Enterprise Strategy Group™

The Role of Network Visibility in Protecting Modern Environments

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP
SEPTEMBER 2025

© 2025 TechTarget, Inc. All Rights Reserved.

Research Objectives

With all the different “detection and response” tools available, security teams can sometimes underestimate the value of network tools like network detection and response (NDR). Even as resources and users leave the traditional perimeter, network visibility plays a critical role in detecting threats to business operations. Network-based tools provide consistent, comprehensive visibility across distributed, heterogeneous environments and remain outside the scope of attacker manipulation. Security leaders need to understand how peer organizations are benefiting from the use of network-based threat detection and response tools like NDR, and the key innovations that have been made to better address increasingly distributed, cloud-centric environments.

To gain insights into these trends, TechTarget’s Enterprise Strategy Group surveyed 400 cybersecurity and IT professionals in North America (U.S. and Canada) involved with network-based threat detection and response (TDR) technology products and services at their organization.

This study sought to:

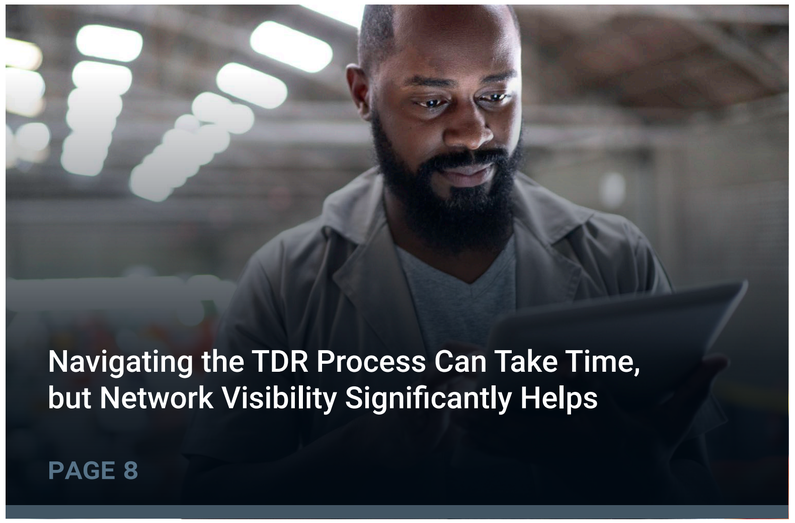
- **Identify** the key TDR challenges security teams face.
- **Determine** what bottlenecks exist in the TDR process and the impact network visibility has.
- **Understand** the key capabilities organizations require from NDR tools and the use cases they are seeking to address.
- **Gauge** whether organizations are seeing benefits from their NDR investments.

© 2025 TechTarget, Inc. All Rights Reserved.

Key Findings

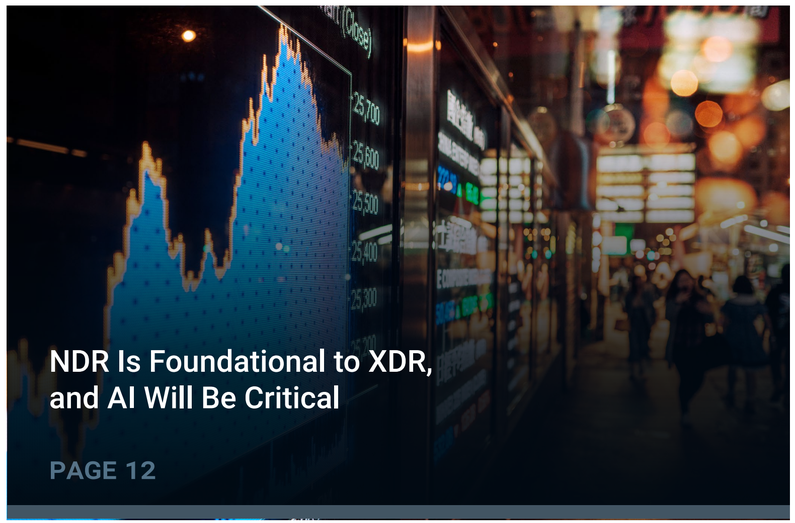
Threat Detection and Response Challenges Persist, but Network Tools Are Often the First Line of Defense

PAGE 4



Navigating the TDR Process Can Take Time, but Network Visibility Significantly Helps

PAGE 8

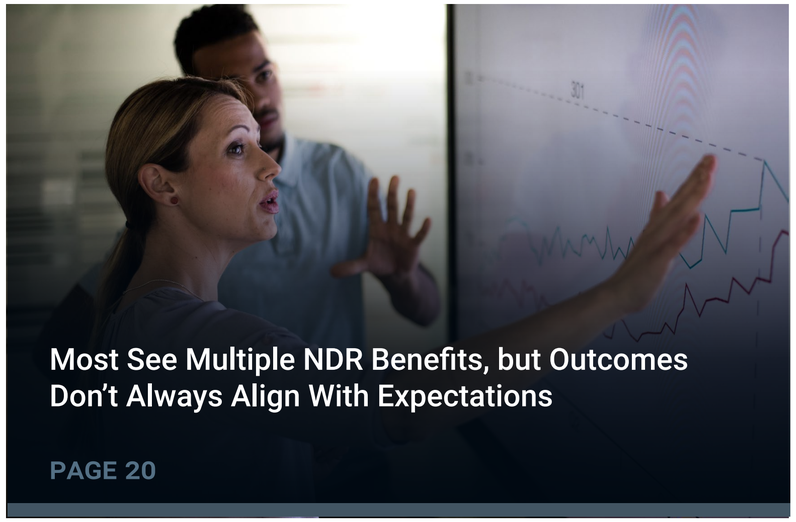


NDR Is Foundational to XDR, and AI Will Be Critical

PAGE 12

NDR Supports a Broad Set of Use Cases, Requiring Many Different Attributes

PAGE 16



Most See Multiple NDR Benefits, but Outcomes Don't Always Align With Expectations

PAGE 20

© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

Threat Detection and Response Challenges Persist, but Network Tools Are Often the First Line of Defense

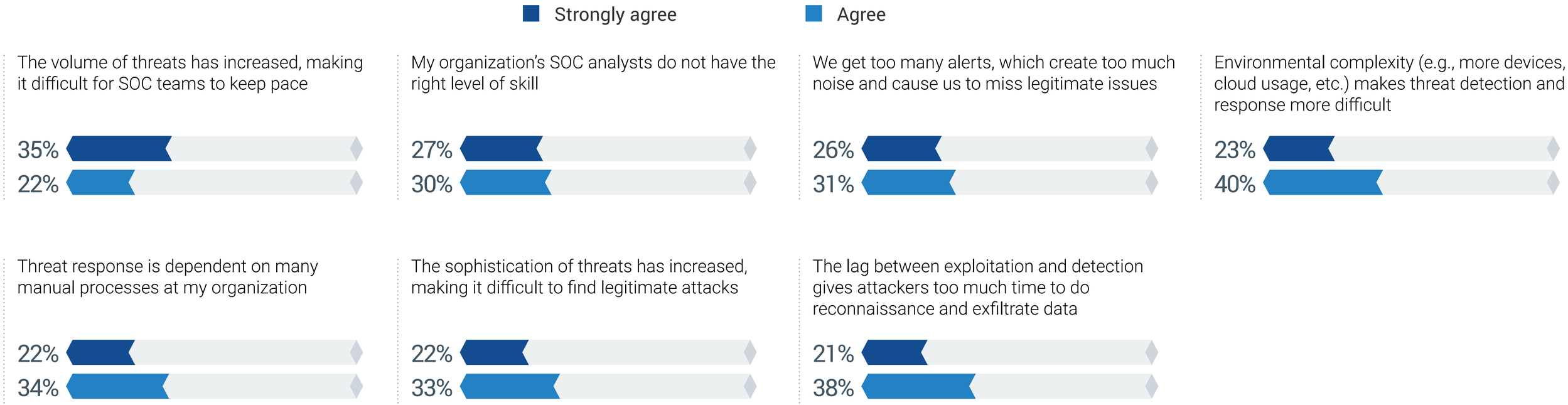
Threat Detection and Response Challenges Persist

Security teams have a lot deal with these days. The threat landscape continues to evolve, challenging even the most advanced organizations. Both the volume of threats (57%) and sophistication of threats (55%) were prominently cited as challenges, with attackers beginning to leverage AI to both expand their target base and generate stealthy attacks.

At the same time, inefficiencies and resource constraints in the SOC itself make dealing with these threats more difficult. The lag between exploitation and detection was reported as a challenge by 59% of respondents and can be exacerbated by other issues like the skill shortage (57%), alert fatigue (57%), and the dependency on manual processes (56%).

Yet the most commonly cited challenge, reported by nearly two-thirds of respondents (63%), was environmental complexity. Detecting all the threats targeting an organization and overcoming inefficiencies and resource constraints in the SOC becomes noticeably more difficult when users, devices, and resources are distributed across campus, branch, cloud, edge, and remote locations.

Threat detection and response challenges.



© 2025 TechTarget, Inc. All Rights Reserved.

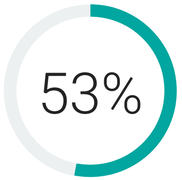
Back to Contents

Despite Market Focus on Extended Detection and Response (XDR) and Cloud Detection and Response (CDR), Network Tools Are Highly Valued

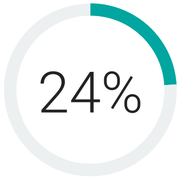
To address many of these issues, many organizations are turning to network visibility. As environments have expanded, much of the industry attention has been on tools focused on cloud or endpoint detection and response (EDR)-centric XDR solutions. But while these can provide value, the broad, layered, and tamper-proof visibility that network tools provide offer significant value as an initial detection mechanism. In fact, nearly two-thirds (65%) use network visibility and telemetry as a first line of defense. More than half (53%) use network tools exclusively for this purpose, while 12% use network visibility along with other tools as a first line of defense.

Further, despite being incorrectly labeled as on-premises solutions, a plurality of 41% say network detection and response or visibility tools are best equipped to provide visibility across hybrid multi-cloud environments. Network vendors have been investing in their platforms over the last few years to address modern environments, and this is clearly bearing fruit in the eyes of many security professionals.

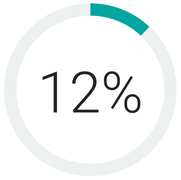
Approaches to threat detection and response.



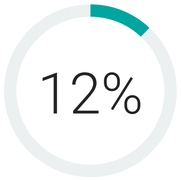
My organization tends to use network visibility and telemetry as a first line of defense for threat detection and response



My organization tends to use endpoint visibility and telemetry as a first line of defense for threat detection and response



My organization tends to use SIEM or XDR as a first line of defense for threat detection and response



My organization tends to use network visibility and telemetry along with other tools as a first line of defense for threat detection and response

Tools best equipped for hybrid, multi-cloud visibility.

41%

Network detection and response or visibility tools

24%

Extended detection and response (XDR) tools

13%

Tools from cloud servicer providers (CSPs)

12%

Endpoint detection and response tools

10%

Dedicated cloud detection and response tools

© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

Most See Value in Unified Network Visibility

There are many examples of convergence across IT and security today, with the convergence of networking and security being a key example. While secure access service edge (SASE) is often highlighted as the key example, SecOps and NetOps using the same visibility tools is another. Nearly all respondents (93%) indicated their SecOps and NetOps teams used the same network visibility tools and data.

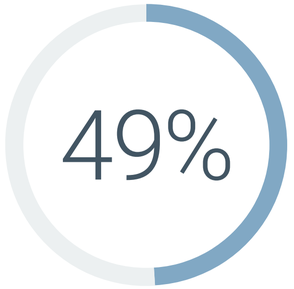
While the most common reason why was deeper visibility and more context, cited by 49%, simplicity was a driving factor as well. Easier deployment and management (47%), better efficacy (46%), and cost efficiency (44%) were all cited. Obviously, these tools must be able to adequately support both constituencies to offer significant value.

Use of the same tools for SecOps and NetOps teams.

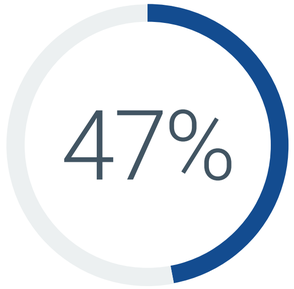
Our SecOps and NetOps teams utilize the same network visibility tools and data

Our SecOps and NetOps teams do not utilize the same network visibility tools and data

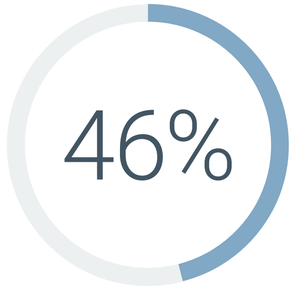
Reasons to use the same tools for SecOps and NetOps.



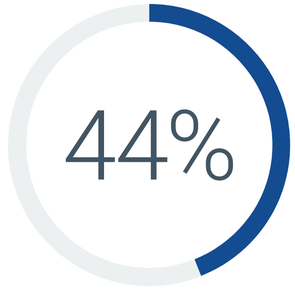
Deeper visibility and more context



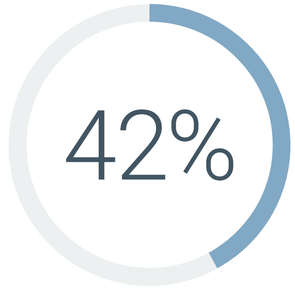
Easier deployment and management



Better efficacy



Cost efficiency



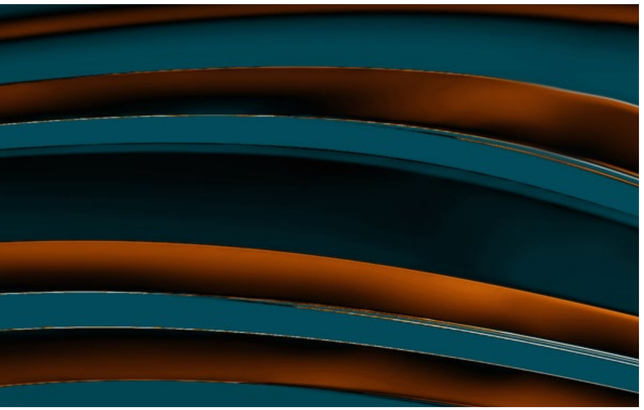
Increased influence with our vendor

Leadership prioritizing SecOps and NetOps teams working more closely together

© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

Navigating the TDR Process Can Take Time, but Network Visibility Significantly Helps



Detection, Triage, Analysis, and Investigation Take up Nearly Two-thirds of the Time for TDR/IR Processes

A byproduct of the previously mentioned challenges around the skill gap, alert fatigue, and process inefficiency is the fact that security teams spend too much time in reactive mode. On the positive side, there is no single bottleneck that stands out. Yet on average, 62% of time is spent on the detection and triage, analysis, and response phases.

This leaves 21% of time for proactive planning, and 17% for post-incident learning and after action. While this model has become common, security teams should aim to improve upon these peer averages. Yet based on this research, prioritizing network visibility and NDR in particular can help with this process.

Average time spent on different phases of TDR/IR processes.

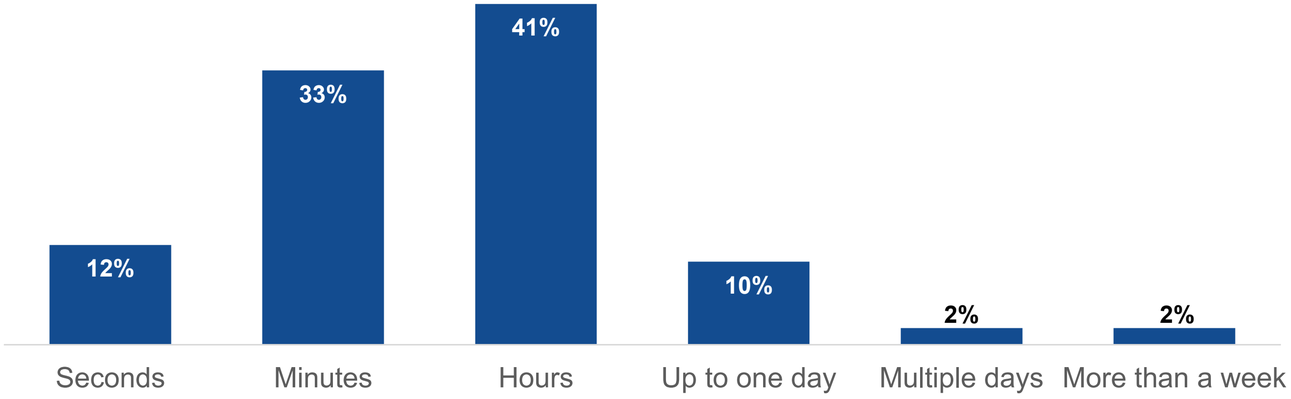
© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

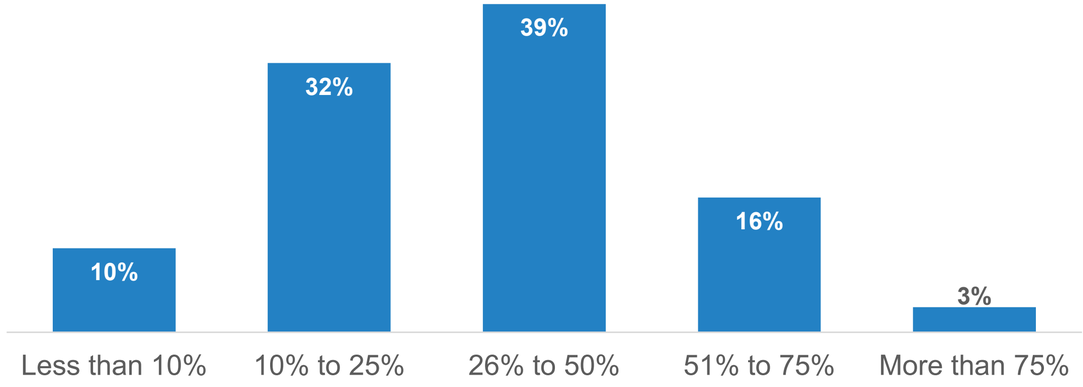
Triaging Anomalies Is Time Consuming

Overall, 55% of respondents indicated that it takes at least hours to determine if an anomaly detection is a malicious true positive. Further, 14% said it takes a day or more. Worse still, 42% said at most, one in four detections actually turned out to be a true positive. This means a massive amount of time is spent validating alerts that turn out to be meaningless.

Average time to determine if anomaly detections are valid.



Percentage of anomaly detections that are true positives.



© 2025 TechTarget, Inc. All Rights Reserved.

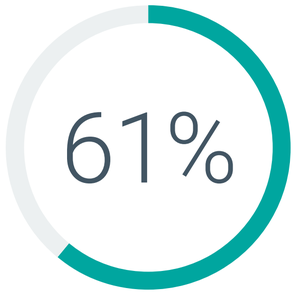
Back to Contents

Network Visibility Helps Move From Detection to Response Faster

In addition to the data showing that those prioritizing network visibility are able to investigate anomalies faster and see fewer false positives, respondents directly report that it makes a difference.

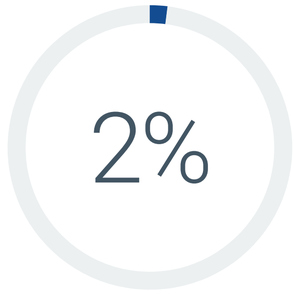
In all, 97% of respondents indicated that network visibility helps with the analysis and investigation phase. Specifically, 61% said network visibility has a significant impact on the analysis and investigation phase, and they are able to move much faster and with more confidence due to it. An additional 38% noted that network visibility has a moderate impact, helping them move somewhat faster and with somewhat more confidence. Clearly, those who have invested in network visibility and NDR are seeing important dividends from that decision.

Impact of network visibility on analysis and investigation.

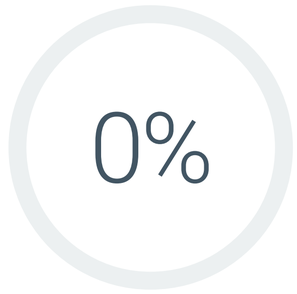


Significant -
we complete this step much faster and/or with more confidence because of it

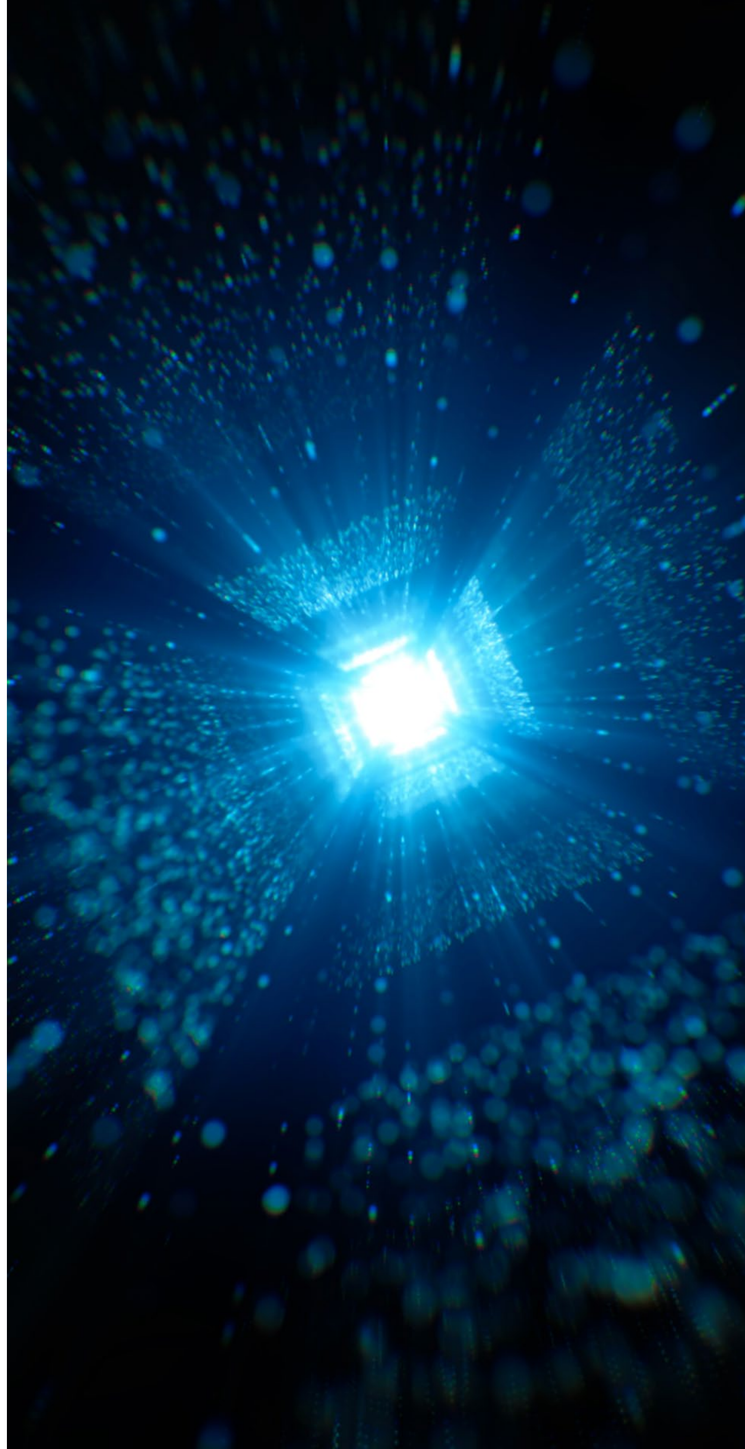
Moderate -
we complete this step somewhat faster and/or with somewhat more confidence because of it



Minimal -
it provides some help but not a lot



None -
it does not help in our analysis process



© 2025 TechTarget, Inc. All Rights Reserved.

NDR Is Foundational to XDR, and AI Will Be Critical

Most See NDR as Foundational to XDR, but There Is Disagreement on Procurement

While network visibility and NDR are clearly helping security teams operate more effectively and efficiently, it is not the only piece of the puzzle. The idea of XDR was an important shift for the industry in recognizing the need to better integrate and normalize security data sources across disparate tool stacks. But in making it overly EDR-centric, some vendors turned off organizations that recognized the value of the network.

Among research respondents, more than half (53%) said NDR would form the foundation of their XDR strategy, while 30% said it would be a secondary part of their XDR strategy. Only 2% said NDR will remain independent of XDR.

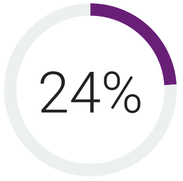
But regarding how NDR will fit in a broader XDR architecture, there is no consensus. Nearly the same percentage indicated they would prefer to have NDR and XDR integrated by a service provider (26%), offered by a single vendor (25%), consumed as a managed service (25%), and connected via a technology alliance (24%).

Preferences for procuring NDR tools.

We would prefer that NDR technologies and the other tools supporting our XDR strategy be integrated by a service provider

We would prefer to get NDR technologies from the same vendor that provides other tools supporting our XDR strategy

We would prefer to procure NDR technologies and the other tools supporting our XDR strategy as a managed service



We would prefer that our NDR vendor participate in technology alliances with other vendors to support our XDR strategy

How NDR fits with XDR.

53%

NDR will form the foundation of our organization's XDR strategy

30%

NDR will be a secondary part of our organization's XDR strategy

15%

NDR will be a part of our organization's XDR strategy, but we do not have a timeline

2%

NDR will remain independent of our organization's XDR strategy

0%

We do not have, or plan to have, an XDR strategy

© 2025 TechTarget, Inc. All Rights Reserved.

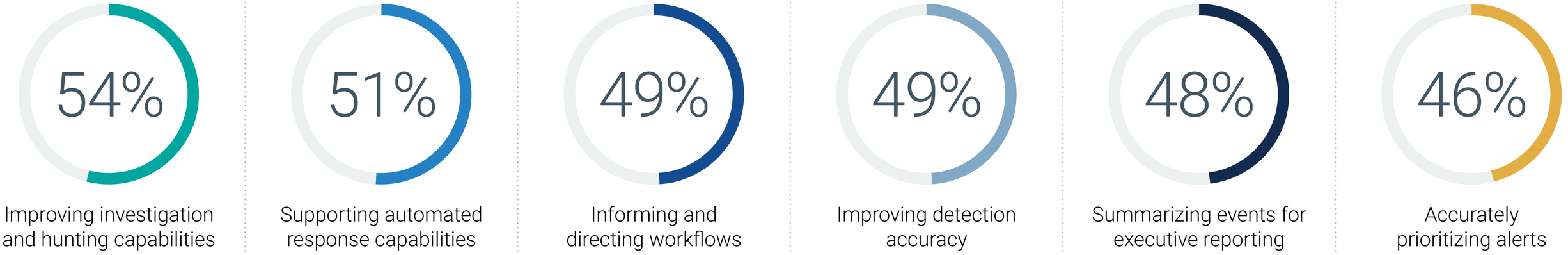
Back to Contents

Most Are Leveraging AI-Based NDR, and Improving Response Is a Key Driver

Another important overarching trend in security is AI. Nearly all respondents (93%) indicated their organization is currently using NDR tools with generative AI capabilities. Further, expectations are high, with security professionals anticipating that AI can help in a variety of ways.

From an augmentation perspective, 54% are using GenAI-enabled NDR to improve investigation and hunting, 49% to inform and direct workflows, and 48% to summarize events for executive reporting. Automation is also important, with 51% looking to support automated response capabilities and 46% expecting the accurate prioritization of alerts. Finally, nearly half (49%) expect to improve detection accuracy.

Expectations of GenAI in NDR solutions.



© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

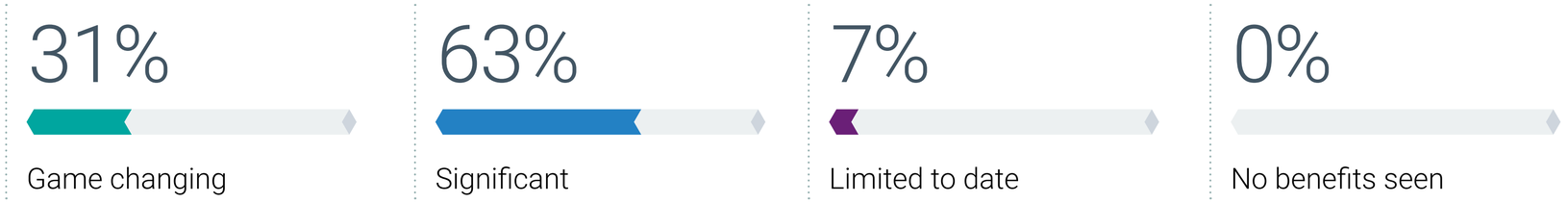
AI Is Clearly Helping Improve SecOps, but Concerns Remain

On the positive side, most are seeing a meaningful impact from their use of GenAI-enabled NDR. Nearly one-third (31%) noted that the impact had been game changing, while 63% said it was significant.

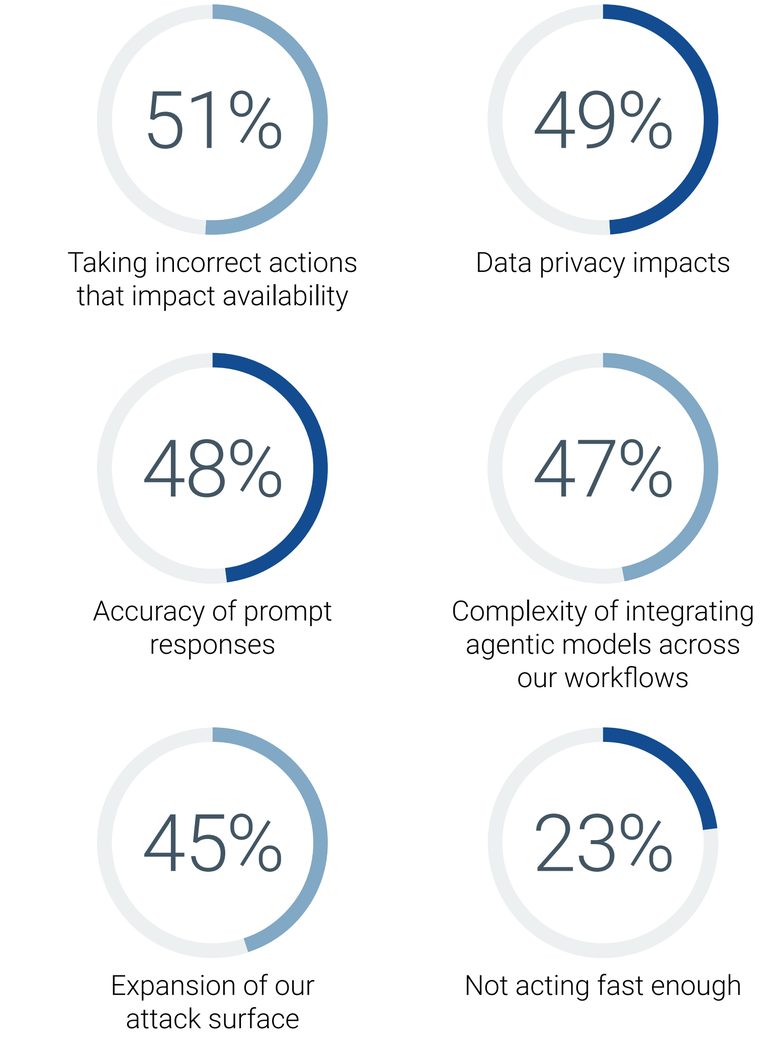
That said, many concerns still exist around AI, especially with the introduction of agentic models already occurring. The most common concern cited was the system taking incorrect actions that impact availability (51%). Even when automation is not in play, the accuracy of prompt responses is also a concern, as noted by 48% of respondents. As agentic solutions come to market, how they integrate and the complexity thereof will be top of mind and was reported by 47%.

Overall, this shows that while there is significant interest in automation and other aspects of AI, these capabilities need to be proven before being fully utilized with confidence.

Impact of GenAI-enabled NDR on SecOps.



Concerns regarding generative and agentic AI with NDR.



© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

NDR Supports a Broad Set of Use Cases, Requiring Many Different Attributes

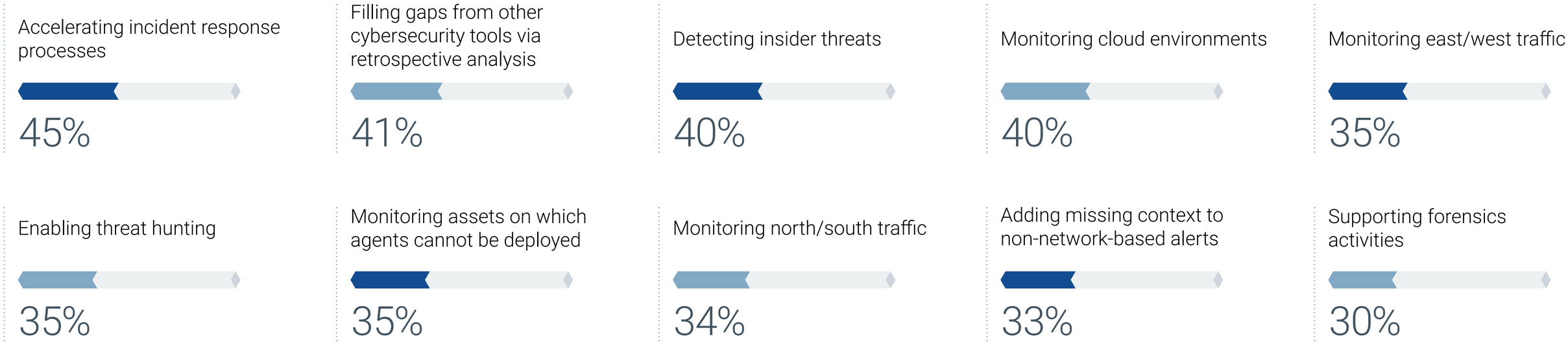
NDR Is Used for Many Different Use Cases

One of the benefits of NDR is that it is versatile and can address a number of different use cases. In this research, no one use case stands out, but rather there was broad agreement across a variety of functions.

The most common use case cited by nearly half of respondents (45%) was accelerating incident response processes. Additional use cases supporting specific SOC functions include detecting insider threats (40%), enabling threat hunting (35%), and supporting forensics (30%).

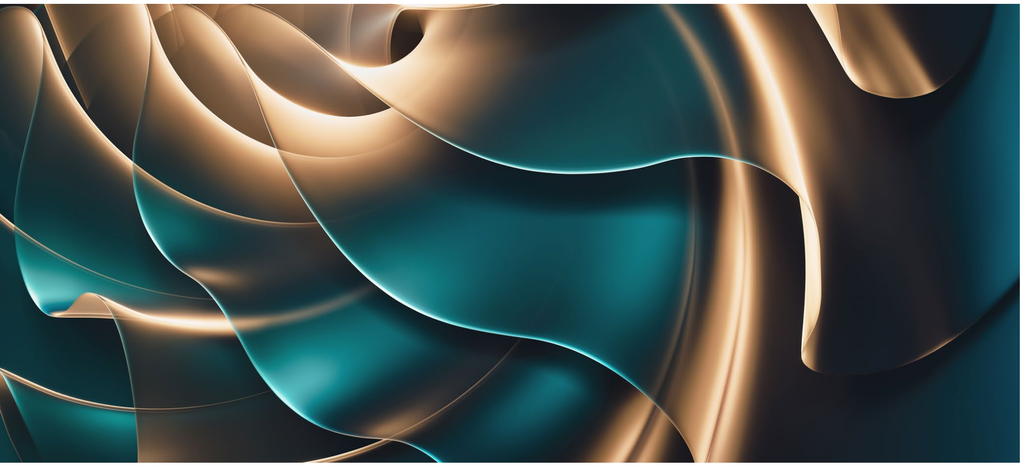
Many use NDR to monitor specific aspects of the environment including cloud (40%), east/west traffic (35%), assets where agents cannot be deployed (35%), and north/south traffic (34%). Other responses reflected how NDR can augment other tools, either by filling gapes via retrospective analysis (41%) or adding missing context to non-network alerts (33%).

Top NDR use cases.



© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

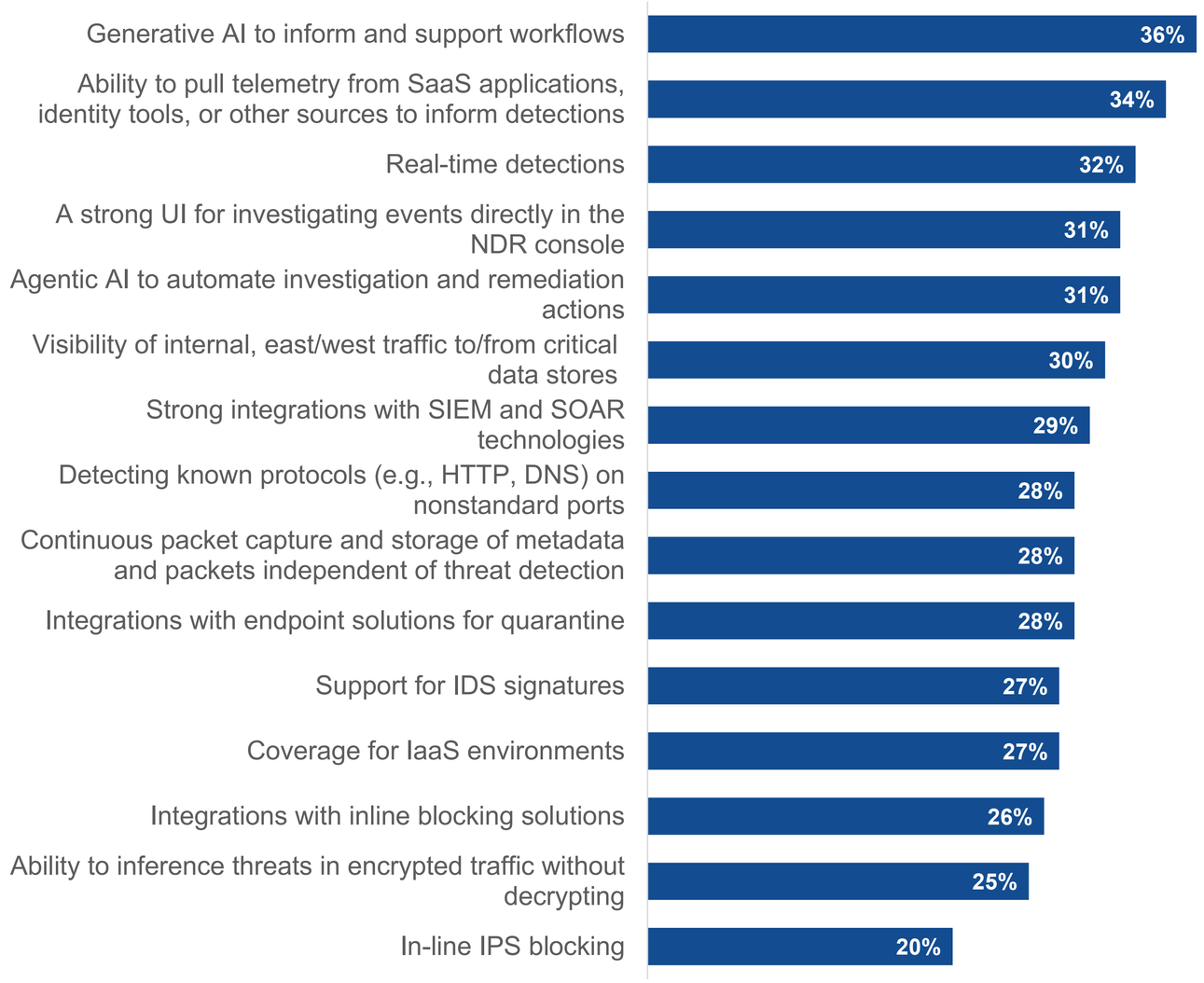


Interest in Many Use Cases Requires a Range of Functionality

To adequately support various use cases, especially in a single organization, NDR solutions must have a broad set of capabilities. In some cases, the importance of an attribute will vary from one organization to another. For example, some security teams may prefer to do more heavy lifting in the NDR console itself, while others may want to send network telemetry directly to the SIEM. As a result, 31% noted the need for a strong UI for investigating events in the NDR console while 29% cited strong integrations for SIEM and SOAR technologies.

While using generative AI to inform and support workflows was the most common response (36%), using agentic AI to automate investigation and remediation actions was lower on the list at 31%. This likely reflects the newness of this market and need to validate capabilities in this area.

Important NDR capabilities.



© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

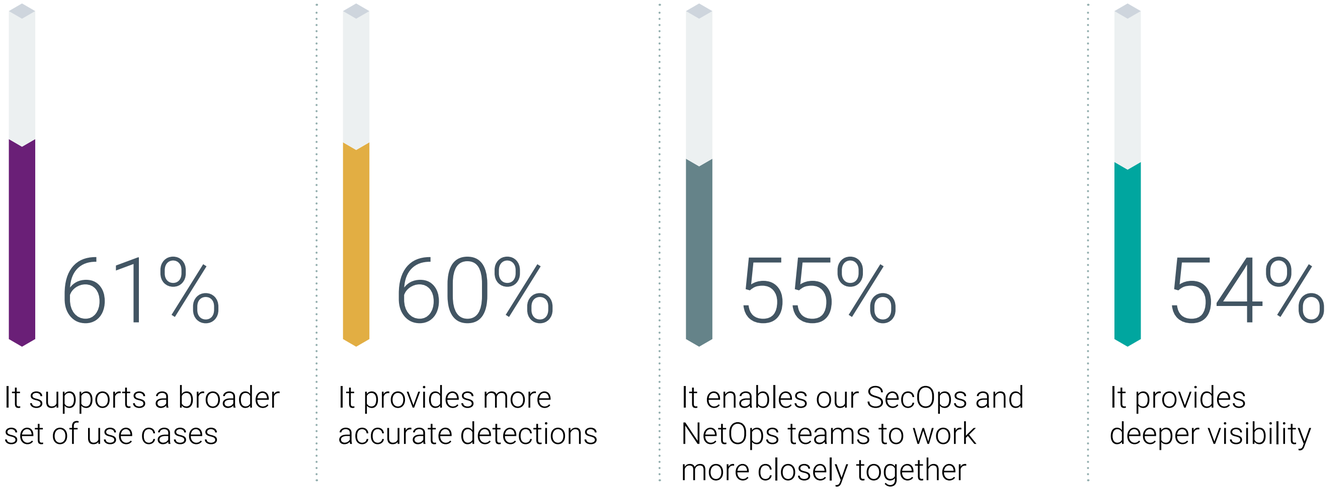
Both Packet Capture and Metadata Are Important

Historically, NDR solutions fall into metadata or packet-based models. More recently, there has been increased overlap with metadata-based solutions supporting some amount of packet capture, and vice versa.

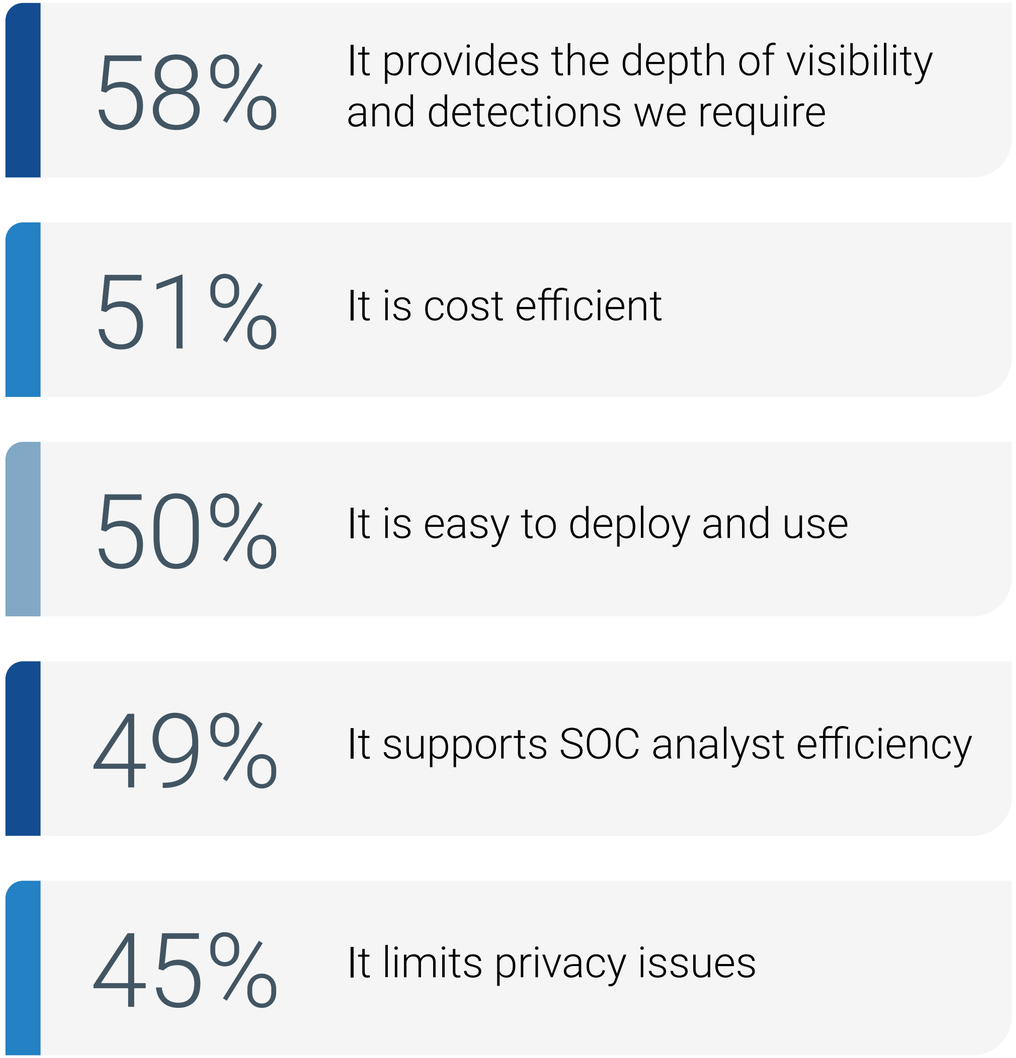
More specifically, respondents generally agreed that continuous packet capture supports more use cases, provides more accurate detections and deeper visibility, and helps SecOps and NetOps teams work better together. At the same time, metadata-based analysis is viewed as providing what is needed relative to visibility and detections, more cost efficient, and easy to deploy and use, with less of an impact on privacy.

While some organizations may prefer one approach over the other, solutions that offer both can better support more use cases and drive better SOC results.

Why continuous packet capture is an important NDR capability.



Why metadata-focused analysis is an important NDR capability.



© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

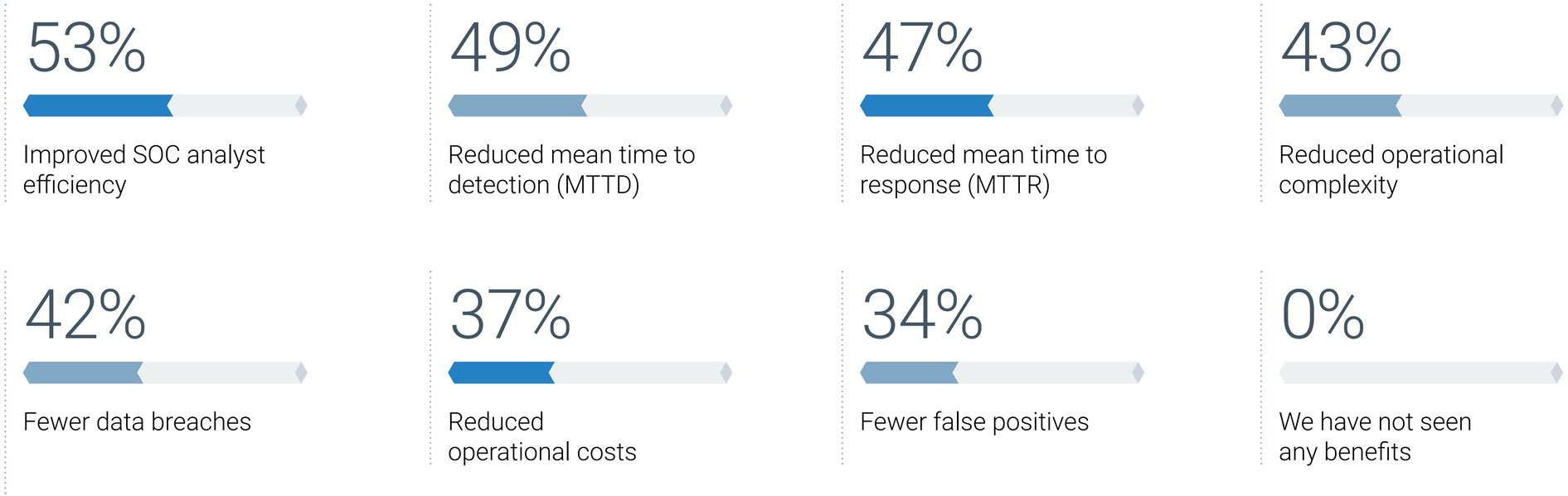
Most See Multiple NDR Benefits, but Outcomes Don’t Always Align With Expectations

Many Benefits Cited as a Result of NDR

Ultimately, the most important question to ask is whether the organizations prioritizing NDR are seeing benefits from that investment. Among respondents, the answer was resoundingly positive. More than half (53%) said SOC analyst efficiency has improved, 49% reported a reduced MTTD, and 47% said it reduced MTTR. Further 42% indicated their organization has seen fewer data breaches as a result of using NDR.

As noted earlier, this is not to say that security teams should rely on NDR alone. XDR, EDR, and SIEMs all have a role in making a SOC successful. However, NDR provides unique value based on the coverage it provides, gaps it fills, use cases it supports, and visibility it enables.

Benefits realized from using NDR.



© 2025 TechTarget, Inc. All Rights Reserved.

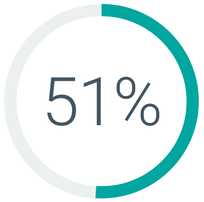
Back to Contents

Future Actions Will Build on Current Success

As a final testament to how respondents feel about NDR, nearly all (91%) say their organization expects to increase spending. More specifically, 50% anticipate investing in NDR tools that offer generative AI capabilities, and 50% say they will invest in common platforms supporting NetOps and SecOps visibility. Additionally, improving collaboration between NetOps and SecOps teams is expected by 51% of respondents.

As shown earlier, nearly all respondents use AI-based NDR tools, use common platforms between NetOps and SecOps, and say collaboration between the groups is good. Ultimately, because they are already seeing benefits and positive results from these areas, respondents hope to accelerate these successes by investing more time and resources in these areas.

Actions to implement or optimize NDR strategies over the next 12-18 months.

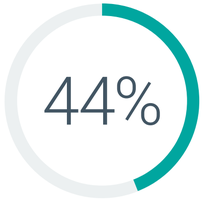


Work to improve collaboration between SecOps and NetOps teams

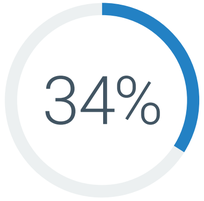
Invest in common platforms for network visibility to support both NetOps and SecOps

Work with managed services providers

Invest in network threat detection and response tools that offer generative AI capabilities



Work with professional services firms to build or refine our strategy



Hire more personnel

© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

VECTRA®

ABOUT

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. The Vectra AI Platform delivers AI-driven Network Detection and Response (NDR) to surface and stop threats across the data center, campus, remote work, identity, cloud, and OT environments. In the first-ever Gartner® Magic Quadrant™ for Network Detection and Response, Vectra AI was named a Leader and positioned highest for Ability to Execute and furthest for Completeness of Vision. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't. For more information, visit www.vectra.ai.

LEARN MORE

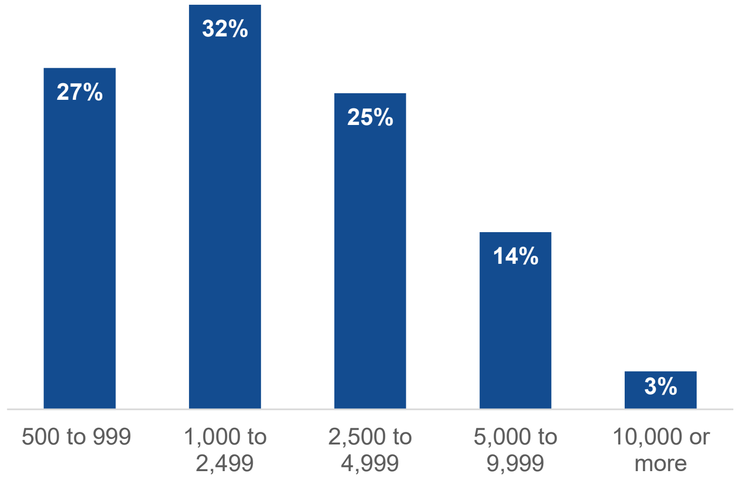
© 2025 TechTarget, Inc. All Rights Reserved.

RESEARCH METHODOLOGY AND DEMOGRAPHICS

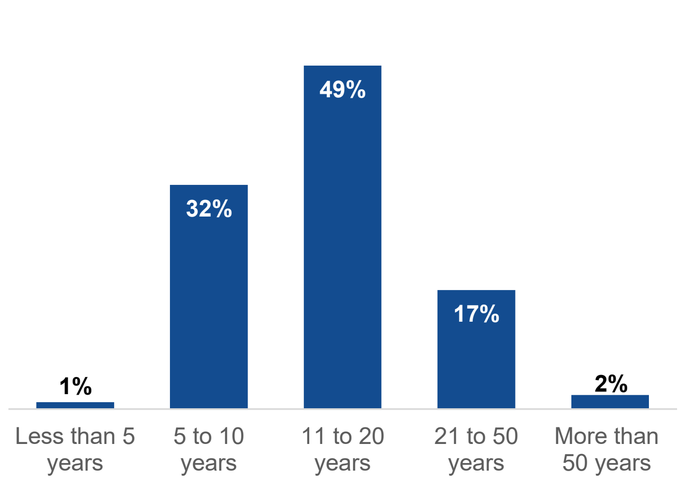
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of cybersecurity and IT professionals from private- and public-sector organizations in North America between June 13, 2025, and June 24, 2025. To qualify for this survey, respondents were required to be involved in evaluating or purchasing network-based threat detection and response technology products and services at their organization. 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 400 cybersecurity and IT professionals.

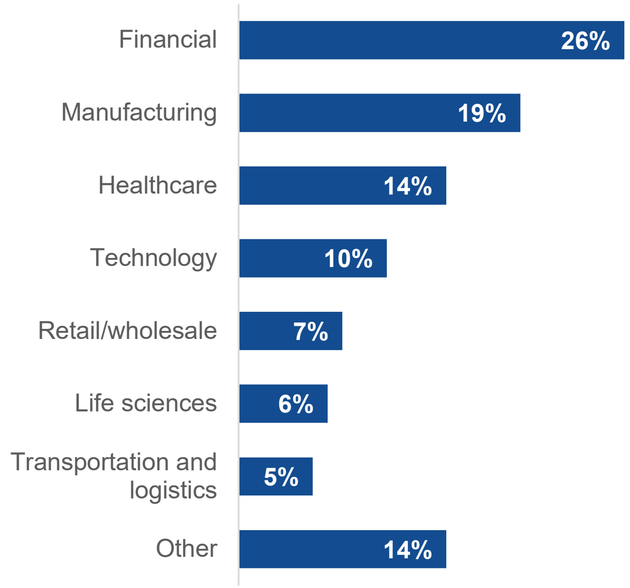
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



© 2025 TechTarget, Inc. All Rights Reserved.

Back to Contents

©2025 TechTarget, Inc. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

© 2025 TechTarget, Inc. All Rights Reserved.