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

- Applicative version of Qosmos ixEngine® , the next-generation DPI software trusted by 75% 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 3600 + protocols
- Extracts 5600+ metadata
- Real-time deep file inspection capabilities
- Endpoint identification (device type, subscriber)
- Delivers granular metadata specific to cybersecurity requirements (MITM detection, domain fronting, evasive traffic)
- Categorization of encrypted traffic thanks to machine learning models
- Extended coverage of Cloud, SaaS, SCADA and IoT protocols and metadata
- Cryptocurrencies & mining pools

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

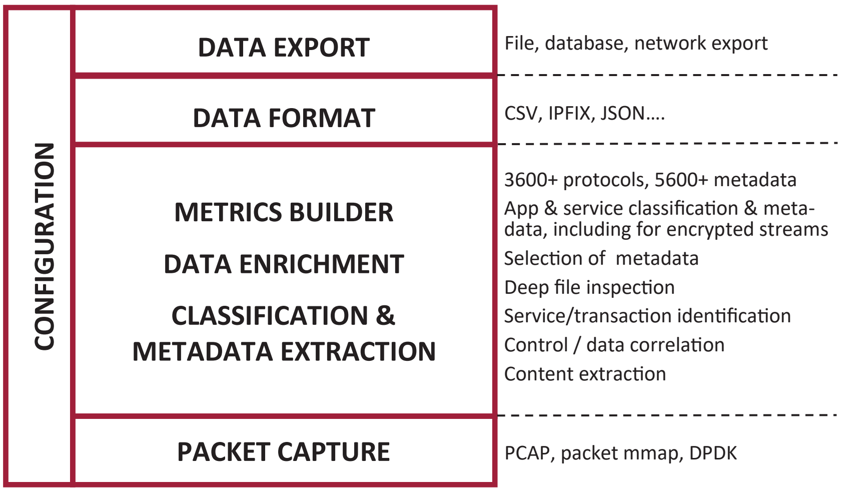
Once upon a time, network boundaries were defined, featuring a stable constellation of gateways, network devices, users and endpoints. Of course, those days are long gone. Cloud computing, virtualization, containerization, micro-segmentation, dynamic provisioning, dynamic workforces, and an explosion 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 an application 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 Qosmos 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



CONFIGURATION	DATA EXPORT	File, database, network export
	DATA FORMAT	CSV, IPFIX, JSON....
	METRICS BUILDER DATA ENRICHMENT CLASSIFICATION & METADATA EXTRACTION	3600+ protocols, 5600+ metadata App & service classification & meta-data, including for encrypted streams Selection of metadata Deep file inspection Service/transaction identification Control / data correlation Content extraction
	PACKET CAPTURE	PCAP, packet mmap, DPDK

Beyond IP Traffic Classification: Metadata Extraction

The Qosmos Probe extracts different **categories** of network-based application metadata and computed metadata:

- **Flow**: Classification (ie: eth.ip.tcp.ssl.youtube), volume, duration, category...
- **Service identification:** File transfer, email send, audio call...
- **Device Identification:** Model, manufacturer, OS, version
- **Identifiers:** GTP-c / GTP-u correlation (IMSI, IMEI, Location, RAT per user plane flow). Sender, receivers...
- **Content extraction :** Export selective packets and files.
- **File metadata:** Name, size, type for emails, file transfers or web files. Check consistency between file extension or announced MIME type with file content.
- **Security-related classification & metadata:** Tunneling, evasive traffic, Man in the Middle indicator...
- **Application performance:** TCP RTT, RTT at application level, audio MOS...
- **Categorization** : Machine learning-based encrypted traffic categorization (audio call, video call and video streaming…)

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 Module:** create your own sensor by using Qosmos Probe Framework API (C, Python)
- **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 record filtering 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., image download on Facebook)
- **Automated DPI** to classify previously unknown traffic using automated algorithms

High-Performance and Throughput

Multi-core support capabilities.

The software typically handles up to 40 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, Ubuntu 18.04
- 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 (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 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 on Enea's Qosmos ixEngine, Qosmos Probe or Qosmos DPI technology: www.qosmos.com

www.enea.com