ENEA

WHITE PAPER

How SSE Leaders Use Next Generation DPI for Market Success

Executive Summary

The Security Service Edge (SSE) model is perfectly adapted to today's diverse, distributed enterprise networks. Using edge clouds that boost agility and bring users and resources closer together, SSE provides a convenient, highly scalable way to ensure users can safely access the Internet, Web, SaaS and IaaS services, and private company apps anywhere, anytime, whether they are using managed or unmanaged devices. While SSE solutions share a common set of core components (ZTNA, CASB, SWG, DLP, next generation Cloud FW, WAF, and IDS/IPS), the ingredient that sets SSE market leaders apart is the use of next generation deep packet inspection (NG DPI) to bring differentiation and high performance to each of these key components.

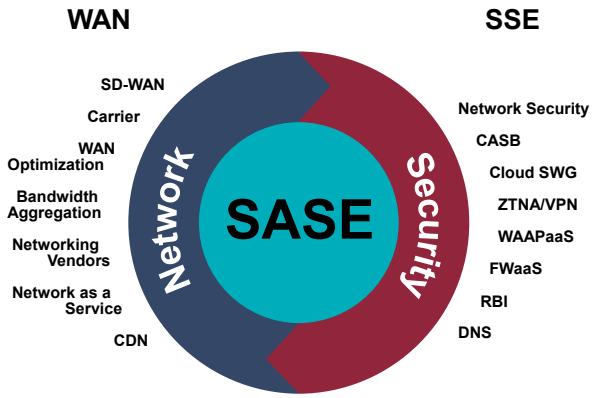
This white paper explains the difference between DPI and NG DPI, details how and where it is used in SSE and describes the functional benefits it brings to the different components, with a list of practical examples for each one. It also looks at whether SSE vendors should build or buy their NG DPI components, comparing open source and commercial products.

CONTENTS

What is Security Service Edge (SSE)?

As enterprise IT functions continue to migrate from the data center to the cloud, the center of gravity for networking and security is shifting there as well. Today's network managers want and need agile, secure access from devices everywhere to resources everywhere, and a distributed cloud architecture offers an effective way to meet this demand.

Gartner's general blueprint for such an architecture is the Secure Access Service Edge (SASE) model. In this model, wide-area networking (WAN) and security are delivered as a unified cloud service.



The security half of this paradigm is represented by what Gartner refers to as the Security Service Edge (SSE), which may be fully integrated with SD-WAN in a single SASE solution, or delivered as a separate cloud security solution that integrates with a partner's (or a vendor's own) SD-WAN offer.

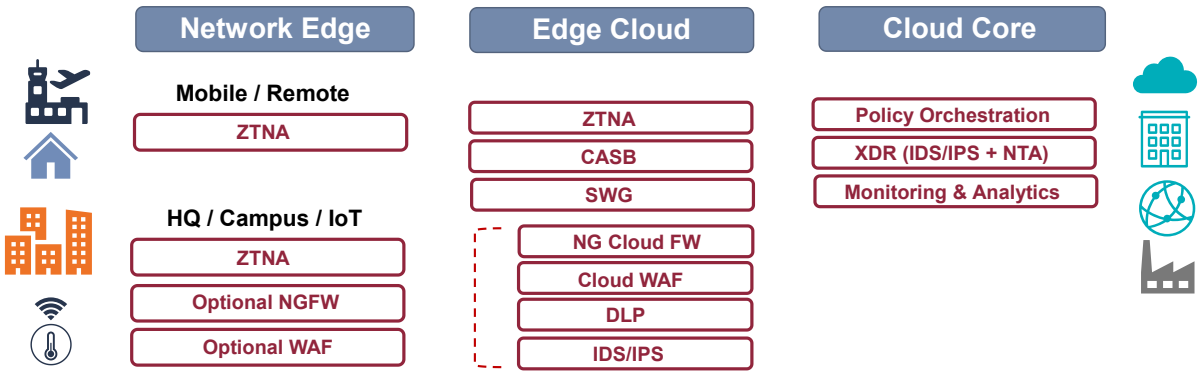
According to Gartner, SSE solutions deliver three primary capabilities:

- Secure access to the **Internet and Web** by way of a Secure Web Gateway (**SWG**).
- Secure access to **SaaS and cloud apps** via a Cloud Access Security Broker (**CASB**).
- Secure remote access to **private apps** through Zero Trust Network Access (**ZTNA**).

Other key components include Data Loss Prevent (**DLP**), a Next Generation Cloud Firewall (**NG CFW**), a Web Application Firewall (**WAF**), and an Intrusion Detection/Prevention System (**IDS/IPS**). These may be deployed as discrete components, or incorporated into an encompassing CASB or SWG.

All these capabilities are provided via edge clouds for scalability and performance, with global monitoring and policy control provided via a core cloud, often accompanied by an Extended Threat Detection and Response (**XDR**) system. Some vendors also offer optional on-premise NGFWs or WAFs to customers who feel they are needed for particularly sensitive locations.

SSE Architecture



What is Next Generation Deep Packet Inspection (NG DPI)?

DPI is a widely deployed technology long used to provide traffic visibility in networking and security solutions. Specifically, it is software that passively analyzes network traffic flows from Layer 2 (data link) to Layer 7 (applications and data) to identify the protocols, applications and services in use, and to extract additional information in the form of metadata to support specific networking and security functions.

Next Generation DPI (NG DPI) has evolved to meet three important challenges:

1) The rise of encrypted traffic, which impacts the essential visibility required to properly manage and secure networks,
2) The emergence of advanced, complex cyberattacks perpetrated by sophisticated criminal actors and nation-states, and
3) The shift to cloud-based solutions, with significantly higher performance and scalability requirements.

NG DPI meets these challenges with these distinguishing capabilities:

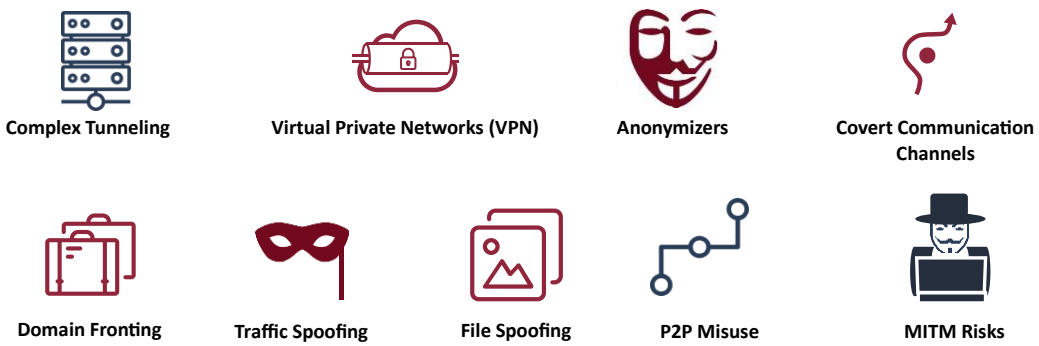
- Encrypted Traffic Classification (ETC).
- Detection of Anomalous & Evasive Traffic.
- Advanced First Packet Processing.
- Extended Protocol & Application Coverage.
- Cloud-Scale Performance.

Encrypted Traffic Classification (ETC)

As the use of encryption expands, and more stringent standards like TLS 1. 3 emerge, NG DPI has developed advanced analytical tools to preserve the traffic visibility required for network management and security—without resorting to decryption (except where required, e.g., for compliance). This helps protect data privacy while also boosting performance.

Methods used to identify applications, categorize traffic, and extract valuable metadata from encrypted traffic include statistical and behavioral analysis, machine learning, DNS-based classification and the use of the first packet processing with advanced multi-tiered caching, with methods often combined for best results.

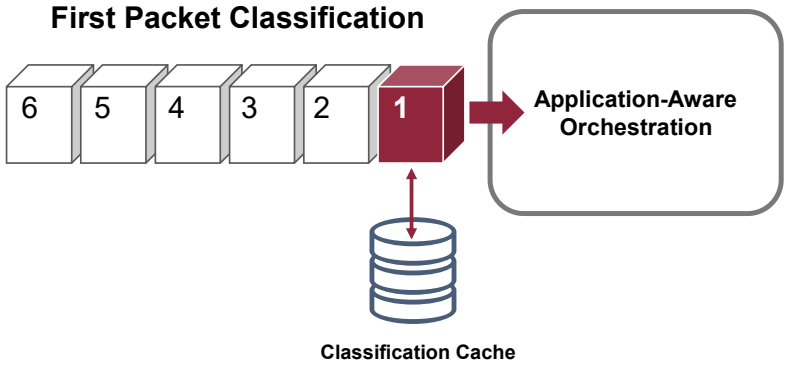
Detection of Anomalous & Evasive Traffic



NG DPI can also produce security-related traffic classification and computed metadata to aid in the detection of advanced threats. This includes identification of evasive techniques like complex tunneling, file spoofing, domain fronting, and the use of covert communication channels, unauthorized VPNs, anonymizers and more. It can also identify anomalous traffic and specific threats, such as potential MITM attacks or the presence of cryptocurrencies and mining pools. It can further extract critical data for analysis by security components, such as embedded links in emails.

Advanced First Packet Classification

First packet processing is a common method of identifying applications by comparing information in the first packet in a flow (e.g., server IP addresses and port information) with a cache of traffic previously classified with DPI.



While this practice is commonly used in SSE and SASE, standard first packet processing scores very poorly in accuracy, granularity and performance. This leaves vendors with an unfortunate choice between passing more traffic through full DPI and reducing speed, or applying security policies based on limited information, thereby introducing potential security risks.

NG DPI addresses this challenge with advanced, machine-learning enhanced first packet processing that produces granular, highly accurate identification of applications and traffic categories, as well as delivering select security-related metadata. As the use of encryption expands and standards harden, this ability to accurately identify protocols and applications from the first packet in encrypted flows will grow in importance.

Extended Protocol & Application Coverage

Conventional DPI engines typically identify a few hundred protocols at best, and many of these haven't evolved in step with the shift to cloud applications and services, the rise of IoT, and the convergence of the IT, OT and Telco industries. An NG DPI engine however, is designed for today's diverse, cloud-centric networks.

It provides accurate coverage of thousands of protocols and applications, with notable depth in those relevant to SSE, including:

- **Cloud and SaaS Applications**
  AWS, Azure, Google AE, Okta, Atlassian, Salesforce, Zendesk, Skype, Dropbox, HubSpot, etc.
- **ICS/SCADA & IoT Protocols**
  Modbus, DNP3, ENIP, GOOSE, OPC, MQTT, PCCC, HDLC over IP, Proficy, Moxa, Alexa, etc.
- **Communication and Content Applications**
  WhatsApp, WeChat, DingTalk, MS Stream, Mango TV, Youtube TV, Kuaishou, Philo, etc.
- **Collaboration and Productivity Applications**
  MS Teams, Slack, Yammer, Sharepoint, Adobe Connect, Ctrip, Fliggy, Office 365, etc.

Also important to SSE is NG DPI's ability to identify service types within applications (e.g. chat, video, voice, file transfer) and custom signatures support for private apps on-premise and in the cloud.

Cloud-Grade Scalability & Performance

Conventional DPI has long been a foundational technology in enterprise cybersecurity. However, traditional DPI can be a resource-intensive technology, and the performance and scalability demands of SSE are very high.

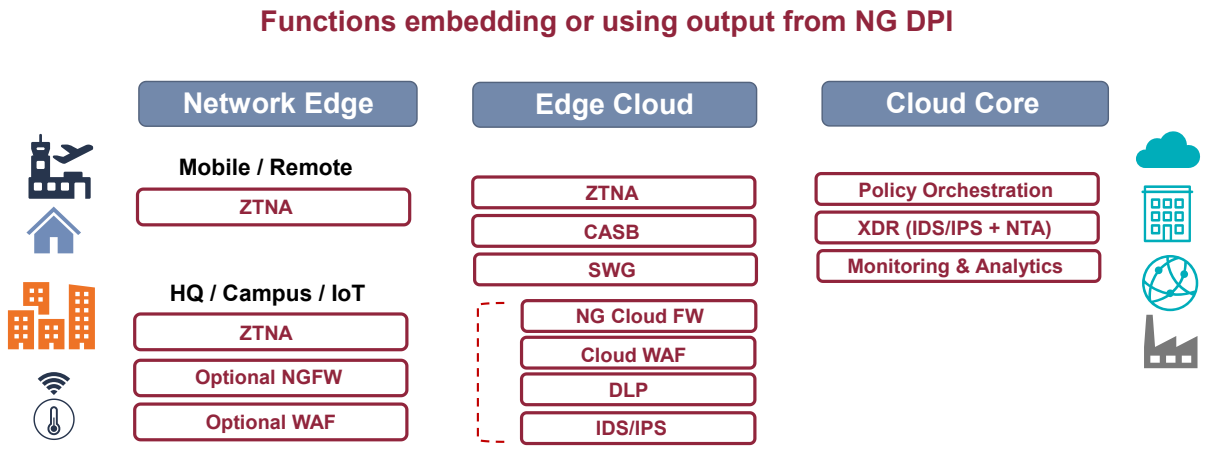
NG DPI meets this cloud challenge in several ways. First, its ability to deliver accurate first packet classification reduces the need for full DPI. And, the high granularity and valuable metadata NG DPI delivers during full DPI processing minimizes the need to use resource-intensive decryption to support inspection.

NG DPI is also unique in that is it is engineered for cloud-scale throughput, speed and scaling requirements. Features include:

- Optimized multi-thread support for high scalability.
- High performance under heavy metadata extraction loads.
- Optimized code for high performance multicore processors.
- Optimized integration with packet processing middleware (e.g., Intel DPDK).
- Support for VPP and hardware acceleration and offloading.
- Cloud-friendly form factors (CNF, SDK, VNF).

Where is NG DPI Used in SSE?

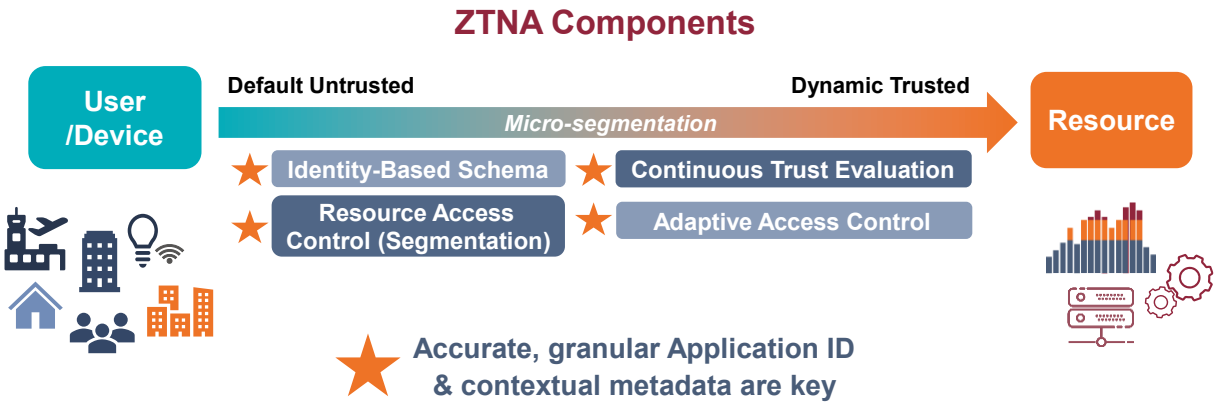
The short answer is—everywhere! To understand how NG DPI capabilities are used within various SSE functions, let's begin with the three SSE pillars: ZTNA, CASB and SWG.



ZTNA (Zero Trust Network Access)

Secure Access to Private Apps (On- or Offsite) for Unmanaged & Managed Devices

The ZTNA model is the cornerstone of SSE. It provides a flexible and convenient complement to (or replacement for) VPNs while strengthening overall network security. Working from a 'trust no one and no thing' vantage point, ZTNA upends the old model of a user connecting to a *network,* to a user connecting to a *resource* – and that resource only – thereby preventing lateral movement.



There are four basic components to ZTNA, with a role for NG DPI in each:

1. **Identity-Based Trust:** In ZTNA, users (people, devices, apps, etc.) are authenticated using an identity-based schema that takes context into account in establishing trust. The contextual data can include single sign-on (SSO) credentials, device ID or profile, location, time, and application risk posture. Context matters in ZTNA because SSE needs to support managed corporate devices and unmanaged devices (BYOD, IoT, etc.), with *agentless* and agent-based options.

   Typically trust evaluation and authentication are performed at the SSE edge cloud closest to the user. However, customers sometimes still request on-premise ZTNA authentication capabilities for some locations.

   In either case, NG DPI in lightweight mode supports initial trust evaluations. It provides contextual data that is valuable because it is based on ultra-reliable telemetry data. This may include device profile, location, and time data as well as first packet identification of private applications and services using custom signatures. This telemetry-based profiling can be a significant aid in repelling spoofing attacks, as well as detecting rogue private apps that are a common problem in shadow IT.

   In the case of on-premise ZTNA authentication, which is not uncommon for SSE within SASE, NG DPI first packet processing supports instant breakout of traffic to the right SSE pillar: ZTNA, SWG or CASB.

2. **Segmentation:** The data gathered in the trust evaluation process is used to support least-privileged access to the target resource using network segmentation. Here, NG DPI provides the ultra-reliable traffic classification required for segmentation. This usually includes metadata and threat indicators to support advanced micro-segmentation and traffic handling rules.

3. **Continuous Trust Evaluation:** In ZTNA, trust is never granted in permanence; it must be continuously earned. This is handled through continuous monitoring supported by NG DPI, which provides real-time traffic analysis that includes the identification of evasive and anomalous traffic.

4. **Adaptive Access Control:** Finally, if the NG DPI-powered monitoring indicates a potential breach, the ZTNA solution can invoke the necessary access controls, such as rerouting or blocking traffic.

EXAMPLES OF ADVANCED ZTNA FUNCTIONS THAT NG DPI ENABLES

- Detect and block a user trying to connect with forbidden anonymizers like Cyberghost or Ultrasurf.
- Prevent domain fronting by revealing the use of routing schemes in Content Delivery Networks (CDNs) and other services that mask the intended destination of HTTPS traffic.
- Detect and block a user trying to connect with RDP or telnet from an unusual location, or to a resource not typically accessed by RDP (traffic that might otherwise be seen as just generic TCP traffic without NG DPI).
- Continuously evaluate trust by monitoring traffic to detect anomalies, such as the transfer of a file using a false MIME type (e.g., an executable masked as an image), or the presence of non-standard tunneling activities over legitimate protocols (such as DNS or ICMP), which may indicate unauthorized or illegal activities.

BENEFITS

- Detect subtle authentication red flags.
- Safely and instantly breakout trustworthy traffic.
- Achieve fine-grained micro-segmentation.
- Rapidly detect and respond to sophisticated breaches of trust.

SWG (Secure Web Gateway)

Secure Access to the Internet, Web & Non-Corporate SaaS for Managed Devices

SWGs are designed to prevent breaches that can occur when corporate devices are used to access non-corporate cloud apps, the Internet and the Web. They also support compliance with access-related regulatory requirements. The functions included in SWG vary by vendor, but they usually include application control, antivirus screening, intrusion detection/ protection, web filtering, sandboxing, SSL inspection and data loss prevention.

Most of these functions are rolled into a NGFW, though some functions are split into separate DLP, WAF, and IDS/IPS components. Some SWG solutions also incorporate a CASB as an SWG service. At a minimum, though, all SWGs inspect inbound Layer 7 HTTP/HTTPs traffic. NG DPI plays a central role in all these SWG functions.

EXAMPLES OF ADVANCED SWG FUNCTIONS THAT NG DPI ENABLES

- Develop fine-grained application controls in line with company policies (e.g., prohibit access to Dropbox or all external file hosts; allow MS Teams but not Zoom).
- Allow full access for certain social networks like LinkedIn, but only partial access to others like Facebook, with a restriction on file uploads, and deny others altogether, like Instagram.
- Prohibit evasive traffic connections over HTTP/S, crypto mining pool traffic inherent to crypto jacking attacks, or P2P apps such as BitTorrent.

BENEFITS

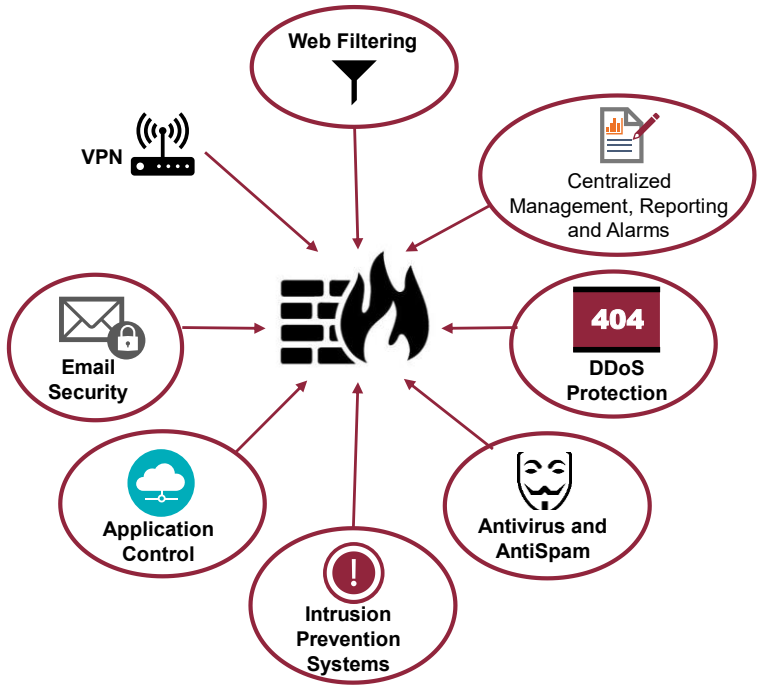
- Develop granular policies based on actions within specific applications.
- Gain reactivity by detecting potential threats from the first packet in a flow.
- Protect privacy by using encrypted traffic classification to reduce the need for decryption.
- Gain efficiency by meeting the inspection needs of multiple SWG functions with a single NG DPI instance.

NG Cloud Firewall (FW) / FWaaS

In the course of developing SSE or SASE offers, many vendors who currently have a basic cloud firewall are seeking to endow it with the application awareness and DPI capabilities found in on-premise NGFWs. Embedding NG DPI is a way to achieve this without ceding roadmap control to NGFW partners. Specifically, embedding NG DPI enables vendors to:

- Develop rules based on an accurate, highly granular identification of applications and services, including evasive traffic.
- Enable efficient security steering or service chaining, from first-packet processing to full DPI to decryption and inspection.
- Improve alerting by reducing false positives.
- Strengthen DDoS, spam and virus protection through deep contextual data about applications, users, data, devices, files and flows.
- Enhance IDS/IPS with significantly expanded whitelists and blacklists.
- Strengthen email security with insights into email sender / receiver addresses, attached files, and embedded links.
- Enhance monitoring and reporting with application-level reporting.

NG Cloud FW Functions Supported by NG DPI



EXAMPLES OF ADVANCED NG CLOUD FW FUNCTIONS THAT NG DPI ENABLES

- Detect a mismatch between a file type and MIME announcement.
- Extract and analyze a URL in an email body.
- Block access to a database if the source IP@ is not valid.
- Incorporate custom signatures into rulesets.
- Use file reconstruction capability to provide objects to anti-virus / malware detection.
- Detect tunneling or obfuscation (protocols such as iodine, openvpn, psiphon, tor, etc.)...

BENEFITS

- Gain roadmap control by transforming a Cloud FW into a NG Cloud FW.
- Accelerate time-to-market by outsourcing a high-maintenance technology.
- Enable smart security steering from the 1st packet.
- Maximize functions that can be executed without decryption.

Cloud WAF (Web Application Firewall)

A WAF protects an organization's web applications by filtering, monitoring, and blocking malicious Layer 7 HTTP/S traffic to and from a web service. While a WAF is typically located in edge clouds in an SSE model, some companies still request an on-premise WAF if they retain any on-premise web-based products or services (ecommerce, finance, logistics, etc.).

Whether on-premise or in the cloud, vendors use NG DPI to enhance WAFs in two important ways. First, because WAF is deployed as an SSL endpoint (proxy) between the enterprise web server and users, full DPI can be run on decrypted traffic. The efficacy of WAF rules can therefore be boosted by using high quality NG DPI results, with NG DPI providing broader and more granular protocol, application and service coverage.

> Attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet.
>
> SANS institute

Through this granular classification and the provision of security-related metadata, NG DPI is used to develop rules to protect against sophisticated Layer 7 attacks, such as SQL Injection, Cross Site Scripting (XSS), DDoS attacks, URL Access, and Cross-Site Request Forgery (CSRF).

At the same time, accurate first-packet processing provides a convenient tool for rapidly expanding application whitelists and blacklists. This strengthens the WAF security posture and can boost performance by eliminating the need for full DPI execution on trusted traffic.

EXAMPLES OF ADVANCED CLOUD WAF FUNCTIONS THAT NG DPI ENABLES

- Reveal applications (e.g., eProxy, HTTP Injector) that combine techniques such as protocol header customization, proxies, tunneling & domain fronting, to evade detection.
- Detect executables concealed in HTTP requests, such as code used in injection attacks (SQL, ORM, EL, LDAP, etc.).
- Detect domain fronting used to evade URL filtering.
- Use metadata and metrics related to traffic flows, applications, services, data, users, and devices for heuristics-based detection of DDoS attacks.

BENEFITS

- Improve detection of advanced Layer 7 attacks.
- Enhance log-based monitoring with ultra-reliable telemetry data.
- Expand whitelists and blacklists.
- Improve detection of malicious traffic using spoofing techniques to avoid detection.

IDS/IPS (Intrusion Detection/Prevention)

Deployed in standalone form or integrated into other SSE components, IDS/IPS plays a valuable role detecting and stopping known cyber-threats, and provides some anomaly-based threat detection as well. However, even the best IDS/IPS solutions (like Suricata) are hampered by limited protocol and application coverage, an inability to analyze encrypted traffic without decryption, and a limited ability to detect new or unknown threats.

Integrating NG DPI with a best-of-breed IDS/IPS solution like Suricata enables vendors to break through these limitations. It is used to:

1) Develop rules that are better adapted to new environments (like multi-cloud networks and hybrid IT/IoT networks),
2) Develop white- and blacklists with the applications most pertinent to a customer's network (including custom and legacy applications),
3) More effectively identify anomalous and evasive traffic (even in encrypted traffic),
4) Speed threat analysis and forensics with meaningful contextual data (while simultaneously reducing the need for full packet capture).

EXAMPLES OF ADVANCED IDS/IPS FUNCTIONS THAT NG DPI ENABLES

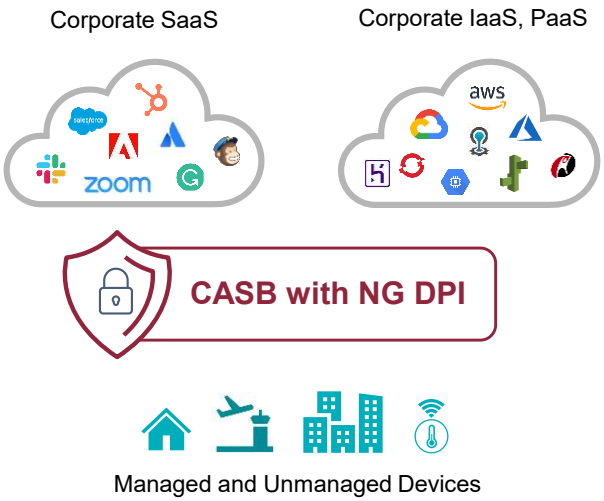
- Extend black-/whitelists with cloud & SaaS apps, ICS/SCADA & IoT protocols, communication and collaboration apps, and business & productivity apps.
- Detect potential TLS session interception (MITM).
- Detect non-standard tunneling activities over legitimate protocols (such as DNS or ICMP).

BENEFITS

- Rapidly expand whitelists and blacklists adapted to SSE environments.
- Safeguard traffic visibility in fully encrypted environments.
- Catch threats that exploit Suricata's publicly-known threat detection methods.

CASB (Cloud Access Security Broker)

CASB's role is to monitor and secure traffic between an organization's approved cloud service providers (SaaS, IaaS, PaaS) and users connecting with either managed or unmanaged devices. CASB is also used to ensure regulatory compliance for an organization's use of cloud services. In addition, CASB plays a discovery role, enabling detailed visibility into cloud app usage to help assess risks and develop appropriate access and usage controls.



CASBs can function in proxy and/or API mode for establishing and managing connections to cloud services. Proxy mode is used for cloud applications and services that:

1) Do not have public APIs (or have APIs that have not been added to the CASB platform),
2) Are not well-suited to API access (e.g., command-and-control oriented tasks), or
3) Have APIs with quality and performance issues, as is often the case with smaller and less well-known cloud apps.

In API mode, CASB establishes connections, monitors traffic, and can perform full scans of both structured and unstructured data at rest in managed cloud apps.

In both modes, NG DPI enhances CASB functions with application-level monitoring and reporting, and the provision of deep contextual data about applications, users, data, devices, files and flows for extended CASB security services, such as DDoS protection, DLP, and malware detection.

And, because of NG DPI's high performance and scalability, it can support the largest multi-tenant CASB deployments on the market. In addition, other unique NG DPI capabilities also enhance CASB performance, such as NG DPI's encrypted traffic classification, which can support safe SSL decryption bypass rules.

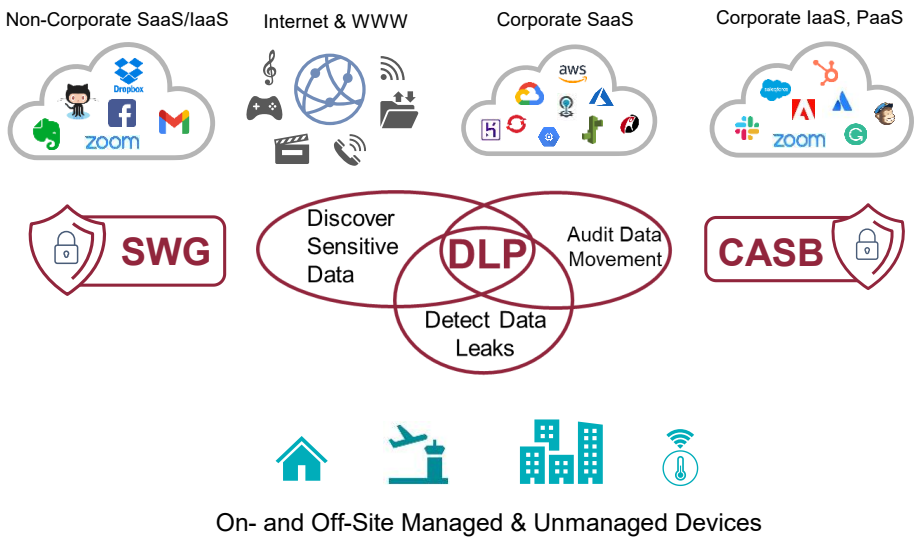
EXAMPLES OF ADVANCED CASB FUNCTIONS THAT NG DPI ENABLES

- Add granularity to CASB policy, for example, transaction-based rules that allow users to access YouTube, but not upload any content to it.
- Deploy CASB agents on managed devices (or a data feed from NG DPI-powered SWG) to discover shadow IT apps that should be brought under CASB management. An example would be to add Dropbox as a sanctioned app (with appropriate rules) after discovering it is widely used within the organization.
- Use detailed NG DPI metadata to build behavioral profiles of users so that anomalous behavior can be detected and investigated.
- Use NG DPI output to build a highly compact audit trail of activities for forensic investigations (reduce storage by up to 150x compared to full packet capture).

BENEFITS

- Enhance CASB with shadow IT discovery.
- Create more accurate - and more compact - audit trails.
- Create accurate behavioral profiles for effective anomaly detection.
- Boost performance for high-volume, multi-tenant deployments without sacrificing granular visibility.

DLP (Data Loss Prevention)



DLP may be integrated into SSE as a single shared resource, or separately embedded in multiple components such as SWGs, CASBs, and NG Cloud FWs. Whatever the architecture, DLP is a must-have function for cloud security.

DLP is used to identify and prevent the theft or misuse of sensitive data, such as social security numbers, financial information or account credentials, and to inspect content and analyze user actions to identify activities that do not comply with company guidelines or government regulations. NG DPI endows DLP with context-awareness to support these essential functions, including:

- Expanded visibility into user identifiers and actions.
- Insights into links and attached files in email.
- Extraction of files and/or file metadata (e.g., file extension, size, type, name, content).
- Access to security metadata that enables the identification of tunneling on protocols like DNS or ICMP.
- Classification of encrypted and evasive traffic.

EXAMPLES OF ADVANCED DLP FUNCTIONS THAT NG DPI ENABLES

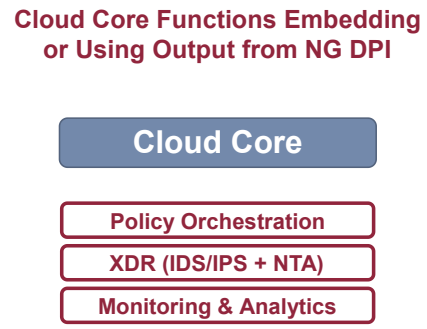
- Use file hashing to detect a subtle discrepancy between a classified, internal use-only file and a file sent out of the organization via email.
- Extract and inspect an emailed file and sender and device data.
- Identify a data loss source and gather the contextual evidence required for incident investigation and remediation.
- Use L7 classification and metadata extraction to rebuild only objects that are relevant for further analysis, e.g., rebuild HTTP objects when the flow is a targeted blog, not YouTube.

BENEFITS

- Detect advanced exfiltration techniques like MITM, file spoofing, and tunneling over standard protocols.
- Enhance rules and monitor usage with application-specific user action metadata (in proxy mode).
- Reduce forensic storage by up to 150x compared to full packet capture.

SSE Core (Controller)

Most SSE solutions feature a centralized cloud controller to orchestrate services and provide globalized reporting across multiple edge clouds. Commonly included capabilities include policy orchestration and automation, extended threat detection and response, global reporting and monitoring, and advanced analytics to enhance customer experience. NG DPI provides the accurate, global traffic visibility these control functions require.



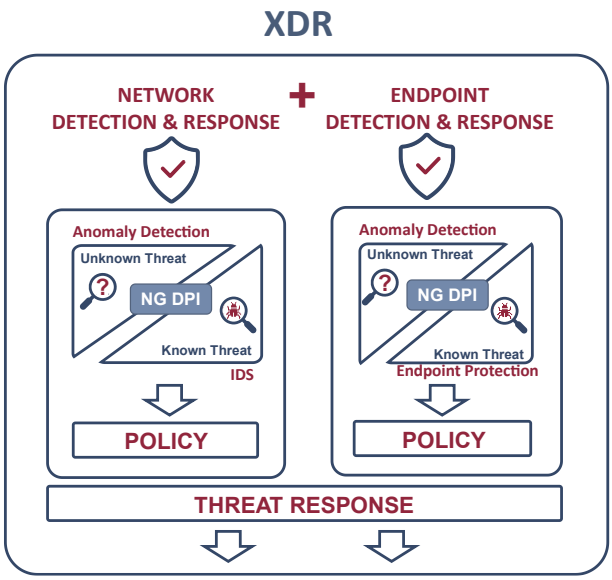
Policy Orchestration & Automation

Policy orchestration and automation is executed using advanced analytics – often ML-based - to ensure standardized, synchronized policies in dynamic environments. SSE vendors depend on NG DPI to deliver the accurate, detailed traffic intelligence needed for granular policy development, and the global traffic visibility required to effectively monitor policy propagation and enforcement across all edge and multi-cloud platforms.

EXAMPLES OF ADVANCED POLICY ORCHESTRATION FUNCTIONS THAT NG DPI ENABLES

- Develop granular application- and action-based policies, such as restricting Facebook actions on managed devices to Logins and Likes only (no file uploads), or blocking its use altogether for all groups other than an organization's social communications team.
- Detect gaps in policy propagation, such as forbidden Box file uploads occurring at several edge locations.
- Discover that unsanctioned Zoom meetings are being used to a greater extent than sanctioned MS Teams meetings, suggesting a need to revisit global SaaS policies for meetings.

XDR (Extended Threat Detection and Response)



With increasingly distributed networks, many organizations have adopted a zero-trust posture that assumes that endpoint and perimeter defenses can and will be penetrated. But while ZTNA strengthens security and reduces attack surface, it cannot provide 100% protection against advanced threats, especially those developed by nation-state actors and sophisticated criminal rings.

This has led to an increased use of behavioral analytics to detect anomalous patterns indicative of an attack. This behavioral analysis is performed on large volumes of enterprise-wide user, device and network traffic data, with rules for actions to be taken to mitigate potential attacks. The resulting solutions—Endpoint Detection & Response (EDR) and Network Detection & Response (NDR)—are increasingly combined into Extended Threat Detection & Response solutions (XDR), with the NDR component of XDR combining network traffic analytics (NTA) and IDS/IPS.

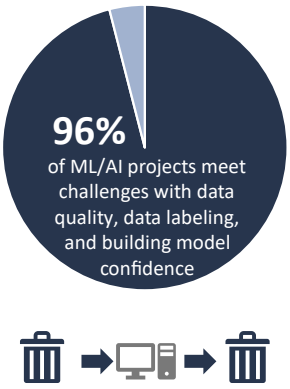
The core cloud controller is the logical location for embedded XDR as it can leverage data consolidated from all SSE functions and edge cloud locations to detect suspicious patterns and behaviors that individual SSE components may have missed.

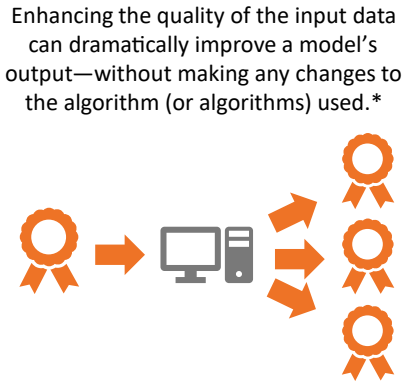
NG DPI is a foundational technology in leading XDR solutions. It provides the reliable, detailed visibility across all types of traffic, whether encrypted or not, and high-quality metadata related to devices, users, files, services and flows, as well as native indicators of compromise.

EXAMPLES OF XDR ACTIONS THAT NG DPI ENABLES

- Gain visibility into traffic using complex tunneling (i.e., multi-layer wrapping of a packet inside another packet), with full protocol paths for multiple levels of encapsulation (up to 16 levels).
- Detect unwanted applications on your network such as crypto miners, untrusted VPNs or games.
- Generate an indicator of compromise when Man in the Middle, Domain Fronting, DGA or other anomalies are detected on the network.
- Detect and analyze the use of remote desktop protocols such as RDP, RFB, TeamViewer, Ammyy admin, and create and enforce rules around them.

Global Monitoring & Analytics





NG DPI is used to support global monitoring, reporting and analytics within and across organizations. It provides detailed traffic visibility at scale for standard network and application performance management (NPM/APM), and supports advanced analytics, especially machine learning, that are used to automate security operations, run behavioral analytics (model hunting and anomaly detection), support product innovation, and optimize user experience.

While NG DPI plays an important role in monitoring and reporting in networking, security and telecommunications markets in general, it is particularly valuable in machine learning applications.

In a recent survey, nearly eight out of ten organizations reported that their ML/AI projects had stalled or been aborted. An overwhelming 96% cited challenges with data quality, data labeling, and building model confidence. These findings support what is common knowledge

among ML practitioners: data quality has an enormous effect on the accuracy and efficacy of ML results. So much so, in fact, that enhancing the quality of the input data alone can dramatically improve a model's output—without making any changes to the algorithm (or algorithms) used.*

This is why ML practitioners rely on NG DPI output to feed their advanced analytics. They know this data is:

- **Accurate**
  It is based on the most trustworthy source available - telemetry data (not insecure log files), and rigorously validated. It is this reliability that enables Tier 1 vendors to use it with confidence in their planning, decision-making and operations.
- **Comprehensive**
  It includes data on *all* network flows provided, and produces highly granular data for these flows, with the broadest protocol coverage in the industry and the availability of thousands of types of packet and flow metadata.
- **Relevant**
  It is precise, contextual data delivered via a framework that offers maximum flexibility in selecting the data features most relevant to the goals of analysts, and to the rules based on that analysis.
- **Real-time**
  It is generated from raw data captured on-the-fly via passive physical or virtual network TAPs that do not affect traffic flow.
- **Always Up-to-Date**
  Updates are continuous and hot-swappable to ensure vendors always stay abreast of constantly changing applications and protocols, and benefit from the latest advancements in data classification, especially for encrypted and evasive traffic.

** See https://bwnews.pr/2UPcZZE and https://bit.ly/3bzgyJ9.*

EXAMPLES OF REPORTING & ANALYSIS THAT NG DPI ENABLES

- Add context to performance reporting with unique insights into users, flows, devices, locations, applications, services, traffic categories, and files.
- Use well-structured, labelled NG DPI output to accelerate data prep tasks.
- Incorporate normally invisible data into machine learning, such as encrypted traffic, encapsulated traffic, and applications, domains and files obfuscated by spoofing techniques.

BENEFITS FOR CONTROLLER FUNCTIONS

- Real-time, global visibility across multi-tenant, multi-edge deployments.
- Granular support for policy development and enforcement.
- Classification of encrypted and evasive traffic.
- Native indicators of compromise captured by metadata.
- High quality data for better ML results.

NG DPI Integration and Implementation

NG DPI plays a foundation role in most SSE components and provides valuable contextual data to all SSE services. This raises the question of how best to integrate it.

Typically, the response comes down to an architectural choice between

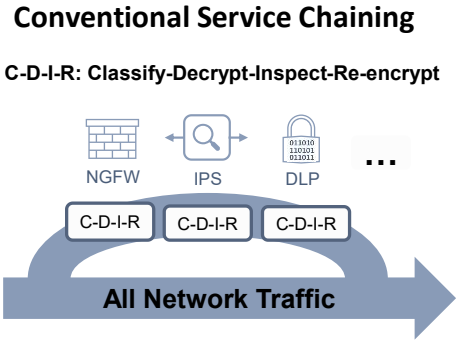
- a conventional service chain architecture,
- a steering model that uses single-pass DPI.

This choice is constrained, of course, by whether the SSE solution is being developed from scratch, or is being constructed via the integration of existing components, possibly coming from disparate business units or acquired companies. In either case, the industry trend in SSE is toward a steering model.

Service Chain Architecture

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. SSE demands a higher performance model.

Conventional Service Chaining

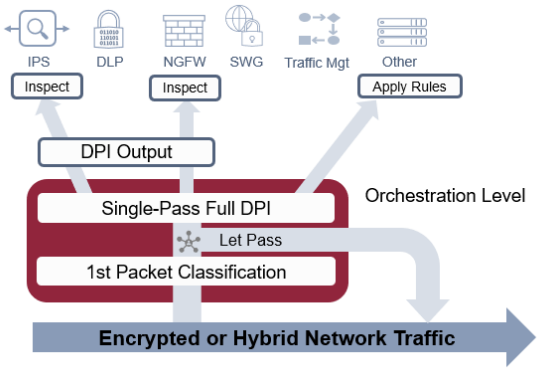


The Steering Model

The steering model is an attractive alternative. In this model, 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 (SWG, CASB, IDS/IPS, NGFW, DLP, etc.).

Using NG DPI, it is possible, for example, to identify an encrypted flow as trusted traffic which can be sent on its way without further analysis (e.g., MS Teams audio call), and a flow that requires full DPI processing, decryption and content (payload) analysis (e.g., SharePoint file transfer).

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) maximizes SSE performance without impacting security.

Integration Accelerators

Some commercial NG DPI solutions propose integration accelerators to help speed and simplify deployment. They can include:

- **Flexible form factor options** such a CNF, SDK, VNF, or standalone software application.
- **Optimized integration** with packet processing middleware (e.g., Intel DPDK).
- **Support for Vector Packet Processing (VPP), Hardware Acceleration and Offloading**, with configuration options for optimal integration with custom flow managers.
- **Independent core-decoding framework** and protocol plugin library, which translates into fast flow signature updates while preserving engine stability. (Protocol plugins should always be hot-swappable.)
- **A highly configurable flow manager architecture** that can handle standard, tunneled and multiplexed flows while allowing different memory allocation modes with maximum flexibility.
- **Support for multiple instances of the DPI component** for maximum implementation flexibility.
- **Professional services** that can help with configuration and integration. They can speed deployment and ensure that product capabilities are fully leveraged within the SSE solution.

Build or Buy?

The choice for DPI is the same as for all software: one can develop it internally or integrate existing commercial or open source solutions. The protocol coverage, performance and accuracy of open source DPI is wholly insufficient for commercial SSE solutions (outside of early prototyping, perhaps).

Developing NG DPI in house is an appealing choice for vendors who generally avoid the use of third-party software in their solutions. However, in the case of NG DPI, the time and resource commitments required to develop commercial grade NG DPI capabilities are enormous. NG DPI is a highly 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 SSE market, trying to develop - or even simply maintain - NG DPI in house can have a negative impact on time-to-market and competitiveness.

This is why most SSE vendors choose to source NG DPI from a commercial provider. There are traffic intelligence products that have been developed by dedicated experts over many years, and the quality and level of detail they have achieved is impossible to reach within project timelines by in-house developers.

Best-of-breed commercial NG DPI products have huge, ready-to-use protocol libraries and use a variety of custom techniques to identify, classify and categorize encrypted traffic as well as detect anomalies indicative of breaches. Delivered as software components that can be embedded in SSE vendor solutions, they not only accelerate product development cycles, optimize costs and lower risks, they also ensure that visibility levels are maintained over time through constant monitoring and updating of the protocol libraries.

Conclusion

Every vendor has a unique approach to designing and implementing SSE, as well as a strategy for integrating it with SD-WAN technology to meet the growing market demand for SASE solutions. Whatever the strategy chosen, SSE, SD-WAN, and SASE all share a common need for universal, real-time application awareness.

In SSE, DPI is a must-have to achieve this global application awareness, and to support all key SSE functions, including SWG, CASB, NGFW, WAF, DLP and XDR. To reach market leadership, however, conventional DPI is not enough.

A high performance, commercial-grade next generation DPI engine is a must for meeting the very specific needs of the converged, cloud-based security environment of SSE. Only NG DPI can deliver vital capabilities like encrypted traffic classification, detection of anomalous and evasive traffic, accurate first packet classification, extended protocol & application coverage (with deep Cloud, SaaS, ICS/SCADA & IoT, and Business application coverage), and cloud-grade scalability and performance.

BENEFITS OF EMBEDDING NG DPI IN SSE

- Accelerated time to market.
- Product differentiation through enhanced threat detection, granular policies and rules, discovery of shadow IT, stellar performance, and application-level monitoring.
- Freedom from constant protocol updating and monitoring.
- Fewer false positives and faster investigation of alerts.
- Lower cost than developing in-house NG DPI.

Enea Qosmos ixEngine®

Enea's Qosmos ixEngine is the market leading commercial grade, NG DPI-based traffic intelligence engine. It is a best-of-breed product that provides Layer 2 to Layer 7 traffic classification and metadata extraction. Using specially-developed traffic identification techniques, it goes beyond traditional DPI to provide next-generation network intelligence that is essential for SSE success:

Maximum Visibility

- Broadest and most accurate protocol coverage.
- 4000 protocols & 5600+ 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.

4 of the Top 5 SASE Vendors
Embed Qosmos ixEngine

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

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.

Learn More

Discover full details of the Qosmos ixEngine at www.qosmos.com/products/deep-packet-inspection-engine/

The full list of protocols recognized by Qosmos technology is available at protobook.qosmos.com

If you would like to know why 4 of the 5 top SASE vendors trust Enea Qosmos technology to fulfill their traffic intelligence needs or to see a demonstration, please contact us at info.enea.com/contact-us-qosmos

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day. Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security.

For more information: www.enea.com

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