ENEA

Application DATASHEET

Qosmos Probe Complements IDS/IPS for Advanced Network Detection & Response

Delivering Deep Traffic Intelligence for Improved Detection of Complex Cyber Attacks

Key Benefits

Proven Technology

- Based on Qosmos ixEngine®, the most widely deployed DPI software in cybersecurity

Unique NTA Support Capabilities

- Fuels machine learning with distinctively granular and reliable data
- Provides critical visibility into encrypted and evasive traffic
- Supports SCADA/IoT protocols and metadata
- Delivers intelligence to support custom, network-specific rules

Best-in-Class Classification and Metadata Extraction

- Broadest protocol & application coverage in industry
- Classifies 3600+ protocols
- Extracts 5600+ application metadata
- Delivers unique, real-time Deep File Inspection and extraction capabilities
- Device Detection and Identification (including IoT)
- Delivers protocol metadata specific to cybersecurity requirements

Smarter Alerts

- Enables highly effective alert prioritization
- Provides deep alert contextualization
- Backed by Qosmos' unique 'no false positives' commitment

Attractive Business Model

- Packages market-leading DPI tech in affordable, easy-to-deploy SW sensor
- Eliminates need for custom DPI development
- Delivers continuous, hot-swappable updates
- Drastically reduces need for full packet capture
- Reduces costly endpoint- and perimeter-based data collection requirements

Network Detection and Response (NDR) is increasingly used to identify complex threats that have evaded conventional endpoint and perimeter defenses. NDR combines two important network-based threat detection tools: IDS/IPS to identify known threats via signatures, and Network Traffic Analysis (NTA) to identify new or unknown threats via anomaly detection.

NTA uses machine learning to create a model of normal behavior for a network, with a cyber sensor providing detailed data about typical applications, services, data characteristics, connections and flow patterns. Then, machine learning and other analytical tools are used to detect deviations from this model using real-time traffic intelligence from the cyber sensor. The anomalies detected often provide a vital early indication of a sophisticated network breach.

Complementing IDS/IPS with a cyber sensor and NTA is a strategy that has proven to be particularly effective against Advanced Persistent Threats (APTs) that can linger for months – or even years – in the absence of behavior-based anomaly detection.

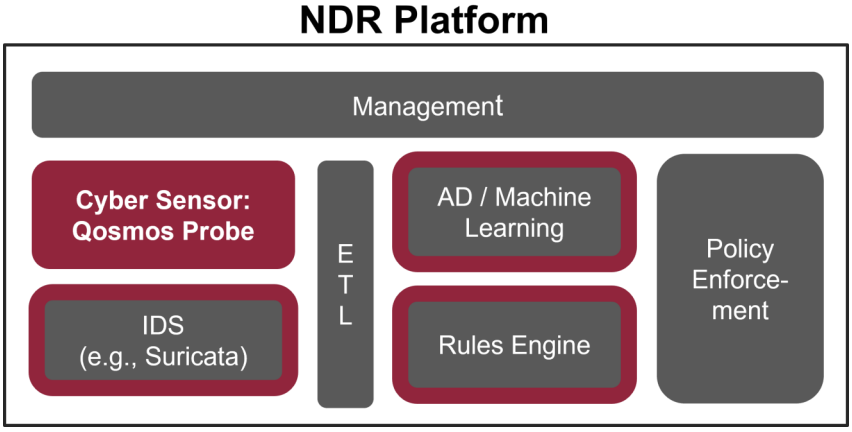
The Qosmos Probe Cyber Sensor

The Qosmos Probe is a best-in-class cyber sensor that non-intrusively gathers raw telemetry input and transforms it into richly classified traffic data – even if the traffic is encrypted (as APT traffic often is).

Deployed across key network assets, Qosmos DPI sensors provide data that is:

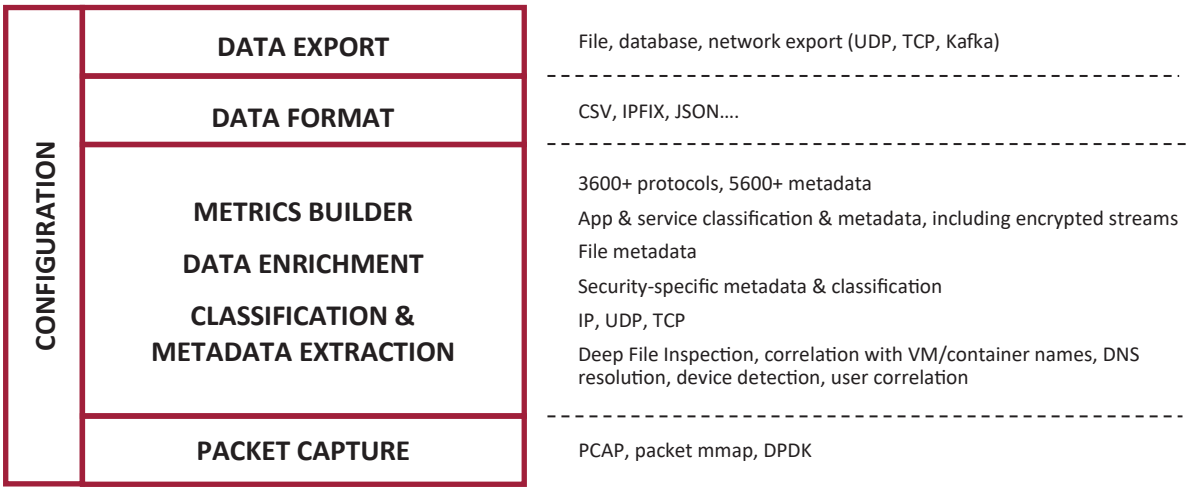
- Reliable: based on the most trustworthy source available - telemetry data (not insecure log files)
- Comprehensive: classified from OSI L2 up to L7 (from Data Link to Application layer)
- Real-time: gathered on-the-fly via passive physical or virtual network TAPs that do not affect traffic flow

The Qosmos Probe DPI sensor is powered by the Qosmos ixEngine, the most widely deployed deep packet inspection (DPI) software in cybersecurity. It is unparalleled in processing throughput and in the depth and breadth of protocol and metadata extracted.



The Qosmos Probe provides essential data that complements IDS/IPS, feeds anomaly detection algorithms in the machine learning module, and enables the creation of advanced rules.

Qosmos Probe Architecture



Performance & Flow Processing

- Up to 40 Gbps traffic per probe, can be stacked and managed as a single entity
- 1 Gbps / core CPU, 4 GB RAM per Gbps
- Classifies traffic encapsulated in tunnels (GTP, GRE, PPOE, etc.)
- Hot-swappable updates (3-week release cycle)

Classification of Encrypted/Evasive Traffic

- Traffic Patterns used to identify Skype with high accuracy (>97% recognition rate)
- Statistical models and machine learning used to detect complex protocols like RC4 encrypted BitTorrent (min. 95% accuracy)
- Domain fronting detection classification techniques for making evasive traffic visible (UltraSurf, Viber, Hotspot Shield, etc.)
- Successful classification of traffic spoofing applications (HTTP Injector, eProxy, etc.) designed to “fool” DPI engines
- Successful detection of ICMP and DNS tunneling traffic
- Detection of popular cryptocurrencies and mining pool traffic (cryptojacking)

Deep File Inspection

Detects file type, checks consistency between MIME type and file extensions, computes file hash and extracts metadata.

- File hashes: MD5, SHA-1, CTPH
- More than 280 file types: application, video, audio, text...

Data Aggregation

- Ability to send cross-flow records (statistics per IP, per application, per host name….) to reduce the number of Events per Second

Custom Signature Module (CSM)

Allows you to create your own classification signatures and load them into the Qosmos Probe in real-time.

Custom Python Modules

Allows users to create new Qosmos Probe features with full autonomy by developing modules in Python and inserting them into the data flow.

Device Detection and Identification

- Discover any device connected in your network
- Identify device manufacturer, model, OS / SW version

Configuration and Management

- NETCONF API
- Multi-Tenant Centralized Management Console for configuration and status information (configuration, counters, errors, log messages, etc.)

Integration in a Physical Appliance

- Runs on commodity hardware (x86_64 architecture)
- CentOS or RHEL 7, Ubuntu 18.04
- DPDK packet capture framework

Integration in Virtual Systems

- Application-level visibility for SD-WAN routing, security and monitoring functions
- “Cloud ready” and supports per-tenant DPI usage

Deliverables

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

To learn more about using DPI for NTA, visit
https://www.qosmos.com/cybersecurity/network-traffic-analysis/

Find out more!

ENEA

www.enea.com

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