ENEA

Solution Brief

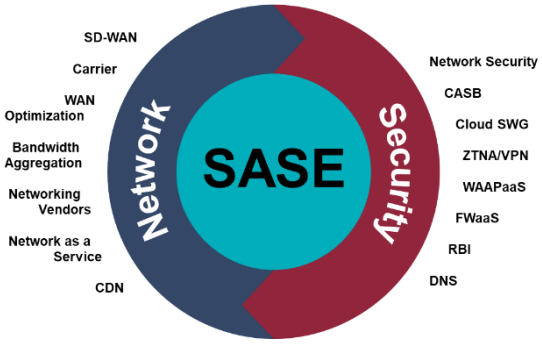
Qosmos ixEngine for SASE Solutions

In the Secure Access Service Edge (SASE) framework, wide-area networking and cybersecurity are fully merged and delivered as a distributed cloud service. This simplifies network management and boosts performance by bringing users and resources closer together. SASE also enhances security by segmenting traffic and applying rules according to the unique profile and context of each traffic flow.

To successfully deliver on these SASE promises requires comprehensive, real-time traffic visibility specifically adapted for today's complex, distributed networks. This is why SASE market leaders trust Enea Qosmos' traffic classification and inspection technology to meet their traffic intelligence needs. The Enea Qosmos ixEngine® has been specifically engineered to meet the special visibility demands of SASE. From accurately identifying applications from the first packet to providing unique insights into users, devices, content and flows, the Enea Qosmos ixEngine provides the contextual foundation upon which superior SASE solutions are built.

Qosmos ixEngine:
Helping Vendors Get on the Fast Path to SASE Success

Within the space of only a couple of years, SASE has evolved from a concept to market-ready products within a competitive field. It is not surprising given that the introduction of the SASE model was followed in short order by an abrupt shift toward mobile work and an accompanying acceleration in cloud adoption.



As conceived by Gartner in 2019, SASE is a model in which WAN and cybersecurity are fully converged and delivered as a cloud service, with a distributed edge architecture that brings computing resources closer to the end users who need them.

Within such a dynamic environment, SASE offers enterprises an appealingly simple solution to the challenge of delivering secure, anywhere/anytime access to applications and services. For vendors, the challenge of delivering such a convenient solution is anything but simple. However, the potential rewards are great.

At Enea Qosmos, we've worked with start-ups and industry veterans to help them reap these rewards by addressing one of the most important challenges for SASE vendors: maintaining real-time, application-level traffic visibility across diverse, distributed networks.

Vendors achieve this visibility by embedding Enea's Layer 2 to Layer 7 traffic classification engine, the Qosmos ixEngine, into their SASE solutions in whatever format is best suited to their architecture (software library in C, VNF, CNF, or standalone software sensor). Once integrated, Qosmos ixEngine delivers the universal application visibility and targeted contextual data SASE requires for converged security and networking services – with or without traffic decryption.

SASE Visibility Challenges & Solutions

Challenge 1: Difference in Edge and PoP Visibility Requirements

In conventional network architectures, traffic visibility needs are often met by decrypting all traffic and running it through a deep packet inspection (DPI) engine. It is a familiar strategy, but one that is ill-suited to the scale and distributed nature of SASE solutions, especially as evolving encryption standards make decryption more complicated and expensive. In SASE, Edge and PoP visibility needs are very different, except in the case of hybrid SD-WAN/SASE deployments in which some Edges require advanced services normally performed at the PoP.

The Enea Solution
Qosmos ixEngine helps vendors meet this challenge by delivering adaptive traffic intelligence that meets the diverse visibility needs of SASE Edges and PoPs, and delivers critical classification information without requiring decryption.

At the Edge

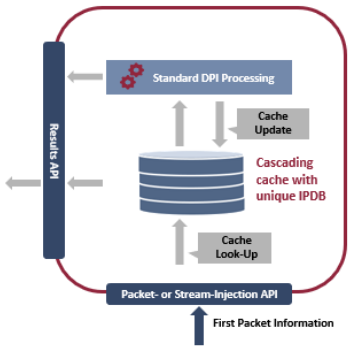
At the SASE Edge, Qosmos ixEngine identifies applications and service categories, and generates important security indicators from the very first packet. This enables safe, high-performance Internet breakout. For locations that require on-premise security and more sophisticated application-based routing (hybrid SD-WAN/SASE deployments, for example), Qosmos ixEngine delivers full DPI capabilities at the edge.

At the PoP (or SD-WAN Edge in Hybrid SASE)

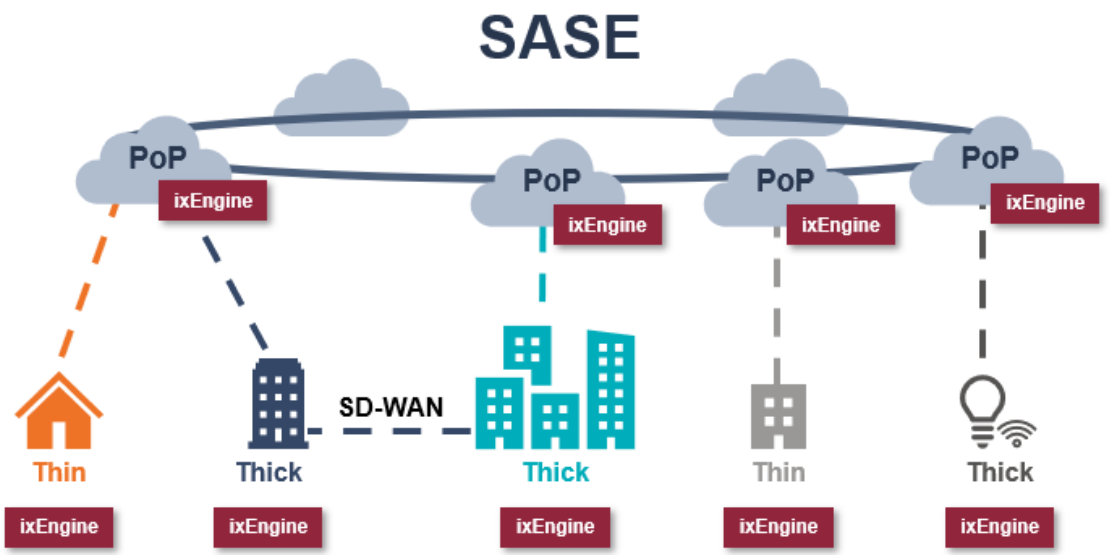
Within the PoP, Qosmos ixEngine provides highly scalable traffic classification, metadata generation, file extraction and deep packet inspection to support advanced traffic orchestration and cybersecurity services.

First Packet Advantage (FPA)

Available as a standard feature in Qosmos ixEngine® and Qosmos ® Probe, the First Packet Advantage (FPA) feature uses an innovative multi-tier cache system to boost application recognition and significantly improve accuracy.



Qosmos ixEngine in SASE solutions



ixEngine Supported Functions

Thin Devices	Thick Devices	PoPs	
App/svc classification	DLP	Cloud Optimization	NGFW
Policy-based routing to PoP	SWG	WAN Optimization	SWG
QoS-related metrics	NGFW	Global Route Optimization	Advanced Threat Prevention
Optional NGFW	VPN	Self-healing Architecture	Cloud & Mobile Security
	Router		

To further support diverse traffic intelligence needs, Qosmos ixEngine can support dynamic traffic steering and/or the sharing of DPI results among multiple SASE functions.

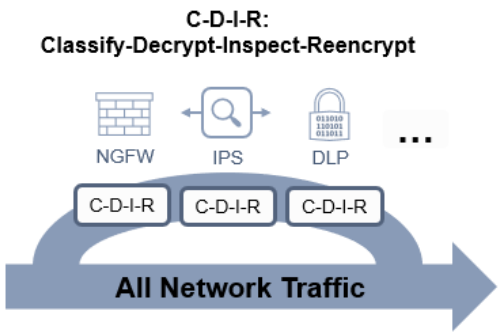
In a conventional service chain architecture, traffic is run through all networking and security functions in a serial fashion, with the same traffic decrypted, processed with DPI, and re-encrypted by each function. SASE demands a higher performance model.

Selective decryption minimizes the time and resources required to extract essential traffic intelligence.

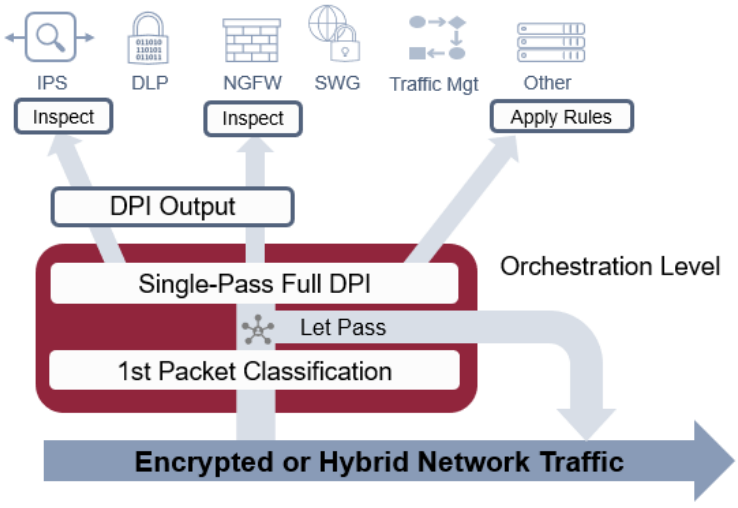
One such model is the steering model, in which upstream encrypted traffic analytics are used to determine if a given flow should be decrypted for in-depth inspection or not, and if so, by which functions (IPS, NGFW, DLP, etc.).

Qosmos ixEngine supports this with granular classification of encrypted traffic. For example, it can identify one encrypted flow as an MS Teams audio call, which does not require decryption, and another as a Sharepoint file transfer, which does require decryption and content analysis.

Conventional Service Chaining



Steering Model with Single-Pass DPI



When decryption and full DPI must be used, running DPI once and sharing the results (i.e., 'single-pass DPI) provides another way of maximizing SASE performance. Qosmos ixEngine supports this with flexible form factor options including deployment as a standalone CNF for microservice environments.

Challenge 2: Maximizing Visibility Without Impacting Performance

DPI is the industry standard for meeting advanced traffic visibility needs. And given the critical role traffic intelligence plays in SASE, DPI is a must. But, the performance demands on SASE are very high, and DPI is a resource-intensive technology.

The Enea Solution

As noted previously, with exceptional first packet capabilities and maximum deployment flexibility, Qosmos ixEngine is well-designed for a minimal, strategic use of full DPI. And when full DPI is must, Qosmos ixEngine delivers high performance that meets the needs of the largest SASE vendors in the market, without sacrificing enhanced features like extensive security metadata and full protocol path visibility (to 16 layers of encapsulation). Performance capabilities include:

- Optimized multi-thread support for scalability up to 96 cores
- High performance under heavy metadata extraction loads
- Optimized code for the industry's highest performance multicore processors
- Optimized integration with packet processing middleware (e.g., Intel DPDK)
- Support for VPP and hardware acceleration and offloading

Challenge 3: Preserving Visibility in Encrypted Environments

Universal, real-time application-awareness is a requirement for SASE. However, changes in encryption standards and the high-performance demands of SASE make it difficult for standard DPI to deliver adequate visibility in encrypted environments.

The Enea Solution

Qosmos ixEngine enables you to meet this challenge by accurately classifying encrypted flows. Techniques used to classify encrypted traffic include:

Handshake Analysis
Extraction of metadata in handshake messages that precede encrypted packets, and which remain clear

Binary Pattern Analysis
Detection & matching of binary patterns against known applications and services

Statistical Analysis
Analysis of packet and flow characteristics using custom models developed by Enea Qosmos R&D

Behavioral Analysis
Analysis of encrypted session behavior versus characteristic protocol behaviors

IP Address Analysis with IPDB
Analysis via a multi-tier cache that uses an Internet Protocol Database (IPDB) with 100s of millions of continuously updated, DPI-validated IP address/ application matches to accurately identify applications from the first packet

In first packet mode, the **Qosmos ixEngine First Packet Advantage** feature reliably identifies:

- Applications
- Key Categories
- Security Indicators

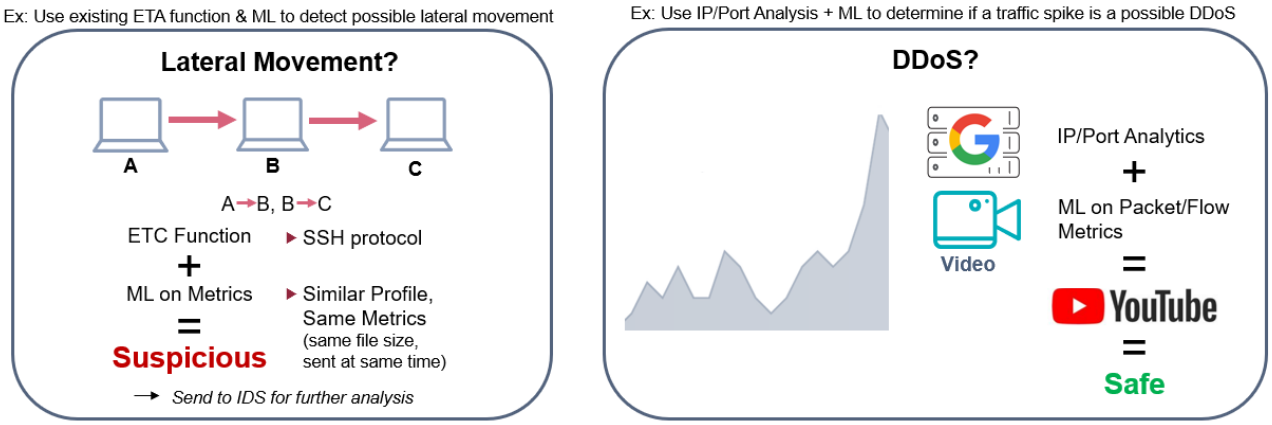
Full L2-L7 inspection of decrypted traffic extracts intelligence about:

- Applications
- Services
- Content (payload)
- Security Indicators
- Users
- Devices
- Flows, and more, with 1000s of types of metadata produced

Machine Learning

The use of machine learning to boost the accuracy and service level granularity of first packet processing, and to help classify applications and identify potential security threats in fully encrypted traffic (i.e., traffic in which the handshake and other remaining clear data are obfuscated).

Machine learning can be combined with other techniques to support visibility, threat detection and analysis needs in fully encrypted streams.



Challenge 4: Insight into Potential Threats

Whether a given flow is encrypted or not, as advanced persistent threats continue to increase in frequency and sophistication, inflicting higher levels of damage, a successful SASE solution has to have a very robust, network-based threat detection and response capability.

The Enea Solution

Qosmos ixEngine supports Network Detection and Response (NDR) with the broadest protocol coverage in the industry, plus thousands of types of extracted and computed metadata, including an extended library of security-related metadata. This traffic visibility contributes to the detection of a wide variety of evasive techniques, such as:

- **Complex Tunneling**
  Provides visibility into traffic that is using complex tunneling. Reveals full protocol paths for up to 16 levels of encapsulation.
- **Virtual Private Networks (VPNs)**
  Accurately identifies dozens of VPN applications, including those most commonly deployed for malicious activities.

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

- **Anonymizers**
  Detects anonymous proxy services that may be cloaking harmful activities, including those using multiple layers of encryption.
- **Covert Communication Channels**
  Detects non-standard tunneling activities over legitimate protocols such as DNS or ICMP, which may indicate unauthorized or illegal activities.
- **Domain Fronting**
  Reveals 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**
  Identifies applications (e.g., eProxy, HTTP Injector) that combine techniques such as protocol header customization, proxies, tunneling & domain fronting, to evade detection.
- **File Spoofing**
  Detects inconsistencies such as a false MIME type or a mismatch between the original hash and computed hash.
- **P2P Misuse**
  Classifies P2P traffic to support forensics and behavioral modeling of network traffic.

Challenge 5: Maintaining Complex Visibility Technology in a Fast-Moving Market

DPI is a very complex and constantly evolving technology. It requires a large, dedicated and highly specialized team to maintain. Given the competitive and fast-changing nature of the SASE market, trying to develop and maintain DPI in house can have a negative impact on time-to-market and competitiveness. Open source DPI is insufficient in quality and performance to support SASE success.

The Enea Solution
Designed with developers in mind, Qosmos ixEngine's ready-to-use libraries accelerate product development cycles, costs and risks, and let developers focus on building complete solutions, relying on the Qosmos division of Enea for its domain expertise in protocols, applications and metadata extraction. Integration accelerators include:

- **Optimized integration** with packet processing middleware (e.g., Intel DPDK)
- **Acceleration and offloading** configuration options for optimal integration with custom flow manager
- **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 while allowing different memory allocation modes with maximum flexibility
- **Support for multiple instances of Qosmos ixEngine** for maximum implementation flexibility

To accelerate integration and ensure that you leverage all the capabilities of our technology, Enea offers global professional services and provides access to a network of expert developers.

Conclusion

Every vendor has a unique approach to designing and implementing a SASE architecture, but all SASE solutions share a common need for universal, real-time application awareness.

4 of the Top 5 SASE Vendors
Embed Qosmos ixEngine

Source: Reports by Gartner, Forrester, 650 Group & Dell'Oro

This is a must-have for every networking and security function within SASE, such as SD-WAN, NGFW (Next Generation Firewall), CASB (Cloud Access Security Broker), SWG (Secure Web Gateway), DLP (Data Loss Prevention) and TDR (Threat Detection and Response).

For real-time application awareness in SASE, you need a commercial-grade traffic intelligence engine, and the OEM engine that is best suited to helping you succeed in the converged, cloud-based networking and security environment of SASE is the Enea Qosmos ixEngine.

Learn More

Discover the full list of protocols recognized by Qosmos technology at https://protobook.qosmos.com, or contact us today at www.qosmos.com/about-us/contact-us/ to request a product demo, and learn why 4 of the 5 top SASE vendors trust Enea Qosmos technology to fulfill their traffic intelligence needs.

Qosmos ixEngine Quick Overview

Qosmos ixEngine provides Layer 2 to Layer 7 traffic classification and metadata generation, plus additional capabilities essential for SASE success:

Maximum Visibility

- Broadest and most accurate protocol coverage
- 3600 protocols & 5400+ of types of metadata
- Deepest coverage for Cloud/SaaS protocols & apps
- Deepest coverage for M2M (ICS/SCADA) & IoT protocols
- Custom signatures support
- Optional device classification for edge access networks
- First Packet Advantage for uniquely effective first-packet processing

Unique Insights

- Identification of anomalous and evasive traffic
- Complex tunneling visibility, with full protocol paths for up to 16 levels of encapsulation
- Extraction of files and embedded links
- ML-enhanced encrypted traffic classification

Fast ramp up

- Ready-to-deploy commercial-grade DPI
- Flexible form factor options (C library, VNF, CNF, SW Sensor)
- Optional built-in rules engine
- Granular, well-structured ready-to-use service and transaction metadata
- Global presence for professional services and support

About 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 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: www.enea.com

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

ENEA

Division Head Office
6 rue Casteres
92110 Clichy, France

www.enea.com