ENEA

DATASHEET

Qosmos ixEngine®

Next-Generation Deep Packet Inspection (DPI) for Maximum Traffic Visibility

More than 70% of telecommunications, networking & security vendors who source DPI software have selected Qosmos ixEngine to embed Layer 2 to Layer 7 flow classification & metadata extraction into their products.

Key Facts

- C libraries designed to be embedded into applications
- 3600+ protocol plugins (including Cloud/SaaS, IoT/SCADA & cryptocurrencies), continuously updated and expanded
- 1000s of types of metadata extracted
- Classification based on flow pattern matching, flow prediction, flow correlation, behavioral and statistical analysis, machine learning and more
- High recognition rate: ability to identify Layers 2 to 7 in the OSI model
- Companion libraries and additional features beyond standard DPI
  - Deep File Inspection Library
  - Rule Engine SDK
  - GTP Library
  - Custom Signature Module
  - Encrypted & evasive traffic classification
  - Security-related metadata (e.g., Man-in-the-Middle risk score)
  - Device classification
  - ML-based traffic categorizer
  - First Packet Advantage (unique 1st packet processing capability)
  - Quick DPI
  - Transactional DPI
  - Automated DPI
- Frequent protocol plugin releases that support In-Service Software Upgrade (aka, hot swapping)
- Multiple-instance support
- Modular architecture for flexibility (separate flow management, DPI framework, protocol plugins and optional modules)
- Up to 10 Gbps* per core on latest x86 architecture

**Performance may vary significantly with traffic patterns and networking environment. Please contact your local representative to get details of each scenario.*

Qosmos ixEngine is a DPI library for software developers who wish to embed detailed, real-time visibility into their networking or security products.

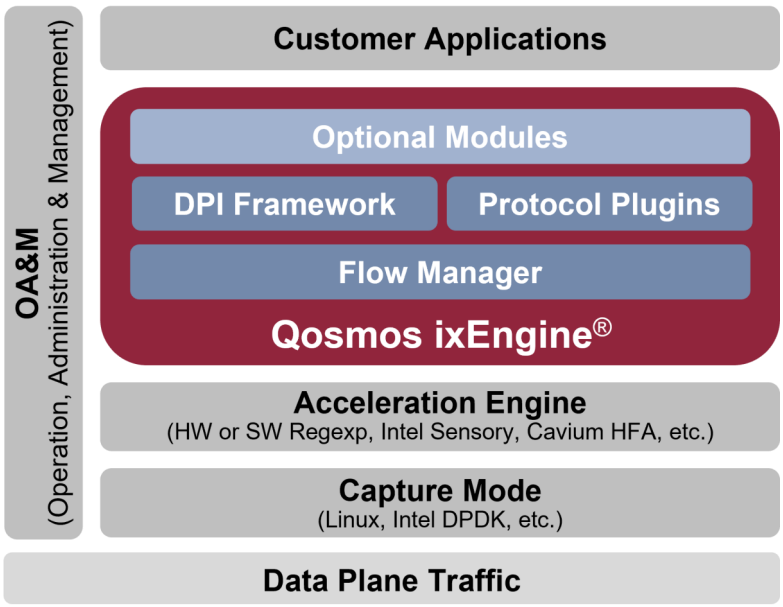
While some technologies are limited to identifying the application behind an IP flow, Qosmos ixEngine goes further to also extract deep, high-fidelity protocol and application metadata.

This enables developers to inject application-level insight into their solutions for complete, real-time visibility into network traffic (including encrypted and evasive traffic), and gain a detailed understanding of network transactions and user behavior.

A series of optional modules are also available to shorten development cycles. These modules, such as the Deep File Inspection function, use the output data from classification and metadata extraction and apply further processing that would otherwise have to be built within the final application.

Designed with developers in mind, Qosmos ixEngine accelerates product development cycles. Ready-to-use software libraries and modules reduce costs and risks associated with developing and maintaining a highly complex technology internally.

Beyond IP Traffic Classification: Metadata Extraction



Qosmos ixEngine® extracts **8 main categories** of network-based application metadata and computed metadata:

- **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
- **Application performance:** such as computed metadata like VoIP MOS and RFactor
- **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 file within an 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 useful for DLP and malware detection
- **Security-related metadata:** e.g., tunneling on DNS or ICMP; JA3/JA3S; NTLM and KRB5-related metadata, MITM indicator…

Up-to-date Protocol Plugins and Metadata

Applications and their protocols change constantly and without notice. Qosmos ixEngine provides the most secure path to reliable, always up-to-date DPI technology. Experts at Qosmos Labs continuously receive information about changes in protocols and applications and update the plugins accordingly. Updates are deployable on-the-fly, without service interruption.

Extensions for Aggregated and Computed Metadata

Qosmos ixEngine features numerous extensions that facilitate operations through metadata extraction, for example, correlating flows for inheritance (signaling and user plane consolidation), and computing KPIs (e.g., MOS for VoIP flows).

Companion Libraries and Additional Features

- **Encrypted & Evasive Traffic Classification** to maintain essential visibility and detect potential threats without using decryption
- **First Packet Advantage** to enable outstanding performance by accurately classifying all traffic from the first packet
- **Machine Learning Categorizer** to boost first packet classification accuracy and preserve visibility in fully encrypted environments by categorizing flows by service type (e.g., streaming video, audio call)
- **MITM Risk Indicator** to detect and quantify the risk that a TLS Proxy, possibly illegitimate, is being used to intercept secure communications
- **Custom Signature Module** to complement Qosmos signatures with user-defined signatures for proprietary protocols or extensions
- **Deep File Inspection** for detecting file types, checking consistency between MIME types and file extensions, computing file hashes and extracting metadata
- **Rule Engine** for the execution of customer-defined rules at run-time (correlations, aggregations, etc.)
- **Transactional DPI** to obtain user transactions within specific applications as metadata (e.g., picture download on Facebook)
- **Automated DPI** to classify previously unknown traffic using automated algorithms
- **Device Classification** to close device visibility gaps in access networks and enable innovation through device awareness

High-Performance & Throughput

Qosmos ixEngine has built-in multi-core support capabilities. The software typically handles up to 10 Gbps* of traffic per core on Intel architecture.

- Optimized multi-thread support for scalability up to 96 cores
- High performance under heavy metadata extraction loads
- Optimized code for the industry's highest performance multicore processors
- Support for VPP and hardware acceleration

Architecture & Integration Scheme

Qosmos ixEngine provides the easiest path to L2-L7 flow analysis for embedded software developers. Qosmos ixEngine's ready-to-use libraries reduce development cycles, costs and risks, and let developers focus on building complete solutions, relying on the Qosmos division of Enea for its domain expertise in protocols, applications and metadata extraction:

- **Optimized integration** with packet processing middleware (e.g., Intel DPDK)
- **Acceleration and offloading** configuration options for optimal integration with custom flow manager
- **Independent core-decoding framework** and protocol plugin library, which translates into fast flow signature updates while preserving engine stability. Protocol plugins are hot-swappable.
- **Switchable IP defragmentation and TCP flow reassembly** process for packet reordering
- **First Packet Processing** option (First Packet Advantage) to enable optimal traffic steering in use cases such as SD-WAN and SASE
- **Optional packet pre-filtering:** depending on application requirements, all packets or only a subset of packets are parsed by the Qosmos ixEngine
- **A unique and highly configurable flow manager architecture** which handles standard, tunneled and multiplexed flows while allowing different memory allocation modes with maximum flexibility
- **Supports multiple instances of Qosmos ixEngine** for maximum implementation flexibility

To accelerate integration and ensure that you leverage all the capabilities of our technology, Enea offers professional services and provides access to a network of expert developers.

Supported OS and Chipset

- Intel x86 (Linux, Solaris, FreeBSD, MacOS, Windows)
- Cavium Octeon (SE, Linux)
- Broadcom XLP (Linux)
- PowerPC (Linux)
- Tilera Gx (Linux)
- ARM (Linux)

Learn More

Discover the full list of protocols recognized by Qosmos technology at **https://protobook.qosmos.com**, or request a free product evaluation at **www.qosmos.com/about-us/contact-us/**

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 connected devices. More than 4.5 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 on Enea's Qosmos ixEngine, Qosmos Probe or Qosmos DPI technology: www.enea.com/qosmos

www.enea.com

Enea®, Qosmos® and Qosmos ixEngine® are registered trademarks of Enea AB and its subsidiaries. All other company, product or service names mentioned above are the registered or unregistered trademarks of their respective owners. All rights reserved. © Enea AB 2022.