ENEA

APPLICATION DATASHEET

Qosmos Probe as a DPI Sensor for Cyber Defense

Extreme Throughput and High-Resolution Traffic Intelligence for the Most Demanding Environments

Key Facts

Full Traffic Visibility

- Provides full visibility into network traffic up to Layer 7, including protocol details: File extensions, content…
- Brings new capabilities that pinpoint key data, decreasing false positives
- Shortens detection & investigation time
- Reduces size of forensic data by up to 150x compared to full packet capture

Best-in-class Classification and Metadata Extraction

- 3400+ protocols classified and 5400 application metadata extracted
- Unique real-time Deep File Inspection capabilities
- Precise end point identification (device, IP, user, domain name, etc.)
- Protocol metadata specific to cybersecurity requirements

Easy Integration

- Standard formats, normalized data streams, and connectors
- Flexible management, including NETCONF API

Powerful Flow Processing

- Classification of traffic encapsulated into all types of tunnels (GTP, GRE, PPOE, etc.)
- IPv6 compliant

As cyber attacks against public cyberspace and national infrastructure become increasingly sophisticated, effective threat analytics require accurate and detailed input from different sources. One key source of information is the network traffic itself. The more detailed the traffic visibility available to analytics solutions, the more accurate the detection and investigation capabilities will be.

A sensor (or software probe) using Deep Packet Inspection (DPI) provides the most granular detail available, delivering a complete picture of activity in any size network. By passively capturing packets, detecting applications, parsing protocols, and extracting traffic metadata, it can significantly improve detection of attacks and raise the performance of proactive threat hunting.

The Qosmos Probe is a DPI sensor that embeds the market-leading DPI engine, Qosmos ixEngine®. It leverages years of experience in cyber defense environments and is a key component of the security technology stack for government-run Security Operations Centers (SOCs). For these sensitive environments, combining DPI information with a proprietary, confidential solution creates an additional layer of security, complementing turnkey commercial products such as IDS, which have technical capabilities that can be known by attackers.

DPI Sensor Applications

1. **A rich information feed to strengthen threat analytics**
   Metadata extracted from traffic flows boosts machine learning for threat analytics platforms. This translates into more accurate alerts, shorter time-to-detection, and fewer false positives.

2. **An expert tool for network forensics and threat hunting**
   A DPI sensor streamlines investigations and improves time-to-detection for network forensics and threat hunting by capturing and storing detailed traffic information in a database where it can be rapidly and easily accessed for query and visualization. In addition, the sensor provides high information resolution using a fraction of the storage required for full packet capture because it only requires traffic metadata (sender, receiver, device type, file type, etc.), discarding irrelevant content, such as video.

Qosmos Technology Reveals Hidden Threats

Encryption

Get maximum visibility into all encrypted traffic to support triage for decryption, advanced analytics for anomaly detection, and forensics.

Virtual Private Networks (VPNs)

Accurately identify the use of dozens of VPN applications, including those most commonly deployed for malicious activities. VPN Protocols detected with blocking use cases.

Anonymizers

Detect anonymous proxy services that may be cloaking harmful activities, including those using multiple layers of encryption.

Complex Tunneling

Gain visibility into traffic using complex tunneling, with full protocol paths revealed for up to 16 levels of encapsulation.

Covert Communication Channels

Detect non-standard tunneling activities over legitimate protocols such as DNS or ICMP, which may indicate unauthorized or illegal activities.

Domain Fronting

Reveal the use of routing schemes in Content Delivery Networks (CDNs) and other services that mask the intended destination of HTTPS traffic (direct or tunneled).

Traffic Spoofing

Identify apps (e.g., eProxy, HTTP Injector) that combine techniques (such as protocol header customization, proxies, tunneling & domain fronting) to evade detection.

File Spoofing

Detect inconsistencies such as a false MIME type or a mismatch between the original hash and computed hash.

P2P Misuse

Classify obfuscated P2P traffic to support forensics and behavioral modeling of network traffic.

Device Identification (roadmap)

Identify OS and Device in the company's network to set specific rules in a BYOD world.

Technical Features

Performance

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

Data Aggregation

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

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...

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)

Custom Signature Module (CSM)

The CSM module allows you to create your own classification signatures and load them into the Qosmos Probe in real-time.

Configuration and Management

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

Integration in a Physical Appliance

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

Deliverables

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

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2019

Find out more
on the Qosmos
website

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. For more information on Enea's Qosmos ixEngine, Qosmos Probe or Qosmos DPI technology: www.qosmos.com

www.enea.com