ESG
a division of TechTarget

Enterprise Strategy Group | Getting to the bigger truth.™

The Evolving Role of NDR

Leveraging AI and Cloud Visibility to Support XDR Strategies

John Grady, Senior Analyst

SEPTEMBER 2022

Research Objectives

The potential for serious business disruptions makes detecting threats quickly and accurately critical to preventing data loss, compliance violations, and lost revenue. Even as resources and users leave the traditional perimeter, the network should play a key role in detecting threats to avoid business disruption. Specifically, network-based tools provide consistent, comprehensive visibility across distributed, heterogeneous environments and remain outside the scope of attacker manipulation. Yet the number of threat detection and response tools that are available can leave users unsure of where to prioritize.

In order to gain insight into these trends, ESG surveyed 376 IT, cybersecurity, and networking professionals responsible for evaluating, purchasing, and managing network security products and services for their organizations.

THIS STUDY SOUGHT TO:

Gain insights into the challenges security teams face with the current threat detection and response landscape.

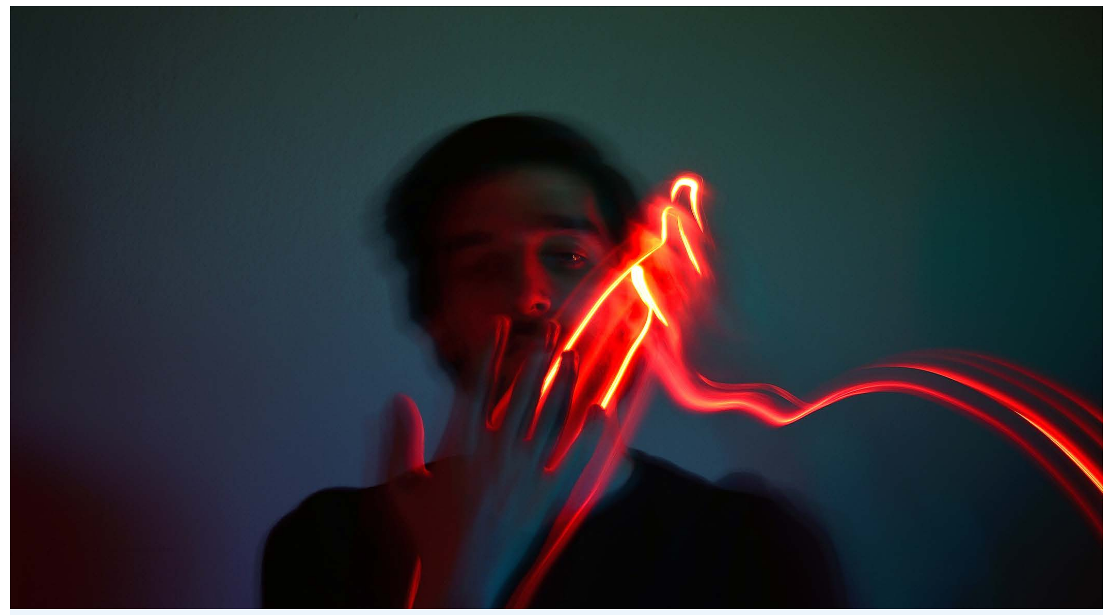
Examine how NDR tools are used today and where they fit into broader XDR plans and strategies.

Gauge the key capabilities organizations require from NDR tools and the use cases they are seeking to address.

Understand why security teams are prioritizing NDR and the benefits they are seeing.

KEY FINDINGS

CLICK TO FOLLOW



Organizations Face Many Threat Detection and Response Challenges

Encrypted threats are a significant problem and can cause issues across the attack chain.

PAGE 4

Security Teams Are Prioritizing NDR for a Variety of Reasons

Many use NDR as a first line of defense due to high fidelity, ease of use, and breadth of coverage.

PAGE 8

Diverse Use Cases Require a Range of Capabilities

Breadth of coverage and investigative capabilities are most important.

PAGE 11

Strong AI Has Become Integral to NDR

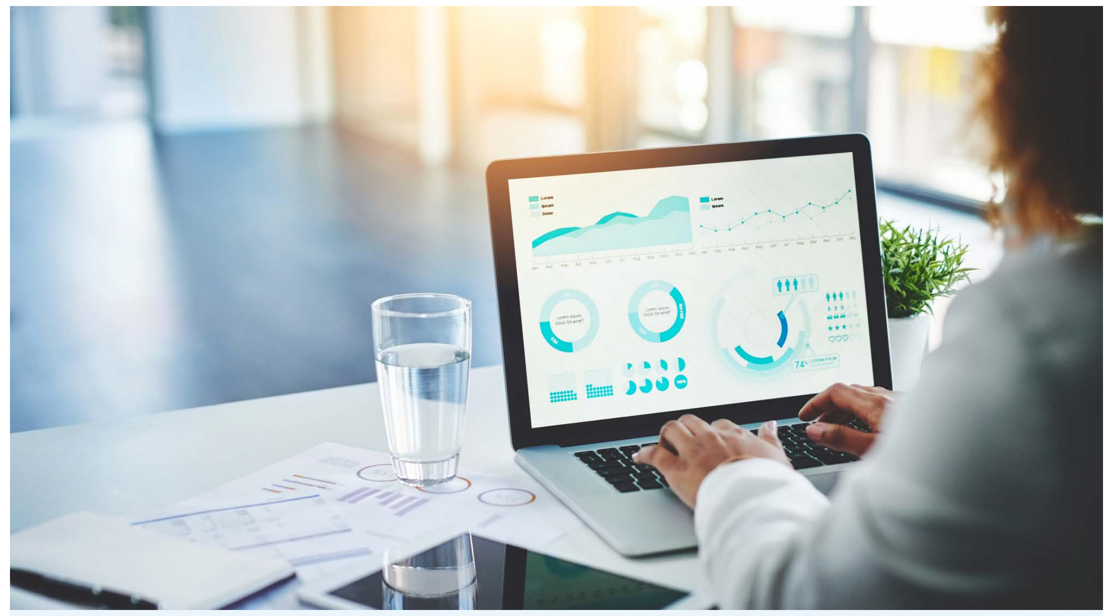
Users expect AI to improve both threat detection and operational efficiency.

PAGE 14

NDR Emerges as a Key Component to XDR Strategies

A majority view NDR as foundational to XDR, and a cloud focus will be critical.

PAGE 16



Security Teams Cite Both Security and Business Benefits from NDR

Many reported fewer breaches, lower costs, and accelerated cloud migrations.

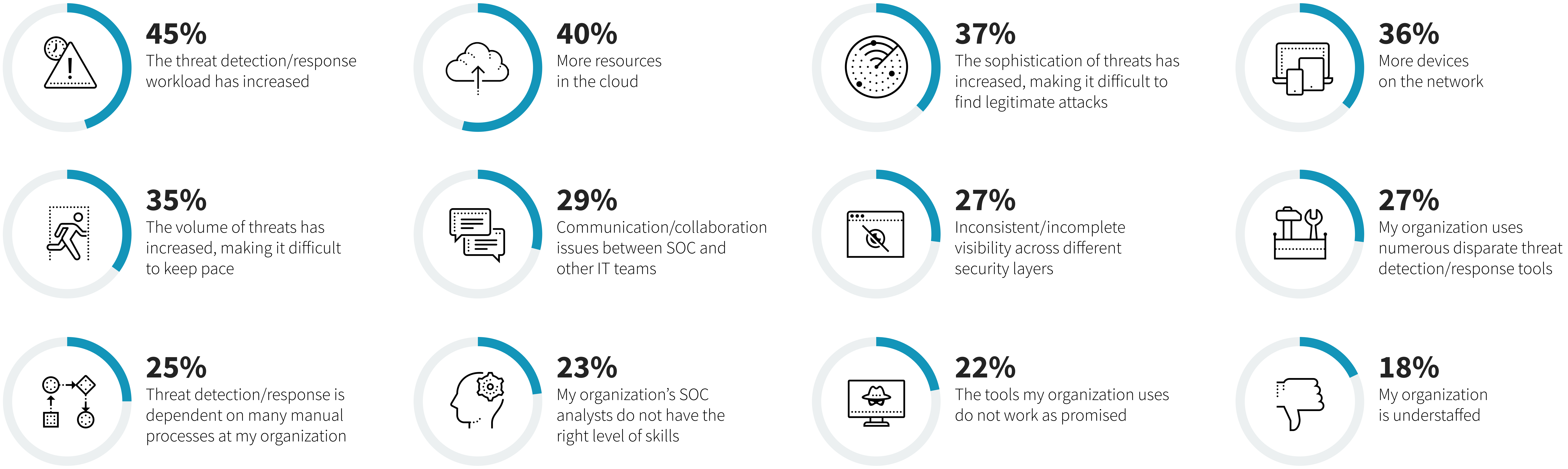
PAGE 19

Organizations Face Many **Threat Detection and Response Challenges**

Complexity, Threats, and SOC Workload Remain Key Issues

Threat detection and response (TDR) continues to become more difficult for many security teams for a variety of reasons. Nearly half of organizations (45%) cited the increasing threat detection and response workload, which in many ways is the result of having to defend more distributed and dynamic environments against increasingly persistent adversaries. Environmental complexity plays a key role, with 40% of organizations citing the increase in cloud-based resources and 36% pointing to the increase in devices on the network as top challenges. The threat landscape is also top of mind, with 37% pointing to the sophistication of threats, and 35% citing the volume of threats as challenges.

Threat detection and response challenges.



45% The threat detection/response workload has increased

40% More resources in the cloud

37% The sophistication of threats has increased, making it difficult to find legitimate attacks

36% More devices on the network

35% The volume of threats has increased, making it difficult to keep pace

29% Communication/collaboration issues between SOC and other IT teams

27% Inconsistent/incomplete visibility across different security layers

27% My organization uses numerous disparate threat detection/response tools

25% Threat detection/response is dependent on many manual processes at my organization

23% My organization's SOC analysts do not have the right level of skills

22% The tools my organization uses do not work as promised

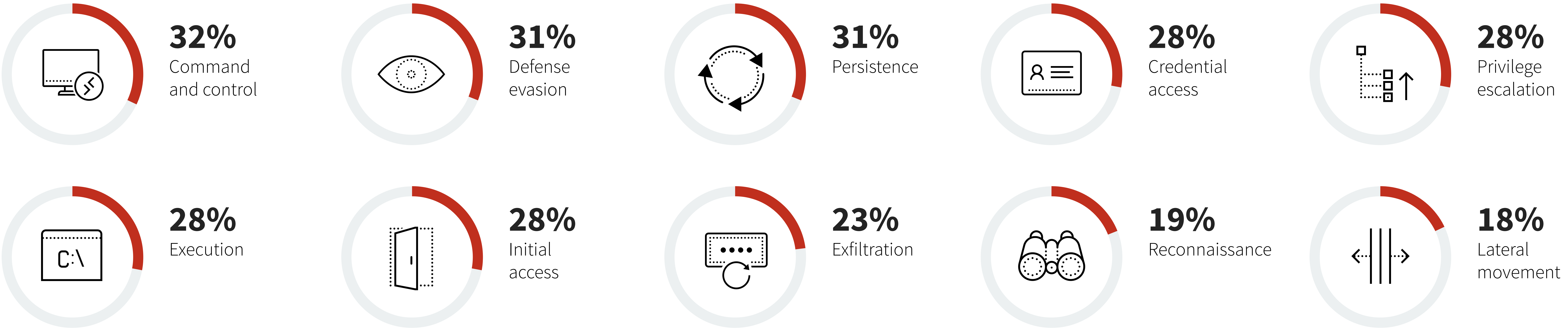
18% My organization is understaffed

> Many security teams can have difficulty **detecting and stopping threats targeting their organization.”**

Issues Are Prevalent Across the Attack Chain

As a result of these challenges, many security teams can have difficulty detecting and stopping threats targeting their organization. Further, issues persist across most of the MITRE ATT&CK Framework. While nearly one-third (32%) of respondents cited difficulty identifying and blocking command and control communications, many also reported issues during the evasive and persistence phases. Problems detecting credential access, privilege escalation, execution, and initial access were all cited by 28% of organizations. Detecting reconnaissance and lateral movement were less problematic, but still reported by 19% and 18% of organizations, respectively.

Areas of greatest difficulty within MITRE ATT&CK framework.



32% Command and control

31% Defense evasion

31% Persistence

28% Credential access

28% Privilege escalation

28% Execution

28% Initial access

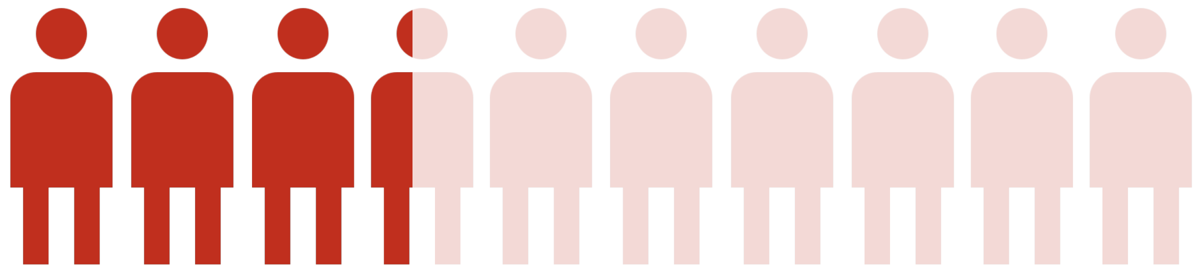
23% Exfiltration

19% Reconnaissance

18% Lateral movement

Attackers Use Encryption Frequently and Across Multiple Stages

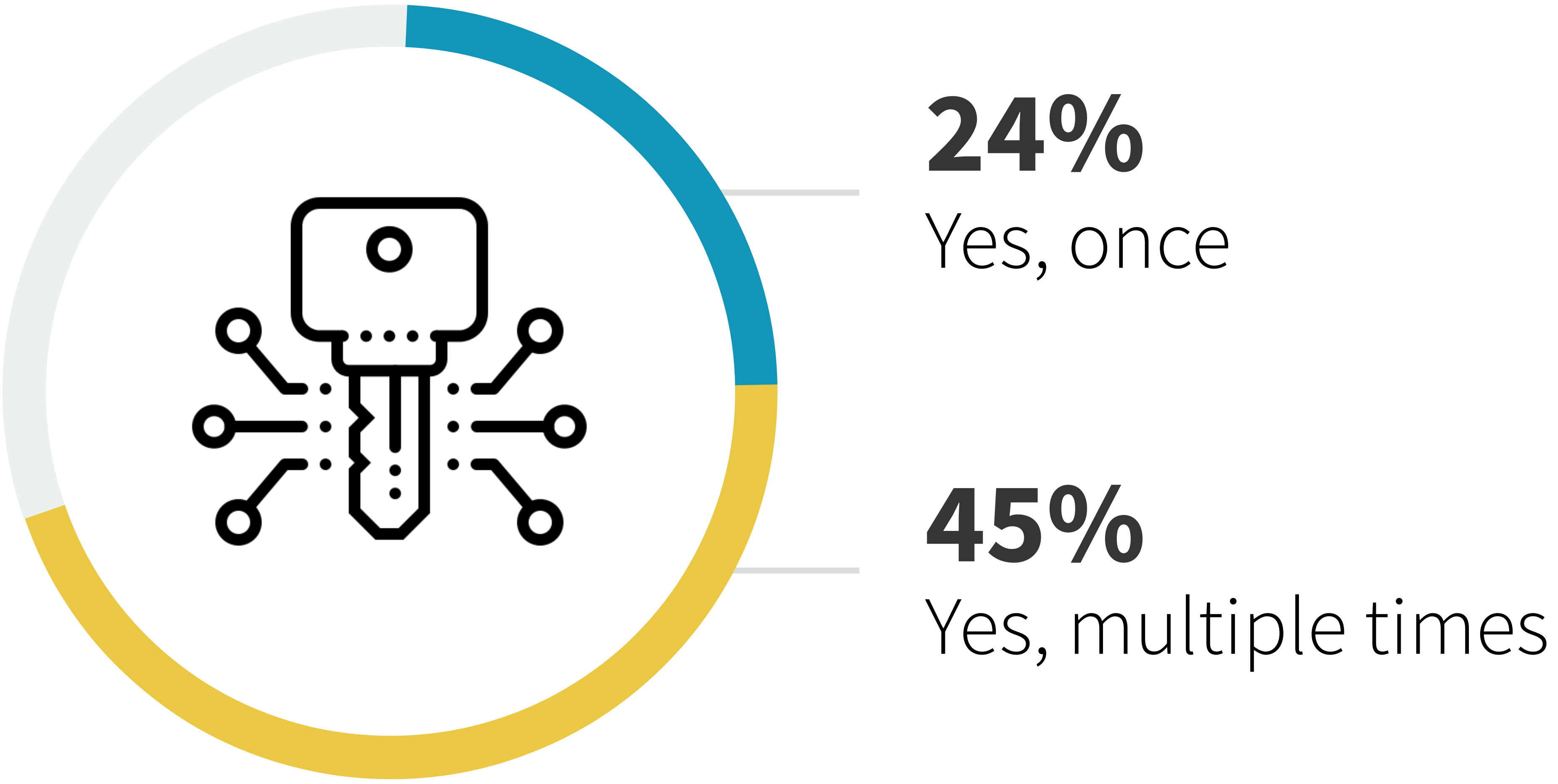
The use of encryption to obfuscate attacks is one reason detection has become more difficult over time. In fact, 24% of organizations have suffered an attack that leveraged encryption once, while nearly half (45%) have suffered multiple attacks that used this approach. Further, encryption is frequently used across multiple stages of the attack. More than two-thirds (70%) of organizations that had suffered an encrypted attack reported that data was exfiltrated through encrypted channels. This was followed by 64% that indicated that command and control communications were encrypted and/or malware was encrypted during delivery. A key reason for this is likely a lack of visibility, with only 34% of organizations reporting that they have visibility into all the encrypted traffic in their environment.



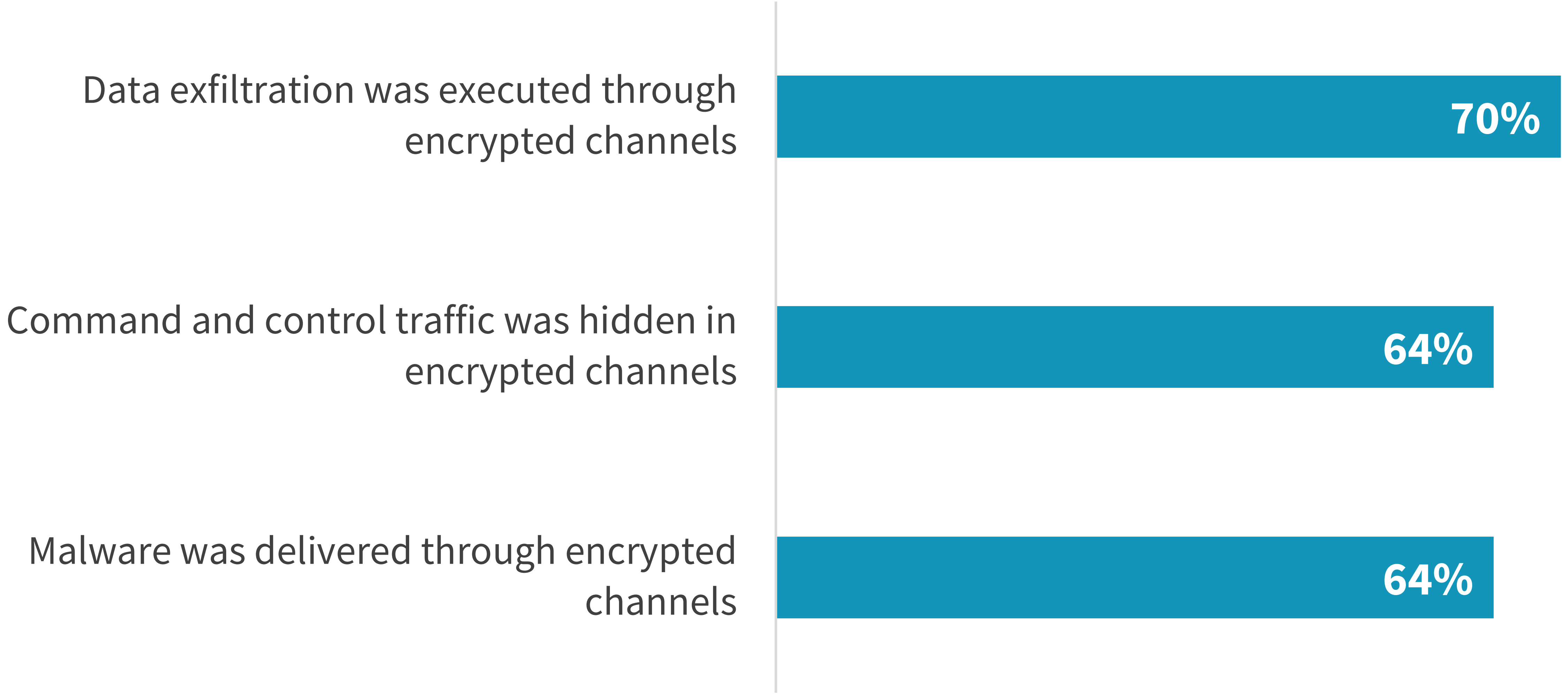
Only 34%

of organizations have visibility into **ALL** their encrypted traffic.

Has your organization ever fallen victim to an attack that used encrypted traffic to avoid detection?



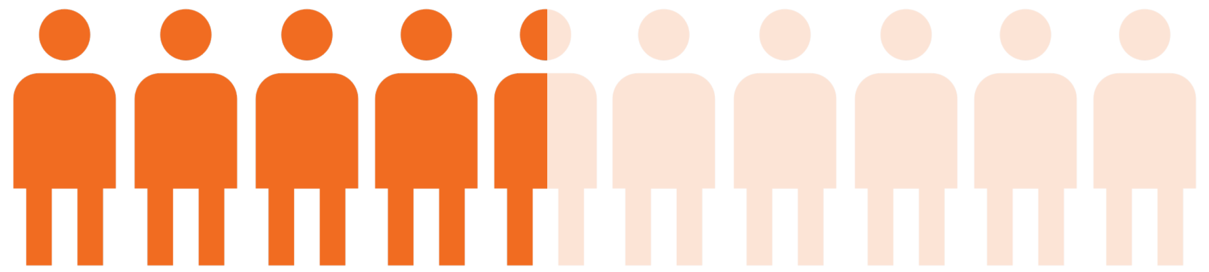
How attacks leveraged encryption.



Security Teams Are **Prioritizing NDR for a Variety of Reasons**

NDR Is Often Used as a First Line of Defense

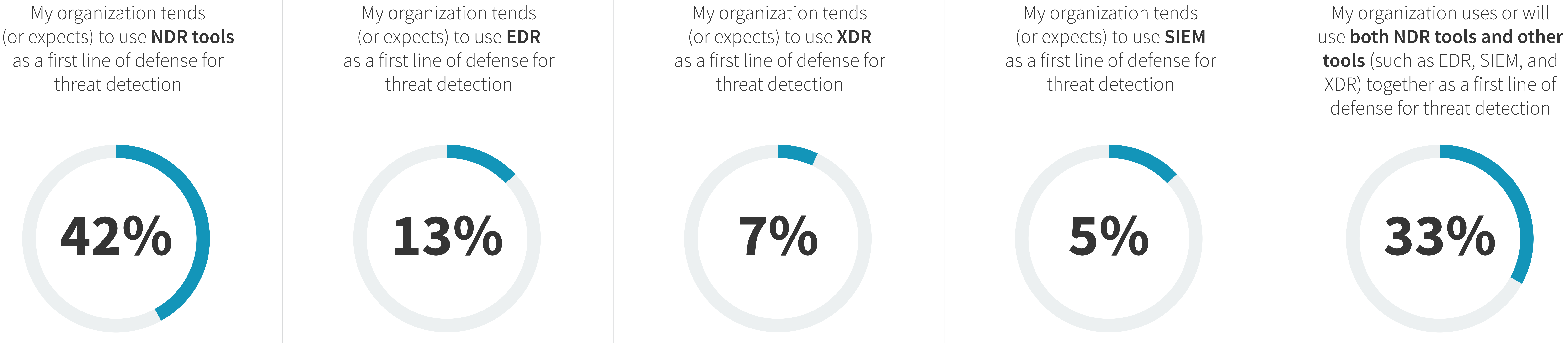
Security teams have a variety of choices when it comes to threat detection and response tools. Security information and event management (SIEM) and endpoint detection and response (EDR) are staples in the SOC, and extended detection and response (XDR) has seen a surge in interest over the last 18 months. Yet even with all these options, 46% say NDR is most effective for threat detection and response. As a result, many are prioritizing NDR. Specifically, 42% say they tend to use NDR as a first line of defense for threat detection. An additional 33% use NDR in conjunction with other tools, such as SIEM, EDR, and XDR, as a first line of defense.



46%

of organizations identify network detection and response technology **as most effective for threat detection and response.**

How organizations use NDR for threat detection and response.

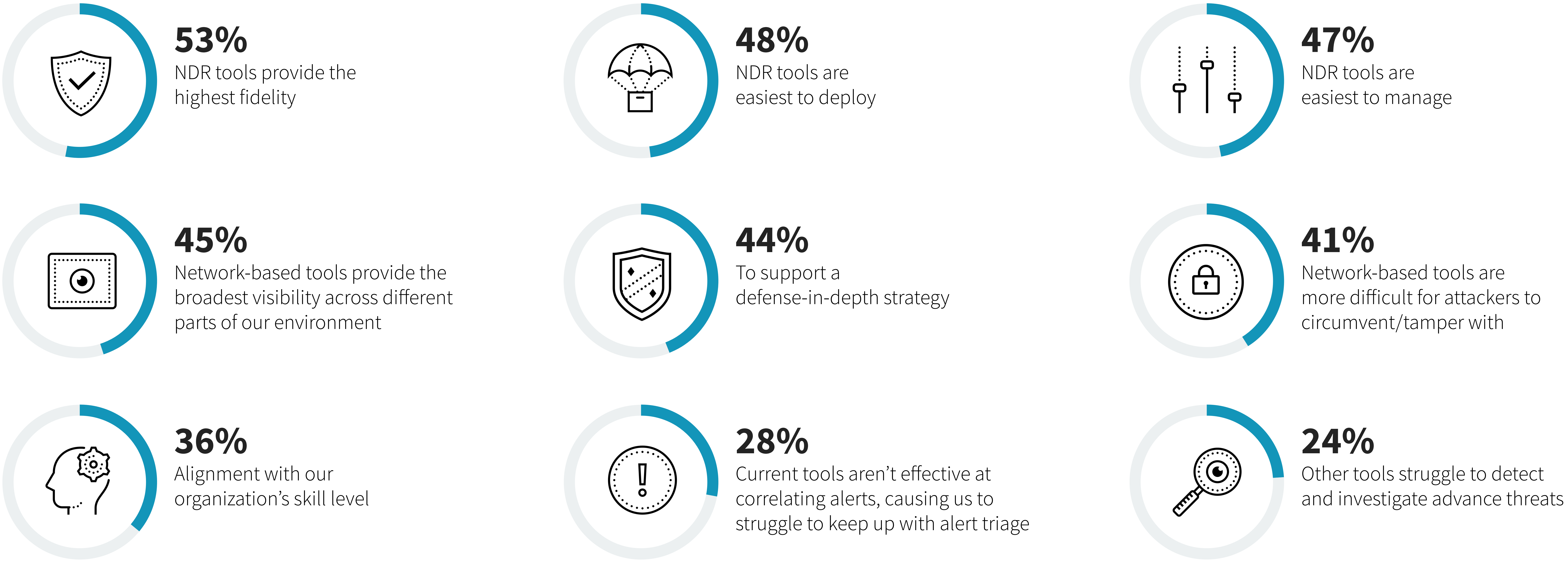


BACK TO CONTENTS

NDR Is Used Due to High Fidelity, Ease of Use, and Breadth of Coverage

The reasons for which an organization may choose to use NDR tools can vary. Both false positives and false negatives can have a significant impact on security teams, making high efficacy critical. As a result, more than half (53%) of organizations use NDR because they feel it provides the highest fidelity. Ease of deployment (48%) and ease of management (47%) were also commonly cited and can help organizations struggling with the cybersecurity skills gap achieve better efficiency. Finally, 45% noted the visibility NDR offers across different parts of the environment as a reason for their use. With attackers seeking to exploit the siloed visibility many organizations have across cloud and on-premises resources, achieving more consistent visibility has become a priority.

Primary reasons for using NDR.



53%
NDR tools provide the highest fidelity

48%
NDR tools are easiest to deploy

47%
NDR tools are easiest to manage

45%
Network-based tools provide the broadest visibility across different parts of our environment

44%
To support a defense-in-depth strategy

41%
Network-based tools are more difficult for attackers to circumvent/tamper with

36%
Alignment with our organization's skill level

28%
Current tools aren't effective at correlating alerts, causing us to struggle to keep up with alert triage

24%
Other tools struggle to detect and investigate advance threats

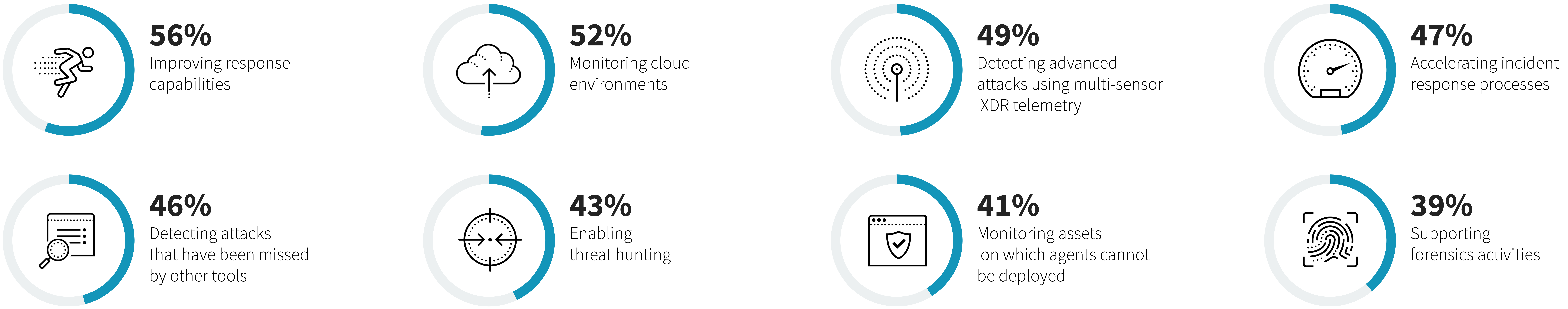
Diverse Use Cases **Require a Range of Capabilities**

> “At the top of the list, 56% of respondents seek to **improve their organization’s response capabilities.”**

NDR Can Support a Diverse Set of Use Cases

Security teams use NDR to support a number of use cases. At the top of the list, 56% of respondents seek to improve their organization’s response capabilities. Relatedly, 47% use NDR to accelerate their incident response processes. The evolution of traditional network traffic analytics (NTA) toward NDR is really focused on these points: streamlining workflows and facilitating integrations to ensure that once a threat is detected, it can be addressed quickly and effectively. More than half of respondents (52%) use NDR to monitor cloud environments, further validating the previous point about the need for consistency across internal and external environments. Along similar lines, 41% use NDR to monitor assets on which agents cannot be deployed. This could point to cloud environments as well as IoT devices, both of which can benefit from agentless deployment models.

Use cases supported by NDR.



56% Improving response capabilities

52% Monitoring cloud environments

49% Detecting advanced attacks using multi-sensor XDR telemetry

47% Accelerating incident response processes

46% Detecting attacks that have been missed by other tools

43% Enabling threat hunting

41% Monitoring assets on which agents cannot be deployed

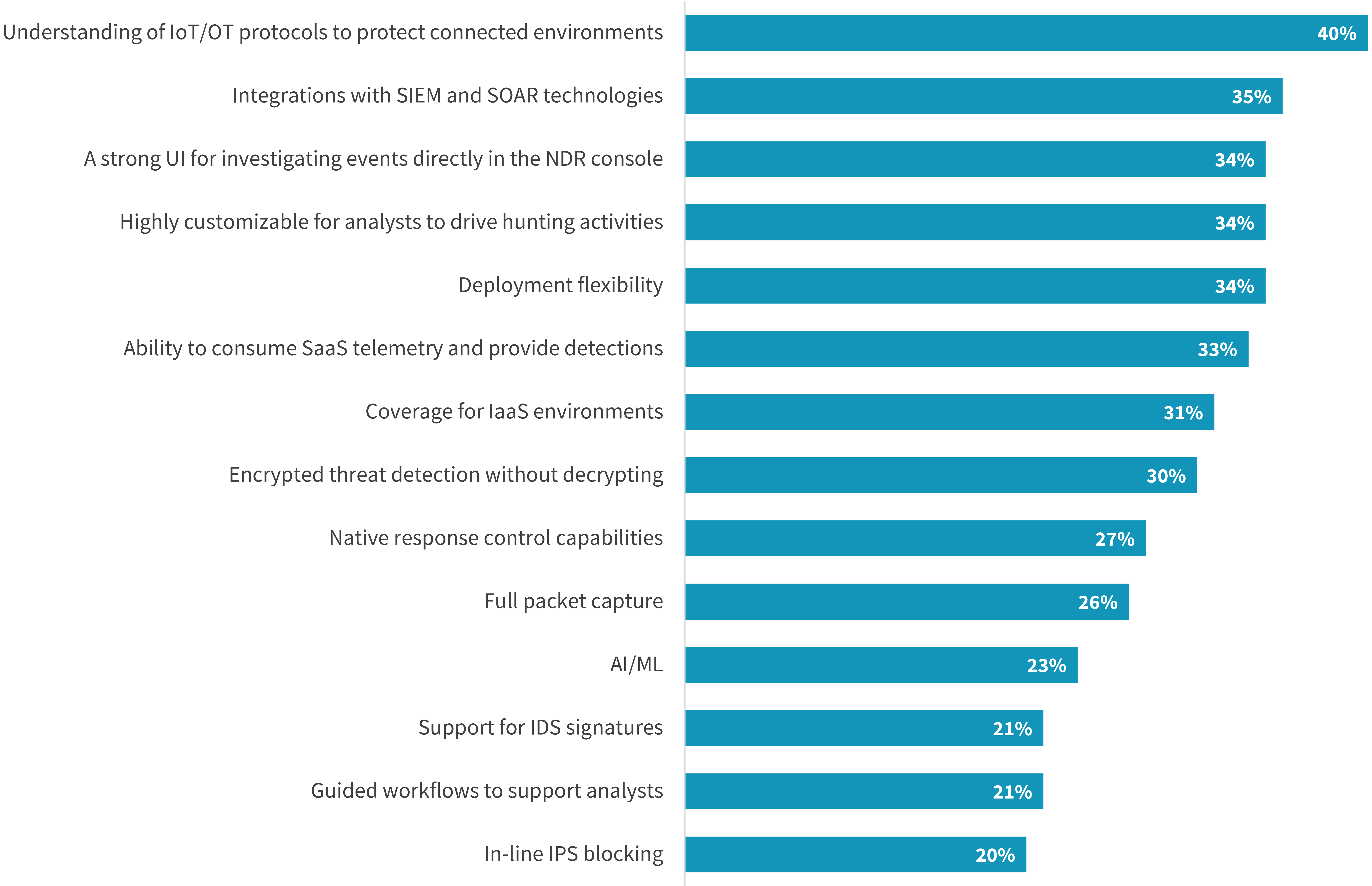
39% Supporting forensics activities

BACK TO CONTENTS

Coverage and Investigative Capabilities Are Deemed Most Important

Supporting such a variety of use cases requires a number of capabilities. To address different parts of the environment consistently, understanding IoT/OT protocols (40%), deployment flexibility (34%), and coverage for IaaS environments (31%) are all important. Additionally, the ability to consume SaaS telemetry (33%) is a newer feature that can help round out NDR coverage. When it comes to investigating incidents, security analysts typically have a preference as to how they like to work. Some prefer to turn to the SIEM early in the process, reflected by the fact that 35% cited the need for integrations with SIEM and SOAR tools. Conversely, others may spend more time in the NDR console itself, either to triage and perform initial analysis or because their organization does not use a SIEM. As a result, 34% highlighted the need for a strong UI to investigate events directly. Finally, 30% cited the need to detect encrypted threats without decrypting, highlighting threat posed from these types of attacks.

Most important NDR attributes.



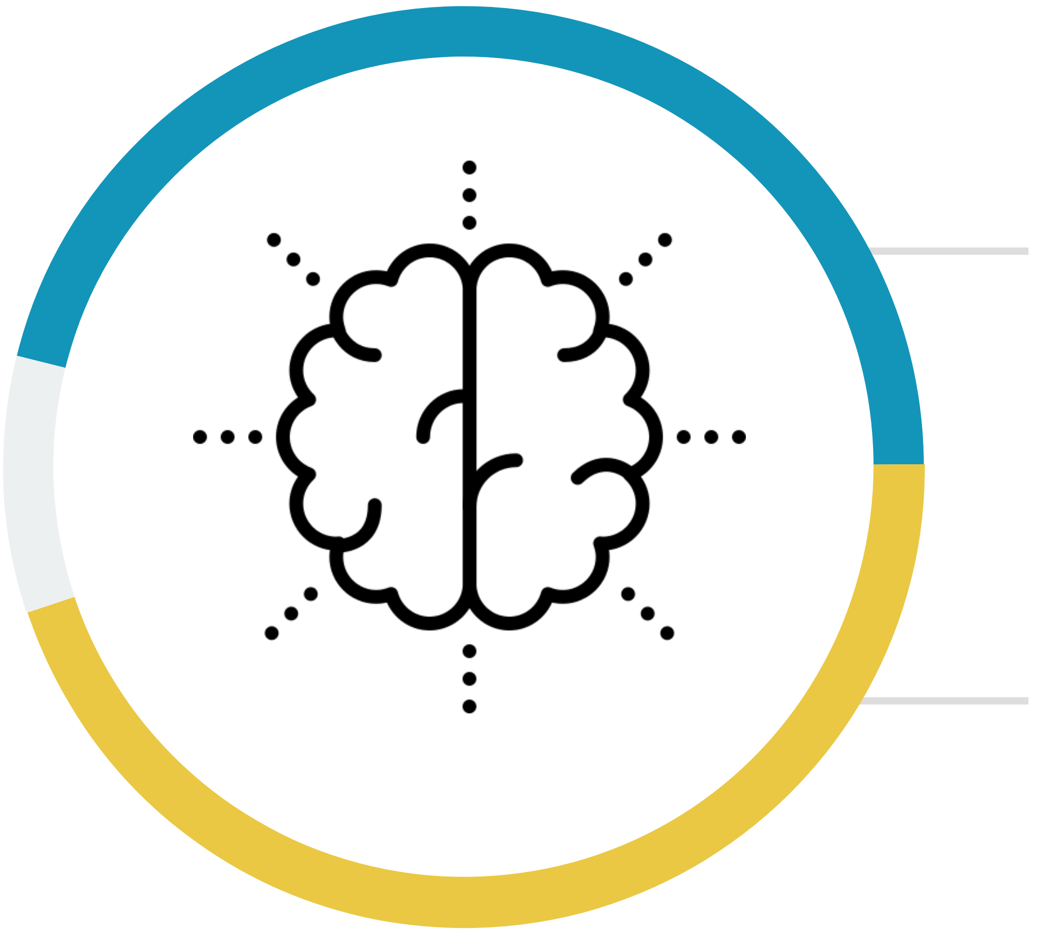
Strong AI Has Become **Integral to NDR**

Expected Benefits from Incorporating AI/ML as Part of NDR

Over the last few years, NDR vendors have added artificial intelligence and machine learning capabilities to their tools. The need for AI/ML support is recognized by users, with 46% indicating strong AI capabilities are critical to NDR, and an additional 45% saying strong AI is important. There is clearly a belief that AI can enable better detections, with 61% of organizations interested in AI-enabled NDR for better detection accuracy, and 59% for better detection speed.

AI/ML may provide benefits from an efficiency and workflow perspective as well. Specifically, accurately prioritizing alerts (47%), informing/directing analyst workflows (45%), and automating response (42%) were all frequently mentioned by respondents. Especially in cloud environments where scale and speed are critical, these capabilities can help security teams keep pace.

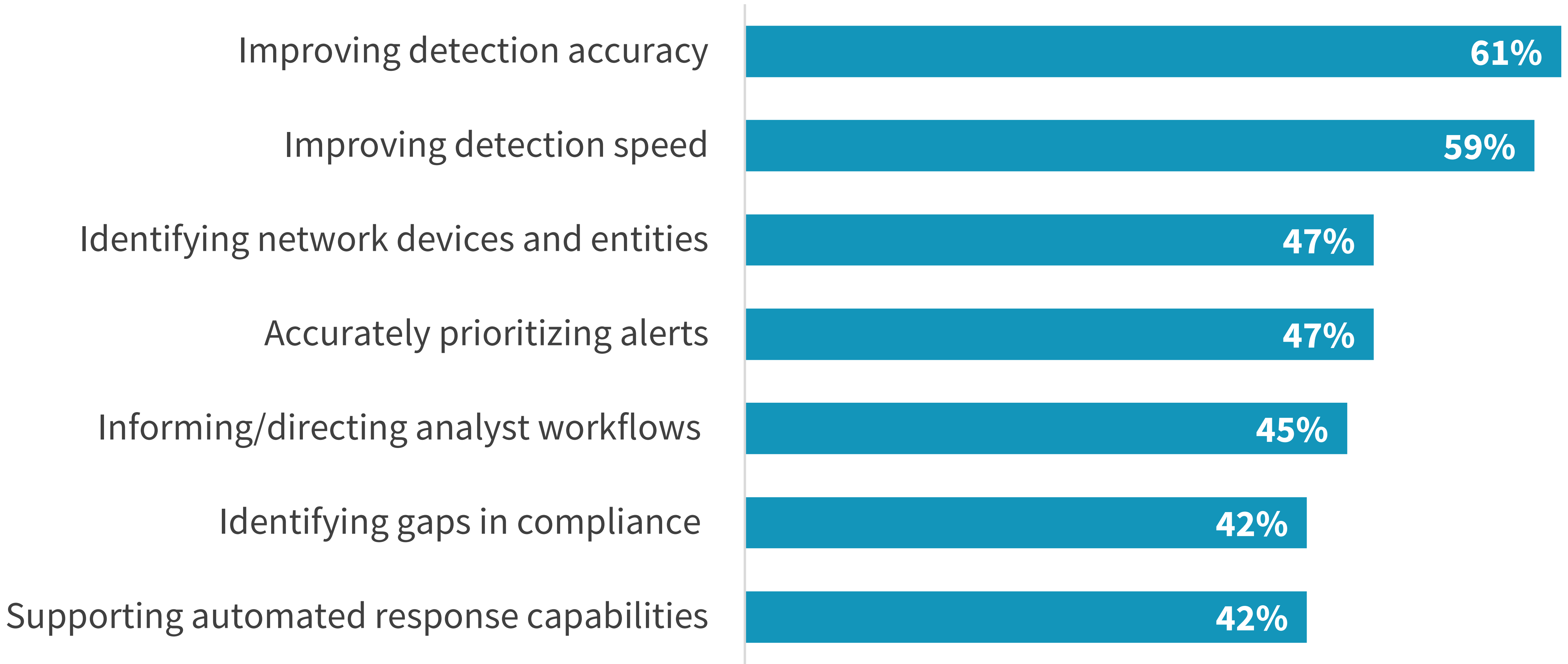
Importance of AI in NDR tools.



46%
Strong AI capabilities are a **critical** attribute of NDR tools

45%
Strong AI capabilities are an **important** attribute of NDR tools

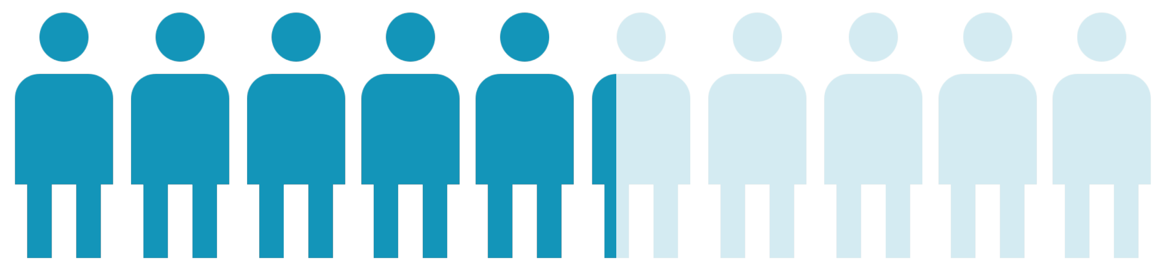
Reasons for leveraging AI/ML capabilities as part of NDR solutions.



NDR Emerges as a **Key Component to XDR Strategies**

Most View NDR As Foundational to XDR

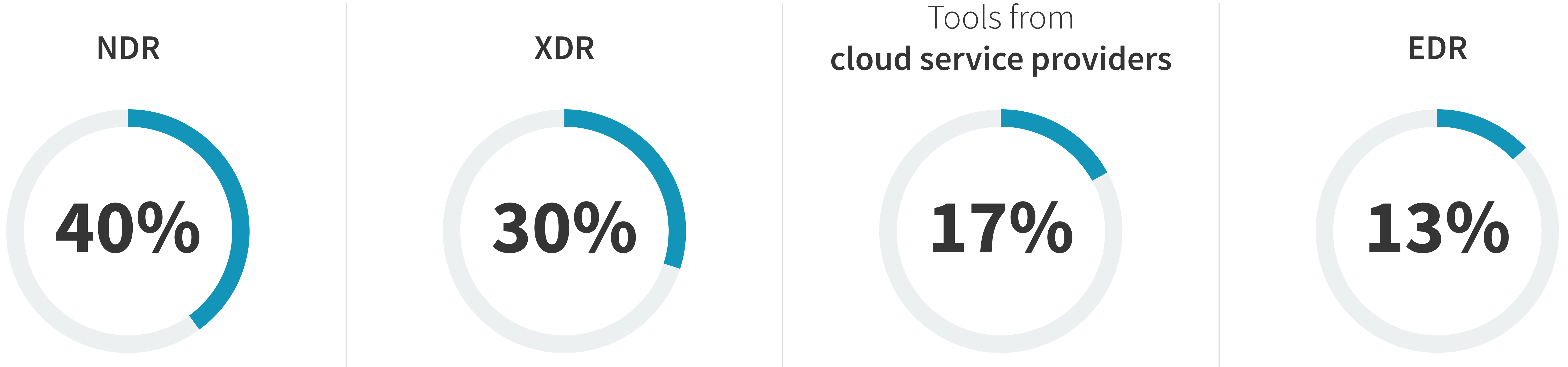
XDR is on the radar for many organizations. In fact, more than half of organizations (52%) say they are in the process of deploying XDR, with an additional 41% planning to in the next 12-24 months. While XDR at times has been described as an extension of EDR, most organizations seem to disagree. Specifically, 56% say that NDR will form the foundation of their organization's XDR strategy. More than one-third (35%) say NDR will be a secondary part of XDR. Only 3% say NDR will remain independent from XDR. For many, this will form the basis of their cloud detection and response strategies, with 40% indicating NDR is most effective at collecting, processing, and analyzing cloud telemetry data, and 30% believing XDR is most effective.



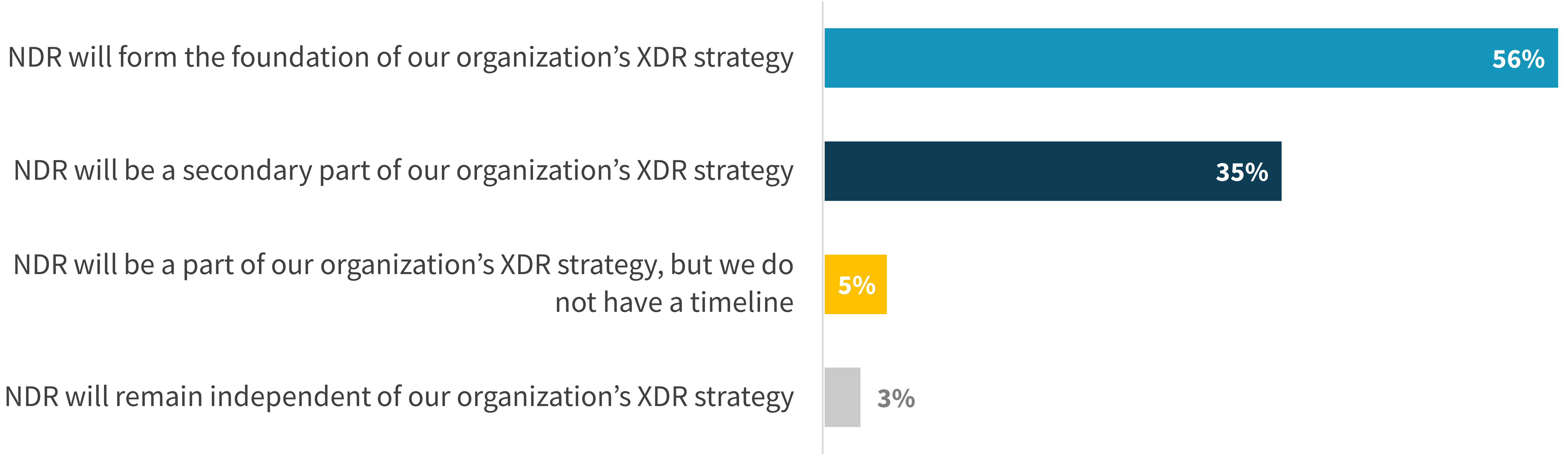
52%

of organizations are in the **process of deploying an XDR solution.**

Most effective TDR tool for collecting, processing, and analyzing cloud telemetry data.



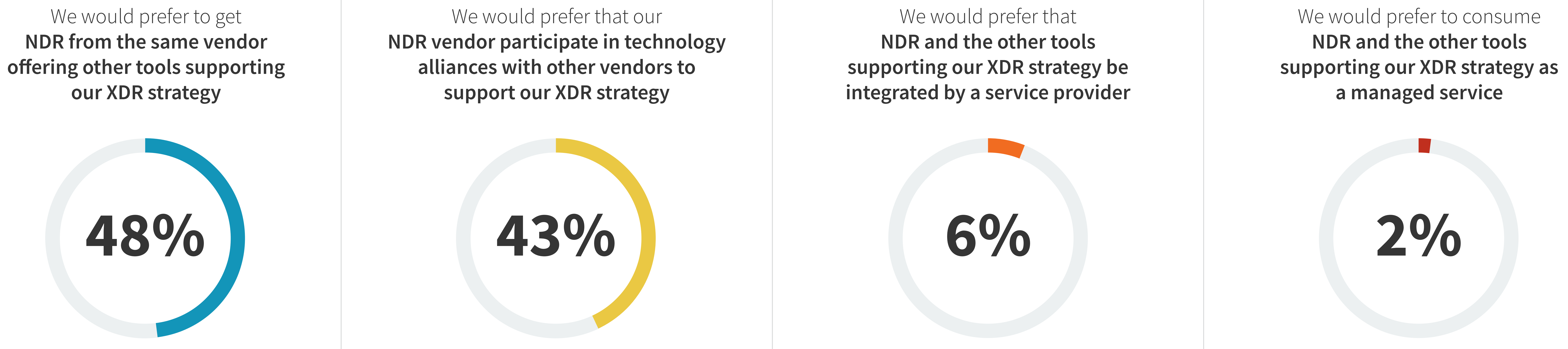
Role of NDR in an XDR strategy.



Limited Agreement on How NDR Will Be Consumed

Nearly half of organizations (48%) say they would prefer to get NDR and other XDR capabilities from the same vendor. At the same time, 43% indicate an alliance approach is most attractive. Overall, 8% will look to service providers (either for integration or management). So, while there is consensus that XDR should be vendor-led, as opposed to service provider-led, organizations disagree on the best approach. Ultimately, choosing a path will depend on the tools that have already been deployed, vendor relationships, and the outcomes expected from XDR.

How NDR will likely be consumed as part of an XDR strategy.

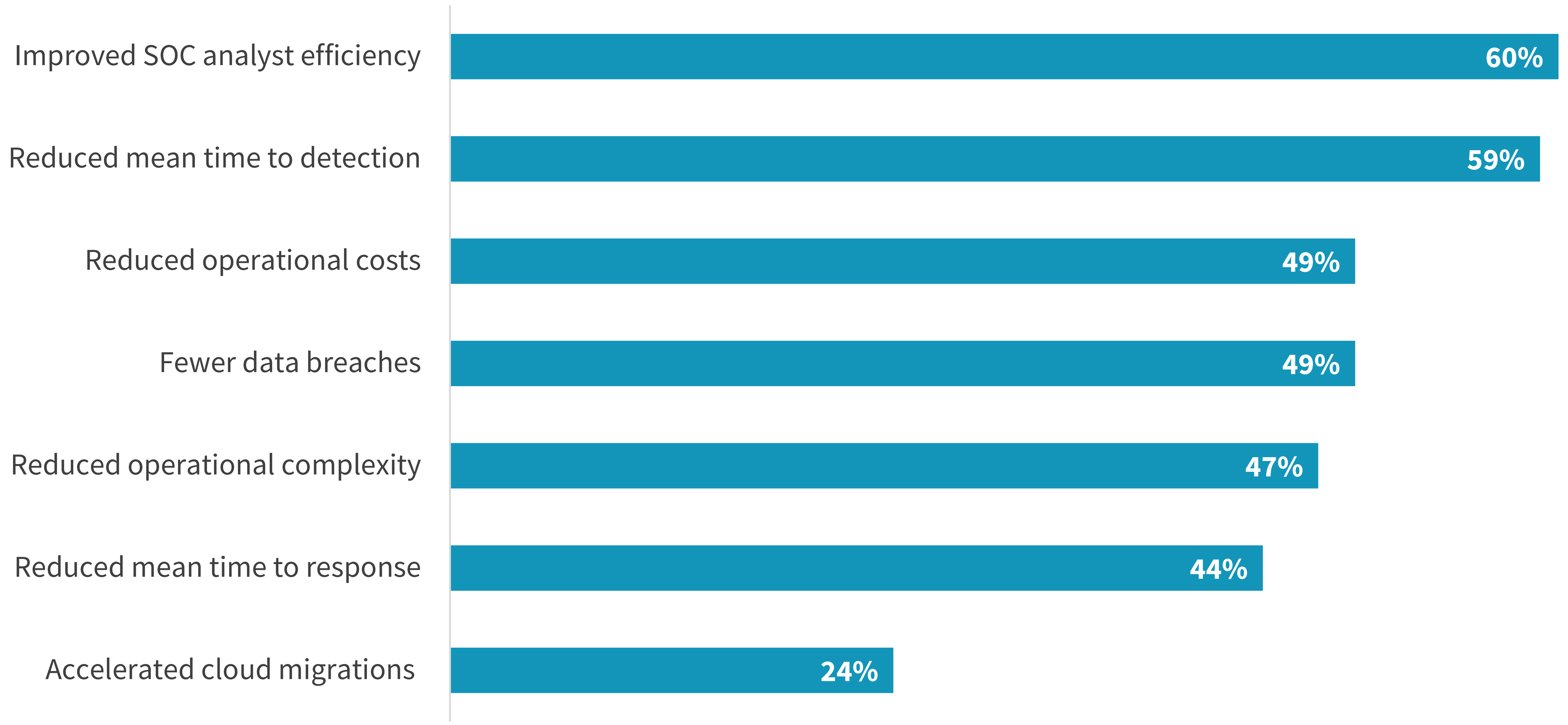


Security Teams Cite **Both Security and Business Benefits from NDR**

Improved Analyst Efficiency and Time to Detection Are Common Benefits from NDR

Security teams reported a variety of benefits due to their organization's use of NDR. In fact, respondents claimed at least three benefits on average. Improved SOC analyst efficiency was reported by 60% of organizations. Similarly, 59% cited reduced mean time to detection, and nearly half (49%) indicated they had fewer data breaches. In addition to positive security outcomes, 49% claimed reduced operational costs, and 47% noted reduced operational complexity. While cited least often, nearly a quarter (24%) said that NDR had helped accelerate cloud migrations. So, while threat detection and response strategies can vary widely, NDR can help organizations achieve both better security and business outcomes.

Benefits realized from NDR.



> "Respondents claimed **at least three benefits on average.**"

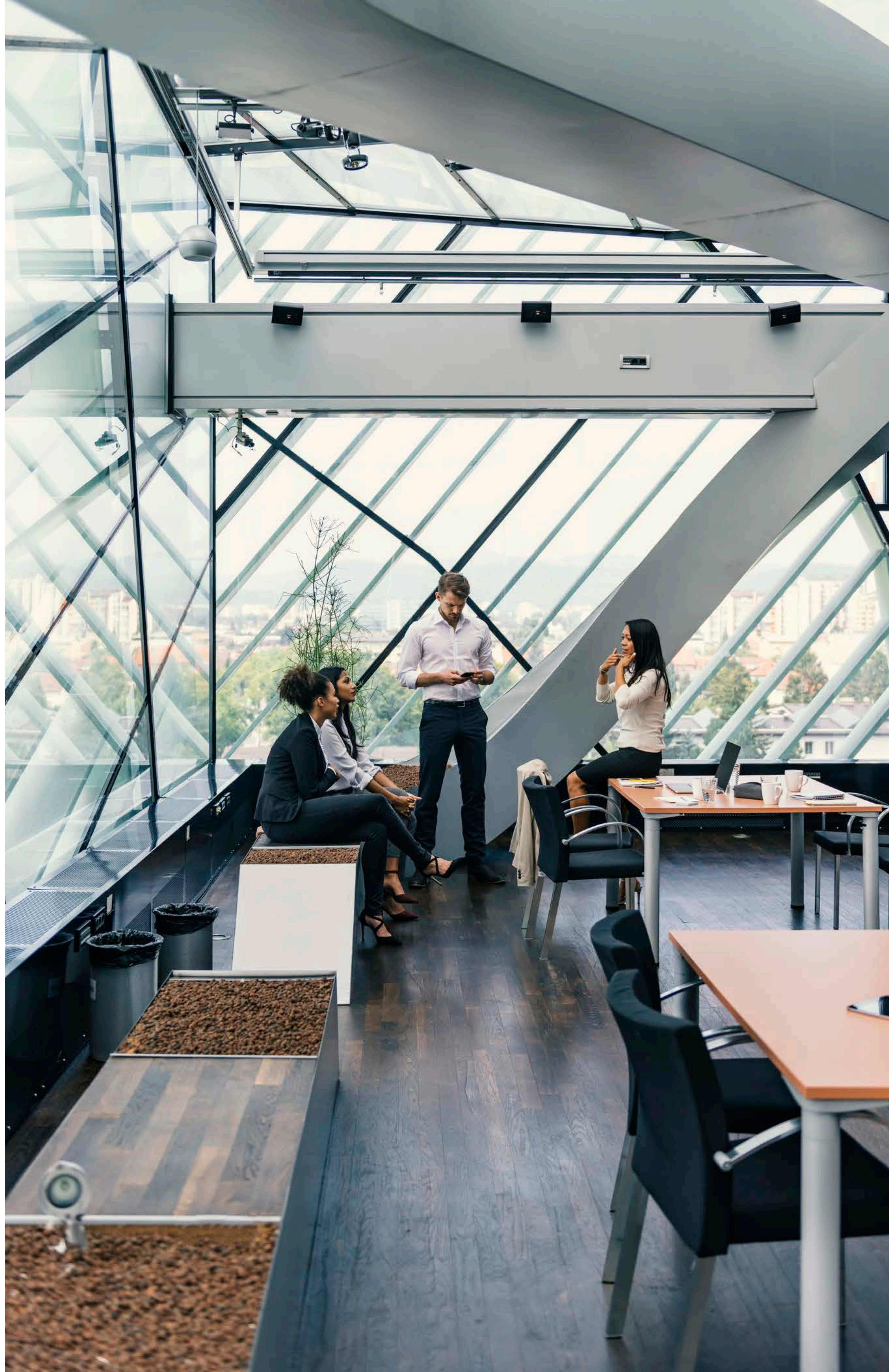
corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

LEARN MORE

ABOUT ESG

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

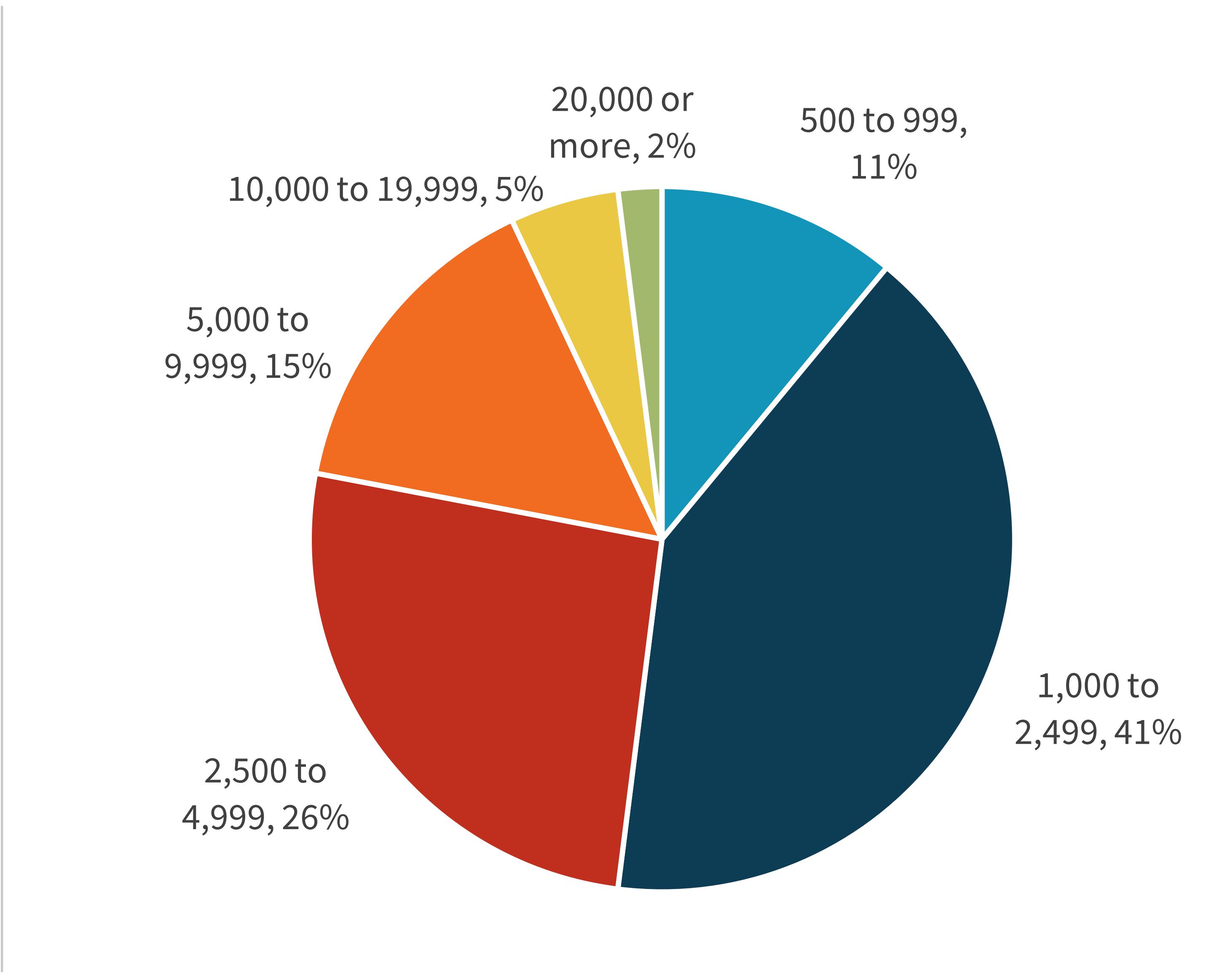


Research Methodology and Demographics

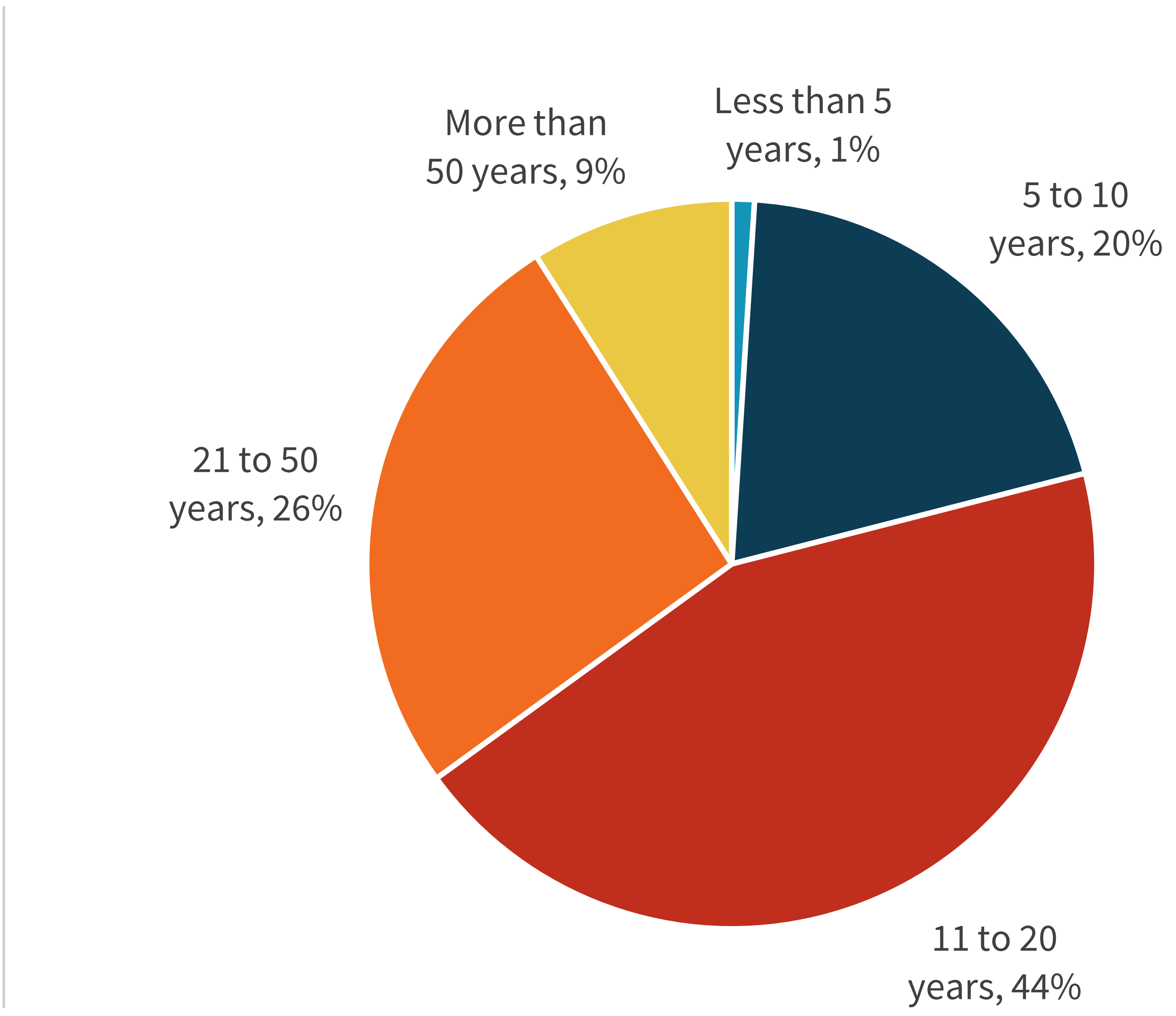
To gather data for this report, ESG conducted a comprehensive online survey of IT, cybersecurity, and networking professionals from private- and public-sector organizations in North America between August 5, 2022 and August 16, 2022. To qualify for this survey, respondents were required to be IT, cybersecurity, or networking professionals responsible for evaluating, purchasing, and managing network security products and services for their organizations. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 376 IT, cybersecurity, and networking professionals.

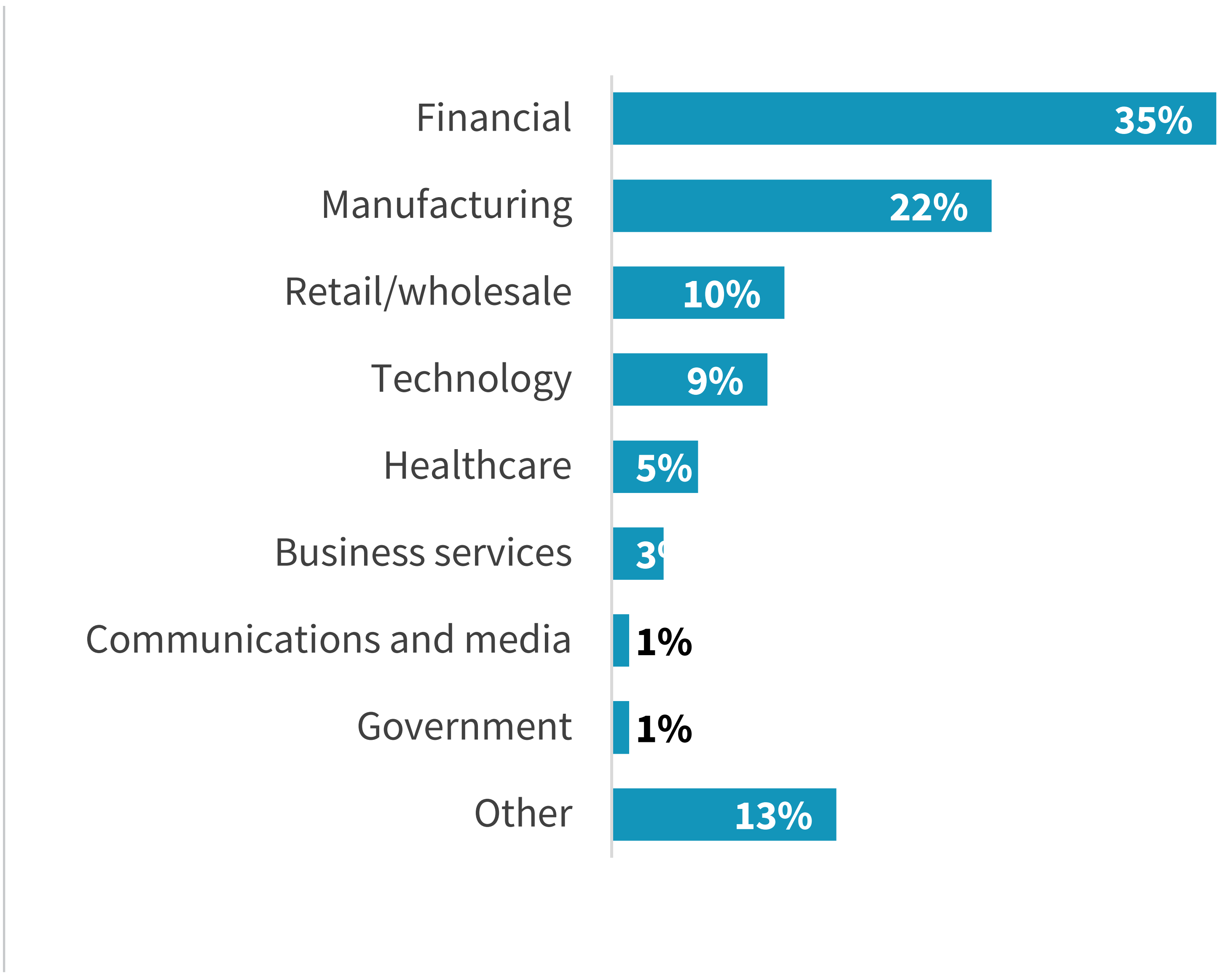
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



ESG
a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.