application.
Previously unseen communication type	**Very Low** IDS are rule-based and do not learn from past data.	**High** Fine grained classification and Custom Signatures enable complete baselining of a network to alert on any new connection type. Low false positive ratio.
Protocol misusage	**Medium** Good coverage for standard protocols (HTTP, FTP…) but limited criteria for misuse.	**High** Detects misuse on top of standard protocols (tunneling, evasive traffic), e.g., non-standard or complex tunneling activities over legitimate protocols such as DNS or ICMP.

Expand Detection of Evasive Traffic

As noted, in addition to scanning for known threats via signatures, Suricata can perform some protocol anomaly detection on the traffic it inspects. By integrating Qosmos ixEngine with Suricata, this anomaly detection capability can be greatly expanded. Qosmos ixEngine can identify a wide variety of evasive techniques used by attackers, producing threat intelligence that can be used to develop or adapt Suricata rules to boost security.

Examples

Anomalous and Evasive Traffic Identified by Qosmos ixEngine

- **Complex Tunneling**
  Provides visibility into traffic that is using complex tunneling (i.e., multi-layer wrapping a packet inside another packet). Qosmos ixEngine can reveal the full protocol paths for such traffic up to 16 levels of encapsulation.
- **Virtual Private Networks (VPNs)**
  Accurately identifies dozens of VPN applications, including those most commonly deployed for malicious activities.
- **Anonymizers**
  Detects anonymous proxy services that may be cloaking harmful activities, including those using multiple layers of encryption.
- **Covert Communication Channels**
  Detects non-standard tunneling activities over legitimate protocols (such as DNS or ICMP), which may indicate unauthorized or illegal activities.
- **Domain Fronting**
  Reveals 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**
  Identifies applications (e.g., eProxy, HTTP Injector) that combine techniques such as protocol header customization, proxies, tunneling and domain fronting to evade detection.
- **File Spoofing**
  Detects inconsistencies such as a false file type (MIME type) or a mismatch between the original hash and computed hash.
- **P2P Misuse**
  Classifies P2P traffic to support forensics and behavioral modeling of network traffic.
- **Man-in-the-Middle Detection**
  Provides a metric measuring the likelihood of a TLS session being intercepted. This score can be used to develop security rules for addressing MITM risks.
- **…And Much More**
  Generation of metadata related to JA3/JA3S, NTLM and KRB5; identification of cryptocurrencies and mining pools; extraction of embedded links in emails for security analytics; session correlation; deep file inspection, etc.

Maintain Visibility in Encrypted Environments

Suricata cannot provide intrusion detection on encrypted traffic; traffic must be decrypted first. This presents a challenge as the use of encryption expands and encryption standards become more rigorous. When decryption is either undesirable or impossible, Qosmos ixEngine can still provide Suricata with vital protocol visibility and valuable security metadata.

Qosmos ixEngine can identify many types of encrypted traffic using the standard First Packet Advantage (FPA) feature, which enables customers to accurately identify applications and services – and even generate security metadata – from the first packet in a flow.
While first packet classification is widely used to accelerate and optimize traffic management, conventional first packet processing tends to produce a high volume of false positives in application identification, which is a real problem for IDS/IPS.

FPA addresses this challenge through an innovative cascading cache that includes Enea's unique Internet Protocol Database (IPDB). IPDB draws upon a reservoir of hundreds of millions of rigorously and continuously verified IP address and application matches to boost classification coverage and accuracy.

> "Many conventional traffic classification engines score poorly in accuracy, granularity, and performance. A solution like Enea's First Packet Advantage, that operates with high accuracy in first packet mode, brings improved protection and performance to vendors and end-customers."
>
> **Roy Chua, Founder & Principal**
> **AvidThink**

In circumstances in which an accurate classification is not possible based on the first packet alone, Qosmos ixEngine applies multi-packet encrypted traffic classification (ETC) methods.

Enea Qosmos Encrypted Traffic Classification Techniques

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

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

Behavioral Analysis
Analysis of encrypted session behavior versus characteristic protocol behaviors

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

Machine Learning- Based Traffic Categorization
In fully encrypted environments, data that was previously clear is no longer visible, e.g. TLS Encrypted Client Hello (ECH), Encrypted Server Name Indication (eSNI), and DNS-over-HTTPS (DoH). Qosmos ixEngine uses machine learning to preserve essential visibility through traffic categorization.

Improve Threat Analysis with Contextual Data

In addition to identifying applications, protocols and services active on a network, Qosmos ixEngine delivers deep network-based intelligence in the form of metadata. This metadata provides important contextual information that makes alert analysis easier, helps detect weak signal threats, and aids in adapting Suricata alerts and rules for a particular network.

Qosmos ixEngine can extract thousands of content-based metadata and produce multiple network metrics in different categories: traffic volume, network KPIs, services and application usage, user identity, content, files, transactions, TLS/certificate decoding, DNS decoding and connected devices.

In addition, Qosmos ixEngine uses the same open standard for identifying flows as Suricata (Community ID). This makes it easy to correlate flow-level data produced by Qosmos ixEngine with data from Suricata and other network monitoring applications.

What's more, this deep contextual metadata is often all that is needed for threat hunting, alert analysis and forensics, reducing the need for expensive full packet capture technology (using Enea Qosmos metadata instead of full packet capture enables a 150x reduction in data storage requirements).

Examples of Metadata Produced by Qosmos ixEngine

- **Volume:** e.g., the volume of traffic per application and per user
- **Service identification**: e.g., service classification for VoIP and IM protocols and applications, even in encrypted streams
- **Application usage**: e.g., SMB:version, user_agent length (for entropy), file hash
- **Identifiers**: e.g., email sender / receiver addresses or any other ID that can be used to implement strong security rules
- **Content**: e.g., link detection and extraction in email; attached files in email, which can be directed to specific processing like 3rd party anti-virus or content inspection
- **File metadata**: such as file extension, size, type, name, content, etc., which can be very helpful for use cases such as DLP or advanced malware detection
- **Security-related classification & metadata**: e.g., tunneling on protocols such as DNS or ICMP, NTLM & KRB5-related metadata, JA3/JA3S hash to fingerprint TLS connections, protocol version (e.g., SMBv1), MiTM likelihood score, etc.
- **Transactions:** e.g., logins, file uploads, file downloads, file shares, etc. (available for decrypted traffic)
- **Connected Devices:** device type, manufacturer and model, OS name and version for 50K+ types of consumer, enterprise, and industrial devices
  (100% passive, agentless solution for access networks).

Conclusion

As an advanced, DPI-based classification and metadata engine specifically developed for integration into third-party applications, Qosmos ixEngine is the number one choice for cybersecurity vendors and operators of critical networks looking to extend and adapt their Suricata IDS/IPS to new network environments and an evolving threat landscape.

Integrating Enea Qosmos DPI-based traffic classification and metadata extraction technology with Suricata improves its general threat detection capabilities, and enables it to be more effectively tailored to specific network environments.

Benefits of Suricata + Enea Qosmos Traffic Intelligence

- Extends protocol signature coverage
- Provides deep contextual traffic insights
- Improves threat detection
- Reduces false positives
- Speeds investigations

Additional Product Details

Probe Data Integration

For data integration, the Qosmos Probe natively supports JSON, CSV or IPFIX. Field names can easily be aliased to match Suricata field names or existing data sets. (An optional Custom Python Module is also available to allow users to customize data output to specialized needs with full autonomy.) Qosmos Probe management is provided with a REST API. Management is centralized to allow management of clusters of sensors from a single entry point.

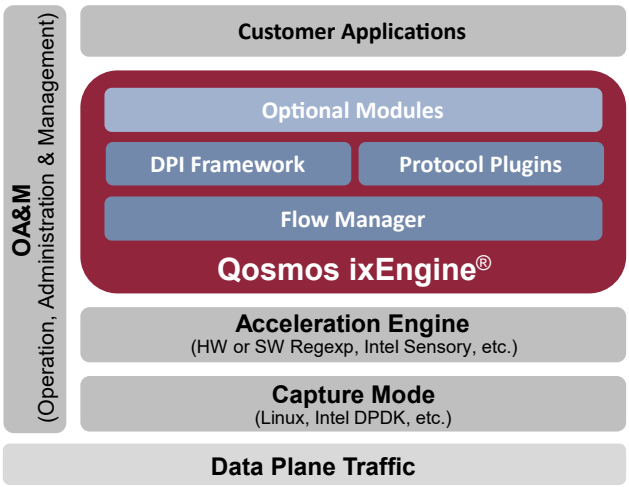
Performance

Qosmos ixEngine has built-in multi-core support capabilities. The software typically handles up to 10 Gbps of traffic per core on Intel architecture. The Qosmos Probe typically requires 1 core to handle 1 Gbps of traffic and requires between 2 and 4 GB of RAM, so a 10G FD link can easily be addressed on a VM with technologies like Intel DPDK for packet acquisition and dispatching. For 40G or above, dedicated hardware is required, and above 40G, smart network adapters (FPGA-based for instance) might be used to ensure no packet loss. But in this case, considering how processing power is constantly improving, a cost-effective solution can always be found.

Signature Updates

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 About Qosmos ixEngine



For more information about Qosmos ixEngine, please visit the Qosmos ixEngine webpage: https://www.qosmos.com/products/deep-packet-inspection-engine/

For more information about the Qosmos Probe, please visit the Qosmos Probe webpage: https://www.qosmos.com/products/probe-solution/

For more information about the protocols recognized by Enea Qosmos technology, explore the Qosmos Labs Protobook: https://protobook.qosmos.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.

For more information: www.enea.com

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

ENEA

Division Head Office
6 rue Casteres
92110 Clichy, France

www.enea.com