ENEA

DATASHEET

# Qosmos Probe as a DPI Sensor for Network Traffic Analysis

Real-Time Protocol & Metadata Intelligence for Superior Network Traffic Analysis

## 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 3300+ protocols
- Extracts 5300+ application metadata
- Delivers unique, real-time Deep File Inspection capabilities
- Identifies precise end points (device, IP, user, domain name, etc.)
- 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

Enterprise Security Operations Center (SOC) staff and Managed Security Service Providers (MSSP) are increasingly using Network Traffic Analysis to identify suspicious activities missed by existing endpoint and perimeter defenses.

NTA uses machine learning, advanced analytics and rule-based detection to identify threats via abnormal patterns in network traffic flows and connections. It is a strategy that has proved particularly effective against Advanced Persistent Threats (APT) that can linger for months – or even years – in the absence of behavior-based anomaly detection.

But effective behavioral analytics require enormous quantities of reliable, detailed traffic data. In other words, NTA requires the kind of data delivered by deep packet inspection (DPI) sensors.

## The Qosmos Probe

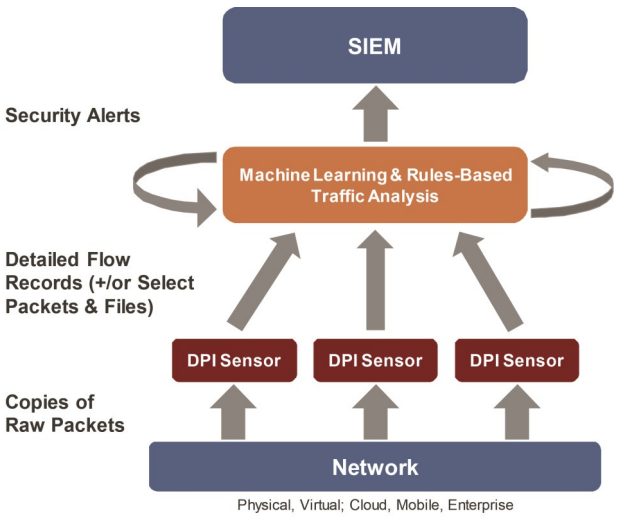
The Qosmos Probe is a best-in-class DPI sensor that non-intrusively gathers raw telemetry input and transforms it into richly classified traffic data – even if the traffic is encrypted (as APT traffic often is).

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

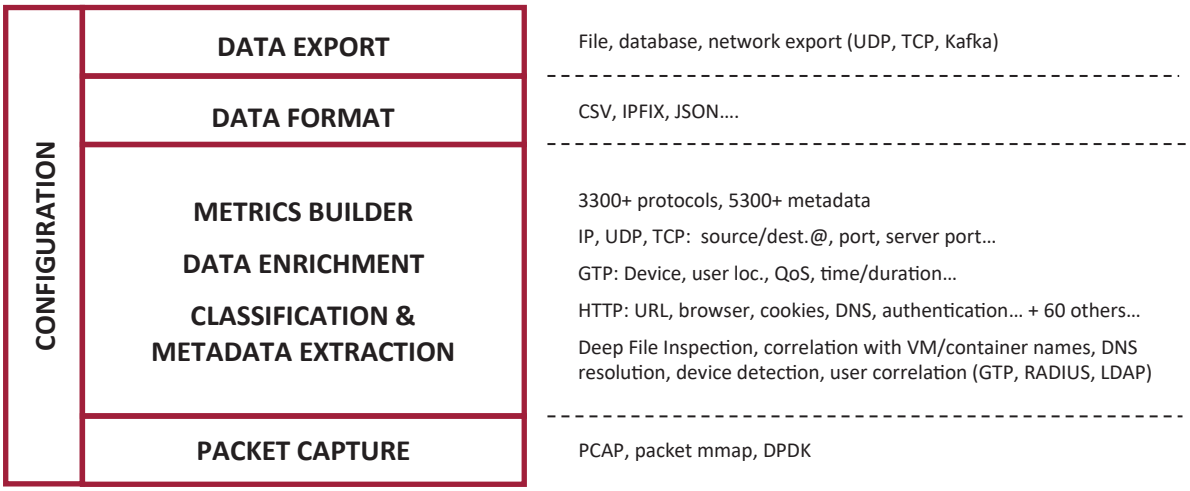
- Reliable: based on the most trustworthy source available - telemetry data (not insecure log files)
- Comprehensive: classified from OSI L2 up to L7 (from Data Link to Application layer)
- Real-time: gathered on-the-fly via passive physical or virtual network TAPs that do not affect traffic flow

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

**Network Traffic Analysis**



## Qosmos Probe Architecture




### Performance & Flow Processing

- Up to 20 Gbps traffic per probe, can be stacked and managed as a single entity
- 1 Gbps / core CPU, 4GB 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, Hotspotshield, 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.

### Analytics Sample for Cyber Security Operations

- Keys: flow_id,application, ip_srv, port_srv, ip_clt, http.server, http.uri_path, http.code…
- Metrics: stc_packet-count, stc_volume, dfi.mimetype*, dfi.ctph*, http.mime_type…

*dfi = Deep File Inspection, i.e. inspection of file content

Statistics aggregation can be exported in CSV, IPFIX or JSON (compatible with ELK and InfluxDB databases)

### 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
- 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, read our MSSP Case Study: https://www.qosmos.com/mssp-uses-qosmos-probe-in-nta-solution-to-improve-service-levels/

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Find out more!

ENEA

www.enea.com

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 already rely on Enea technologies in their daily lives. Enea’s leading DPI-based IP traffic classification and network intelligence software is embedded by vendors and integrators into their products sold to telcos, cloud service providers and enterprises. For more information on Enea’s Qosmos Probe or Qosmos DPI technology: www.qosmos.com