Use Case Datasheet

Qosmos ixEngine® Content Extraction for Malware Protection and Data Loss Prevention

Industrial strength extraction of network traffic content for developers of security solutions such as malware protection, data loss prevention and threat intelligence platforms.

Key Facts about Qosmos ixEngine

- C Libraries designed to be embedded into applications
- 3000+ protocol plugins, continuously supported and updated
- 4700 application metadata extracted
- Classification of networking protocols and applications based on flow pattern matching, bi-directional flow correlation, heuristics and statistical analysis
- High recognition rate: ability to identify layers 2 to 7 in the OSI model
- Ability to develop custom application plugins based on description
- Protocol plugin In-Service Software Upgrade (ISSU)
- Modular architecture (flow management, regular expression engine, http parsing, etc.)
- Up to 10 Gbps* per core on latest x86 architecture

Specific Security Features

- Built-in rule engine for efficient development of NGFW, DLP, and malware prevention products
- Deep File Inspection: Detection of file type, consistency check between MIME type and file extension, file hash computation, and extraction of metadata
- Transactional DPI: description of user activity within an application (e.g. “download file” inside Facebook)

The Challenge

Organizations of all types are facing new cyber threats due to the evolving work environment: employees now have access to social networking, file sharing applications, cloud storage, webmail, instant messaging, SaaS applications (CRM, virtual desktop infrastructure). In addition, employees bring their own devices to the office and regularly work from home or remote locations. These trends increase the risk of infection by infiltration of malware and the risk of exfiltration of sensitive information.

Security vendors have responded with new solutions for malware protection, data loss prevention (DLP) and threat analysis. To be effective, these products need to dig deep into the payload of network traffic and extract detailed information such as file content (typically decrypted payload).

Strengthening Solutions with Qosmos ixEngine

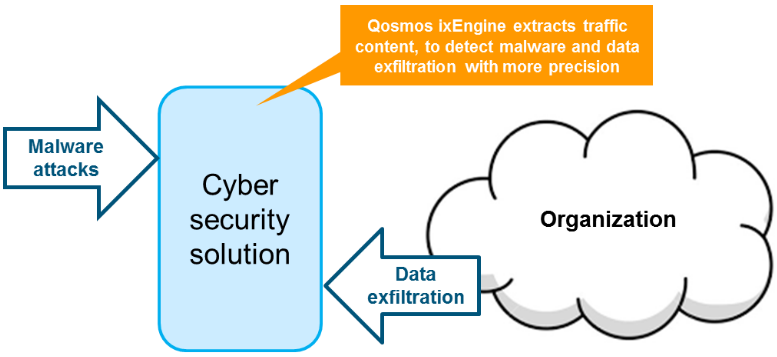
Enea’s Qosmos ixEngine is a Deep Packet Inspection (DPI) library which classifies protocols, and extracts metadata and file content. It provides extraction and facilitates reconstruction of network traffic content within cyber security solutions. This gives developers the ability to expose file movements at the network level to track potential malware and data exfiltration.

Qosmos software can be used to extract raw traffic content and metadata to reconstruct complete emails, attached files, images, videos, transferred files (uploaded or downloaded via FTP, HTTP, Dropbox), Websites, etc.

Qosmos ixEngine Capabilities

- Content and file extraction: The most comprehensive and mature file extraction library supporting over 60 protocols for file extraction, including all transport types for Server Message Block (SMB) and all generic HTTP transfers
- Deep file inspection: Efficient file type detection, file hashing, and metadata extraction for file reconstruction

These capabilities are already built into the Qosmos DPI engine, which means that developers are able to focus all efforts on sensors and the features and performance of the overall security solution.


Qosmos ixEngine extracts traffic content, to detect malware and data exfiltration with more precision
Malware attacks
Cyber security solution
Organization
Data exfiltration

Use Case: Qosmos ixEngine® for Malware Protection and Data Loss Prevention (DLP)

The following example illustrates how Qosmos ixEngine can be used in different parts of a complete security solution.

Initially, network traffic is captured through a tap or port mirror using, for example, Intel® DPDK libraries for fast packet processing.

The traffic is then scanned by an Intrusion Detection & Prevention System (IDS / IPS), which could be open source (Snort, Suricata), or proprietary. Results are fed to the mitigation system.

Step 1: Object & Content Extraction

Qosmos ixEngine ingests network traffic considered as clean by the IDS and extracts content elements. The software reorders content, extracts payload and saves content of each object into a file (even if there are multiple objects in a single packet).

- Streamed raw content: downloaded files, uploaded files, emails, attached files and file types (MS Office, PDF, .exe, etc.)
- Metadata: URLs, IP address, sender, receiver, file type, etc.

Step 2a: Object Reconstruction

Software for object reconstruction can be developed in-house by the security vendor, or with the help of Qosmos Professional Services.

Based on the information from Qosmos ixEngine, each object is reconstructed: files, pictures, JavaScripts, emails, email attachments, etc.

- Emails: body of text , metadata (sender, receiver, IP address, etc.), attached files (content, photos, etc.)
- File Transfer: HTTP downloads, FTP files, etc.

Step 2b: File Analysis

This step focuses on checking file integrity and is performed in parallel with object reconstruction.

- File hashes: CRC, SHA-1, MD5
- Extension types: MIME mismatch, real file extension

At this stage, the Qosmos ixEngine Deep File Inspection module can be used to detect file type, check consistency between MIME type and file extension, compute file hash, and extract metadata.

Step 3: Investigation

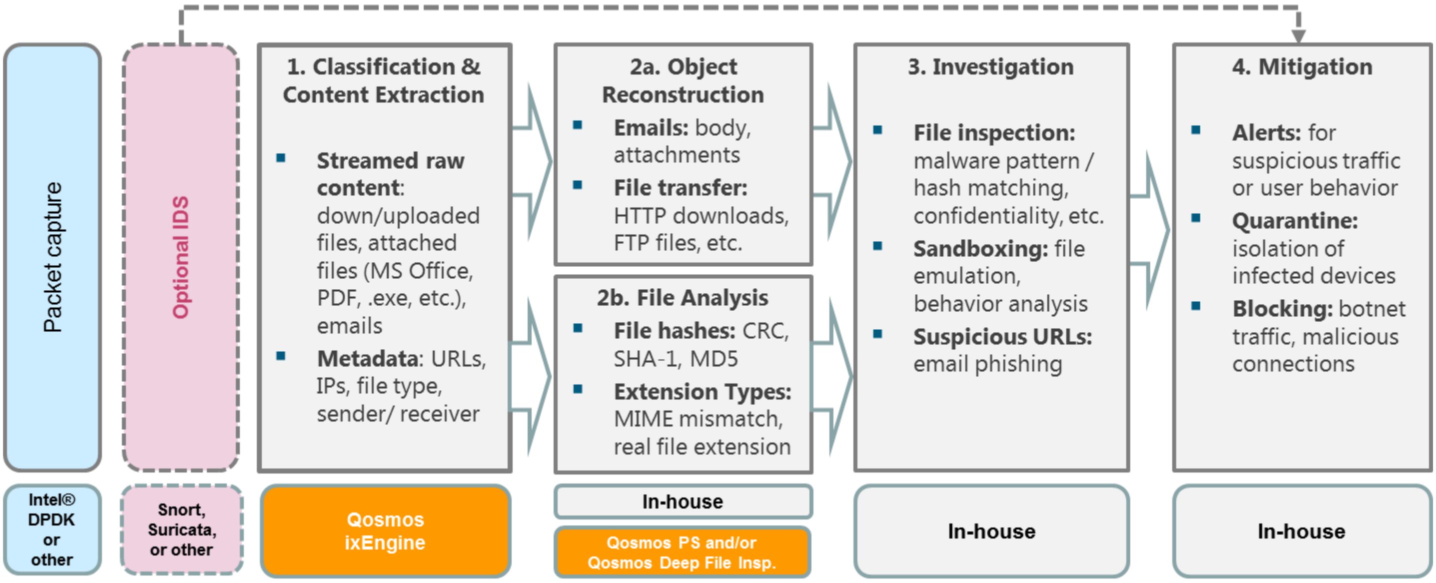
Investigation methods are part of a security vendor's core expertise, based on a combination of techniques such as:

- File inspection: malware pattern matching, confidentiality, file integrity check, etc.
- Sandboxing: removing suspicious software from traffic and running it in an isolated environment to observe and analyze behavior
- Identifying suspicious URLs in emails (phishing)

Step 4: Mitigation

Features and functionality for this step are always developed in-house by cyber security experts, leveraging advanced techniques such as deception-based methods (honey pots), self-optimizing protection, or machine learning algorithms. Effective mitigation also requires connection between several functions such as policy enforcement by NGFW or network behavior anomaly detection.

- Alerts: for suspicious traffic or user behavior
- Quarantine: isolation of infected devices
- Blocking: botnet traffic, malicious connections



Packet capture

Optional IDS

1. Classification & Content Extraction

- **Streamed raw content**: down/uploaded files, attached files (MS Office, PDF, .exe, etc.), emails
- **Metadata**: URLs, IPs, file type, sender/ receiver

2a. Object Reconstruction

- **Emails:** body, attachments
- **File transfer:** HTTP downloads, FTP files, etc.

2b. File Analysis

- **File hashes:** CRC, SHA-1, MD5
- **Extension Types:** MIME mismatch, real file extension

3. Investigation

- **File inspection:** malware pattern / hash matching, confidentiality, etc.
- **Sandboxing:** file emulation, behavior analysis
- **Suspicious URLs:** email phishing

4. Mitigation

- **Alerts:** for suspicious traffic or user behavior
- **Quarantine:** isolation of infected devices
- **Blocking:** botnet traffic, malicious connections

Intel® DPDK or other

Snort, Suricata, or other

Qosmos ixEngine

In-house

Qosmos PS and/or Qosmos Deep File Insp.

In-house

In-house

Find out more on the Qosmos website!

Qosmos, a division of Enea, is the leader in IP traffic classification and network intelligence technology used in physical, SDN and NFV architectures. Qosmos ixEngine software development kit and components are embedded by vendors and integrators into their products sold to telcos, cloud service providers and enterprises. For more information: www.qosmos.com

Copyright © 2017 Enea. All rights reserved. Enea, the Enea logo, Qosmos, Qosmos Classifier, Qosmos Service Aware Module, Qosmos Service Aware Module for vSwitch, Qosmos SAM and Qosmos ixEngine are trademarks of Qosmos Tech. Other names and brands may be claimed as the property of others.