

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
- ▶ 3400 protocol plugins (including IoT/SCADA & cryptocurrencies), continuously supported and updated
- ▶ 5400 application metadata extracted
- ▶ Classification of protocols and applications based on flow pattern matching, flow prediction, bi-directional flow correlation, behavioral analytics, statistical analysis and more
- ▶ High recognition rate: ability to identify Layers 2 to 7 in the OSI model
- ▶ Companion libraries for further analysis and easier integration
 - Deep File Inspection Library
 - Rule Engine SDK
 - GTP Library
- ▶ Additional features beyond standard DPI
 - Encrypted & evasive traffic classification
 - First packet classification
 - Custom Signature
 - Quick DPI
 - Transactional DPI
 - Automated DPI
- ▶ Frequent protocol plugin releases that support In-Service Software Upgrade (aka, hot swapping), to keep up with the fast changing nature of IP traffic
- ▶ Supports multiple instances of DPI engine
- ▶ Modular architecture for flexibility (separate flow management, DPI framework, protocol plugins and optional modules)
- ▶ Up to 10 Gbps* per core on latest x86 architecture

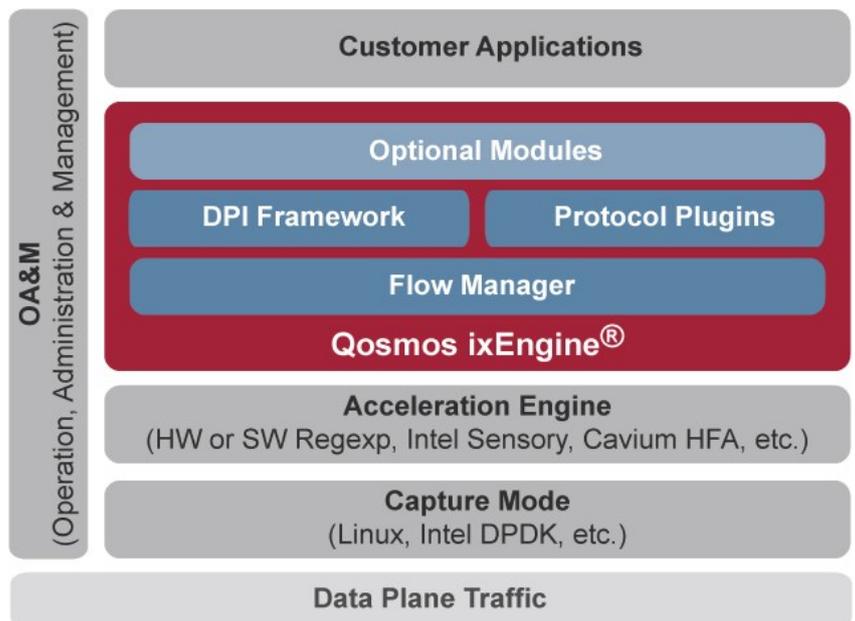
Qosmos ixEngine is a DPI library for software developers who wish to embed detailed, real-time visibility into their networking or security products.

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 a Rule Engine or a 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.



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

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 helpful for use cases such as DLP or advanced malware detection
- ▶ **Security-related metadata:** e.g., tunneling on protocols such as DNS or ICMP; JA3/JA3S; NTLM and KRBS-related metadata

Up-to-date Protocol Plugins and Metadata

Applications and their protocols change constantly and without notice. Qosmos ixEngine provides the more 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 a number of extensions designed to facilitate operations through extraction of application metadata. The extensions can correlate flows for inheritance (signaling and user plane consolidation), and compute KPIs (e.g., MOS for VoIP flows).

Companion Libraries and Additional Features

These libraries and special features provide additional processing of classification data and metadata to better suit some use cases:

- ▶ **Custom Signature Module** to complement Qosmos signatures with user-defined signatures for proprietary protocols or extensions
- ▶ **Deep File Inspection** for detection of file type, consistency check between MIME type and file extension, file hash computation, and extraction of metadata
- ▶ **Rule Engine** for the execution of customer-defined rules at runtime (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
- ▶ **Encrypted & Evasive Traffic Classification** to keep up with the rise of encryption over public and private networks as well as identify abnormal or illegal use of traffic cloaking applications

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
- ▶ Leveraging of 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 to enable optimal traffic steering in use cases such as SD-WAN
- ▶ **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)
- ▶ Tiler 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 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 around the globe 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

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 2020.