



Enterprise Strategy Group | Getting to the bigger truth.™

THREAT DETECTION AND RESPONSE LANDSCAPE

Jon Oltsik, Senior Principal Analyst and ESG Fellow

Contents

Research Objectives **3**

Key Research Findings **4**

The complexity of the threat detection landscape continues to increase and current efforts to combat this trend are insufficient. **5**

Organizations are implementing endpoint detection/response (EDR) technologies, typically after some type of security incident. **8**

On-premises, tightly-integrated endpoint security suites are the preferred EDR deployment model, with threat intelligence and data analytics topping attribute priorities. **11**

Network traffic analysis (NTA) tools act as a first line of defense for threat detection/response, but organizations demand tight integration between endpoint and network tools. **14**

Managed detection/response (MDR) services are gaining popularity as organizations look for help with advanced skills and process improvement. **17**

Organizations will increase threat detection/response spending, build integrated cybersecurity technology architectures, and improve collaboration between cybersecurity and IT operations teams. **20**

Research Methodology **22**

Research Objectives

Organizations are moving beyond security information and event management (SIEM) for threat detection and response. Some are acquiring network and/or endpoint detection tools as well as adding technologies to help them automate and orchestrate incident response. Rather than deploy and operate new detection/response tools, other organizations are outsourcing these activities to third-party service providers.

In order to get more insight into these trends, ESG surveyed 372 IT and cybersecurity professionals at organizations in North America (U.S. and Canada) responsible for evaluating, purchasing, and managing threat detection/response products, processes, and services. This study sought to:

- Determine current people, process, and technology approaches to threat detection and response.
- Establish key trends for endpoint detection and response (EDR), network traffic analysis (NTA), and managed detection and response (MDR).
- Identify threat detection and response (TDR) technology challenges and shortcomings impeding security and business objectives.
- Monitor enterprise TDR strategies as they evolve.

Survey participants represented a wide range of industries including manufacturing, financial services, health care, communications and media, retail, government, and business services. For more details, please see the Research Methodology and Respondent Demographics sections of this report.



Key Research Findings



The complexity of the threat detection landscape continues to grow and current efforts to combat this trend are insufficient. When asked about their organizations' technologies and processes related to threat detection and response (TDR) activities, more than three-quarters of respondents said these tasks have become more difficult over the last two years. The vast majority of respondents said improving TDR is a high priority for their organization and have a formal plan and funding for these improvements.



Organizations are implementing endpoint detection/response (EDR) technologies, typically after some type of security incident. Many organizations currently leverage EDR technology, and more than two-thirds of these users deployed the technology in response to experiencing some type of security incident. Among those organizations that deployed EDR in a reactive manner, the vast majority have detected at least one additional incident since the initial deployment.



At present, more than half of current EDR users favor an on-premises deployment model approach but may be open to cloud-based SaaS options in the future. Most current users opt for full-function EDR designed for highly-skilled analysts and manual use cases, with the most preferred features being threat intelligence integration, automated remediation, capturing a wide range of metadata, and built-in analytics.



Network traffic analysis (NTA) tools act as a first line of defense for threat detection/response, but organizations demand tight integration between endpoint and network tools. Nearly nine in ten respondents report currently using NTA tools, with built-in analytics and threat intelligence capabilities identified as two of the most important attributes of this technology. While 43% of respondents indicate that they use NTA tools as their first line of defense, more than two-thirds of organizations using both NTA and EDR deem their interoperability to be very important.



Managed detection/response (MDR) services are gaining popularity as organizations look for help with advanced skills and process improvement. More than half of respondents currently use managed detection and response services, with the three most commonly identified motives being actual or perceived lack of internal skills, desire for rapid deployment, and existing MSSP relationships.



Organizations will increase threat detection/response spending, build integrated cybersecurity technology architectures, and improve collaboration between cybersecurity and IT operations teams. The vast majority of organizations expect to increase spending on threat detection and response over the next 12-18 months. The likeliest targets for this spending windfall will involve developing or purchasing integrated security software architectures, improving alignment between IT and security operations teams, and automating security operations.

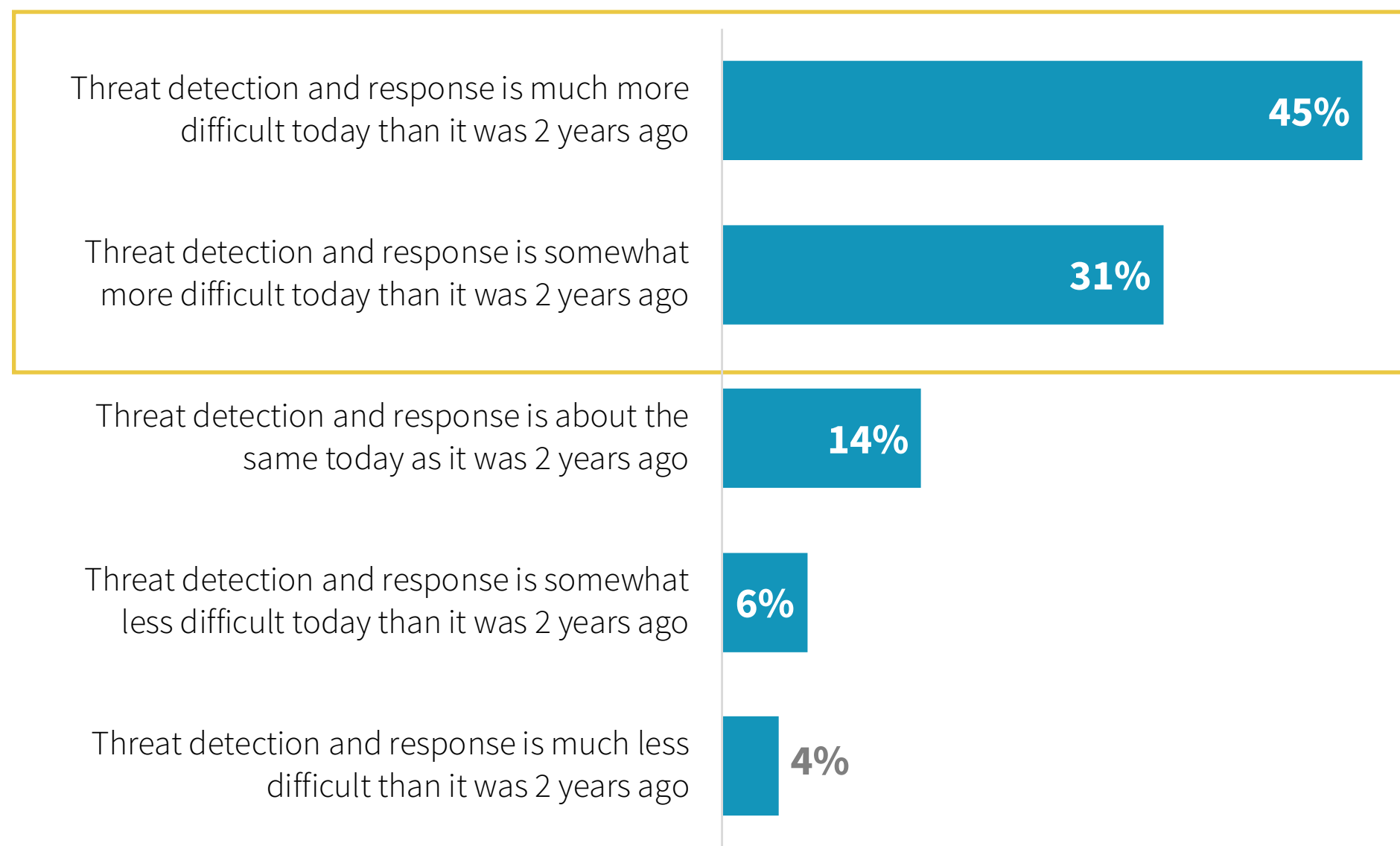
The complexity of the threat detection landscape continues to increase and current efforts to combat this trend are insufficient.



Threat detection is more difficult today due to sophisticated threats and growing attack surfaces.

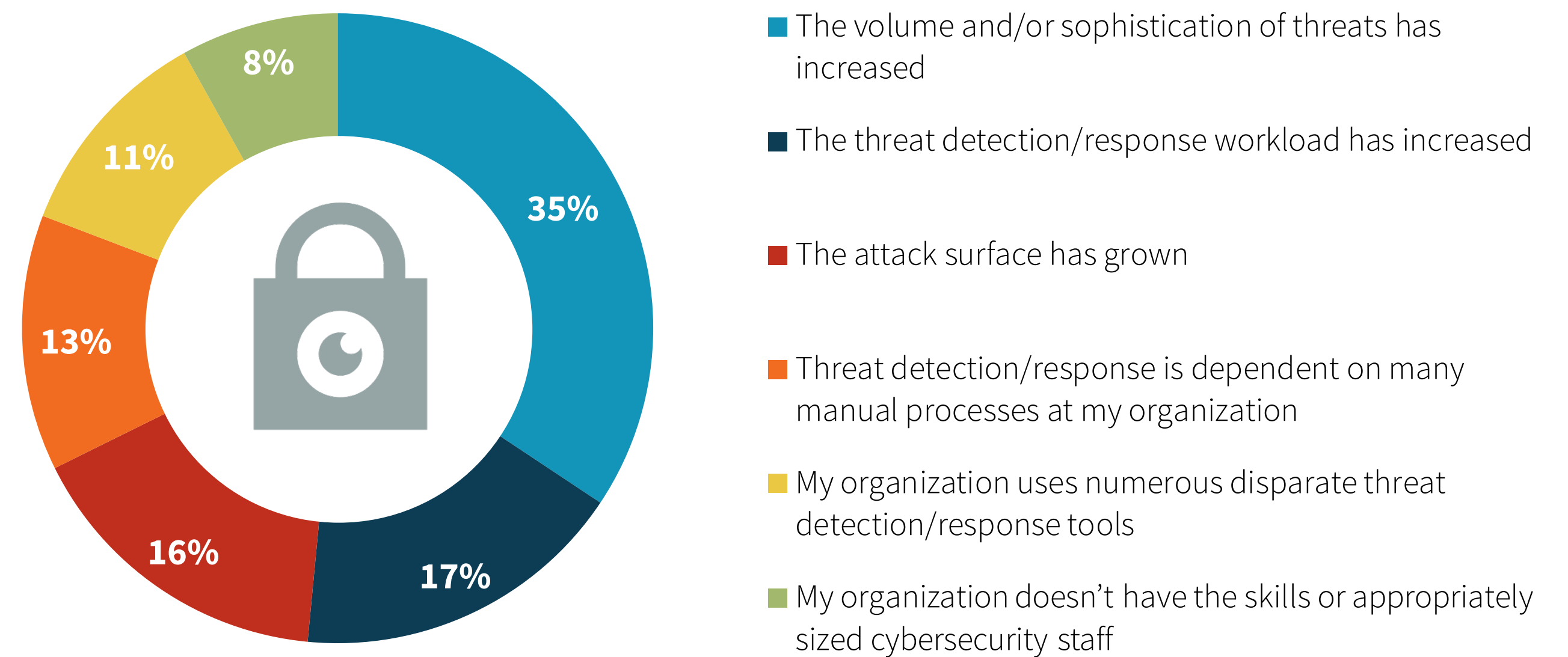
Cyber-threats are more targeted and sophisticated than in the past. When asked about their organizations' technologies and processes related to threat detection and response activities, more than three-quarters (76%) of respondents said that threat detection and response has become more difficult over the last two years.

TDR Landscape Today Compared to 2 Years Ago



Why has threat detection and response grown more difficult? Many organizations are collecting, processing, and analyzing more internal and external security telemetry to enhance situational awareness, improve threat detection, and accelerate incident response. It follows then that two-thirds of respondents cite this as the primary reason for the spike in threat detection and response difficulty in the form of amplified threat volume (34%), increased workload (17%), or an enlarged attack surface (16%).

Primary Reason TDR Is Harder



Improving threat detection is a top priority, but several technical challenges loom as obstacles.

Given both the importance and increasing complexity of threat detection and response, it makes sense that organizations would prioritize efforts and resources to fortify their TDR capabilities. Specifically, 82% of respondents said that improving threat detection and response is a high priority for their organization and 87% reported having a formal plan and funding to improve TDR.



82%

of respondents said that improving threat detection and response is a high priority for their organization



87%

reported having a formal plan and funding to improve TDR

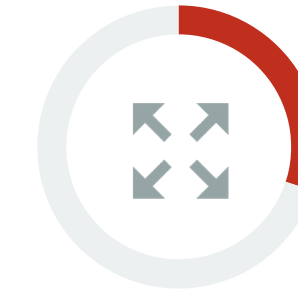
Although the business is asking for better TDR, organizations face technical challenges including too many tactical firefighting activities (36%), an expanding attack surface exacerbated by increasingly scalable infrastructure (30%), a lack of end-to-end monitoring (30%), and an overabundance of manual processes (26%).

Top organizational challenges regarding threat detection/response



36%

too many tactical firefighting activities



30%

an expanding attack surface exacerbated by increasingly scalable infrastructure




30%

a lack of end-to-end monitoring



26%

an overabundance of manual processes

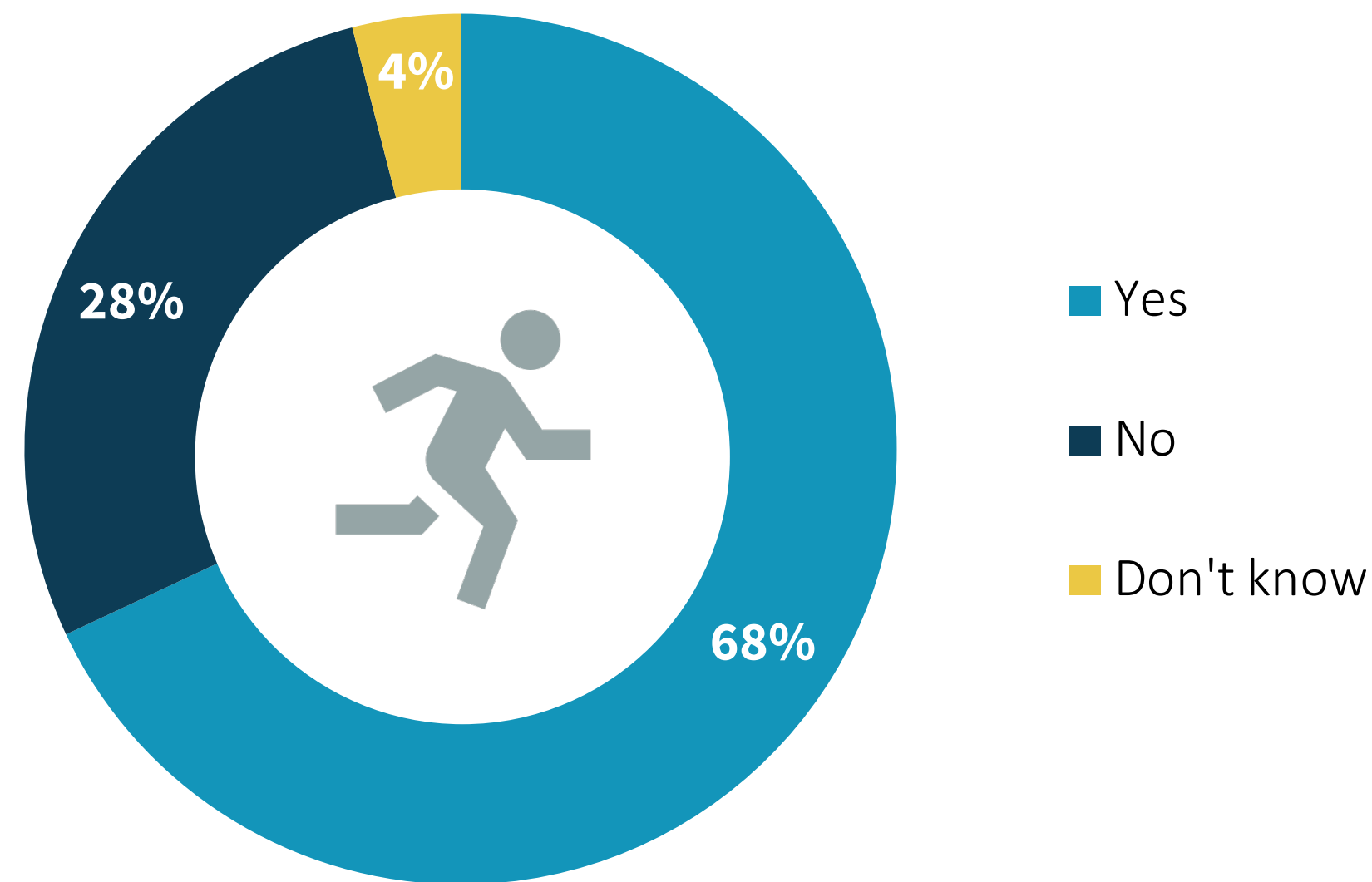


Organizations are implementing endpoint detection/response (EDR) technologies, typically after some type of security incident.

Most initial endpoint detection and response technology deployments were reactionary.

Endpoint detection and response (EDR) technology refers to endpoint software used to capture and monitor endpoint behavior as a means for detecting and mitigating suspicious or malicious activities. Many organizations are implementing or are interested in implementing EDR software on some or all endpoints, and more than two-thirds of current users attribute their initial deployment to some type of security incident such as a system compromise, data breach, etc.

Was Initial EDR Deployment Reactive?

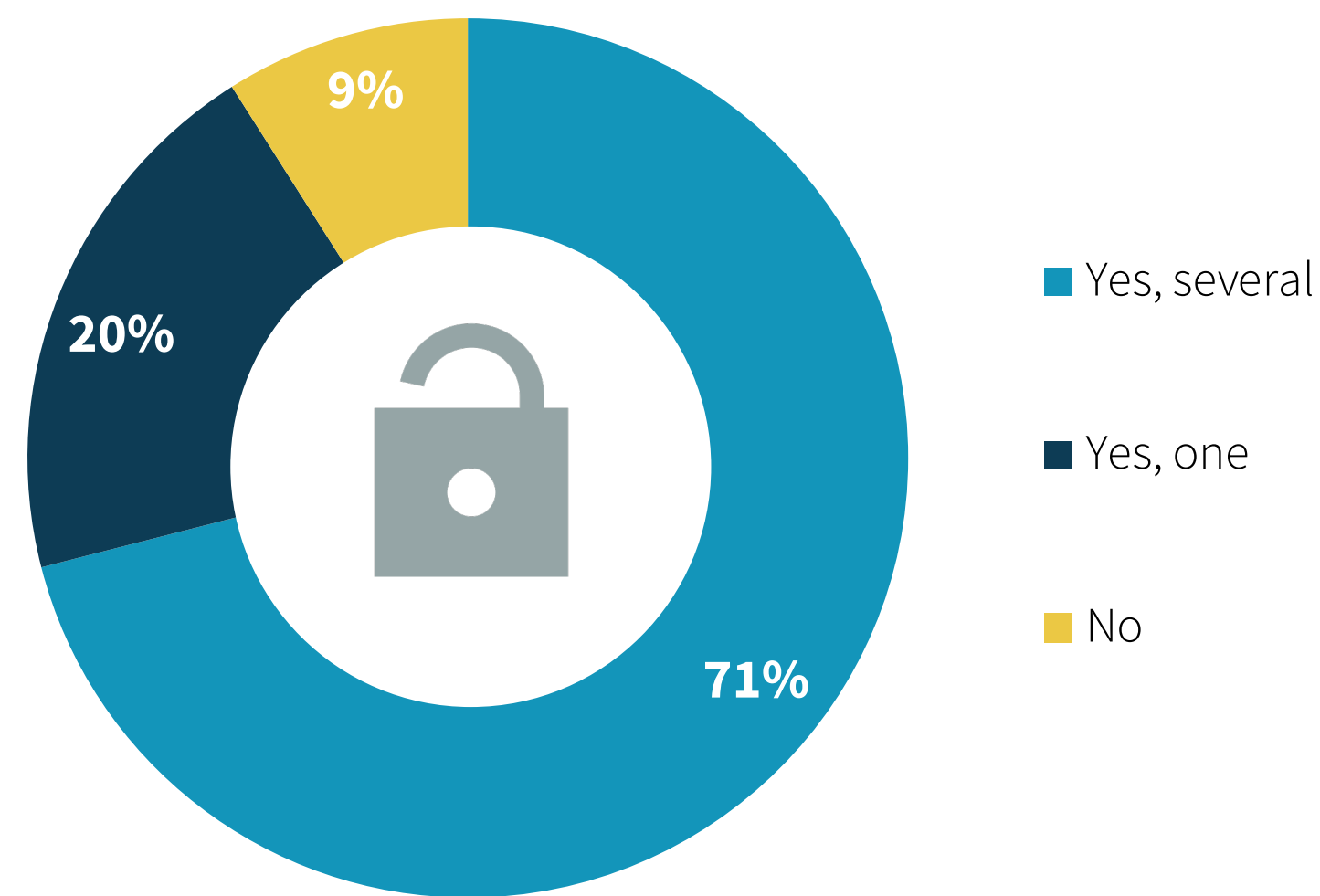


More than two-thirds of current users attribute their initial deployment to some type of security incident such as a system compromise, data breach, etc.”

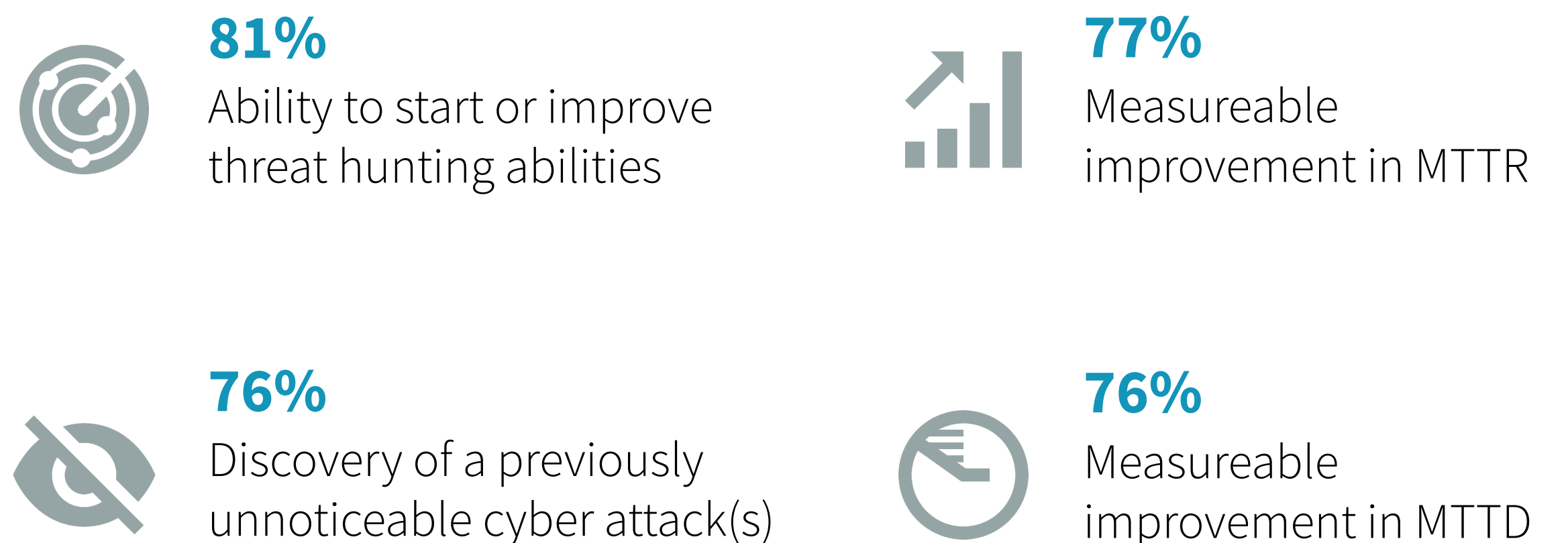
Most have experienced at least one additional incident post-EDR implementation.

Among those organizations that deployed EDR in a reactive manner, the vast majority have detected at least one additional incident since the initial deployment. Specifically, 20% indicated experiencing one incident, while nearly three-quarters (71%) have uncovered several incidents since first implementing EDR tools. Regardless of their EDR adoption driver, current users reported achieving measurable benefits in multiple areas. Indeed, more than three-quarters identified improved threat hunting (81%), faster mean time to respond (77%), discovery of in-process cyber-attack (76%), and faster mean time to detect (76%).

Has your organization detected any additional security incidents since deploying EDR technology?



Percentage of organizations that have achieved measurable EDR benefits



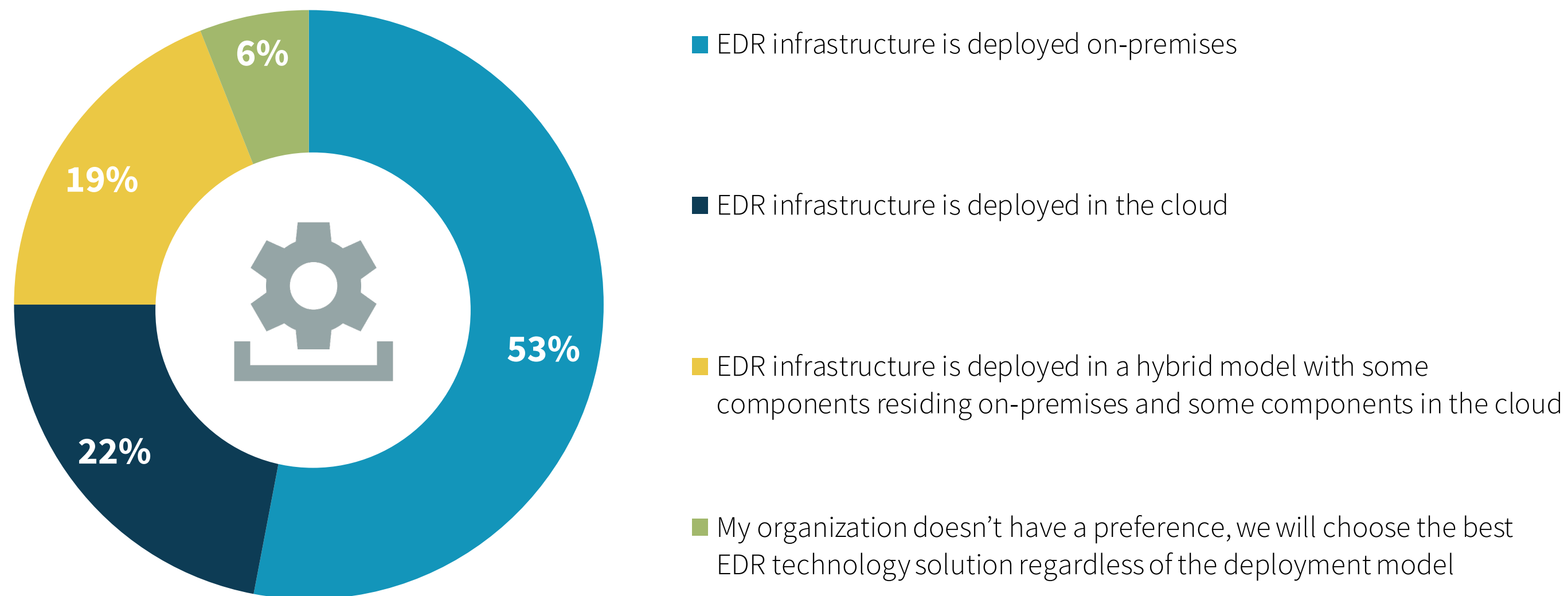
At present, more than half of current EDR users favor an on-premises deployment model approach but may be open to cloud-based SaaS options in the future.



On-premises, tightly-integrated endpoint security suites are preferences for EDR deployments.

In terms of the preferred deployment model for endpoint detection and response infrastructure, including data collectors, databases, management servers, etc., more than half (53%) of current EDR users favor an on-premises approach. It is worth noting that 41% are amenable to public cloud-hosted EDR implementations to some extent, with more than one in five identifying it as their current preferred approach. This makes sense in light of the fact that 79% of cybersecurity professionals are comfortable storing their organization’s EDR data in the cloud. As far as procurement, 81% would prefer to consume EDR technology from a single endpoint prevention software vendor, with more than half (52%) indicating a desire for tight integration with those types of solutions.

Which of the following EDR deployment models is preferred by your organization?



EDR Technology Preferences Favor Tightly Integrated Endpoint Security Suites



52%

EDR technology that is **tightly-integrated** into endpoint prevention software from a single vendor



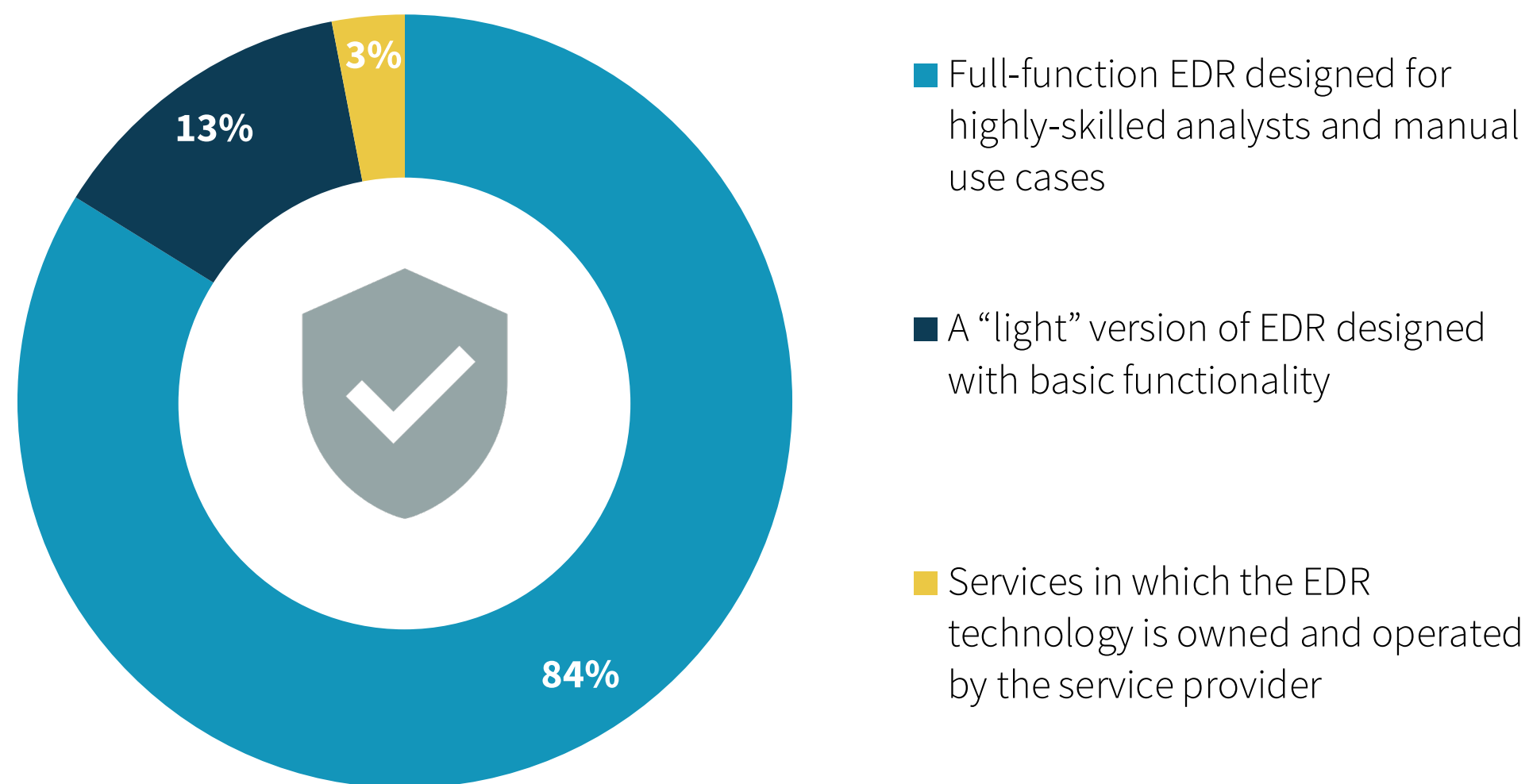
29%

EDR technology that is bundled with endpoint prevention software from a single vendor

Important EDR attributes include threat intelligence, automation, and analytics.

EDR software includes heuristics or behavioral analytics designed to identify suspicious/malicious activities that may go undetected by human analysts. EDR tools can also be used to construct a timeline of all endpoint actions taken, including the original system compromise, all system processes, and network connections to internal and external resources. With all of these features and capabilities, it is not surprising that 83% of current users opt for full-function EDR designed for highly-skilled analysts and manual use cases.


Organizations Want Advanced EDR



The most important attributes of an EDR solution include threat intelligence integration (40%), automated remediation (37%), capturing and storing a wide range of metadata (34%), and built-in analytics (32%). Given the focus on threat intelligence and analytics capabilities, it follows that 83% of current users believe that using EDR effectively requires advanced security analytics skills.

Important EDR Attributes Include Threat Intelligence, Automation, and Data Capture



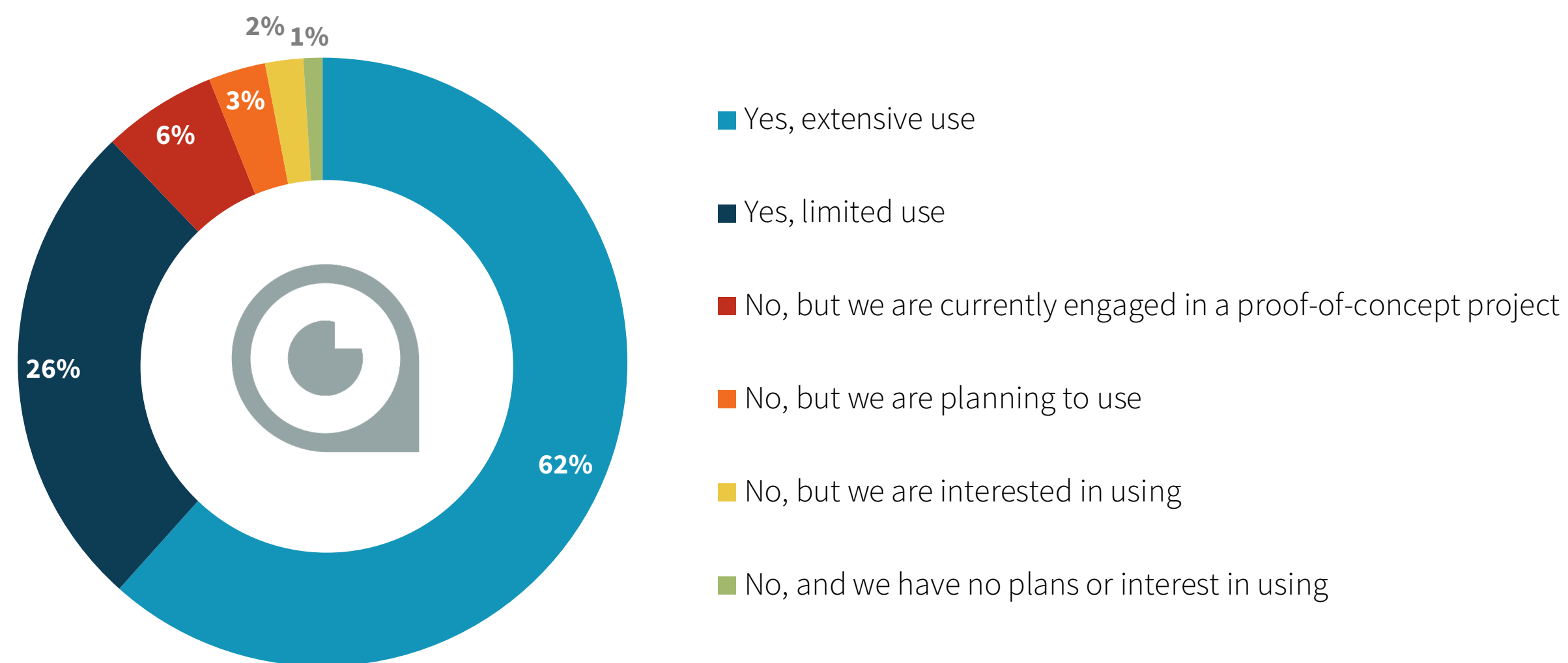


Network traffic analysis (NTA) tools act as a first line of defense for threat detection/response, but organizations demand tight integration between endpoint and network tools.

Threat detection and response is often anchored by network traffic analysis technology, with key attributes including analytics, threat intelligence, IoT affinity, and network visibility.

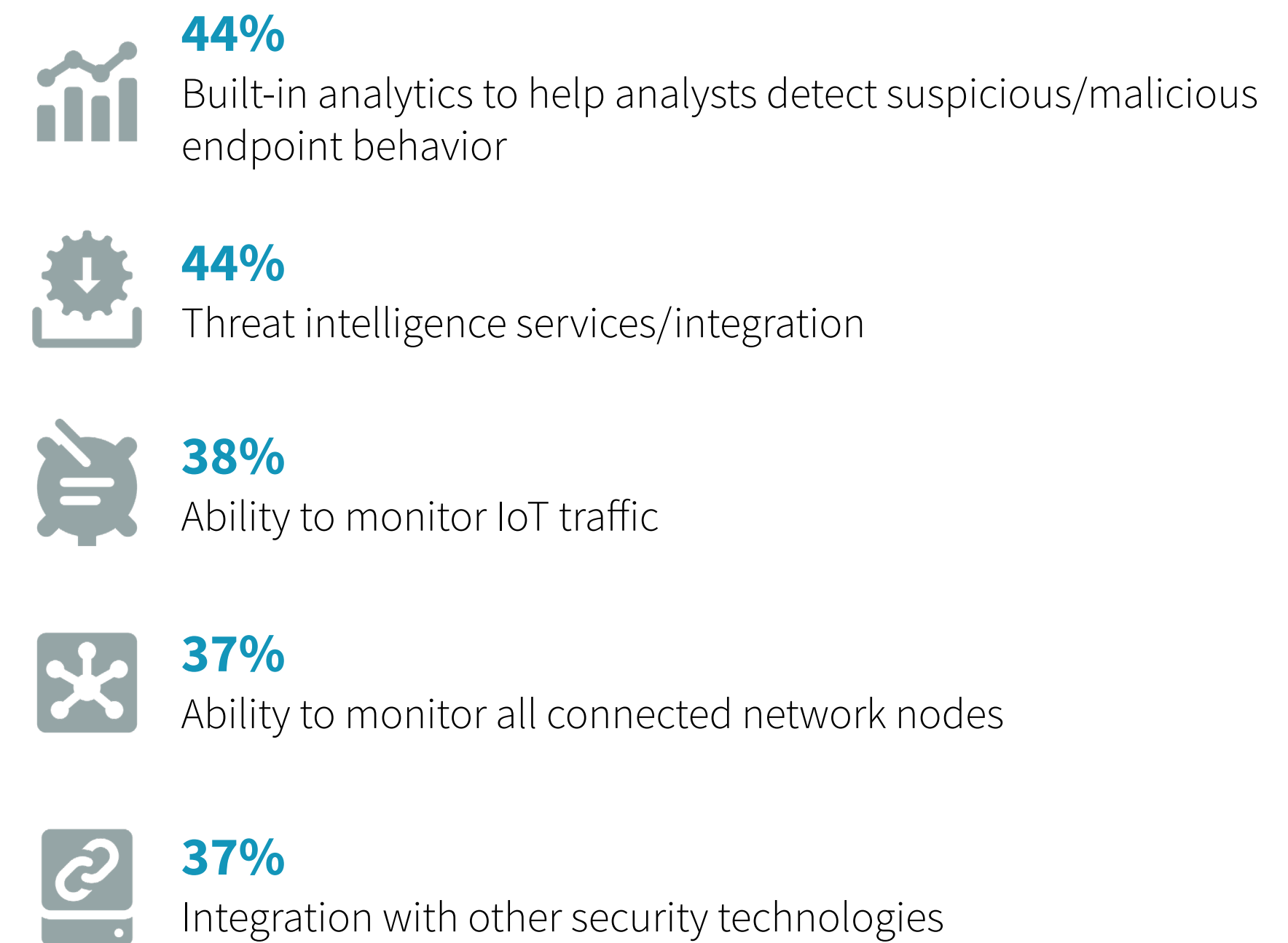
Network traffic analysis (NTA) technology is designed to capture, process, and analyze network traffic (i.e., connections, flows, packets, metadata, etc.) to detect and investigate malicious/suspicious network activities that may indicate a cyber-attack. In terms of NTA technology plans, nearly nine in ten report currently using it, with 61% categorizing this usage as extensive.

Majority of Organizations Use NTA to Some Extent



As was the case with EDR technology, built-in analytics and threat intelligence capabilities are two of the most commonly identified NTA attributes in terms of importance. Other top considerations include monitoring—across IoT devices, network nodes, and cloud traffic—and integration with other security technologies.

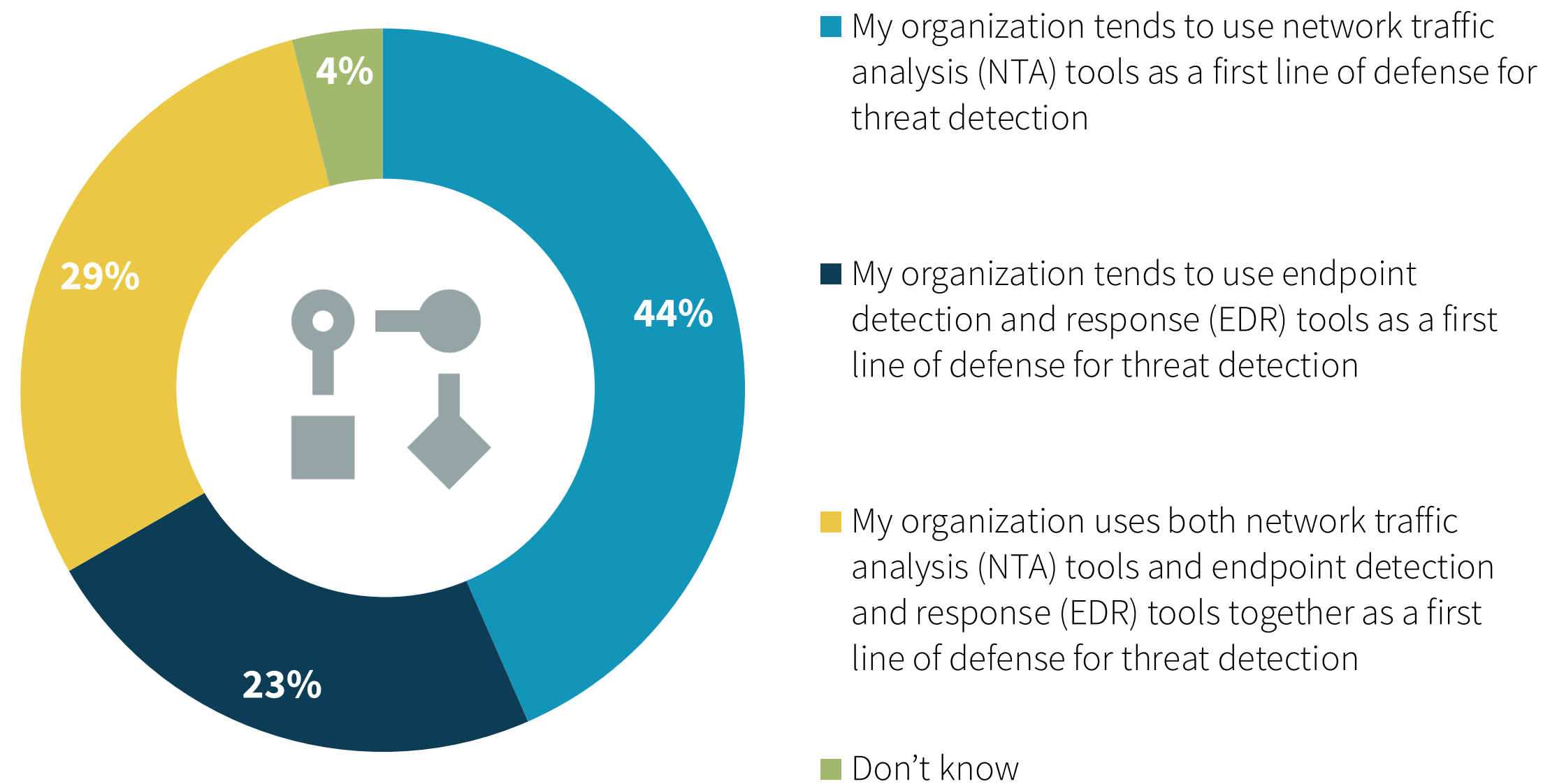
Key NTA Attributes include Analytics, Threat Intelligence, IoT Affinity, and Network Visibility



NTA is a first line of defense that can serve as pivot point to EDR, amplifying the importance of interoperability.

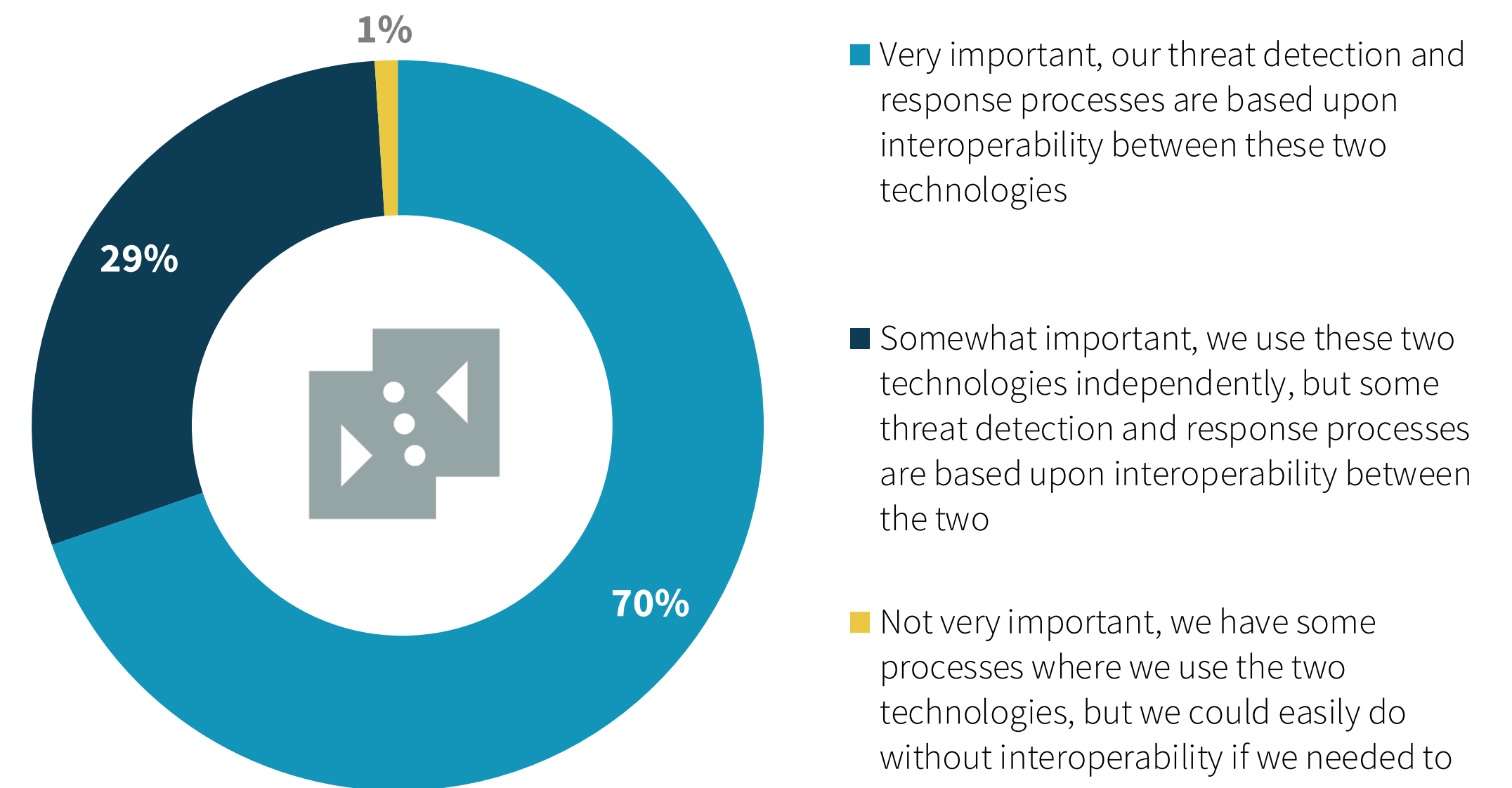
Security analysts tend to use NTA for preliminary threat detection and then pivot to other tools. It is worth noting however that 29% of organizations don't have a "first line of defense" but rather rely on NTA and EDR for threat detection demonstrating the growing importance of network and endpoint security interoperability.

NTA Is a First Line of Defense that Can Serve as Pivot Point to EDR



Indeed, more than two-thirds (69%) of respondents whose organizations use both NTA and EDR deem their interoperability to be very important, regardless of which is considered the "first line of defense." In fact, their threat detection and response processes are based on the interoperability between the two technologies.

More than Two-thirds Believe NTA and EDR Interoperability Is **Very Important**



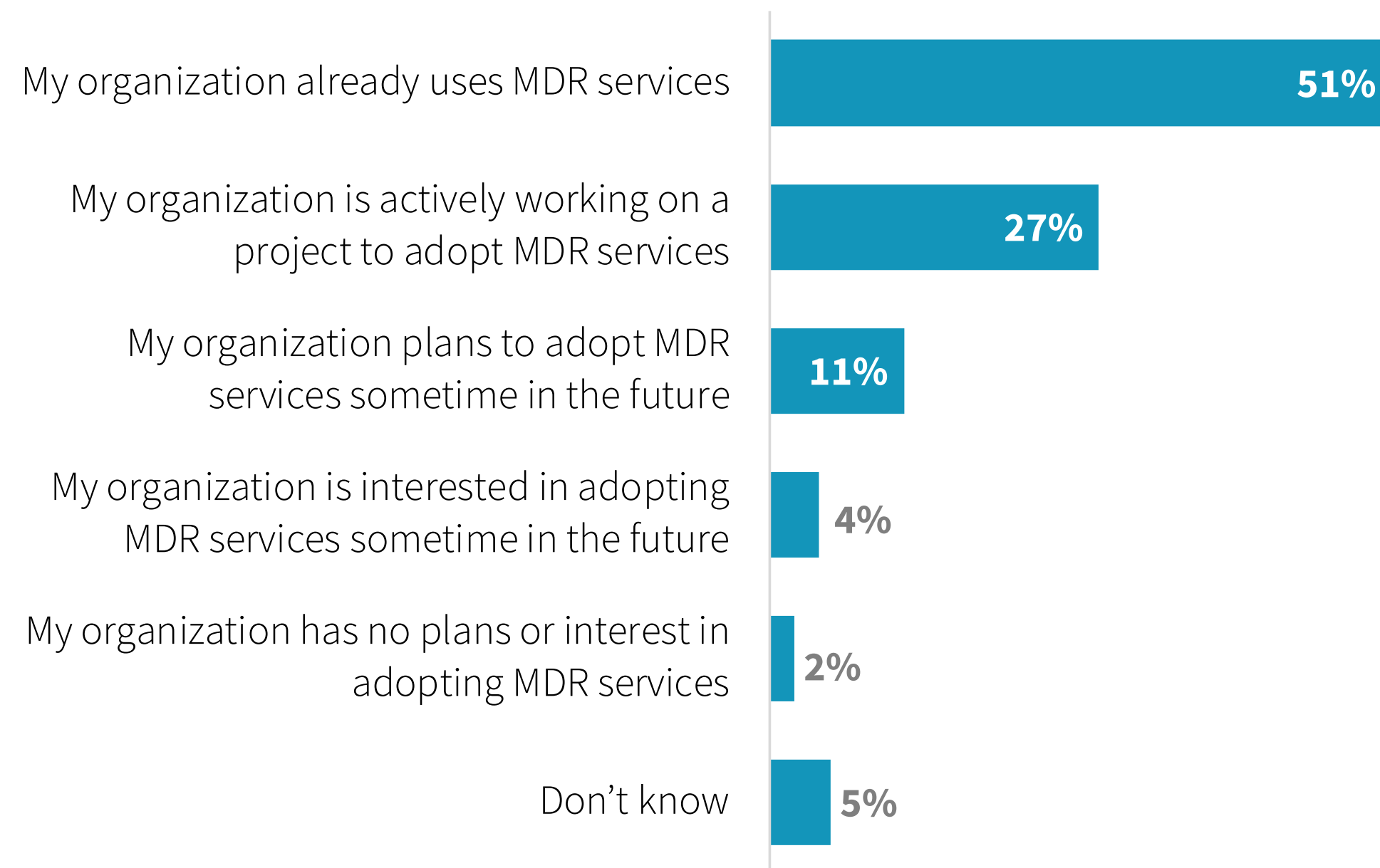
Managed detection/response (MDR) services are gaining popularity as organizations look for help with advanced skills and process improvement.



Most organizations are using or interested in MDR services to improve threat detection and leverage existing MSSP relationships.

Managed detection and response (MDR) services and third-party managed security services are primarily used for detecting and responding to suspicious activities or verifiable cyber-attacks. MDR services can include staff augmentation, threat detection, threat hunting, threat response recommendations, and hands-on remediation and response actions. When asked about plans for managed detection and response services, more than half (51%) of respondents reported their organization was already using them, with another 42% indicating either plans for or interest in these services.

Plans for Managed Detection and Response Services



The three most commonly identified motives for MDR usage were actual or perceived lack of internal skills (50%), desire for rapid deployment (32%), and existing MSSP relationships (29%).

Why Use MDR?



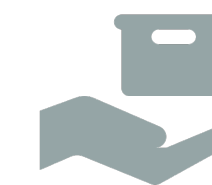
32%

Rapid threat detection/response improvement



29%

Already working with MSSP(s)



28%

MDR service provider can do a better job



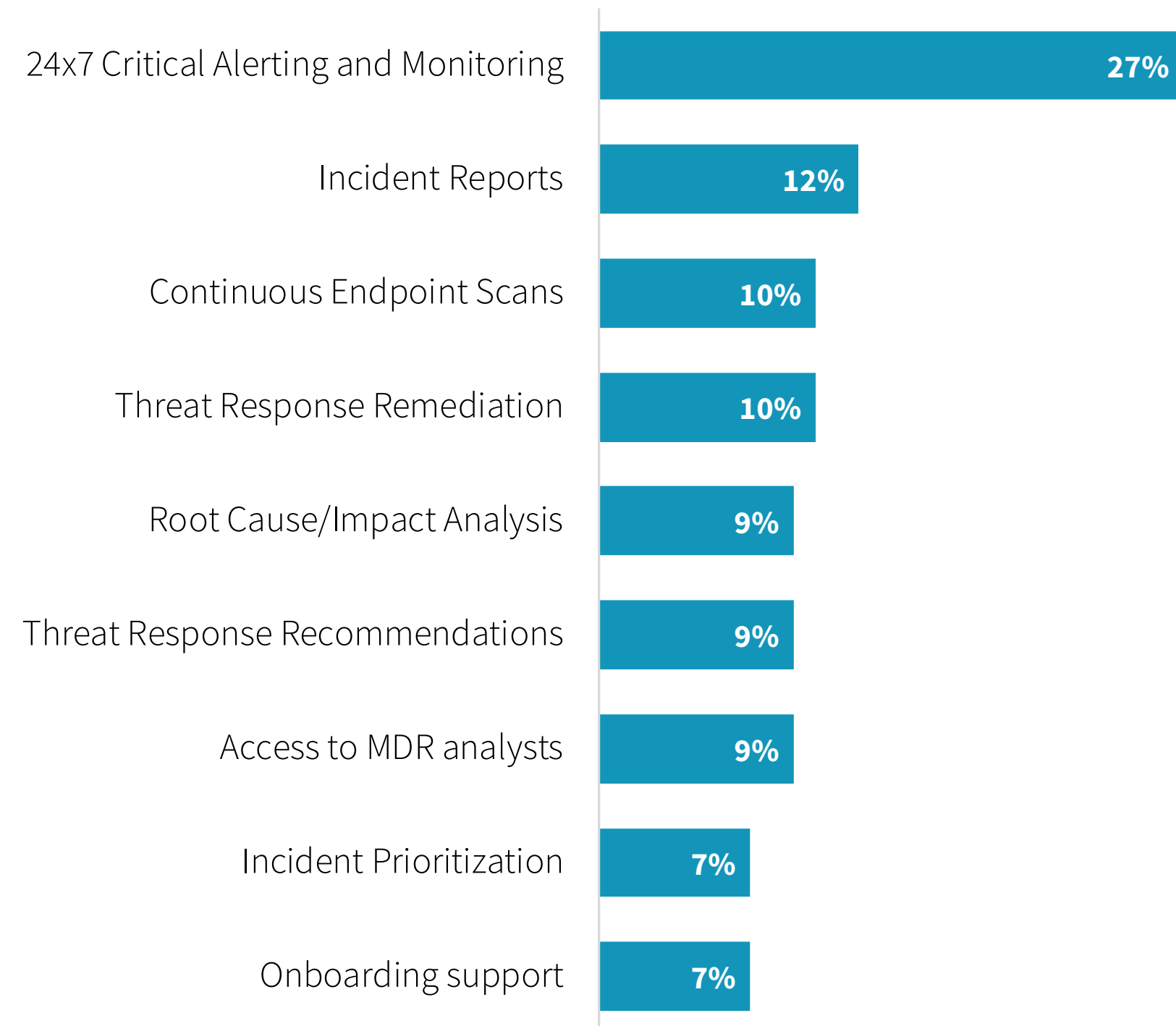
27%

TDR technologies were beyond our internal abilities

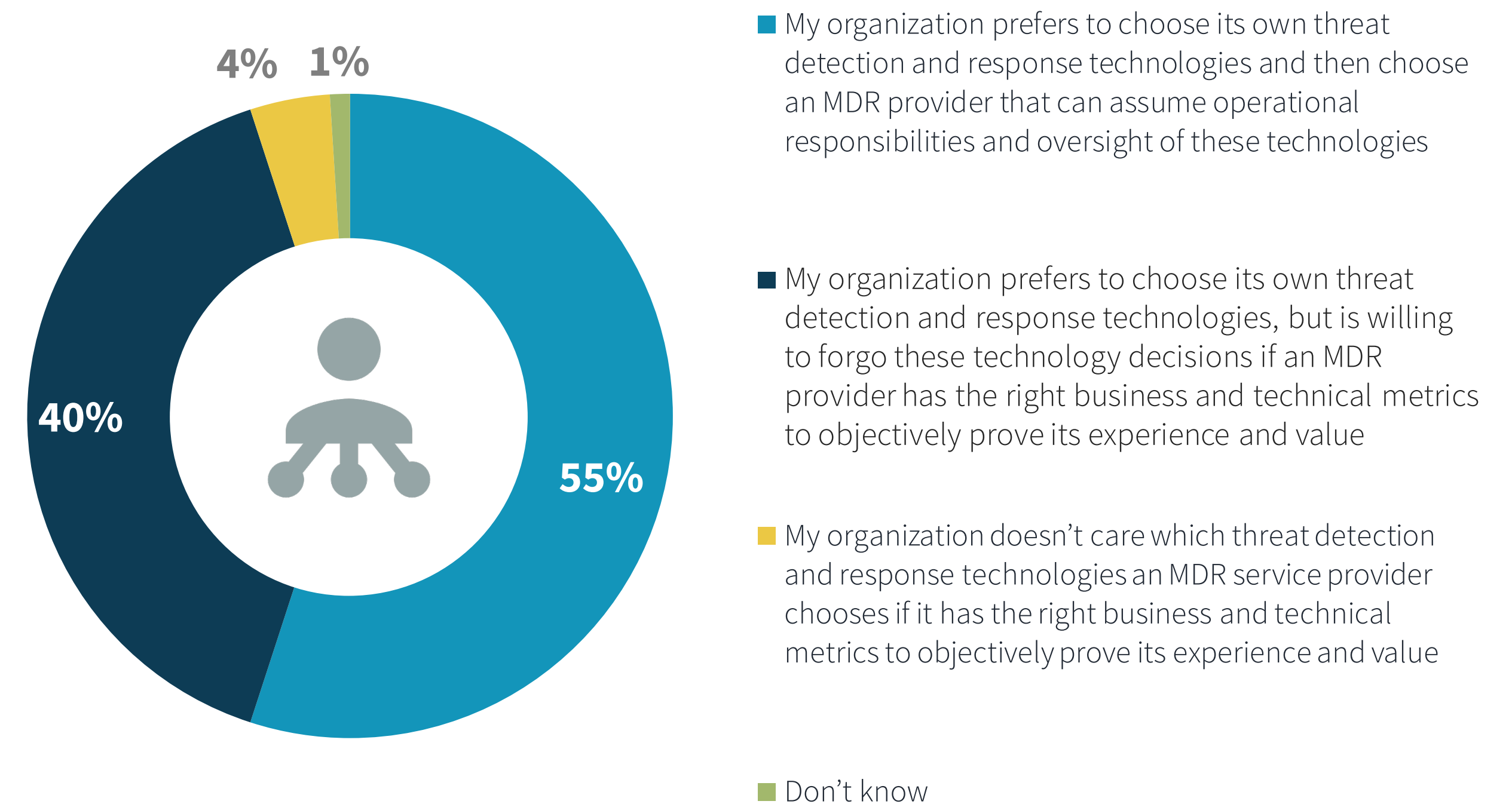
MDR preferences skew toward managed products over generic managed services.

Security professionals believe the most important attribute of MDR services is around-the-clock critical alerting and monitoring (27%). When it comes to the threat detection and response technologies underlying an MDR service, the majority of current and potential users prefer to maintain control of the selection. Specifically, 55% of respondents would rather choose their own TDR technologies and then have an MDR provider assume operational control.

Around-the-clock Alerting and Monitoring Is Far and Away **Most Important** MDR Feature



MDR Preferences Skew toward Managed Products over Generic Managed Services



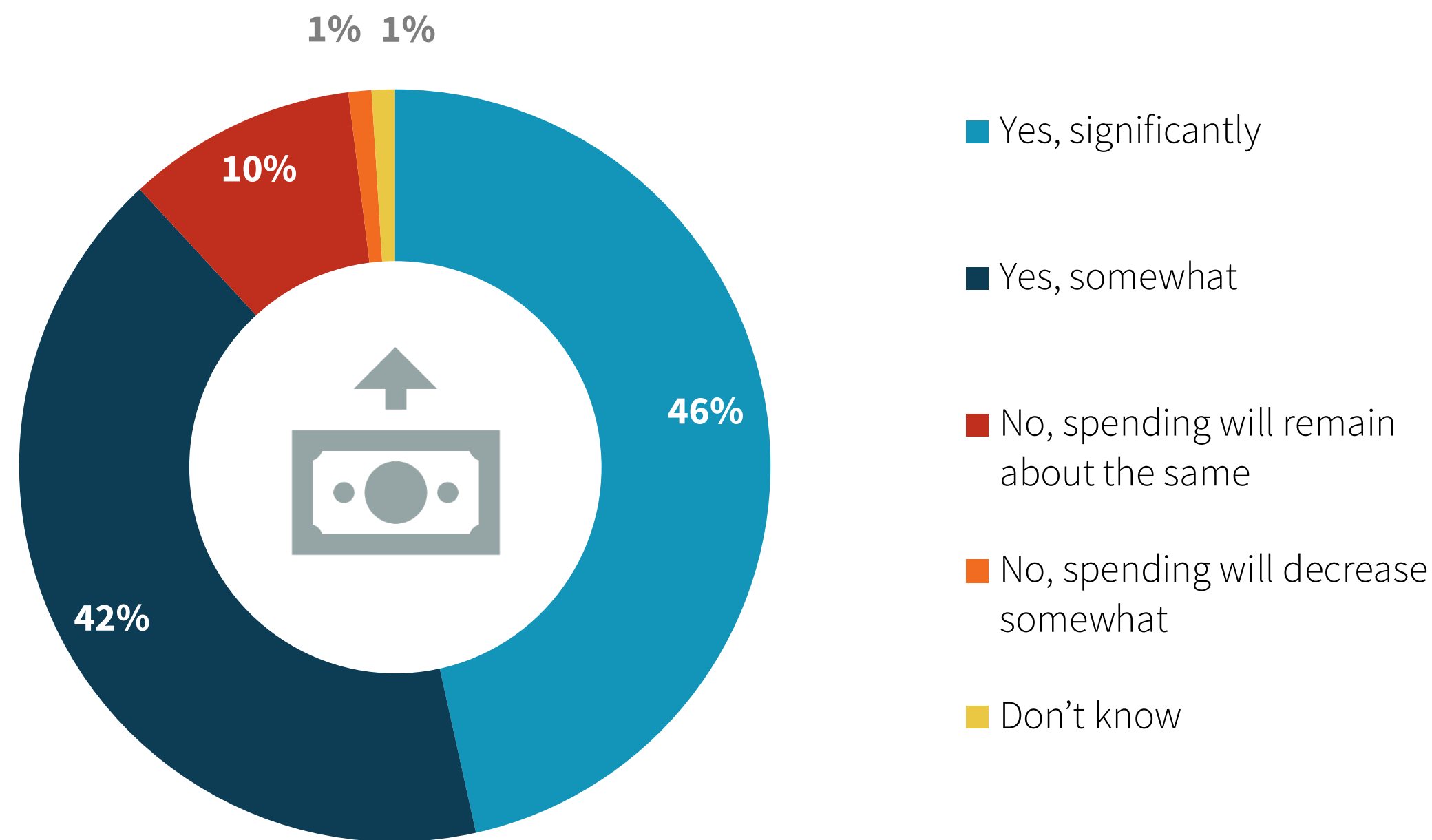
Organizations will increase threat detection/response spending, build integrated cybersecurity technology architectures, and improve collaboration between cybersecurity and IT operations teams.



The vast majority of organizations expect to increase TDR spending over the next year and a half.

Almost nine out of ten of organizations expect to increase spending on threat detection and response technologies, services, and personnel over the next 12-18 months, with nearly half anticipating this increase to be substantial.

Most organizations expect to increase TDR spending



In terms of the areas in which these investments will be likeliest allocated, the highest priorities will involve developing or purchasing integrated security software architectures, improving alignment between IT and security operations teams, automating security operations, conducting additional penetration testing, and hiring more security analysts.

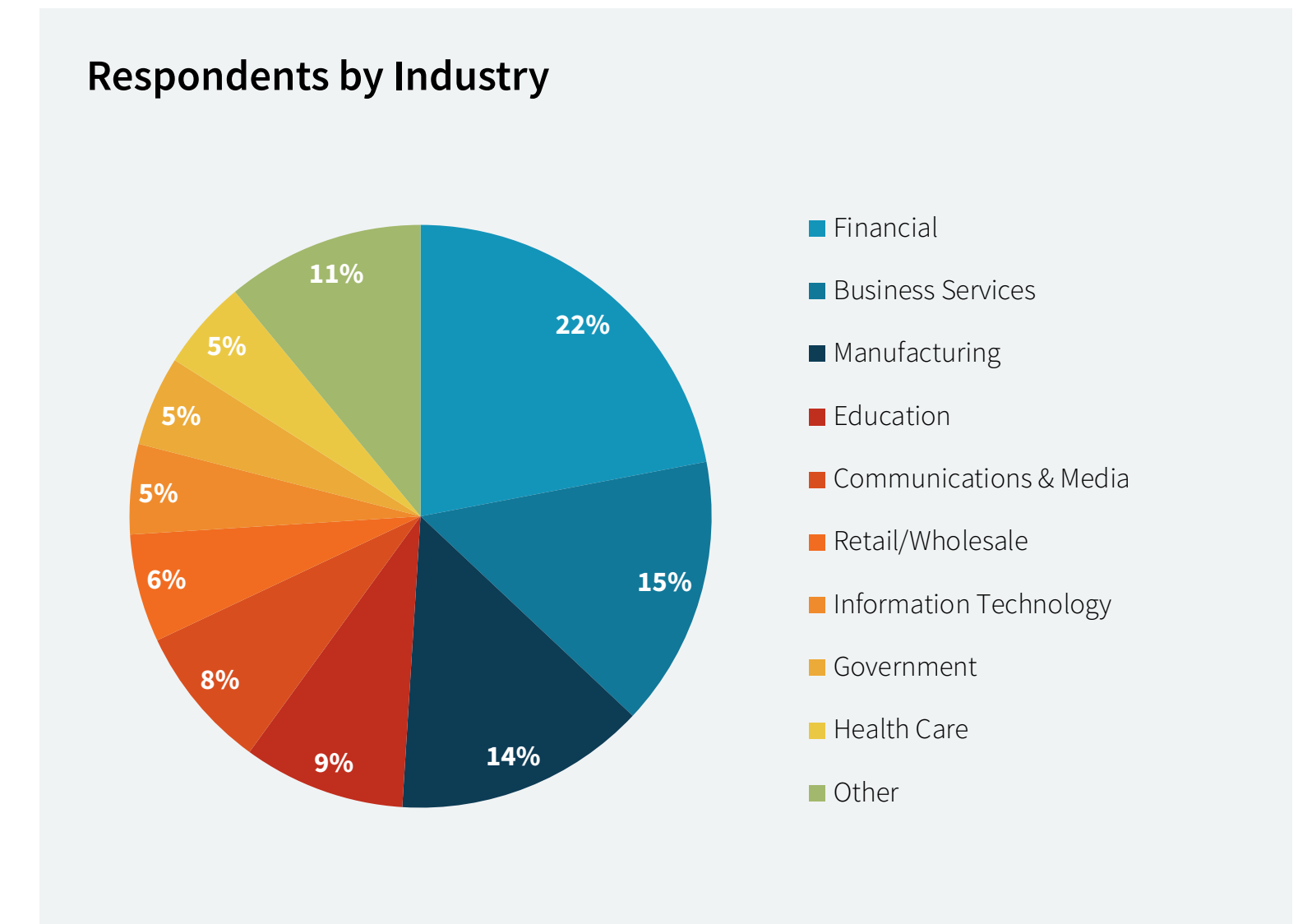
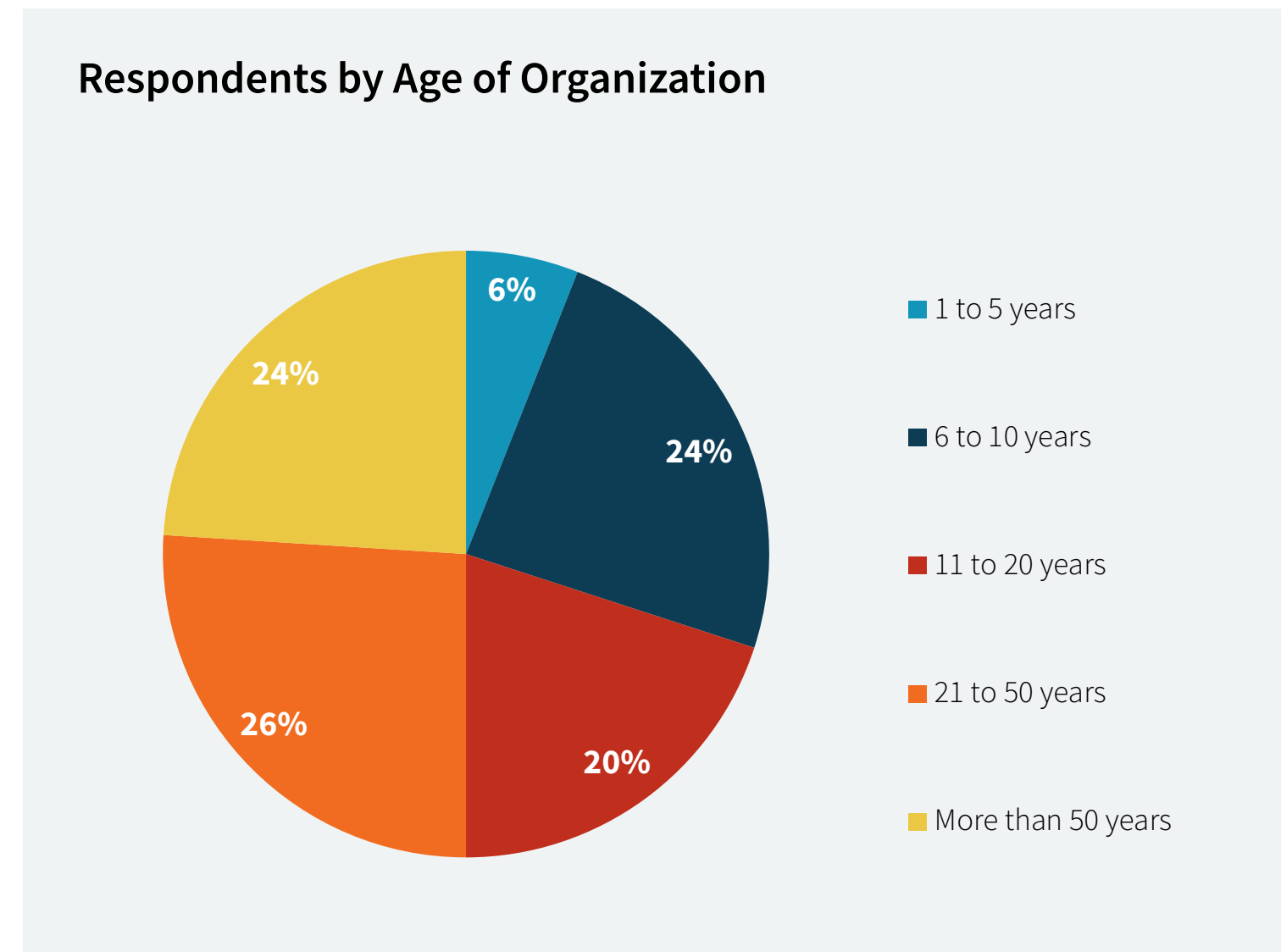
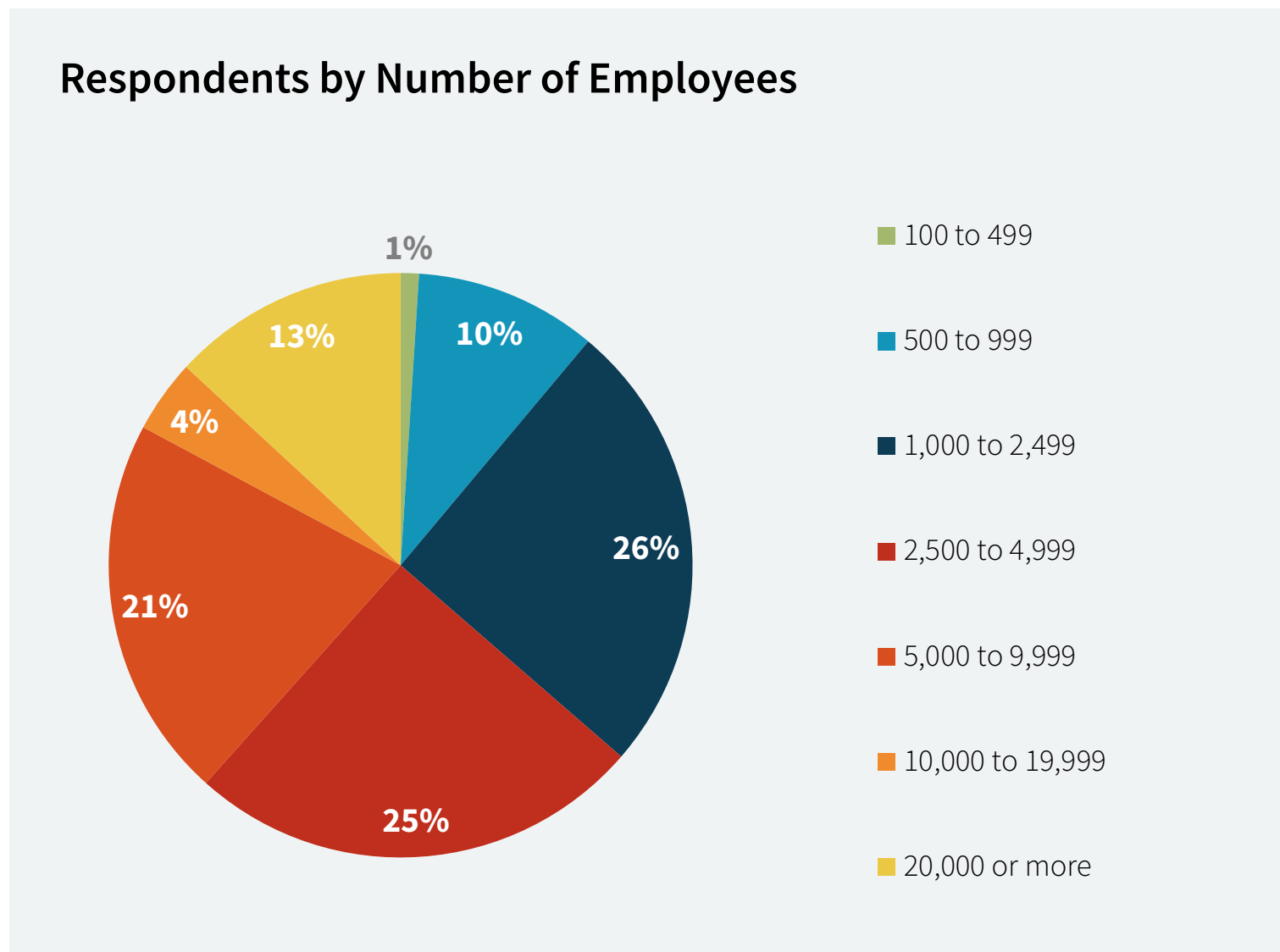
Near-term TDR Strategies Include Integrated Security Architecture, Organizational Alignment, and Automation and Orchestration



Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between December 13, 2018 and December 23, 2018. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally responsible for evaluating, purchasing, and managing threat detection/response products, processes, and services. 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 372 IT and cybersecurity professionals.



AWAKE

Awake Security offers the only advanced network traffic analysis (NTA) solution that applies artificial intelligence to every packet that crosses the wire on-premise, in the cloud, and for IoT and OT networks. Unlike legacy NTA providers, Awake processes the full packet including performing encrypted traffic analysis. With this information, the platform autonomously profiles entities such as devices, users, and applications, while also preserving these communications to provide historical forensic context. This gives Awake the unique ability to model, hunt for, and visualize attacker tactics, techniques, and procedures that span the dimensions of time, entities, and protocols. And, through tight integrations with other security technologies, Awake enables autonomous triage, evidence collection, and remediation.

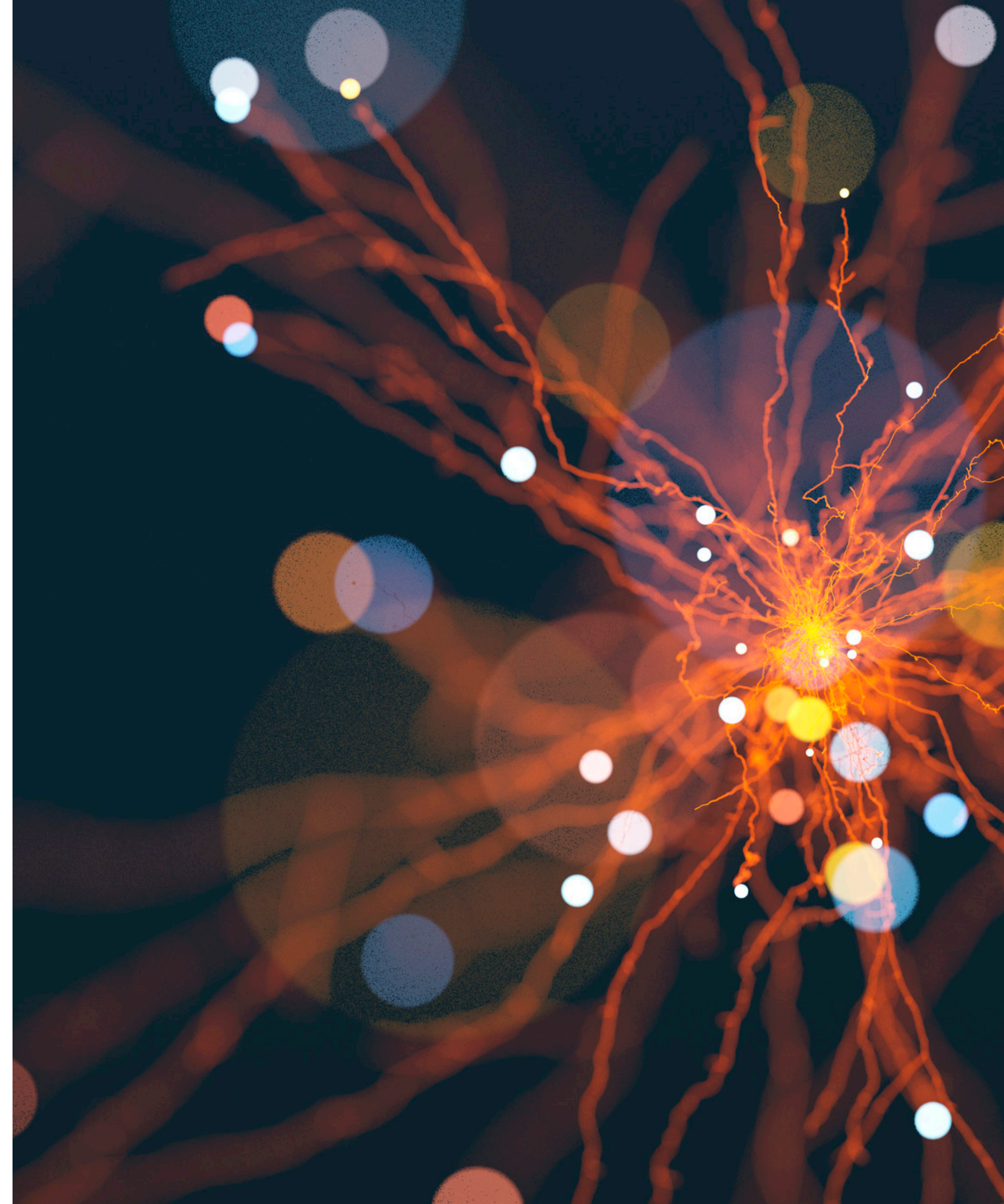
Awake uses an ensemble of machine learning approaches that deliver high-fidelity detection. This contrasts with the first-generation NTA approach that relies primarily on unsupervised learning to spot anomalies from “normal” baselines. Often anomalies are not malicious resulting in false positives and conversely pre-existing compromises are missed because a purely unsupervised approach assumes they are part of the “normal” baseline.

Awake is **ranked #1** for time to value because of its frictionless approach that delivers answers rather than alerts and recognized as the #1 information security solution being evaluated by global 1000 companies in Enterprise Technology Research’s (ETR) **Summer 2019 Emerging Technology Study**.

LEARN MORE

ABOUT ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.



All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. 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 The Enterprise Strategy Group, Inc., 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 ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.
© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.