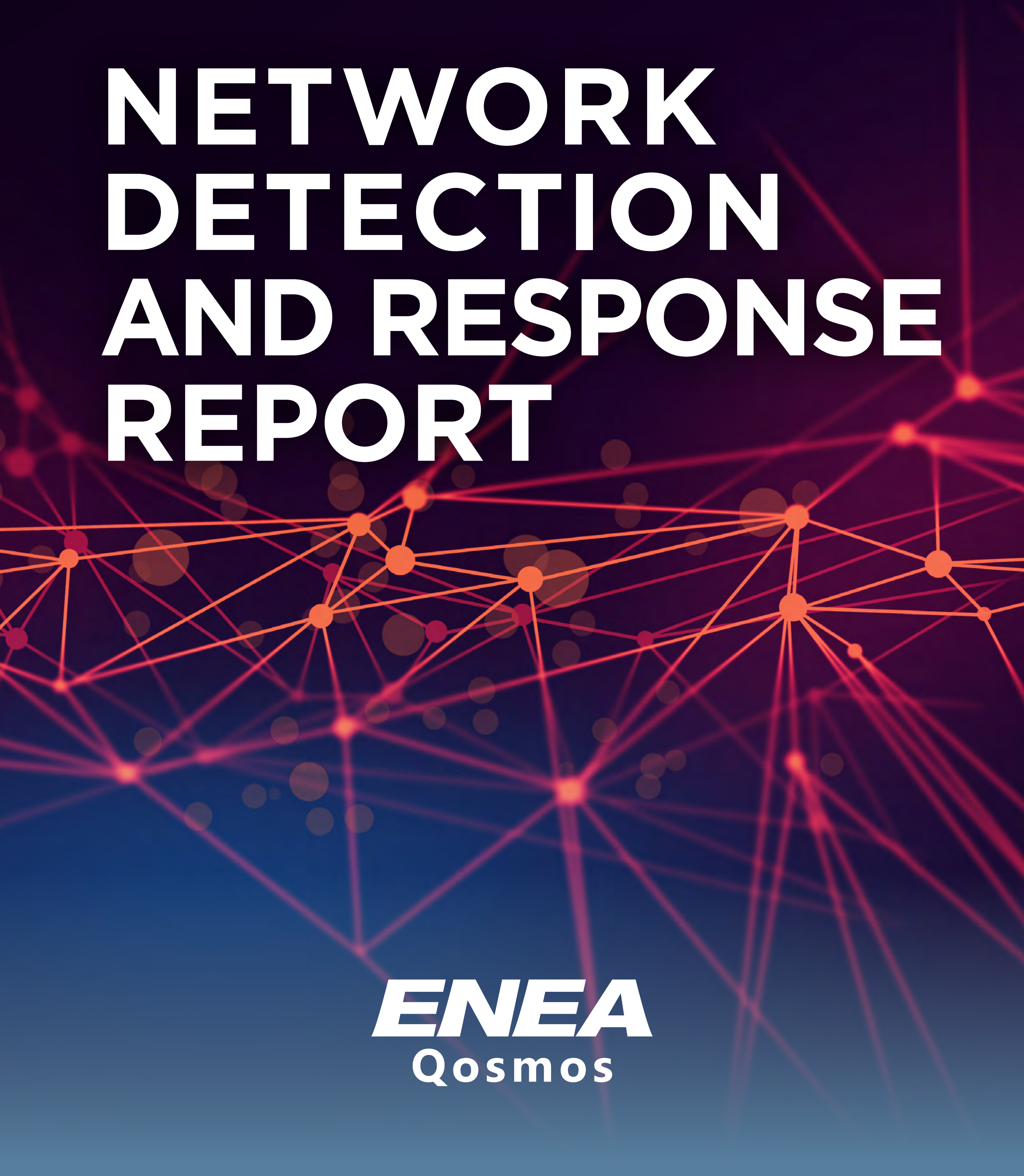
2021

Cybersecurity INSIDERS

NETWORK DETECTION AND RESPONSE REPORT



ENEA Qosmos

EXECUTIVE SUMMARY

Recent high-profile incidents at companies like SolarWinds, Microsoft, T-Mobile, Facebook, Colonial Pipeline, JBS and Acer highlight the significant harm caused by advanced cyber-attacks. These types of attacks can successfully circumvent endpoint and perimeter defenses, remain hidden and active in networks for a long time, and are capable of causing extensive damage.

Network Detection and Response (NDR) solutions are designed specifically to detect and respond to advanced cyber threats. NDR is a solution that combines the signature-based threat detection capabilities of IDS/IPS with Network Traffic Analysis, which detects unknown or hidden threats through the identification of behavioral anomalies in network traffic.

But how familiar are security professionals with NDR? How many have or plan to deploy an NDR solution? What features and capabilities do they expect in an NDR solution? And what concerns are holding some back from adopting NDR?

To find the answers to these questions, we conducted a survey of Cybersecurity Insiders' 500,000-member information security community.

For a panel discussion about options and strategies for addressing the needs and concerns raised in this survey, we invite you to watch our webinar **How to Use Network Detection & Response to Mitigate the Inevitable Breach.**

Many thanks to Enea Qosmos for supporting this important research project.

We hope you find the information shared by respondents useful in assessing and honing your own cybersecurity strategies, and we hope that you enjoy reading the report.

Thanks

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

KEY FINDINGS

FINDING 1:

NDR Adoption

NDR is viewed as an essential tool in the battle against advanced persistent threats (APTs), with NDR experiencing a rapid adoption rate. 73% of respondents consider the anomaly detection capabilities of network traffic analysis (NTA) to be critically important for detecting APTs, and 55% have already deployed or plan to deploy a full NDR solution that combines the anomaly detection capabilities of NTA with threat signature detection capabilities of IDS/IPS for maximum protection against APTs.

FINDING 2:

NDR Capabilities

Cloud adoption and IoT/IIoT are creating network and connected device blind spots, and security professionals expect NDR to address this.

- 9 out of 10 organizations expect NDR to cover hybrid IT/IoT LAN/WAN networks, with special concerns for cloud workload traffic and dedicated IoT/IIoT and OT/ICS networks.
- Beyond anomaly detection, the additional capability professionals want most in an NDR solution is connected device identification.

FINDING 3:

Threat Priorities

Command and control attacks (69%), ransomware (57%), and data exfiltration (50%) top the rankings of specific threats respondents expect NDR to detect.

FINDING 4:

Barriers to Adoption

The top barriers to NDR adoption are concerns over solution cost and uncertainty regarding the maturity of machine learning-based behavioral analytics.

NETWORK VISIBILITY GAPS

Network visibility is an issue affecting all types of traffic, layers, and devices – and it is further complicated by encryption and the complexities of virtualization. When asked about the most significant gaps in network visibility, survey respondents prioritized cloud workload traffic (46%), followed by connected device communication (42%) and SaaS apps (39%).

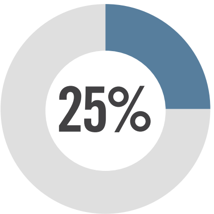
Where do you feel you have the most significant network visibility gaps?

46% Cloud workload traffic

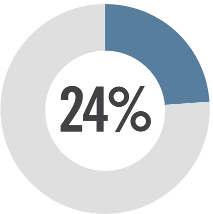
42% Connected devices

39% SaaS apps

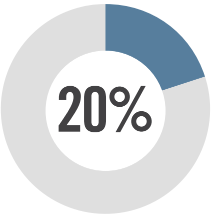
34% Local traffic (East-West)



Public internet traffic



IoT/IIoT traffic



Traffic between enterprise sites

TRAFFIC DATA SOURCES

Which data sources are most relevant to tap into to gain better visibility into network traffic? Cybersecurity professionals in our survey primarily rely on logs from network equipment, such as routers, switches, firewalls, etc. (85%). This is followed by logs from host applications, such as web servers, or email servers (58%) and logs and notifications from endpoint agents (54%).

What individual data sources do you currently rely on for network traffic visibility?

85%

Logs from network equipment

(routers, switches, firewalls, SWG, etc.)

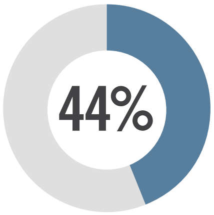
58%

Logs from host applications

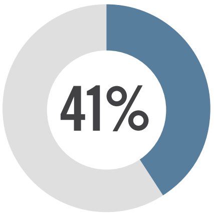
(web server, email server, etc.)

54%

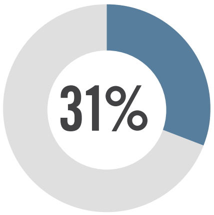
Logs/notifications from endpoint agents



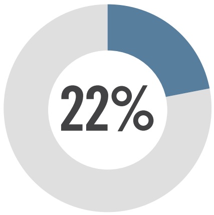
Network sensors with Deep Packet Inspection (DPI)
(via SPAN, mirror port, or network TAP)



Alerts from IDS



NetFlow records



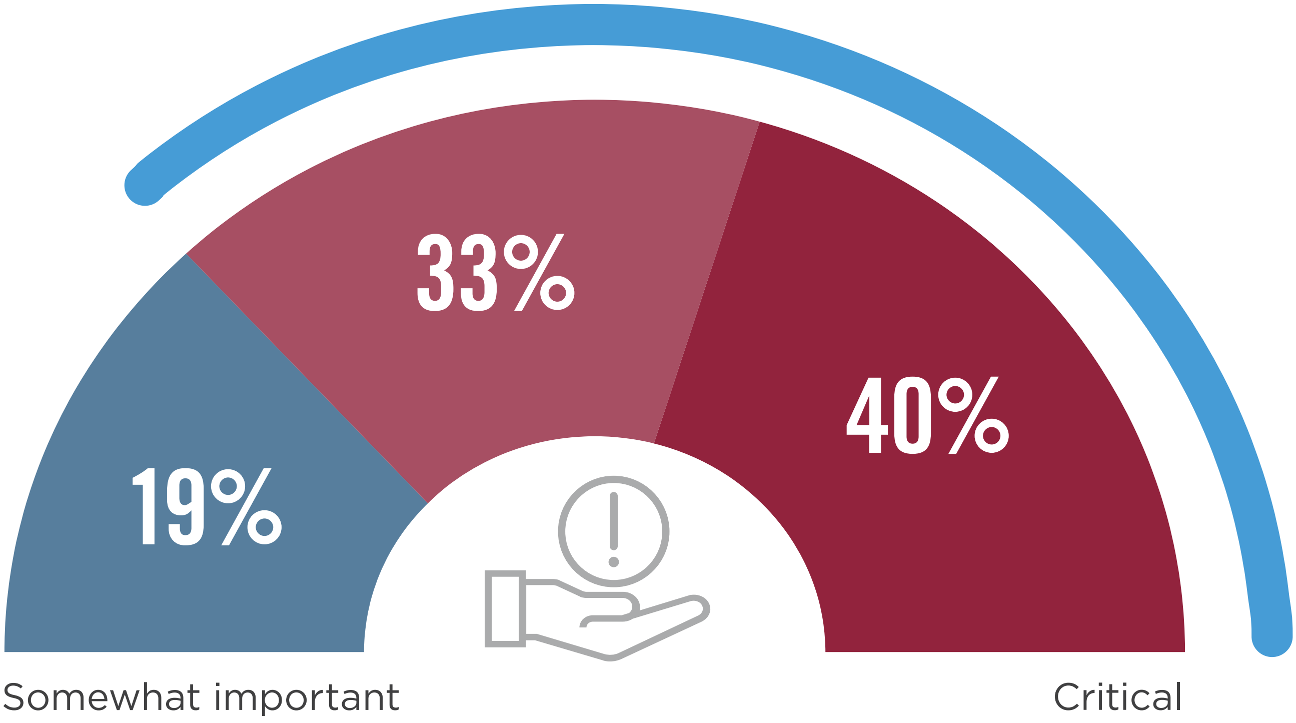
Full packet capture

NETWORK TRAFFIC ANALYSIS

Network traffic analysis is rising in importance, especially when detecting anomalies that evade traditional endpoint detection. 73% of cybersecurity professionals agree that traffic analysis is important or critically important to detecting such anomalies.

▶ **How important has network traffic analysis become in your environment to detect anomalies that have evaded traditional endpoint detection?**

73% consider network traffic analysis important to critical in detecting anomalies that have evaded traditional endpoint detection



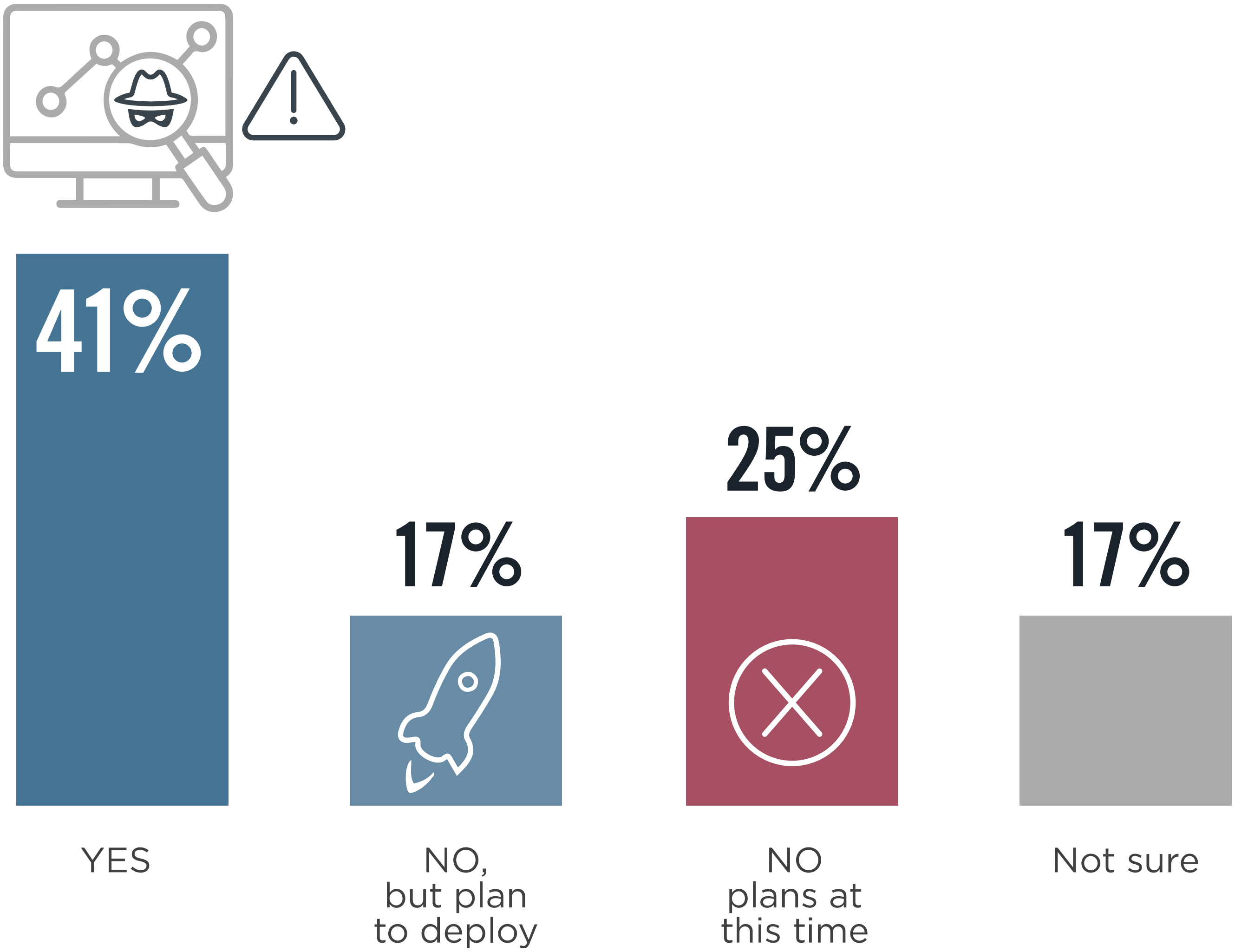
■ Somewhat important ■ Important ■ Critical

Not sure 8%

NETWORK-BASED INTRUSION DETECTION

Intrusion detection systems are a critical component in organizations' security posture. They can be deployed in standalone form, or integrated into broader security platforms. 41% of organizations confirm they are using standalone IDS in their network. Of those who don't use a standalone IDS, 17% have plans to deploy one.

▶ **Do you use a standalone network-based IDS?**

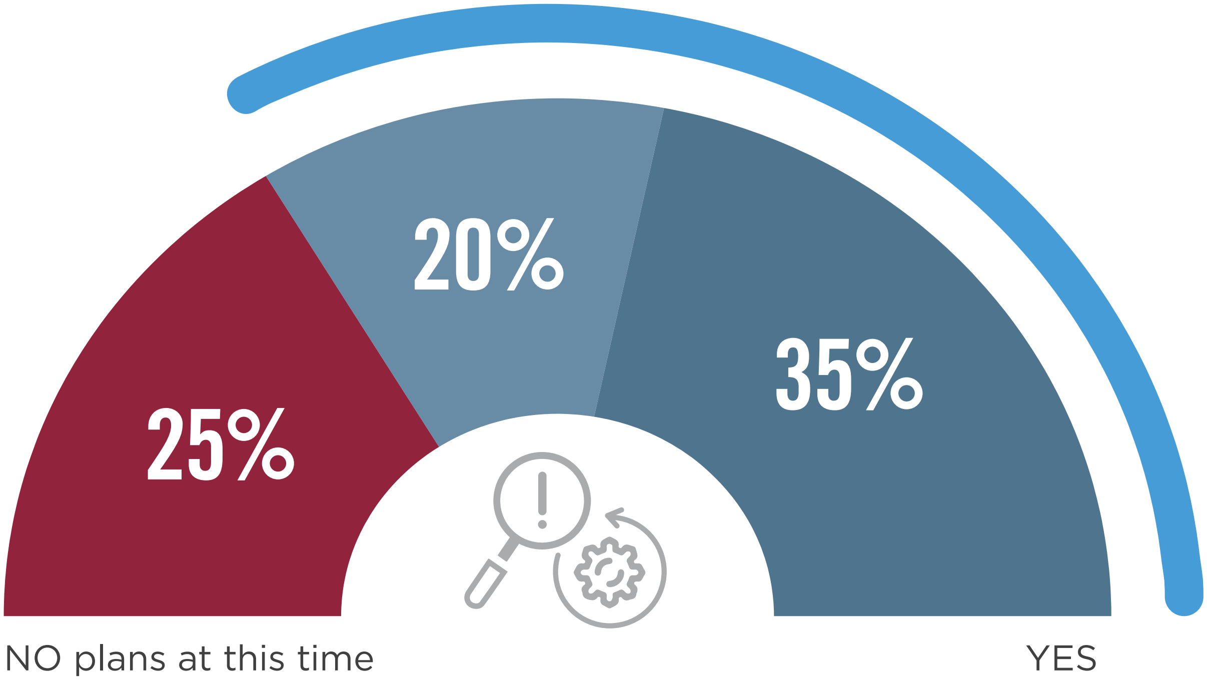


NDR USAGE

Network detection and response solutions are rapidly gaining momentum as part of organizations' security investments. 35% of organizations are already using NDR solutions in their network and 20% have plans to deploy one.

Do you use an NDR solution?

55% **have either already deployed an NDR solution or have plans to do so**



Not sure 20%

THREAT DETECTION & RESPONSE PRIORITIES

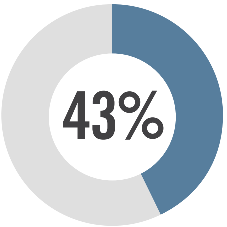
Cybersecurity professionals prioritize threats within the complex and evolving threat landscape based on their likelihood and capacity to inflict damage. Command and control attacks (69%) top the list of threats considered most essential to be addressed by network detection and response. This is followed by ransomware (57%) and data exfiltration (50%).

Which threats do you consider it most important for your NDR to address?

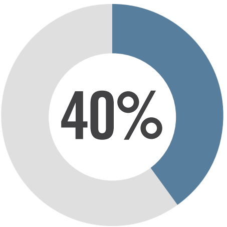
69%
Command and control attacks

57%
Ransomware

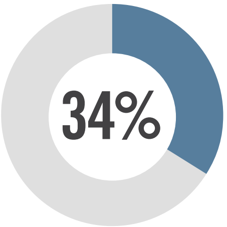
50%
Data exfiltration



Malware lateral movements



Malware intrusion
(file analysis)



DDoS attacks

Phishing attacks 26% | Illicit cryptomining 16%

NDR ADVANTAGES OVER IDS/IPS

We asked cybersecurity professionals what advantages they see provided by network detection and response versus standalone intrusion detection/protection solutions. 74% highlight the better capacity to detect anomalous and suspicious behavior, followed by enablement of proactive threat hunting (57%) and the provision of contextual data to improve alert investigation and analysis (50%).

What do you think are the most important advantages of NDR versus standalone IDS/IPS?

74%

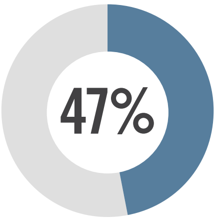
Detect anomalous or suspicious behavior (flows, packets, users, endpoints)

57%

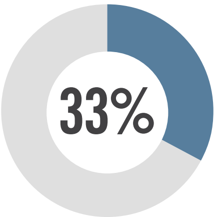
Enable proactive threat-hunting

50%

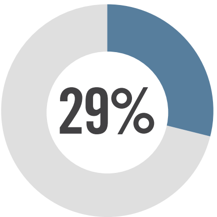
Provide contextual data to improve alert investigation and analysis



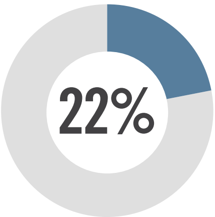
Discover unmanaged/ unauthorized devices on the network



Reduce false positive IDS/IPS alerts



Improve post-incident forensics

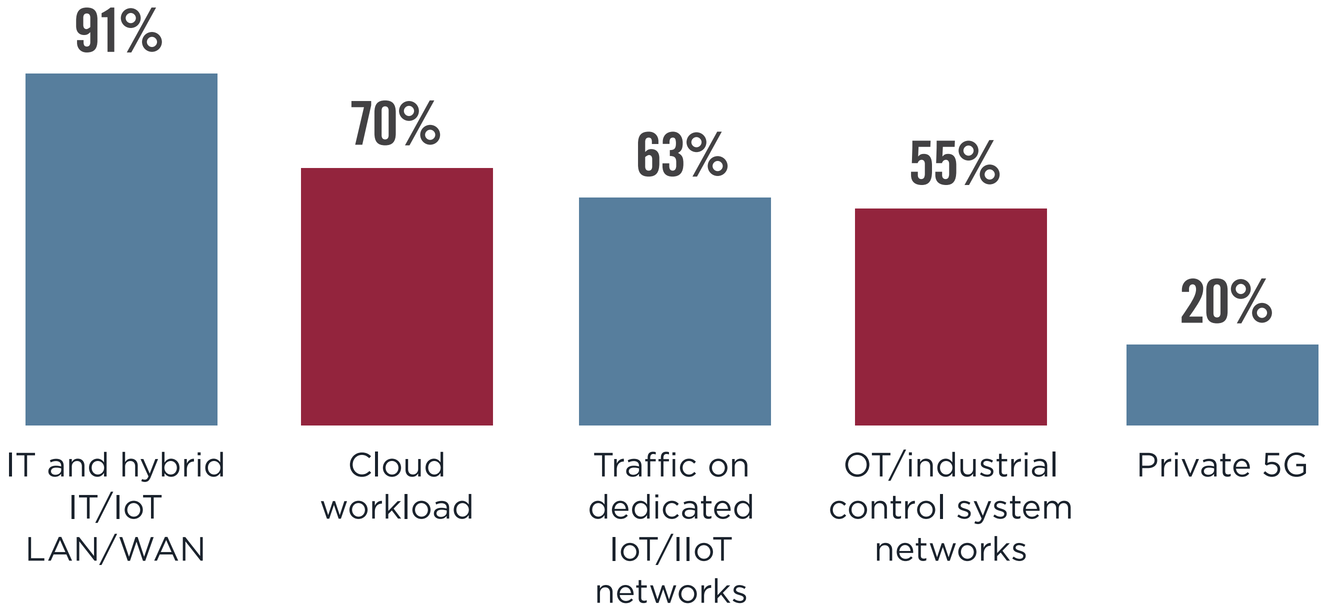


Provide visibility on encrypted traffic

NETWORK MONITORING & PROTECTION

We asked organizations what networks they think a network detection and response solution should monitor and protect. 9 out of 10 organizations prioritize support for IT and hybrid IT/IoT LAN/WAN (91%), followed by cloud workload traffic (70%) and traffic on dedicated IoT/IIot networks (63%).

▶ **What kind of networks do you think an NDR solution should be able to monitor and protect?**



NDR SOLUTION CAPABILITIES

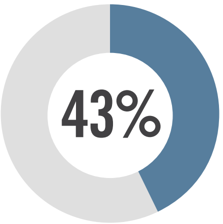
What network detection and response capabilities do organizations see as most important? Device detection is the single most mentioned capability (60%), followed by flexible querying capabilities for threat hunting (47%) and automatic suggestions for rules and incidence response (45%).

Beyond anomaly detection, what additional capabilities do you think are most important for an NDR solution?

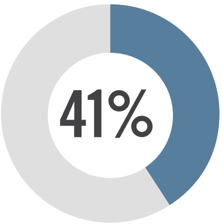
60%
Device detection

47%
Flexible querying capabilities for threat hunting

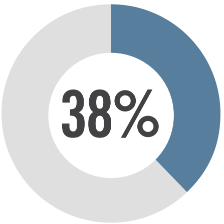
45%
Auto-suggestions for rules and incidence response



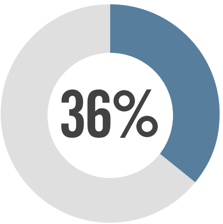
Malware detection



Integration of external threat intelligence feeds



L2-L7 classification of encrypted traffic without using decryption



Easy pivoting from an alert to relevant source data

Phishing detection 33% | DNS/IP reputation 31% | Service-based support from external threat analyst professionals 26% | SSL proxy for decryption and inspection 17% | Other 3%

NDR ADOPTION BARRIERS

Why are some organizations delaying the adoption of network detection and response? The primary barriers include cost and budget factors (40%), followed by concerns about the reliability of behavioral analytics and machine learning (31%), and a preference for NDR capabilities to be integrated into an existing platform (rather than deploying a standalone solution) (29%).

If you do not plan to adopt NDR, what are the primary reasons?

40%

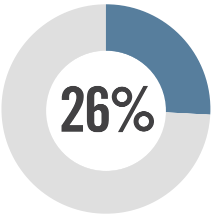
Too expensive/ not enough budget

31%

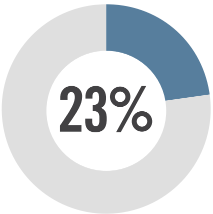
Concerns about reliability of behavioral analytics and machine learning

29%

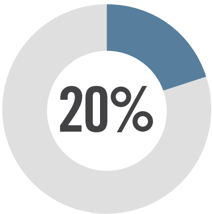
Prefer NDR capabilities to be integrated into an existing platform (rather than deploying as a standalone solution)



Too much overlap with existing threat detection tools



Insufficient coverage of cloud workloads

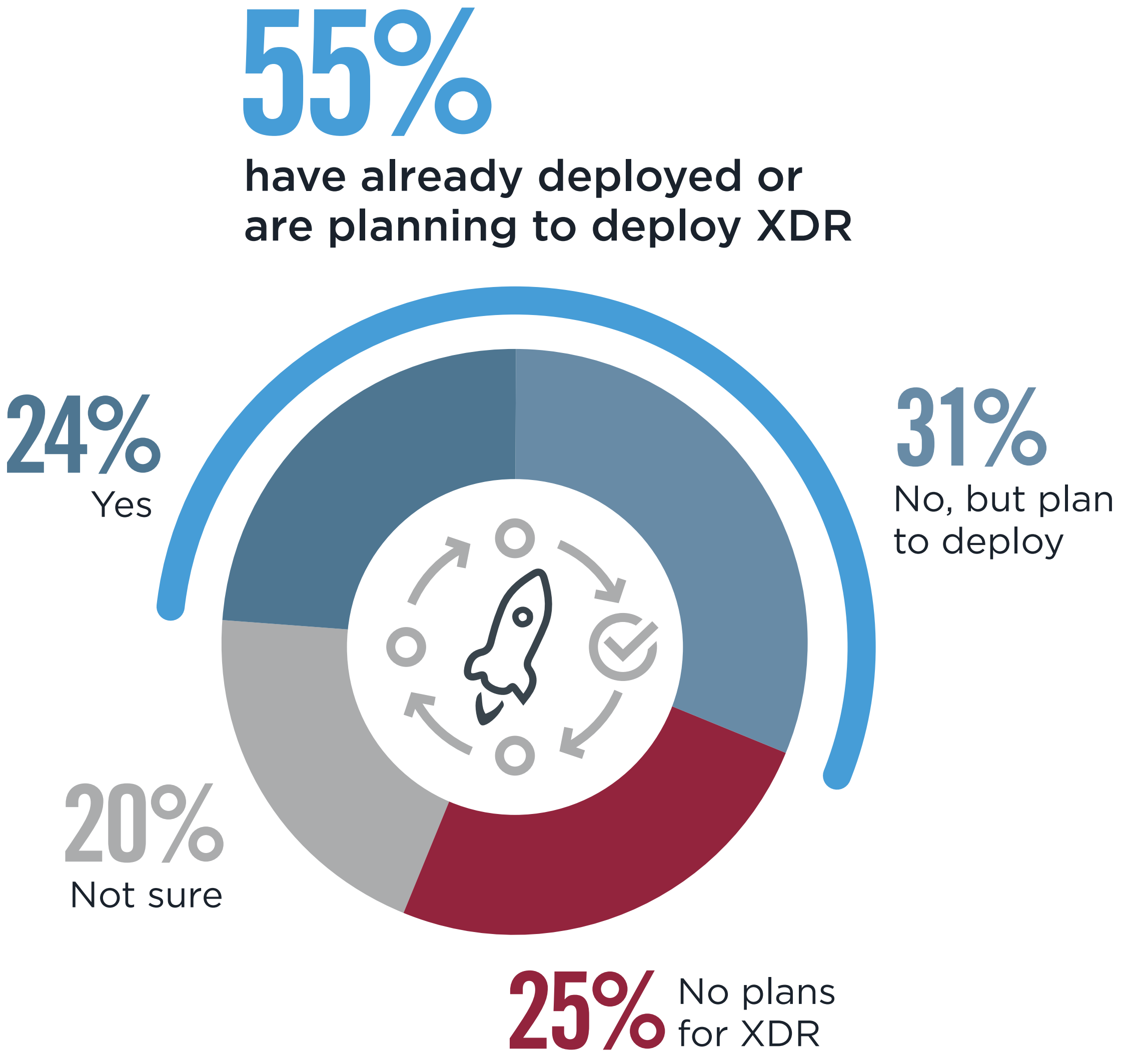


Insufficient coverage of OT/IoT network traffic

XDR ADOPTION

When asked about their adoption of XDR (i.e., a platform that integrates NDR, EDR, and other threat detection and response tools), a majority of professionals (55%) have already deployed or are planning to deploy an XDR solution.

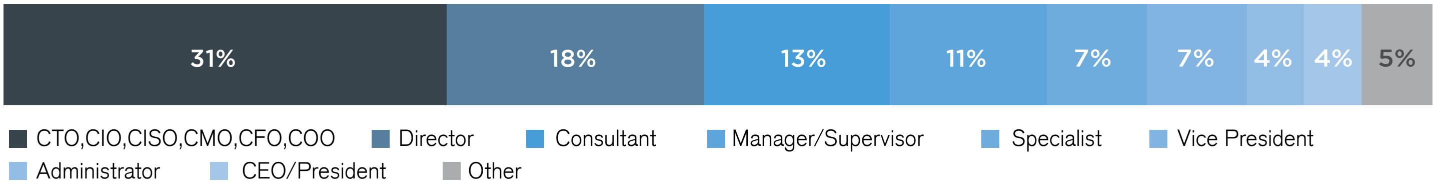
Have you deployed an XDR solution (i.e., a platform that integrates NDR, EDR (Endpoint Detection and Response) and other threat detection and response tools)?



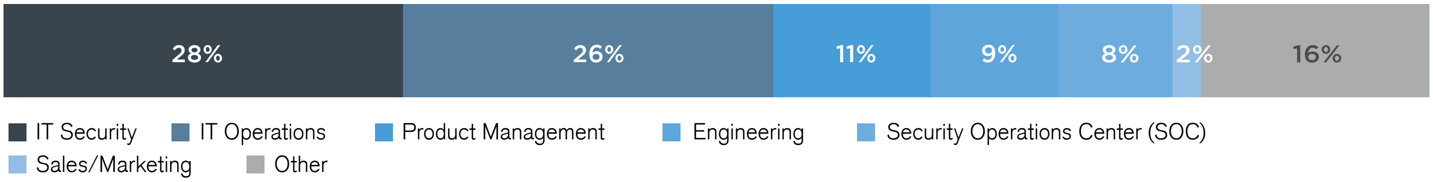
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 315 cybersecurity professionals, to gain more insight into the latest trends, key challenges, and solutions for network detection and response. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

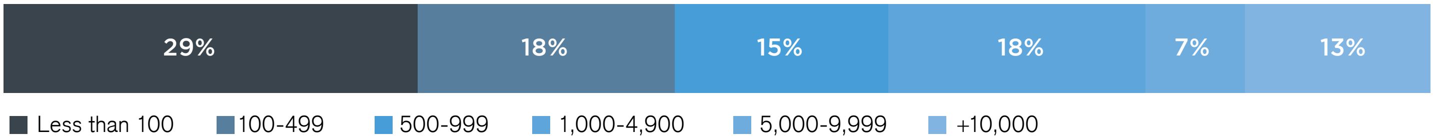
CAREER LEVEL



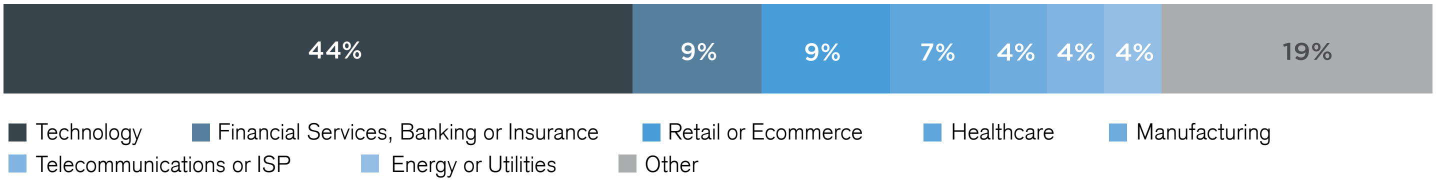
DEPARTMENT



COMPANY SIZE



INDUSTRY



ENEA
Qosmos

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 and protect services for mobile subscribers, enterprise customers, and the Internet of Things. More than 3 billion people rely on Enea technologies in their daily lives.

The Qosmos Division of Enea specializes in Deep Packet Inspection (DPI) software, which recognizes thousands of protocols and metadata to provide the most accurate picture of real-time data activity on networks. As a DPI sensor, the Qosmos Probe strengthens cybersecurity through efficient data analysis and traffic visibility up to the application level:

- Analysis of data flows in real time at n x 10 Gpbs, up to Layer 7
- Recognition of over 3600 protocols and ability to extract more than 5000 metadata
- Fewer false positives when using information from the probe to improve IDS rules
- Forensic data reduced by up to 150x compared to full packet capture

www.qosmos.com