ENEA

Intel® Network Builders
PARTNER
intel.
networkbuilders.intel.com

Strengthening Threat Detection with DPI-Based Traffic Intelligence

Sebastien Synold, Product Manager, DPI & Traffic Intelligence, Enea

Erik Larsson, Head of Marketing, DPI & Traffic Intelligence, Enea

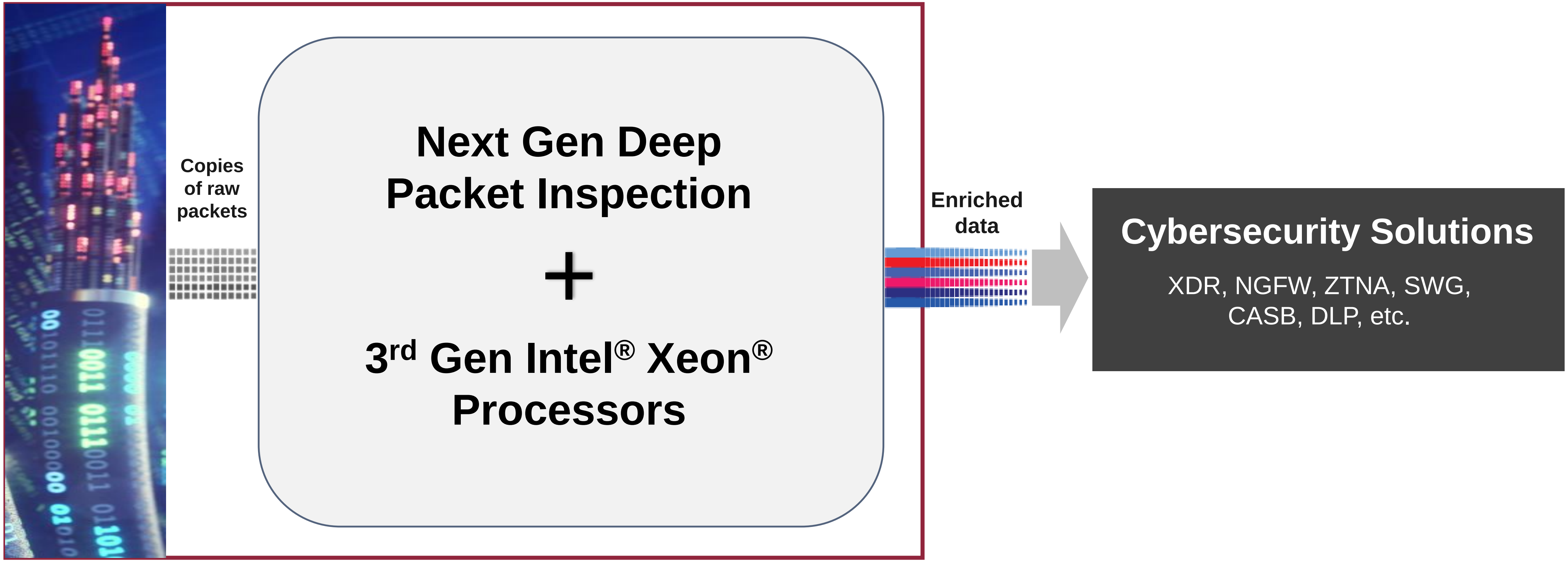
Tuesday, December 6th 2022

Speakers

Erik Larsson
Head of Marketing
DPI & Traffic Intelligence

Sebastien Synold
Product Manager
DPI & Traffic Intelligence

Summary: Strong Cybersecurity Needs DPI + Intel Xeon



Copies of raw packets

Next Gen Deep Packet Inspection

+

3rd Gen Intel® Xeon® Processors

Enriched data

Cybersecurity Solutions

XDR, NGFW, ZTNA, SWG, CASB, DLP, etc.

Contents

- About Enea
- Next Gen Deep Packet Inspection
- eXtended Detection and Response
- Enea Qosmos Probe
- Test results with 3rd Gen Intel® Xeon® Processors
- Summary

ENEA

About Enea

Publicly Listed

NASDAQ

Stockholm

Revenue (MUSD)

~100

No. of Employees

~650

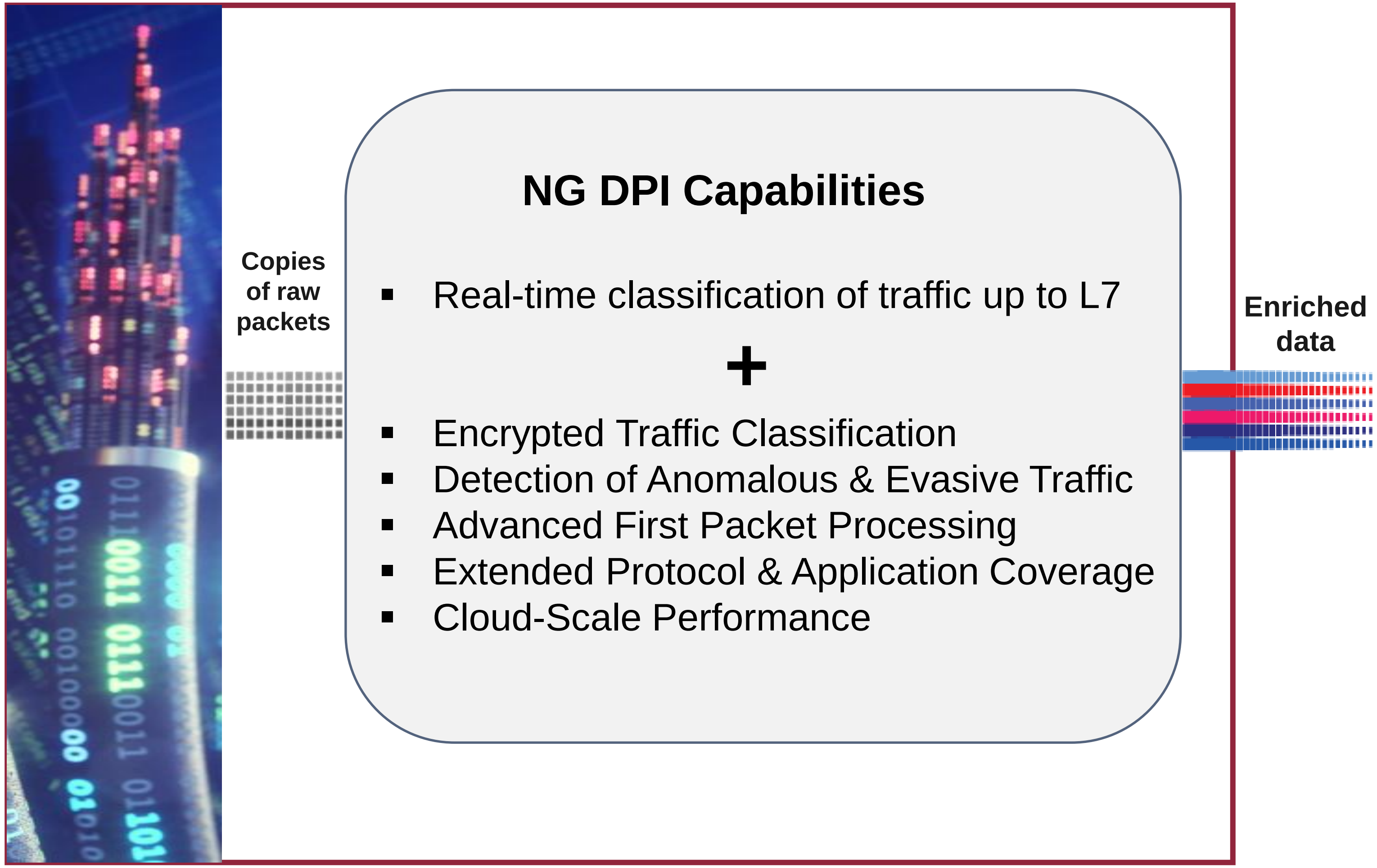
Enea's Qosmos product line is the most widely used Deep Packet Inspection software by telecom and cybersecurity vendors

Contents

- About Enea
- Next Gen Deep Packet Inspection
- eXtended Detection and Response
- Enea Qosmos Probe
- Test results with 3rd Gen Intel® Xeon® Processors
- Summary

ENEA *Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries*

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



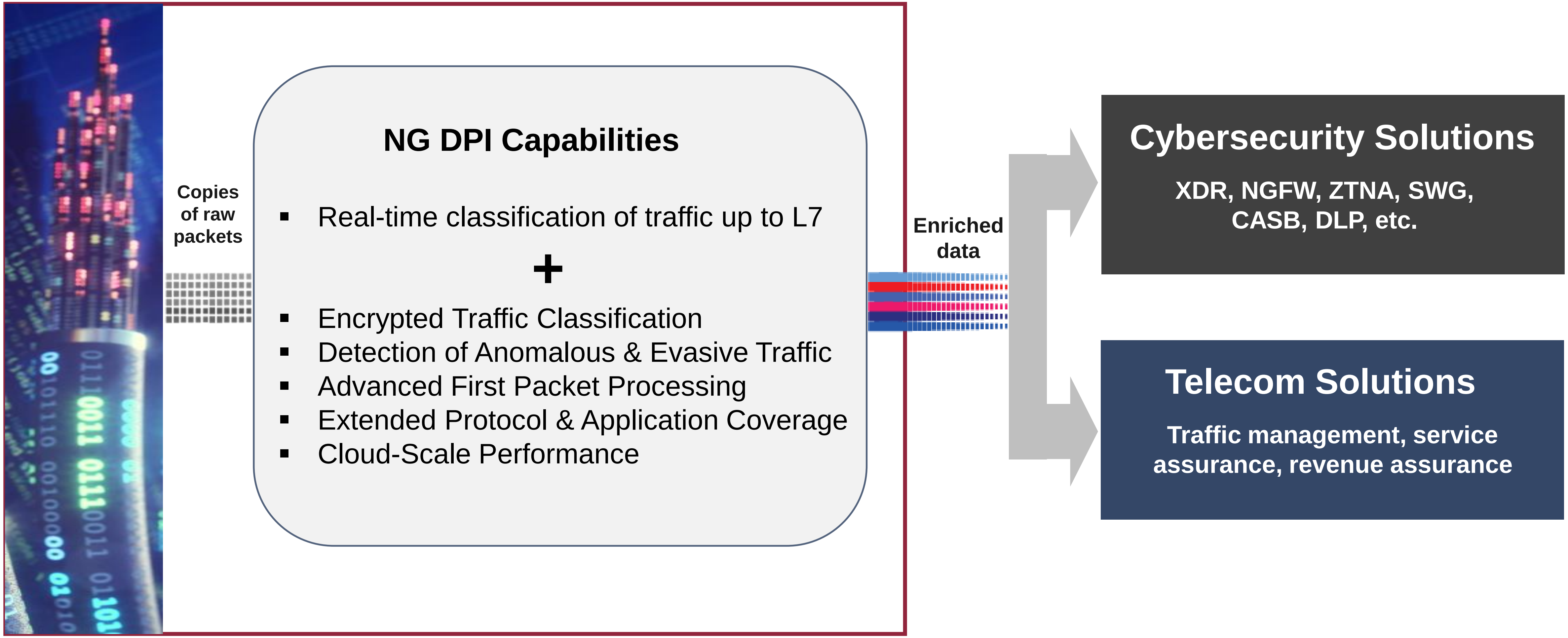
NG DPI Capabilities

- Real-time classification of traffic up to L7

+

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

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



Copies of raw packets

NG DPI Capabilities

- Real-time classification of traffic up to L7

+

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

Enriched data

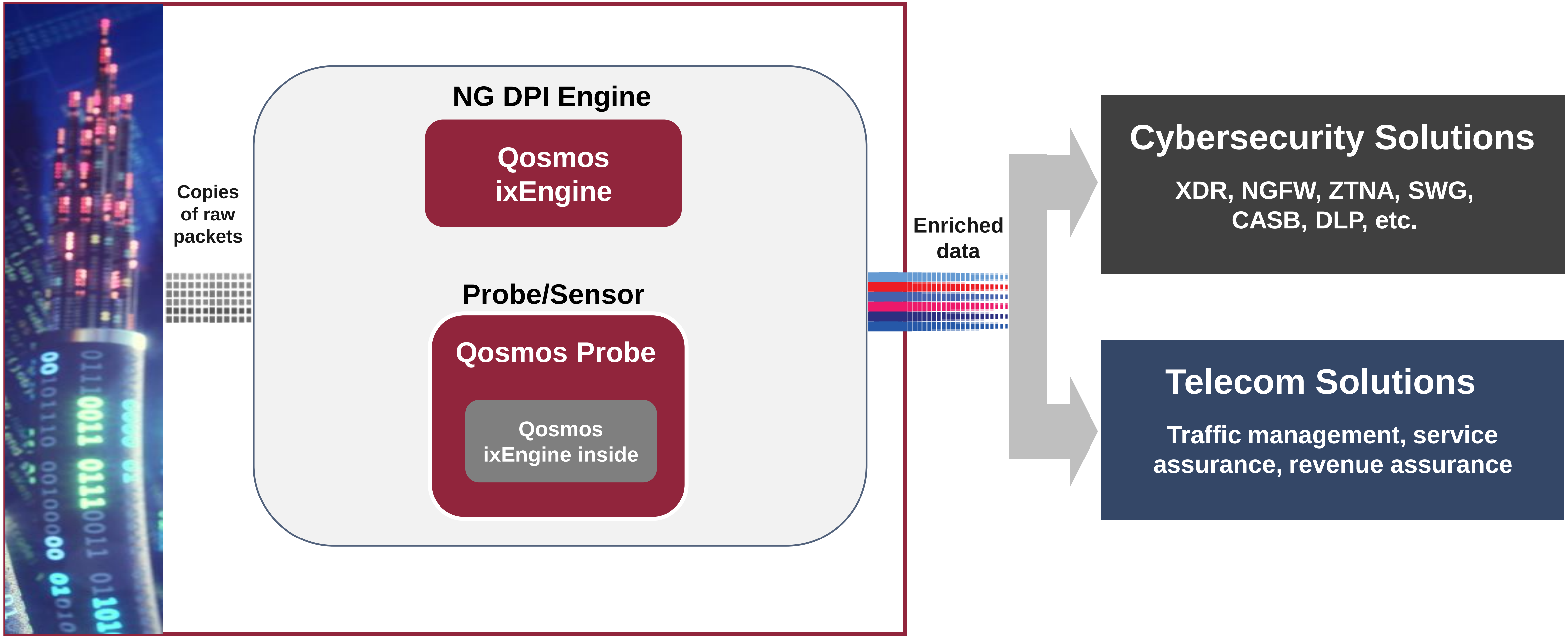
Cybersecurity Solutions

XDR, NGFW, ZTNA, SWG, CASB, DLP, etc.

Telecom Solutions

Traffic management, service assurance, revenue assurance

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



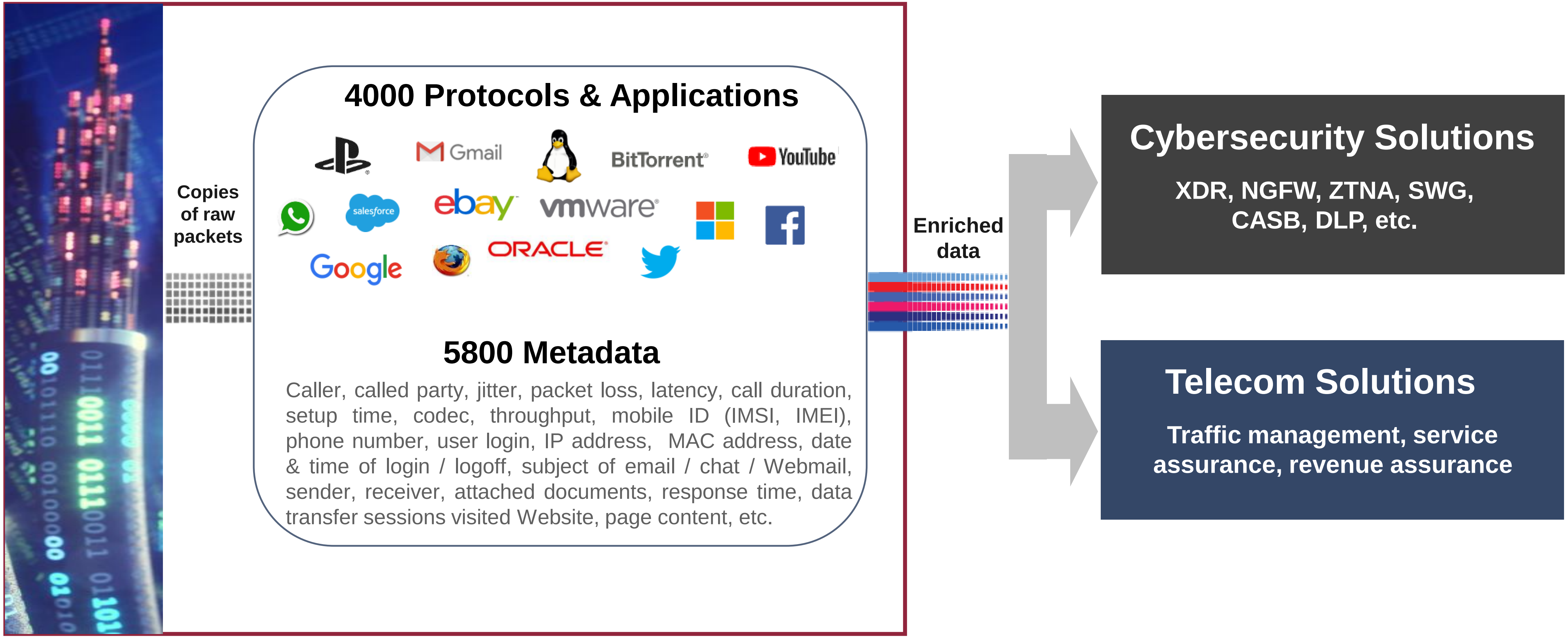
Cybersecurity Solutions

XDR, NGFW, ZTNA, SWG, CASB, DLP, etc.

Telecom Solutions

Traffic management, service assurance, revenue assurance

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



Copies of raw packets

4000 Protocols & Applications

5800 Metadata

Caller, called party, jitter, packet loss, latency, call duration, setup time, codec, throughput, mobile ID (IMSI, IMEI), phone number, user login, IP address, MAC address, date & time of login / logoff, subject of email / chat / Webmail, sender, receiver, attached documents, response time, data transfer sessions visited Website, page content, etc.

Enriched data

Cybersecurity Solutions

XDR, NGFW, ZTNA, SWG, CASB, DLP, etc.

Telecom Solutions

Traffic management, service assurance, revenue assurance

ENEA

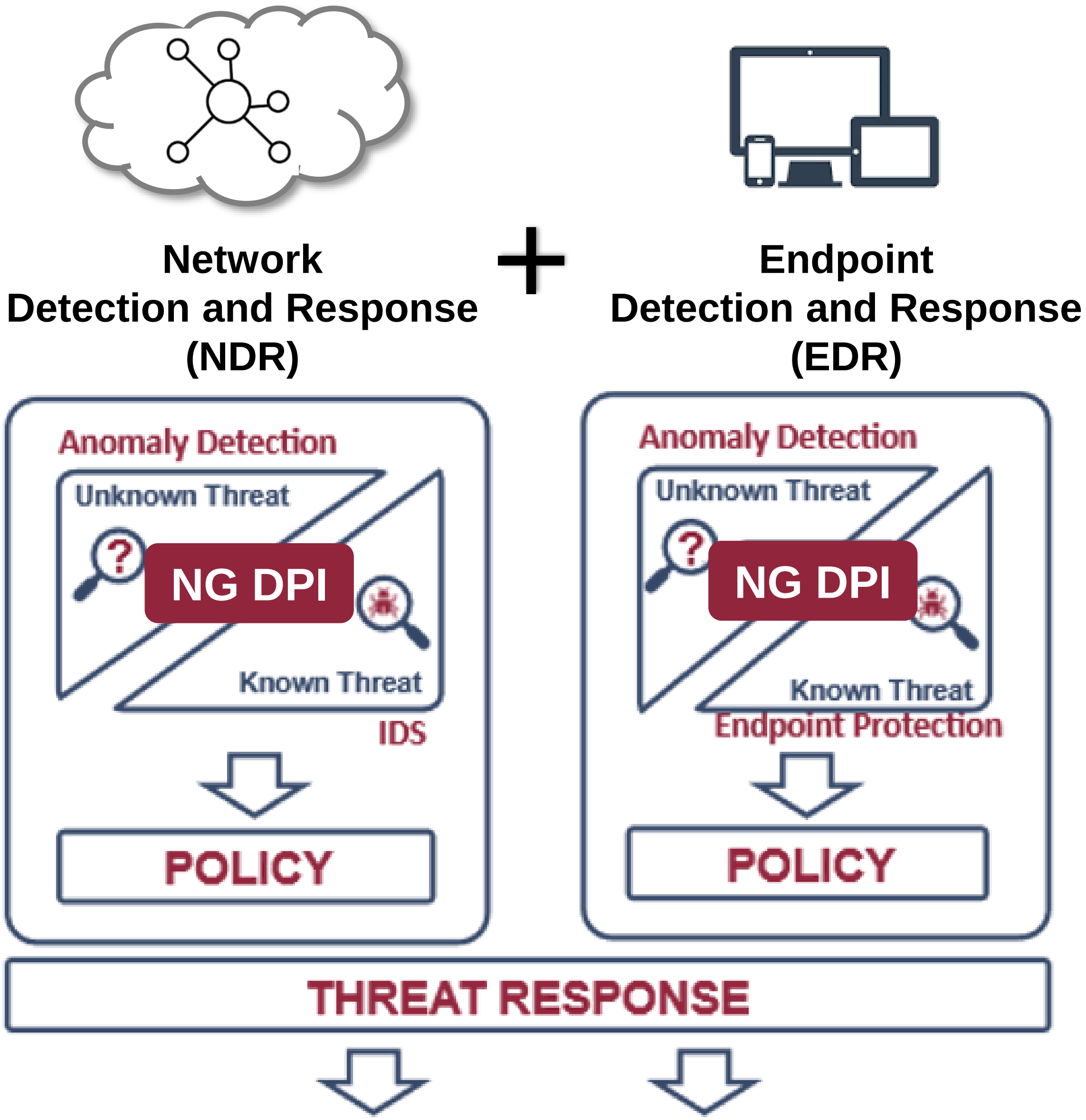
Contents

- About Enea
- Next Gen Deep Packet Inspection
- eXtended Detection and Response
- Enea Qosmos Probe
- Test results with 3rd Gen Intel® Xeon® Processors
- Summary

ENEA

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

NG DPI in eXtended Detection and Response (XDR)



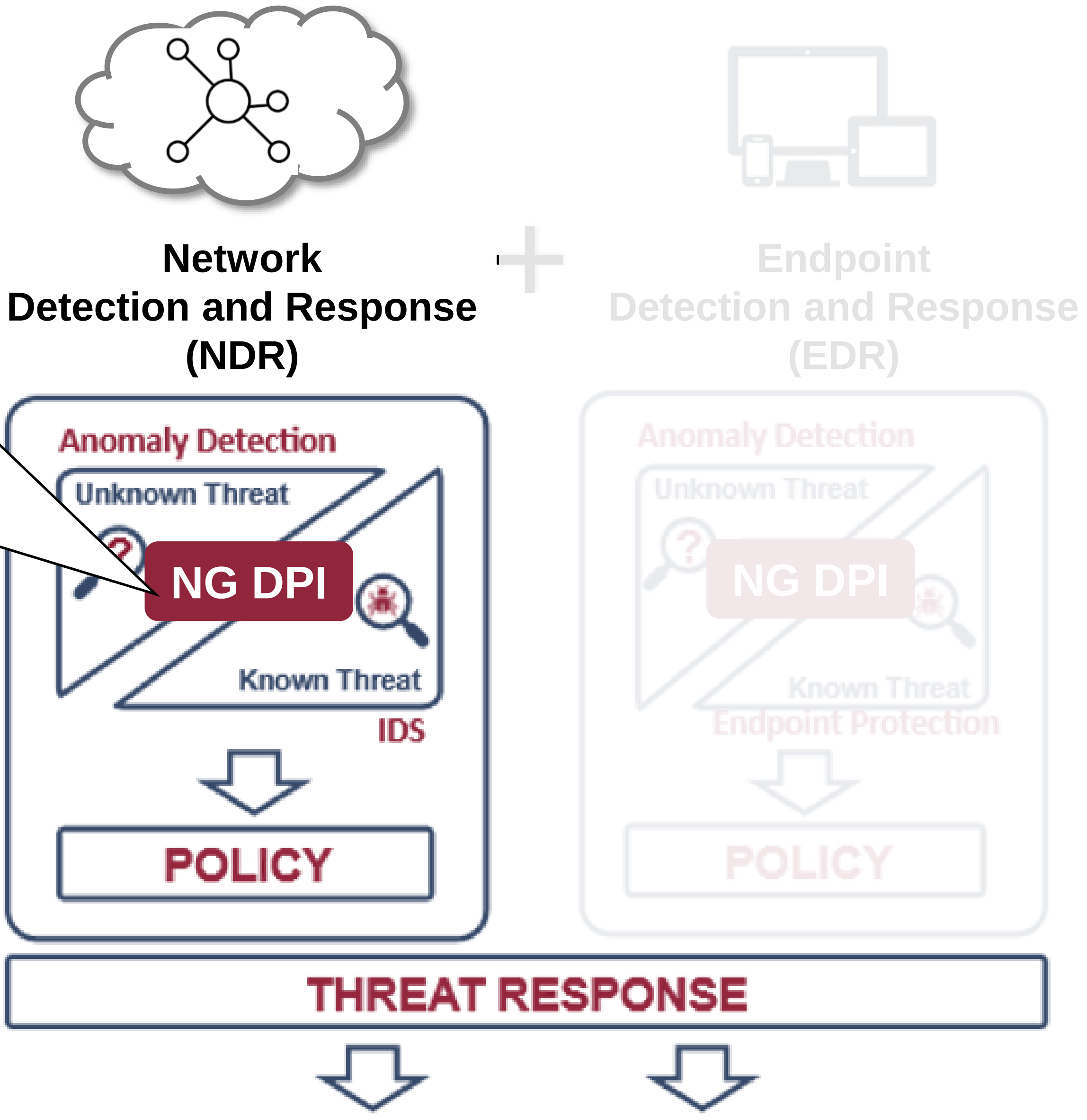
Network
Detection and Response
(NDR)

+

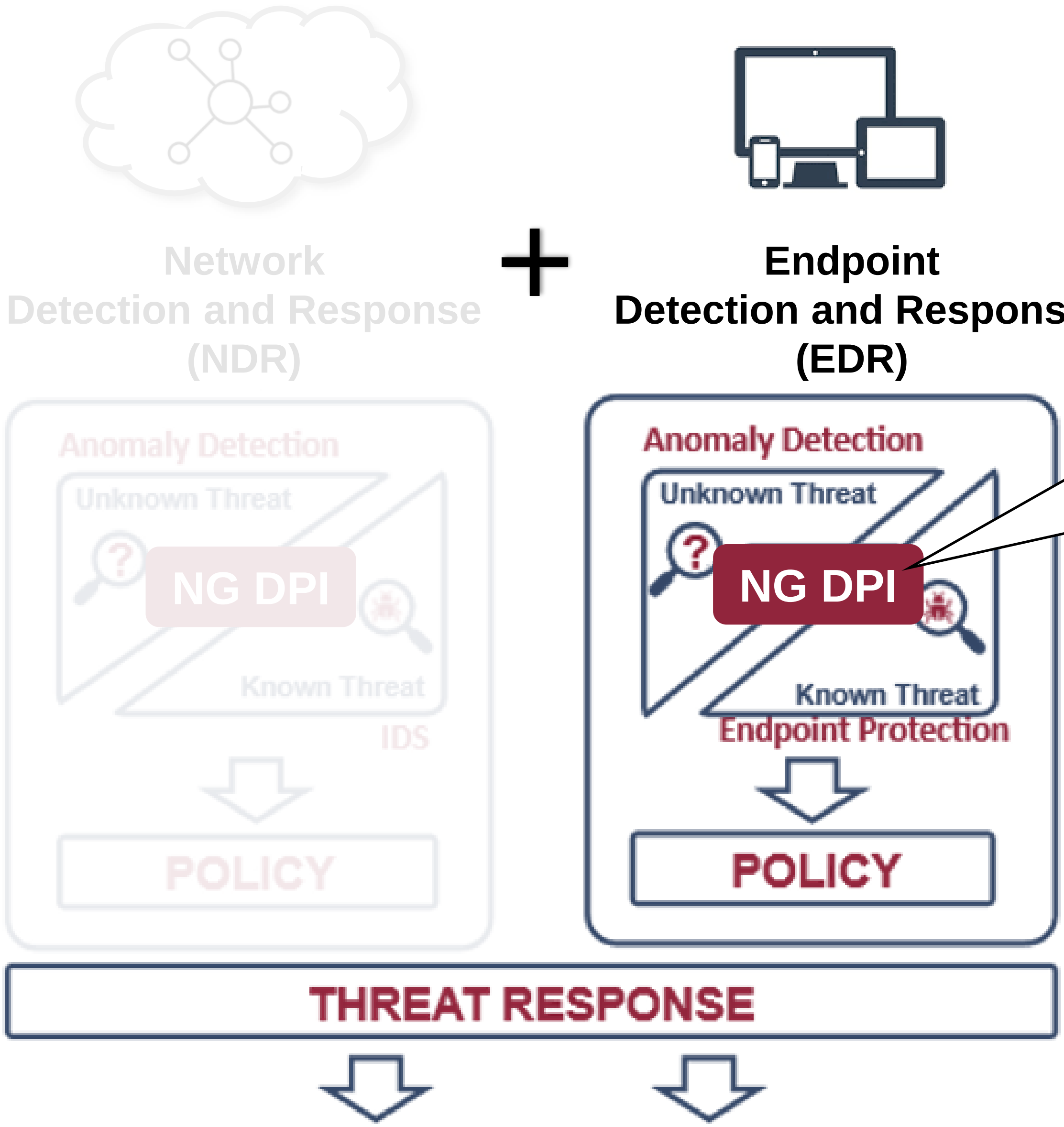
Endpoint
Detection and Response
(EDR)

Role of NG DPI in NDR

1. Build models of normal behavior to detect future anomalies
2. Accurately determine which abnormalities represent threats
3. Rapidly qualify threats and IPS alerts using contextual data
4. Develop effective rules in response to these assessments

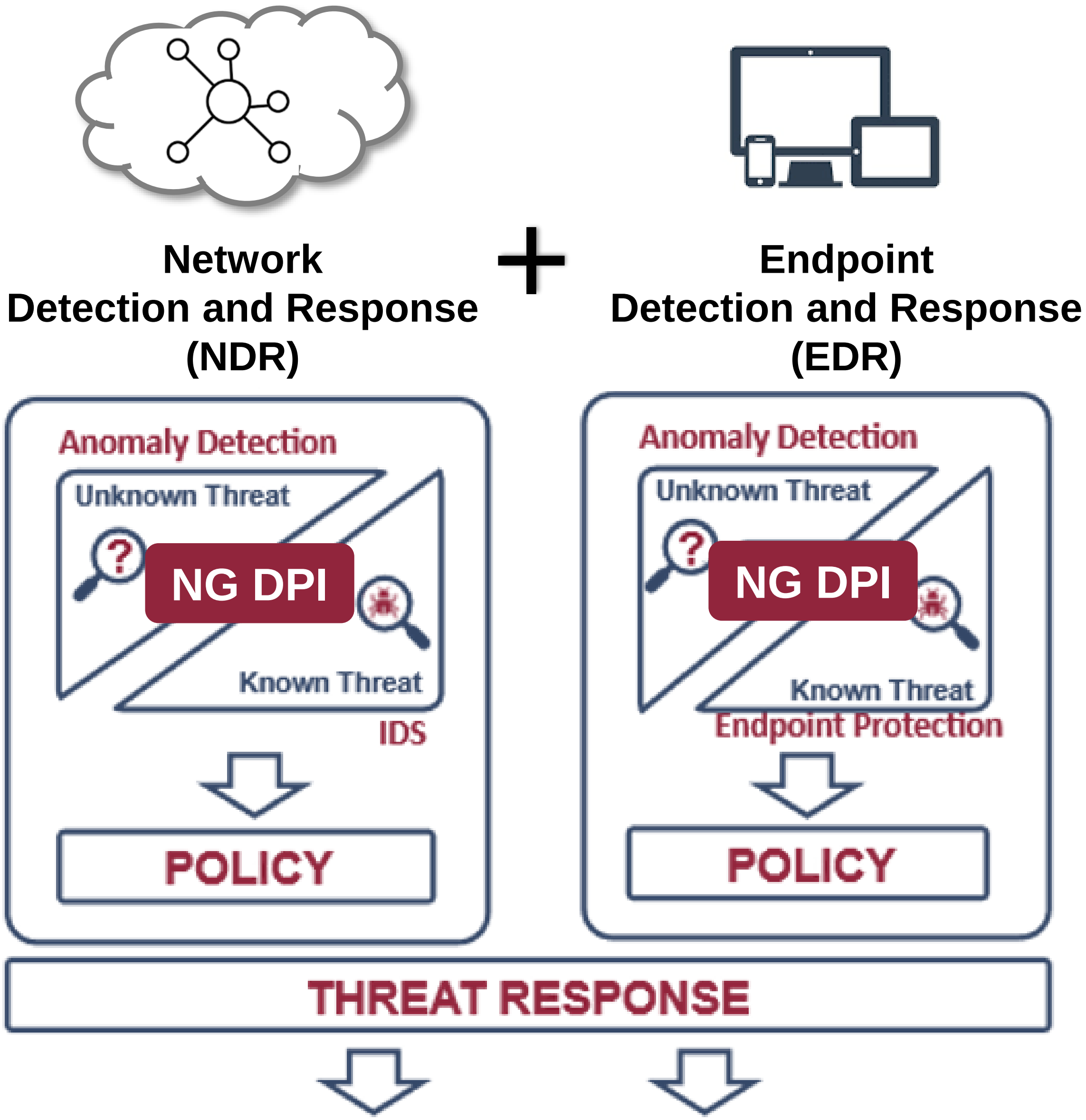


Role of NG DPI in EDR



Build rule-based threat detection with contextual data including device ID, device profile, location, time, and info to compute application risk posture

Examples of XDR Actions that NG DPI Enables



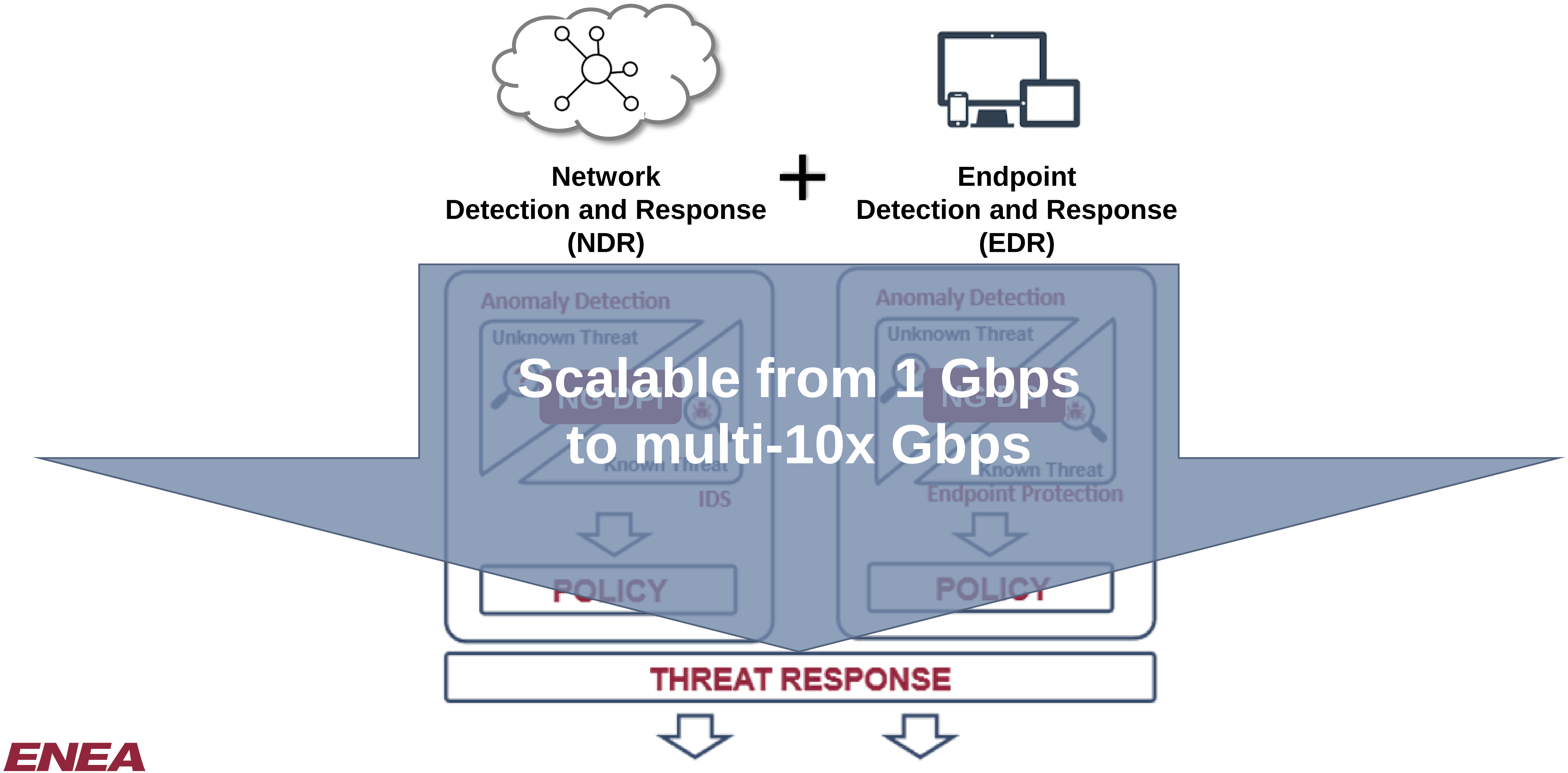
1. Gain visibility into traffic using complex tunneling (i.e., multi-layer wrapping of a packet inside another packet), with full protocol paths for multiple levels of encapsulation (up to 16 levels).

2. Detect unwanted applications on your network such as crypto miners, untrusted VPNs or games.

3. Generate an indicator of compromise when Man in the Middle, Domain Fronting, DGA or other anomalies are detected on the network

4. Detect and analyze the use of remote desktop protocols such as RDP, RFB, TeamViewer, Ammyy admin, and create and enforce rules around them

Importance of Processing Speed for XDR



Network
Detection and Response
(NDR)

+

Endpoint
Detection and Response
(EDR)

Scalable from 1 Gbps
to multi-10x Gbps

ENEA

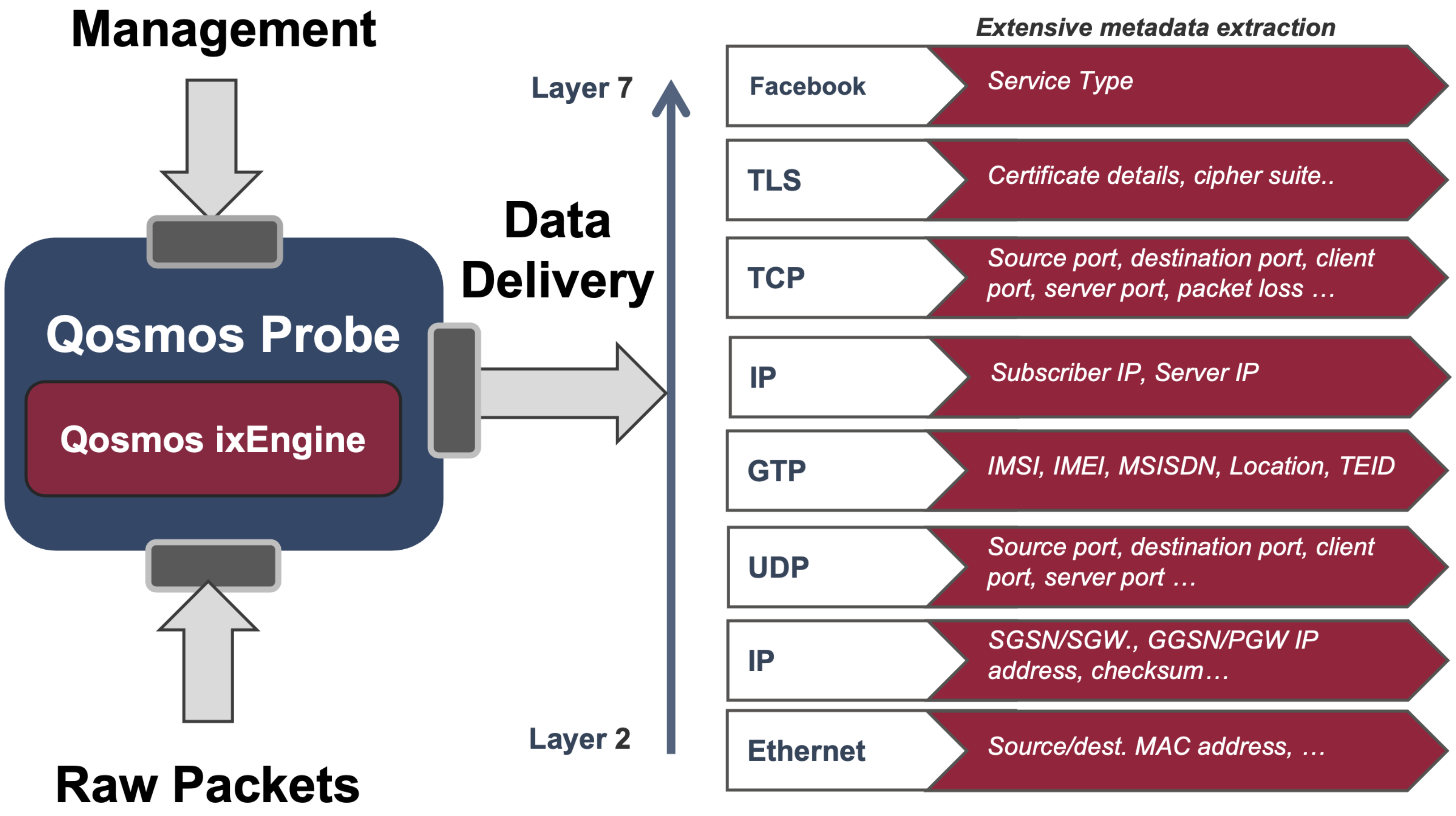
Contents

- About Enea
- Next Gen Deep Packet Inspection
- eXtended Detection and Response
- **Enea Qosmos Probe**
- Test results with 3rd Gen Intel® Xeon® Processors
- Summary

ENEA

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Next Gen Deep Packet Inspection: Qosmos Probe



Management

Qosmos Probe

Qosmos ixEngine

Raw Packets

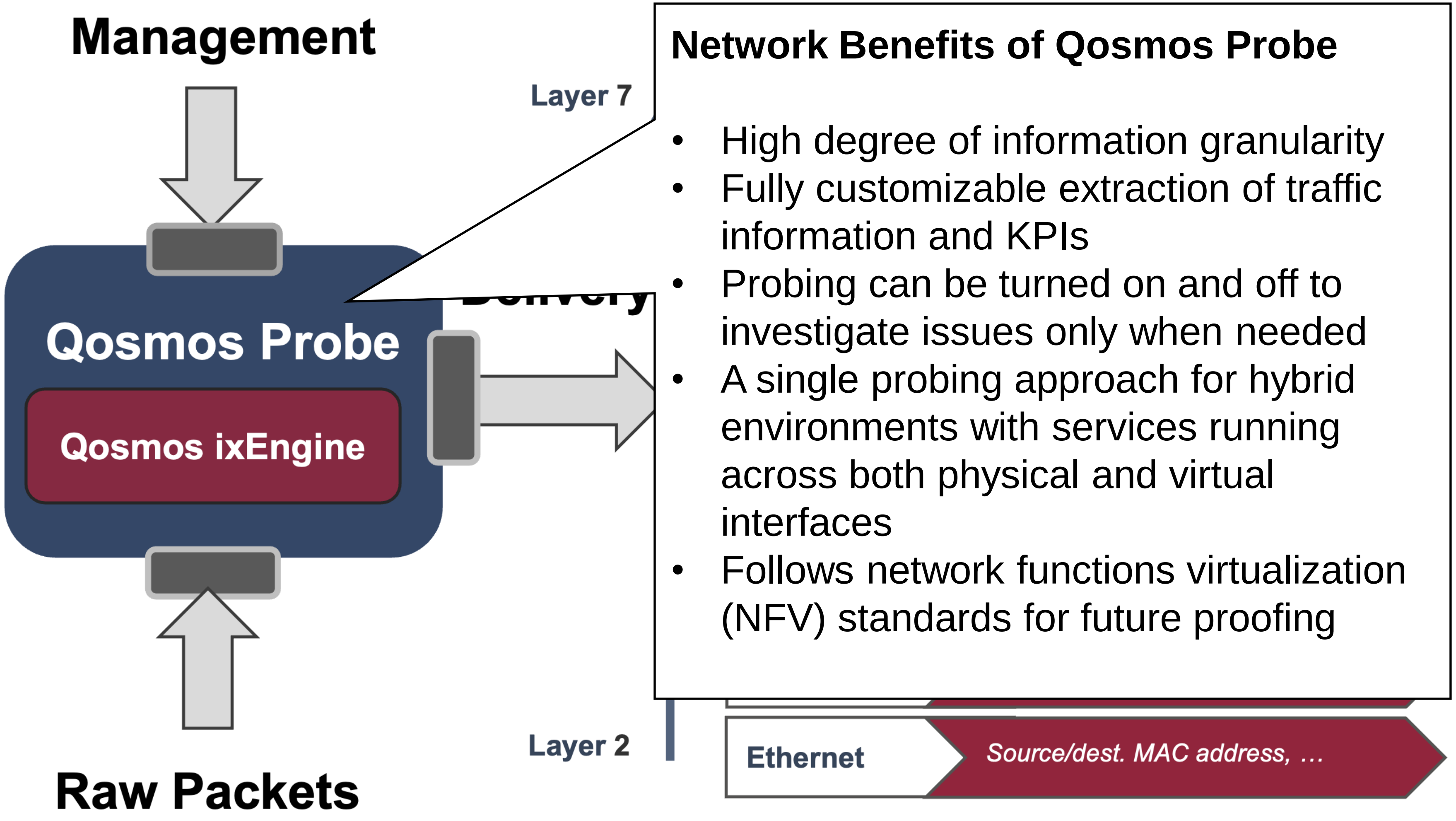
Data Delivery

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, …*

Next Gen Deep Packet Inspection: Qosmos Probe



Network Benefits of Qosmos Probe

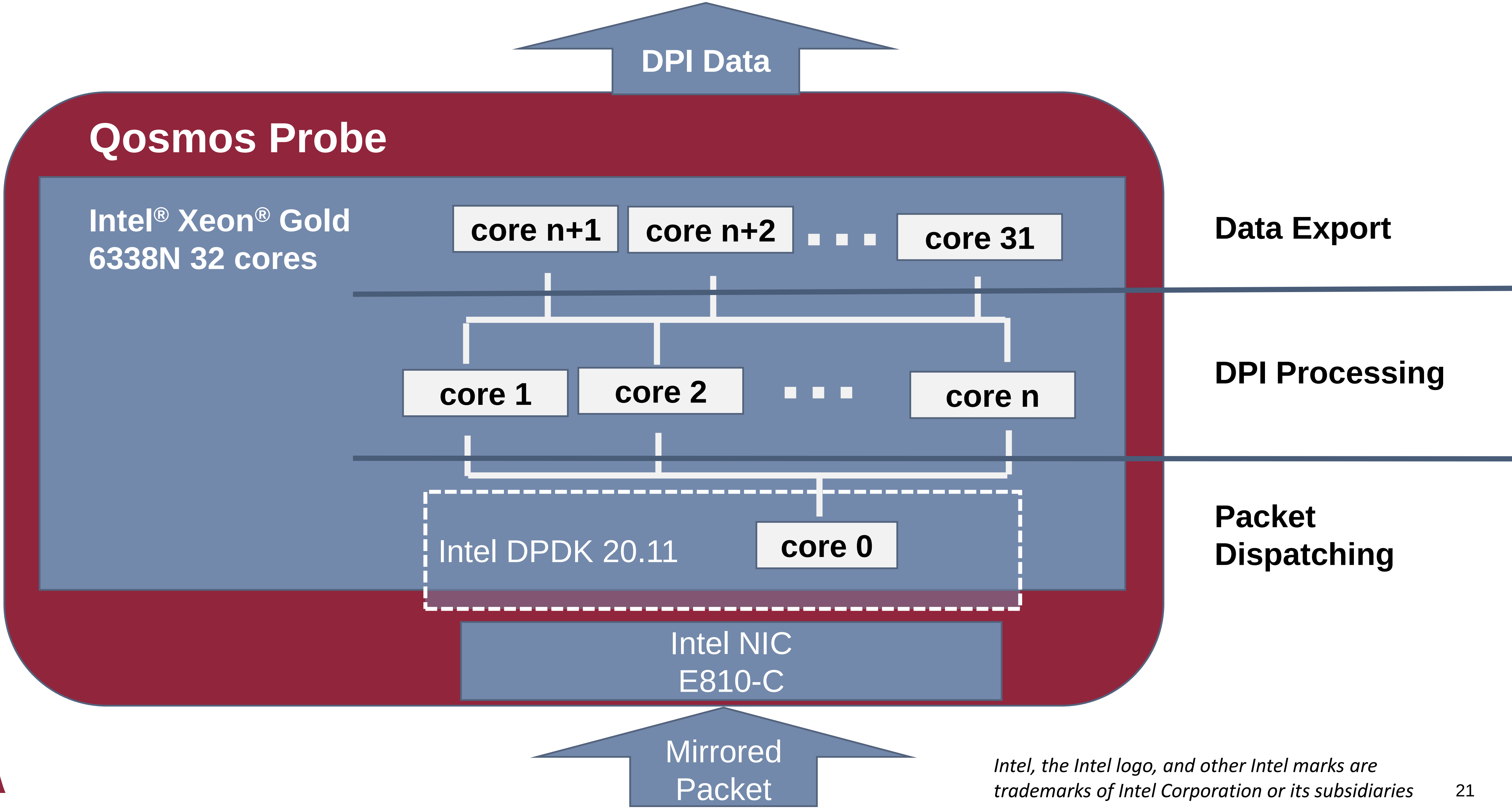
- High degree of information granularity
- Fully customizable extraction of traffic information and KPIs
- Probing can be turned on and off to investigate issues only when needed
- A single probing approach for hybrid environments with services running across both physical and virtual interfaces
- Follows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

Contents

- About Enea
- Next Gen Deep Packet Inspection
- eXtended Detection and Response
- Enea Qosmos Probe
- Test results with 3rd Gen Intel® Xeon® Processors
- Summary

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Intel-Based Qosmos Probe Architecture



Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Test: Software Configuration

- ## Data export

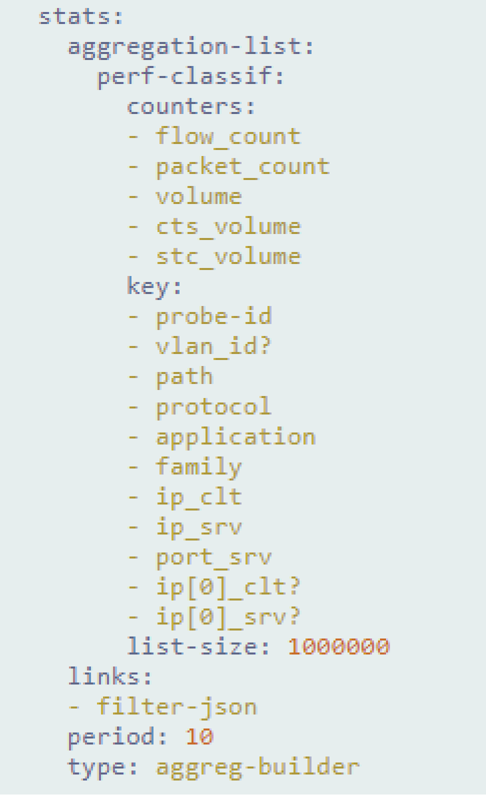
Classification only:

- Flow aggregation per IP / Server Port / Application
- Flat JSON frames sent every 10 seconds over UDP

Classification + Metadata:

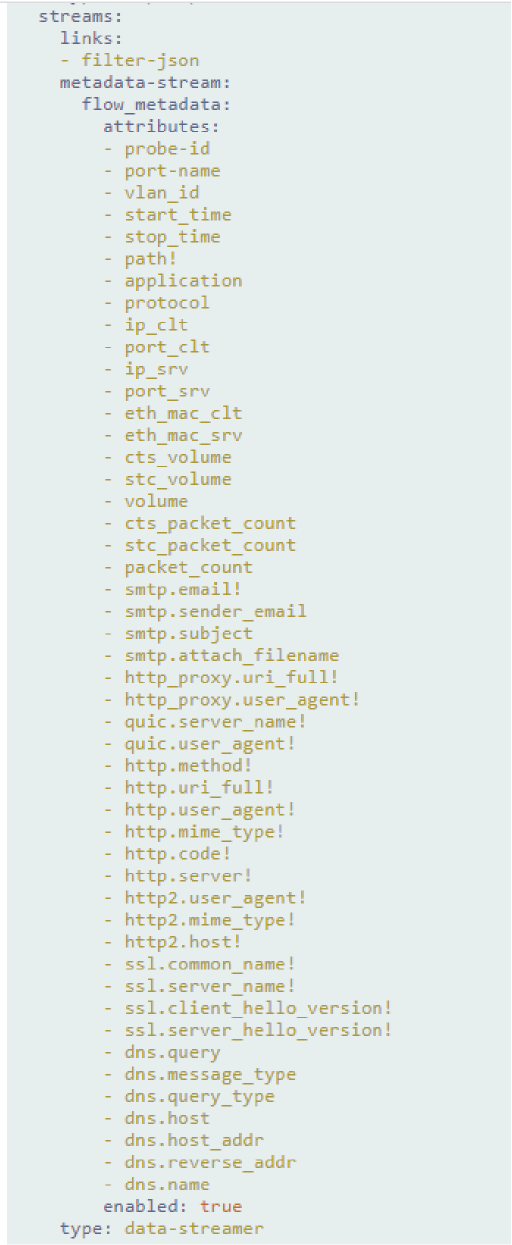
- 1 record per flow with classification results and metadata for HTTP, HTTP2, SSL/TLS, QUIC, DNS and SMTP
- Structured JSON frames sent over UDP at flow expiration

Classification Only



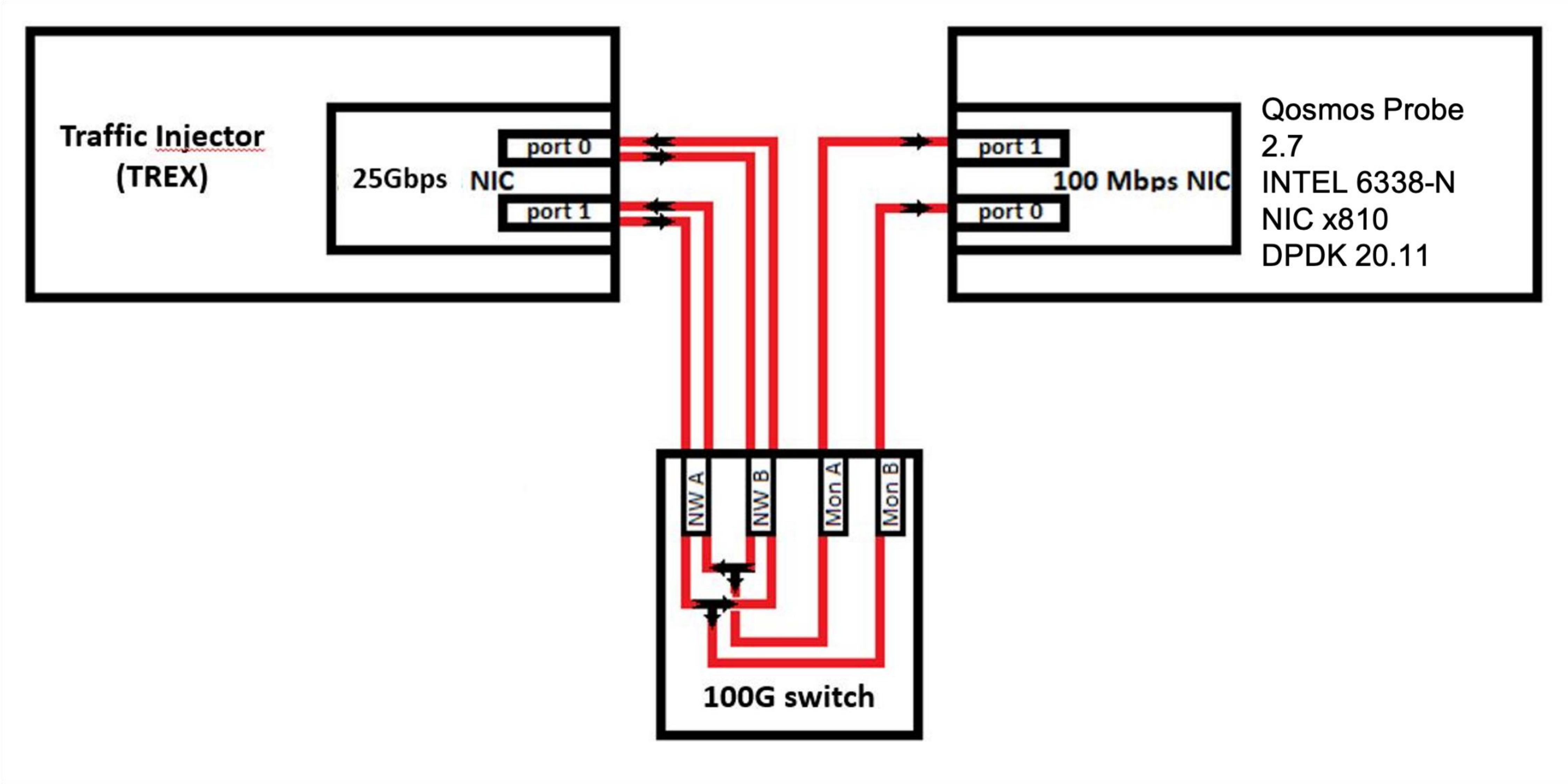
```
stats:
  aggregation-list:
    perf-classif:
      counters:
      - flow_count
      - packet_count
      - volume
      - cts_volume
      - stc_volume
      key:
      - probe-id
      - vlan_id?
      - path
      - protocol
      - application
      - family
      - ip_clt
      - ip_srv
      - port_srv
      - ip[0]_clt?
      - ip[0]_srv?
      list-size: 1000000
  links:
  - filter-json
  period: 10
  type: aggreg-builder
```

Classification + Metadata



```
streams:
  links:
  - filter-json
  metadata-stream:
    flow_metadata:
      attributes:
      - probe-id
      - port-name
      - vlan_id
      - start_time
      - stop_time
      - path!
      - application
      - protocol
      - ip_clt
      - port_clt
      - ip_srv
      - port_srv
      - eth_mac_clt
      - eth_mac_srv
      - cts_volume
      - stc_volume
      - volume
      - cts_packet_count
      - stc_packet_count
      - packet_count
      - smtp.email!
      - smtp.sender_email
      - smtp.subject
      - smtp.attach_filename
      - http_proxy.uri_full!
      - http_proxy.user_agent!
      - quic.server_name!
      - quic.user_agent!
      - http.method!
      - http.uri_full!
      - http.user_agent!
      - http.mime_type!
      - http.code!
      - http.server!
      - http2.user_agent!
      - http2.mime_type!
      - http2.host!
      - ssl.common_name!
      - ssl.server_name!
      - ssl.client_hello_version!
      - ssl.server_hello_version!
      - dns.query
      - dns.message_type
      - dns.query_type
      - dns.host
      - dns.host_addr
      - dns.reverse_addr
      - dns.name
      enabled: true
  type: data-streamer
```

Test Network

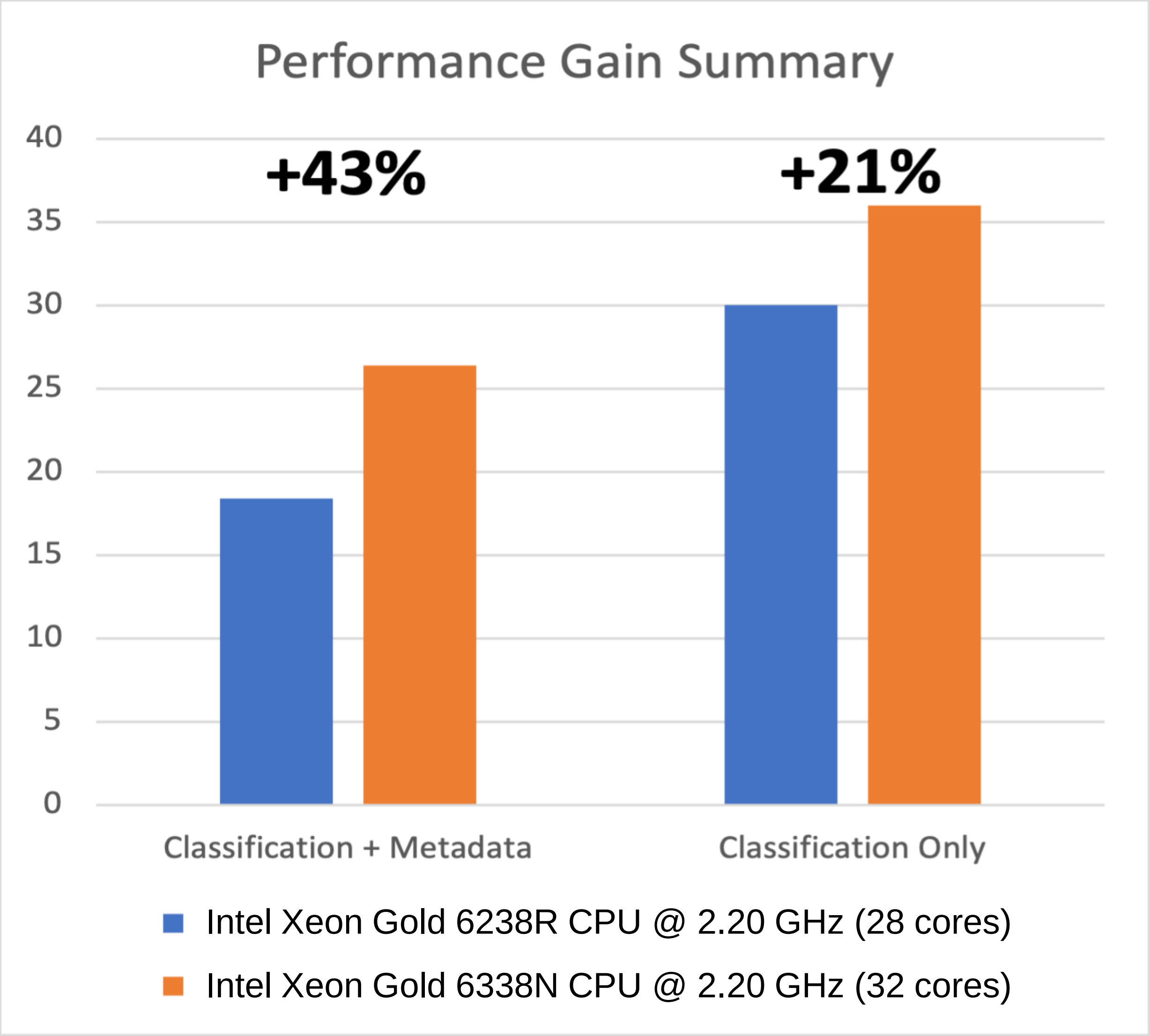


Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Gen-over-gen Performance Increases

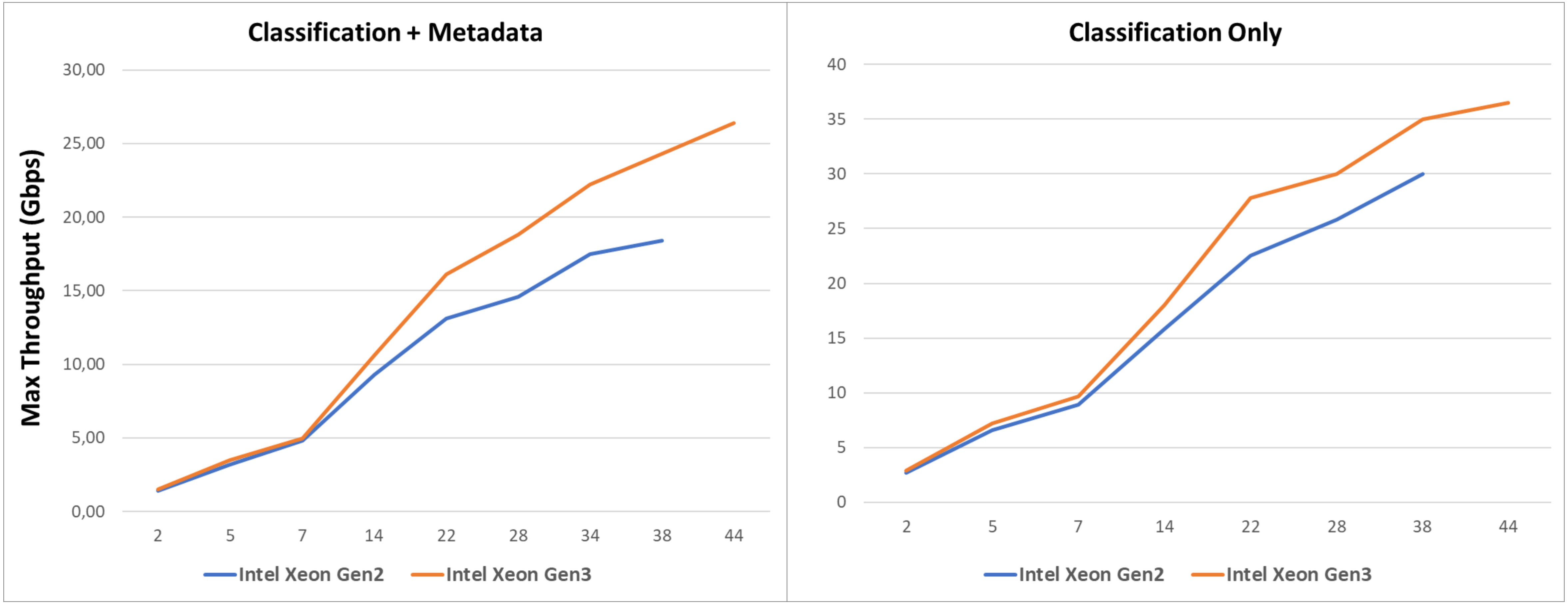
- **Qosmos probe running on Intel® Xeon® Scalable processors (higher is better)**

- **Config 1 Gen 3 (orange):**
  - 44 HT cores for DPI
  - 16 HT cores for data export
  - 1 physical core for DPDK
- **Config 2 Gen 2 (blue):**
  - 38 HT cores for DPI
  - 14 HT cores for data export
  - 1 physical core for DPDK



Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Scalability



- **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**

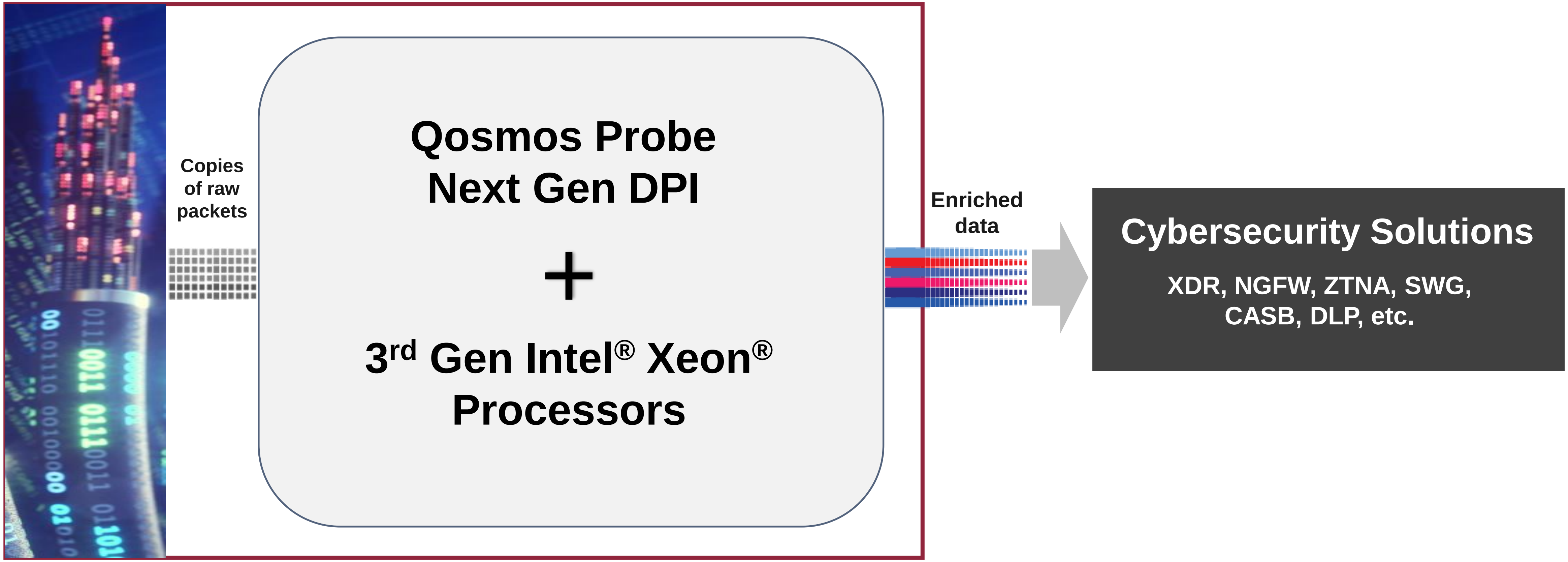
Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Contents

- About Enea
- Next Gen Deep Packet Inspection
- eXtended Detection and Response
- Enea Qosmos Probe
- Test results with 3rd Gen Intel® Xeon® Processors
- **Summary**

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Summary: Emerging Security Applications Need Next Gen DPI and High-Performance Packet Processing



Copies of raw packets

Qosmos Probe
Next Gen DPI

+

3rd Gen Intel® Xeon® Processors

Enriched data

Cybersecurity Solutions

XDR, NGFW, ZTNA, SWG, CASB, DLP, etc.

Tests of the Qosmos probe with 3rd Gen Intel Xeon Gold 6338N CPUs shows marked improvement in performance and scalability

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Questions
&
Answers

ENEA

ENEA

www.enea.com