Solution Brief

Network Detection and Response
Cybersecurity

Enea Qosmos Probe Shows High Performance for Cyber Security

Enea's next-gen deep packet inspection software, brings full visibility to high-traffic dynamic networks. Tests with 3rd Gen Intel® Xeon® processors, show increased performance and scalability[1]

The constant increase of network traffic in private and public networks can potentially make traffic inspection hardware cost prohibitive. The ability to analyze packets at line rate with advanced detection methods is mandatory for sensitive networks. While many applications depend on visibility to data flows on the network, it is especially important for advanced cybersecurity applications to instantly see packets to analyze them and minimize risk of a cybersecurity breach.

To gain ubiquitous visibility and eliminate cyber security blind spots, Enea*, a member of the Intel® Network Builders ecosystem, has been working with Intel architecture-based servers to test the performance of its Qosmos Probe*, an advanced, deep packet inspection (DPI)-based classification network traffic sensor that recognizes more than 4,000 protocols and applications. Qosmos Probe is an application based on the Qosmos ixEngine market-leading embedded software development kit (SDK).

Emerging Security Applications Need Packet Visibility

In a recent 2022 survey by Evanta* (a Gartner* company), the top issue facing CIOs is cybersecurity with challenges caused by the quickly changing landscape and legacy technology.[2] Traffic throughput is increasing in all types of networks, with IP traffic volume tripling in the past 5 years[3]. Cyber threats are getting more sophisticated and spread even faster on high-speed networks, challenged by shadow IT devices and highly incentivized cyber criminals.

The growing prevalence of cloud computing, virtualization, containerization, micro-segmentation, dynamic provisioning, hybrid workforces, and an explosion in the volume and types of end devices have transformed networks into constantly evolving ecosystems. As a result, it's no longer easy to get full traffic visibility needed to ensure network performance, availability, and security simply by embedding traffic intelligence software on firewalls and a few core network devices. This software needs to be embedded on virtualized servers throughout the network and have the agility to evolve with the network to provide the visibility needed for always changing network environments.

Cybersecurity is one key area that benefits from virtual sensors. Network detection and response (NDR) and extended threat detection and response (XDR) systems are increasingly used to identify advanced cyber threats that evade conventional endpoint and perimeter defenses, these systems need accurate understanding of traffic flows from all parts of the network and at all throughput speeds. This requires a combination of traffic intelligence software and hardware technology capable of processing packets efficiently at line rate.

Network Benefits of Qosmos Probe

- High degree of information granularity
- Fully customizable extraction of traffic information and KPIs
- Probing can be turned on and off to investigate issues only when needed
- A single probing approach for hybrid environments with services running across both physical and virtual interfaces
- Follows network functions virtualization (NFV) standards for future proofing

CPU performance makes the difference in allowing DPI software to examine all seven layers of a data packet and make a forwarding decision at wire speed. In tests conducted by Enea and detailed in the paper below, 3rd generation Intel® Xeon® Scalable processors showed up to 43% better throughput for a probe application.

Qosmos: Performance and Agility

The Qosmos Probe identifies and classifies network traffic, and provides detailed information about traffic flows, building a strong and accurate data foundation for XDR traffic analysis, threat identification, and network protection activities.

The Qosmos Probe delivers the same exceptional layer two to layer seven flow classification and metadata extraction (see Figure 1) as the Qosmos ixEngine in an application that can be readily deployed on commercial off-the-shelf hardware alongside any node, anywhere in an organization's physical, virtual, or cloud infrastructure. The Qosmos Probe provides complete, real-time visibility into all network traffic, including encrypted and evasive traffic, and it supports Internet of Things (IoT) and Supervisory Control and Data Acquisition (SCADA) traffic for hybrid information technology (IT) and operational technology (OT) networks. It also offers the comprehensive data required for understanding network transactions and user behavior.

In addition to working with EDR/XDR systems, the Qosmos Probe provides essential data that complements intrusion detection systems (IDS) and intrusion protection systems (IPS), feeds anomaly detection algorithms in the machine learning module, and enables the creation of stronger algorithms.

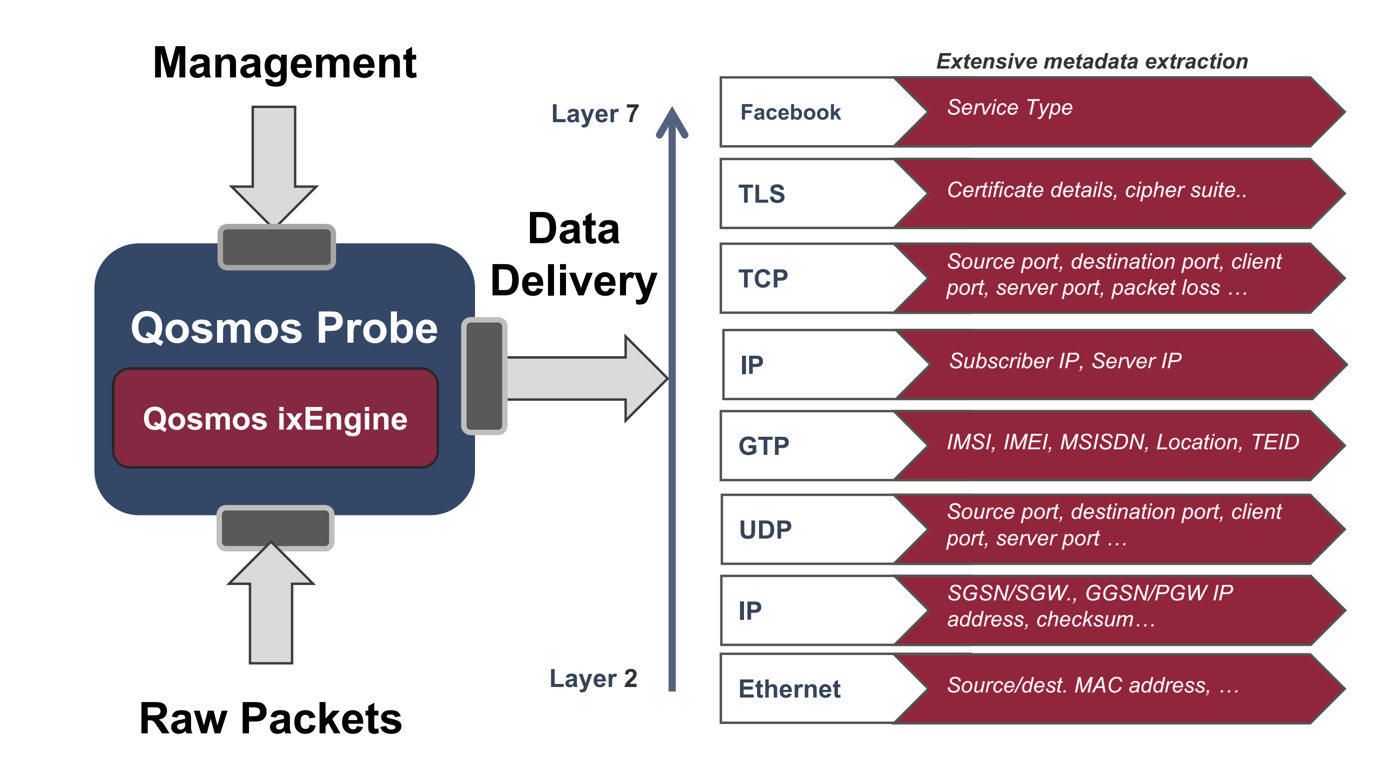
Management
Qosmos Probe
Qosmos ixEngine
Raw Packets
Data Delivery
Layer 7
Layer 2
Extensive metadata extraction
Facebook
Service Type
TLS
Certificate details, cipher suite..
TCP
Source port, destination port, client port, server port, packet loss …
IP
Subscriber IP, Server IP
GTP
IMSI, IMEI, MSISDN, Location, TEID
UDP
Source port, destination port, client port, server port …
IP
SGSN/SGW., GGSN/PGW IP address, checksum…
Ethernet
Source/dest. MAC address, …

Figure 1. Qosmos Probe and Qosmos ixEngine provide deep packet inspection.

Intel® Xeon® Scalable CPUs are crucial for the overall XDR solution performance, scale, and efficiency, delivering the extensive processing capacity required by the XDR application to complete tasks in real-time, at high traffic rates with cost-effective CPU optimization. With support for higher memory speeds, enhanced memory capacity, and up to four-socket scalability, Intel® Xeon® Gold 6300 processors deliver improved performance, enhanced memory capabilities, advanced security technologies, and built-in workload acceleration. 3rd Gen Intel® Xeon® Scalable processors include Intel® Software Guard Extensions (Intel® SGX), which protects data and application code in real time from the edge to the data center and multi-tenant public cloud. For faster virtual networking, the software also makes use of Intel-developed, open source Data Plane Development Kit (DPDK), a collection of libraries that accelerate packet processing workloads.

Qosmos Probe is a culmination of Enea's extensive experience as the leading provider of commercial-grade traffic classification software for cybersecurity and networking solutions. The probe can classify more than 4,000 protocols and applications and can extract more than 5,600 types of metadata, including metadata that help cybersecurity analysts detect man in the middle attacks, domain fronting and evasive traffic. In addition, the software provides endpoint identification.

Qosmos Probe Test Set Up

To test the throughput performance of the Qosmos probe, Enea and Intel joined forces to test the probe on servers using two generations of Intel® Xeon® Scalable processors. The tests used real-world network traffic and measured the performance and scalability of both the classification-only and classification + metadata data export models.

The software used to benchmark performance and scalability for the test was the Qosmos Probe 2.7 running on two single-socket systems under test (SUT). The first SUT (Gen2 SUT) is a server that uses a 2.20 GHz Intel® Xeon® Gold 6238R processor, part of the 2nd Generation Intel® Xeon® Scalable processor family. The CPU supports PCIe Gen3.0 and has six memory channels.

The other configuration (Gen3 SUT) is a server based on a 2.20 GHz Intel® Xeon® Gold 6338N, part of the 3rd Generation Intel® Xeon® Scalable processor family. Delivering modern performance and security that scales with business needs, Intel® Xeon® Scalable processors are optimized for common, critical, and emerging usages. The processors offer optimized performance, scale, and efficiency across a broad range of workloads. The CPU supports PCIe Gen 4.0 and has eight memory channels.

While the CPUs in both SUTs operate at the same clock frequency, the performance from the Gen3 SUT is higher because it has more cores (32 compared to 28 for the Gen2 SUT). The scalability test results (Fig. 4) also show that the Gen3 SUT performance benefits from additional processing efficiencies and additional memory cache.

Hyperthreading was turned on for the tests which lets the operating system treat each physical core as two virtual cores. This gave a capacity of 64 cores for the Gen3 SUT and 56 cores for the Gen2 SUT. The Intel-developed, open-source Data Plane Development Kit (DPDK) libraries were utilized for even load distribution. Total memory in both systems was 512 GB DDR4 RAM.

The software used for the tests was version 2.7 of the Qosmos probe. For the Gen3 SUT, 44 hyperthreaded (HT) cores were dedicated to the probe for DPI, 16 HT cores for data export and 1 physical core for DPDK. The Gen2 SUT was allocated 38 HT cores for DPI, 14 HT cores for data export and one physical core for DPDK.

Data Export

The tests measured both the classification-only export mode as well as classification and metadata. The classification only tests involved flow aggregation per IP/server port/application and flat JSON frames sent every 10 seconds over UDP. The classification + metadata tests involved one record per flow with classification results and metadata for HTTP, HTTP2, SSL/TLS, QUIC, DNS and SMTP. It used structured JSON frames sent over UDP at flow expiration.

Emulating a data center server, the test network connected a TRex open source stateful traffic generator to a switch using a 25GbE network adapter (see Figure 2). Boosted by DPDK, TRex generates L3-7 traffic, with support for multiple streams, the ability to change any packet field, and provides per stream/group statistics, latency, and jitter. Acting as both a client and sender, TRex sent data to the switch, which mirrored the packets and forwarded them to the Qosmos probe on a 100 GbE link.

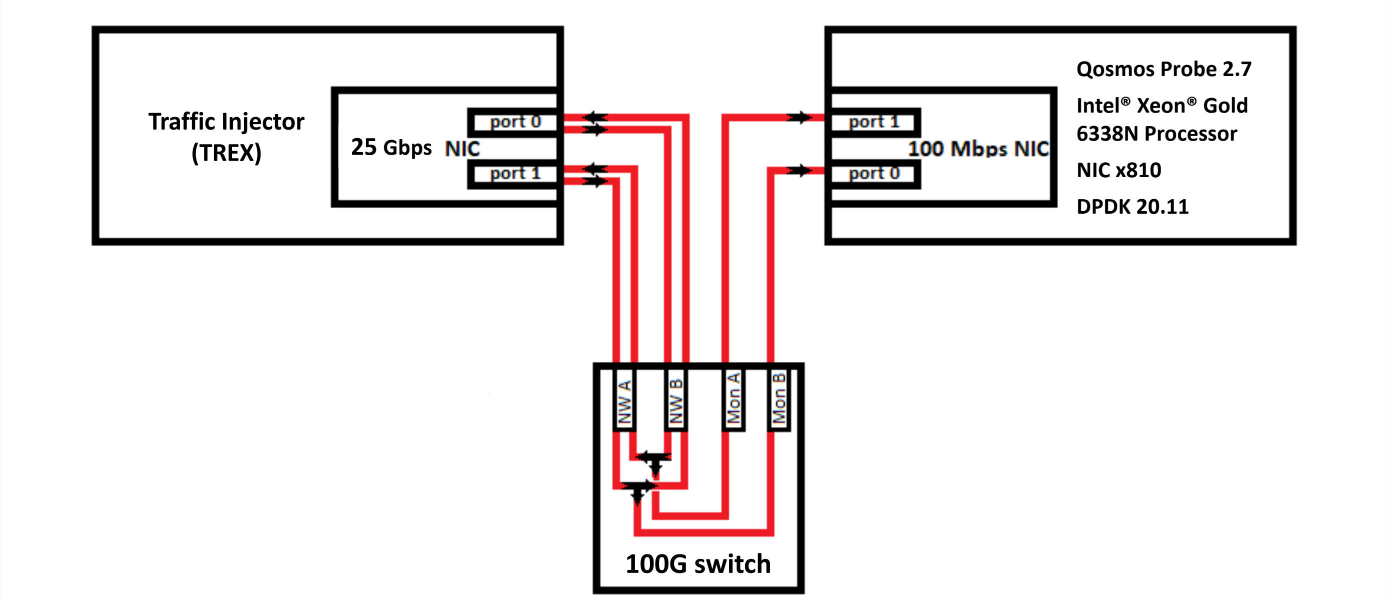

Figure 2. Data flow through the test network.

Test Results

As seen in Figure 3, the test scenarios produced max throughput of 36 Gbps on a single CPU for classification-only testing, and max performance of 26.4 Gbps on a single CPU for full flow classification + metadata tests. This is a generational performance gain of 21% for classification only testing and a 43% performance increase when the metadata tests results were conducted.

Scalability

Performance scalability was also tested (see Fig. 4) to demonstrate the impact of more efficient processing on the performance. The tests showed that CPU performance was comparable up to eight cores, at higher core counts, the performance of the 3rd generation CPU scales significantly faster. The Gen3 SUT performance difference at 38 cores illustrates the comparable generational performance advantage of the latest processor. In the tests, the Gen3 SUT showed 32% better performance in the classification and metadata tests and 17% better performance in classification only tests at 38 cores.

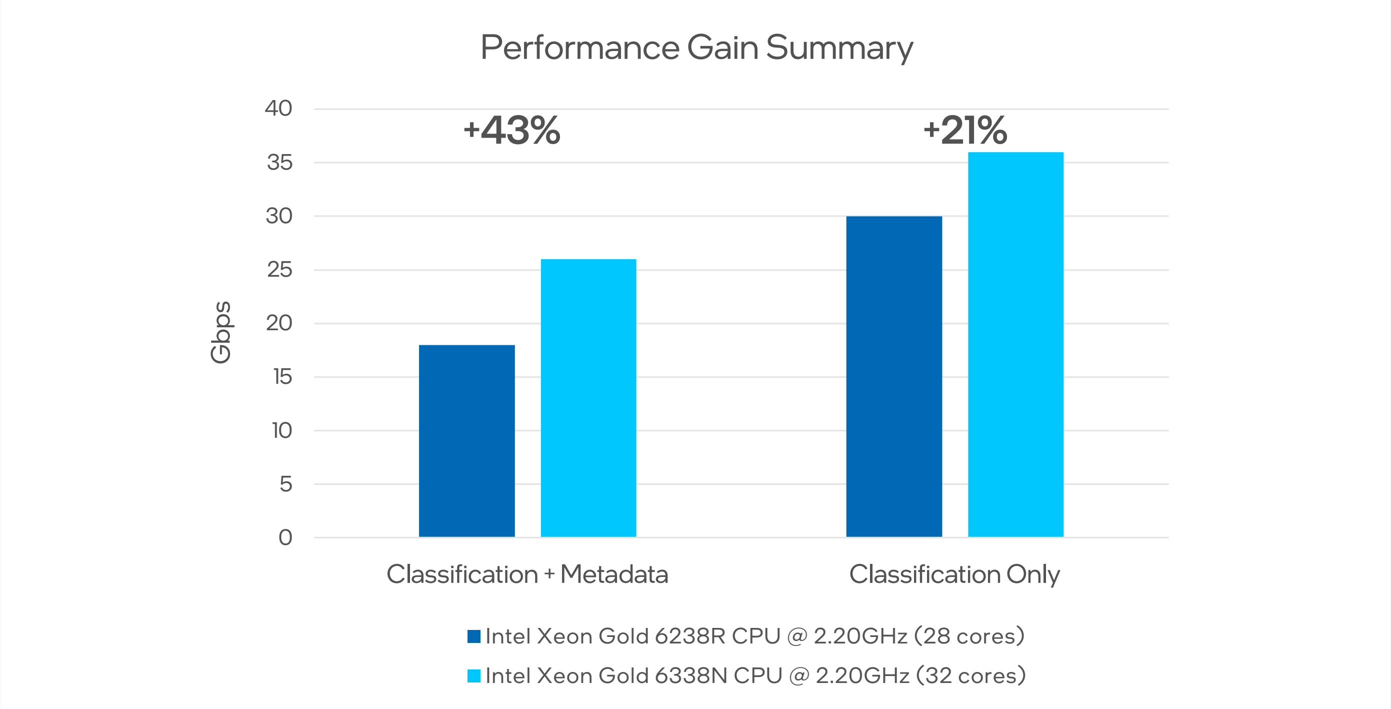

Figure 3. Gen-over-gen performance increases for Qosmos probe running on Intel® Xeon® Scalable processors (higher is better).

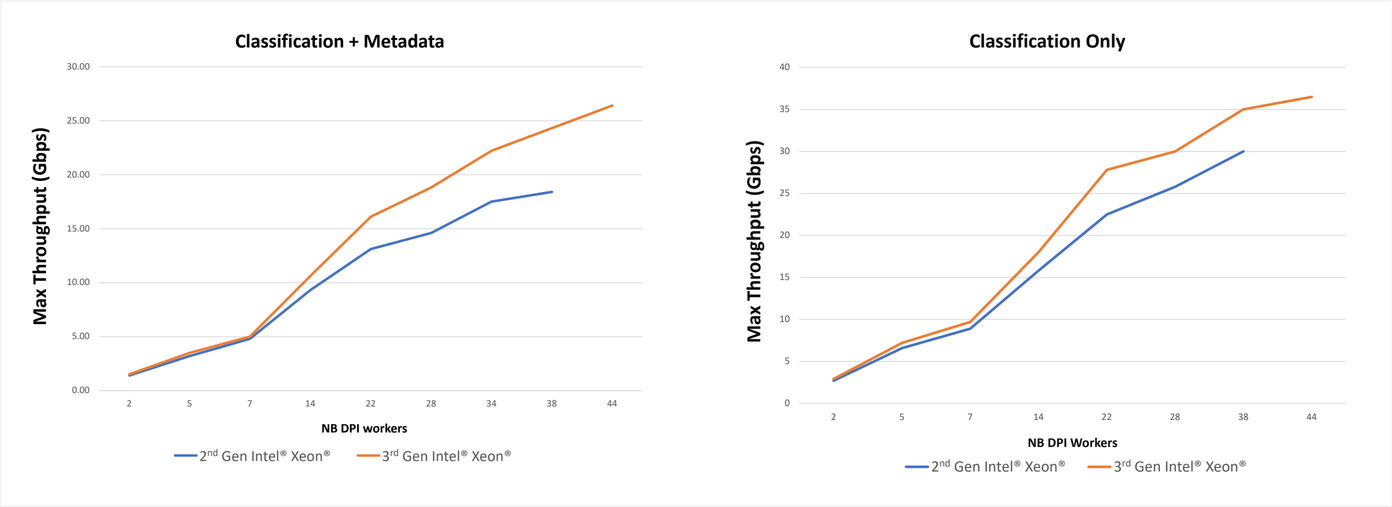

Figure 4. Scalability tests show the higher performance of the 3rd generation Intel® Xeon® Scalable processor's architecture (higher is better). At 38 cores, the tests show the comparable generational performance improvement.

Conclusion

Software probes provide the valuable DPI needed for network security applications to do their job. These probes must have performance and agility to capture the right data flows in real time. Enea's Qosmos Probe demonstrates significant performance increases when used on the latest Intel Xeon Scalable processors. Utilizing the 3rd generation Intel® Xeon® Gold 6338N CPUs, tests of the Qosmos probe showed marked improvement in performance gain and scalability with Qosmos Probe classification-only and with a significant improvement with classification + metadata. Using the 32 cores CPU with optimized hyperthreading, the new architecture in the 3rd generation improves scalability, is more efficient, and the memory cache is optimized.

Learn More

Qosmos

Enea

Intel® Xeon® Gold Processors

Intel® Network Builders

Notices & Disclaimers

[1] New: 2-node, 2x Intel® Xeon® Gold 6338N on zis21 with 512 GB total DDR4 memory, microcode 0xd000230, HT yes Turbo no CentOS Linux 7.9.2009, 3.10.0-1160.el7.x86_64, 1TB SATA, Qosmos Probe 2.7.0, Compiler GCC 7.5.0, 37 libs, test by Enea on 07/1/2022.

Baseline: 2-node, 2x Intel® Xeon® Gold 6238R on uber-probe with 256 GB total DDR4 memory, microcode 0x5003302, HT yes Turbo no CentOS Linux 7.9.2009, 3.10.0-1160.el7.x86_64, 256 GB SATA, Qosmos Probe 2.7.0, Compiler GCC 7.5.0, 37 libs, test by Enea on 07/1/2022.

[2] https://www.evanta.com/resources/cio/infographic/2022-cio-leadership-perspectives

[3] https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

0123/LV/H09/PDF ♻ Please Recycle 354050-001US