ENEA

DATASHEET

# Qosmos Probe

## A Network Traffic Sensor with Next-Generation Deep Packet Inspection (DPI)

A unique sensor that combines the power of the Qosmos ixEngine® with the agility of a software agent to bring full traffic visibility to today's complex and highly dynamic networks

### Key Facts

**Proven Technology**

- Standalone version of Qosmos ixEngine® , the next-generation DPI software trusted by more than 70% of telecommunications, networking & security vendors who embed commercial-grade traffic classification

**Best-in-Class Classification & Metadata Extraction**

- Broadest protocol & application coverage in the industry
- Classifies 3400 protocols
- Extracts 5400 flow & application metadata
- Offers unique, real-time Deep File Inspection capabilities
- Identifies precise end points (device, IP, user, domain name, etc.)
- Delivers granular metadata specific to cybersecurity requirements
- Provides critical visibility into encrypted and evasive traffic
- Supports SCADA/IoT protocols and metadata, and identifies cryptocurrencies & mining pools
- Features first packet classification to support requirements like SD-WAN

**Attractive Business Model**

- Affordable, easy-to-deploy SW sensor
- Eliminates costly custom traffic classification development
- Delivers continuous updates
- Drastically reduces need for full packet capture
- Reduces costly endpoint- and perimeter-based data collection requirements

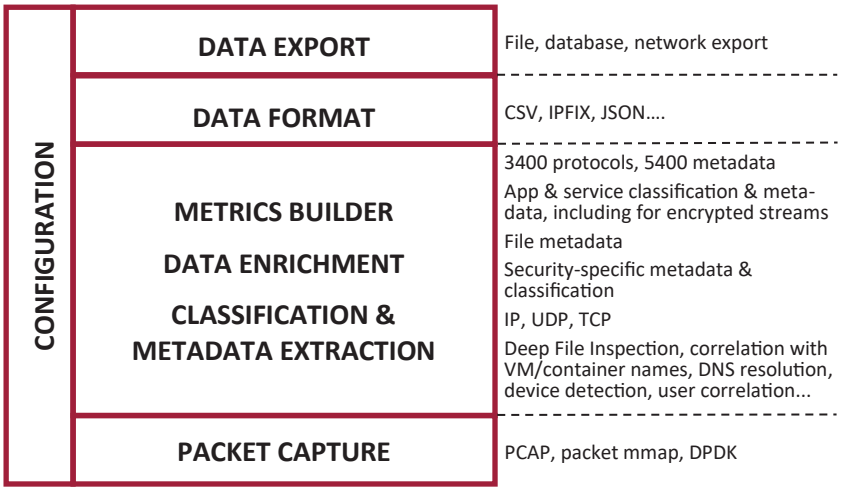
Once upon a time, network boundaries were defined, featuring a stable constellation of gateways, network devices, users and endpoints. Of course, those days are long gone. Cloud computing, virtualization, containerization, micro-segmentation, dynamic provisioning, dynamic workforces, and an explosion in the volume and types of end devices have transformed networks into constantly evolving ecosystems.

As a result, you can no longer get the full traffic visibility needed to ensure network performance, availability and security simply by embedding traffic intelligence software on firewalls and a few core network devices. You need to be able to set a pair of eyes wherever and whenever needed to eliminate blind spots.

To meet this need, we created the Qosmos Probe. It is a standalone version of our market-leading embedded (SDK) product, the Qosmos ixEngine. The Probe delivers the same exceptional Layer 2 to Layer 7 flow classification and metadata extraction as ixEngine, but in an application you can rapidly deploy on commodity hardware alongside any node, anywhere in your physical, virtual, or cloud infrastructure.

The Qosmos Probe provides complete, real-time visibility into all your network traffic, including encrypted and evasive traffic, and it supports IoT/SCADA traffic for hybrid IT/OT networks. It also offers the comprehensive data required for understanding network transactions and user behavior.

**Qosmos Probe Functional Architecture**



## Beyond IP Traffic Classification: Metadata Extraction

The Qosmos Probe 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 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. 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, protocol version (e.g., SMBv1)

## Up-to-date Protocol Plugins and Metadata

Applications and their protocols change constantly and without notice. The experts at Qosmos Labs continuously receive information about changes in protocols and applications and update the plugins accordingly.

## Extensions for Aggregated and Computed Metadata

The Qosmos Probe 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 for specific 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
- **Advanced Filtering** to enable the filtering of records using multiple criteria (protocol, IP address, L7 metadata…) so that only the most relevant data is transmitted to the analytics system
- **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 and Throughput

Qosmos ixEngine has built-in multi-core support capabilities. The software typically handles up to 20 Gbps of traffic per Probe.

- High performance under heavy metadata extraction loads
- Optimized code for the industry's highest performance multicore processors
- Optional packet pre-filtering: depending on requirements, all packets or only a subset of packets are parsed by the Qosmos Probe

## Configuration and Management

- NETCONF API
- Multi-Tenant Centralized Management Console for configuration and status information (configuration, counters, errors, log messages, etc.)
- Independent core-decoding framework and protocol plugin library, which translates into fast flow signature updates while preserving engine stability. Protocol plugins are hot-swappable.
- A unique and highly configurable flow manager architecture which handles standard, tunneled and multiplexed flows

## Integration in a Physical Appliance

- Runs on commodity hardware (Intel x86_64 architecture)
- OS: CentOS or RHEL 7
- DPDK packet capture acceleration

## Integration in Virtual Systems

- Application-level visibility for security and monitoring functions (APM/NPM, Service Assurance)
- "Cloud ready" and supports per-tenant DPI usage

## Deliverables

- The Qosmos Probe is delivered as a fully customizable Linux application: Probe Software Package (e.g. VM, container, RPM…).

## Learn More

For further details about the Probe, and the full list of protocols recognized by Qosmos technology, visit www.qosmos.com/products/probe-solution

You can also request a free product evaluation at any time at www.qosmos.com/about-us/contact-us

ENEA

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

www.enea.com