Enterprise Strategy Group™
by TechTarget

The Future of SecOps in an AI-driven World

Dave Gruber | Principal Analyst

ENTERPRISE STRATEGY GROUP

JANUARY 2025

Research Objectives

Security operations (SecOps) is a mainstay of modern security programs. Once focused on reactive, alert-driven activities, today's security operations have expanded to a risk mitigation function, inclusive of both proactive and reactive strategies like security posture management, core security controls optimization and tuning, detection and response, and recovery in the event of a harmful cyberattack. This expanded agenda has also increased collaboration with other functions, including risk management, IT, OT, software development and engineering, supply chain management, and more. With such a broad scope of responsibility, it's no surprise that the number and complexity of systems and technologies involved continue to grow, heavily influenced by the more recent explosion of generative AI (GenAI) adoption.

Despite all of this, for the first time in the past five years, this research indicates that the scales are tipping, as more organizations reported this year that SecOps is getting easier. This improvement is fueled by three industry mega-trends: tool consolidation, the application of GenAI within SecOps, and the effectiveness of extended detection and response (XDR) solutions.

To gain further insights into these mega-trends and other developments in the security operations space, TechTarget's Enterprise Strategy Group surveyed 366 IT and cybersecurity professionals at large midmarket and enterprise organizations in North America (US and Canada) involved with security operations technology and processes.

THIS STUDY SOUGHT TO:

- **Define** current, planned, and visionary use cases for GenAI in security programs.
- **Validate** whether current AI-driven solutions are making a difference and quantify how much impact AI is having on program improvement.
- **Determine** how confident security leaders are in AI, where they believe it will impact program design and operation most, and what projects and budget increases are planned to leverage this new opportunity.
- **Understand** what vendor messages are getting the most attention, including messages that buyers feel promise more than what's possible.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.

Key Findings

The SecOps Scale Continues to Tip in a Positive Direction

PAGE 4

Consolidation and Platformization Are Increasingly Common for Security Tools and the Data Stack

PAGE 8

XDR and SIEM Are Both Providing Measurable Value, but XDR May Still Replace SIEM Someday

PAGE 12

GenAI Use Cases for SecOps Are Limited at This Point but Poised for Significant Contribution

PAGE 18

> "Leveraging GenAI and machine learning, organizations further report that they are finally **improving their ability to operationalize threat intelligence** to keep up with current threats and adversaries that many target them."

Dave Gruber | Principal Analyst
ENTERPRISE STRATEGY GROUP

The SecOps Scale Continues to Tip in a Positive Direction

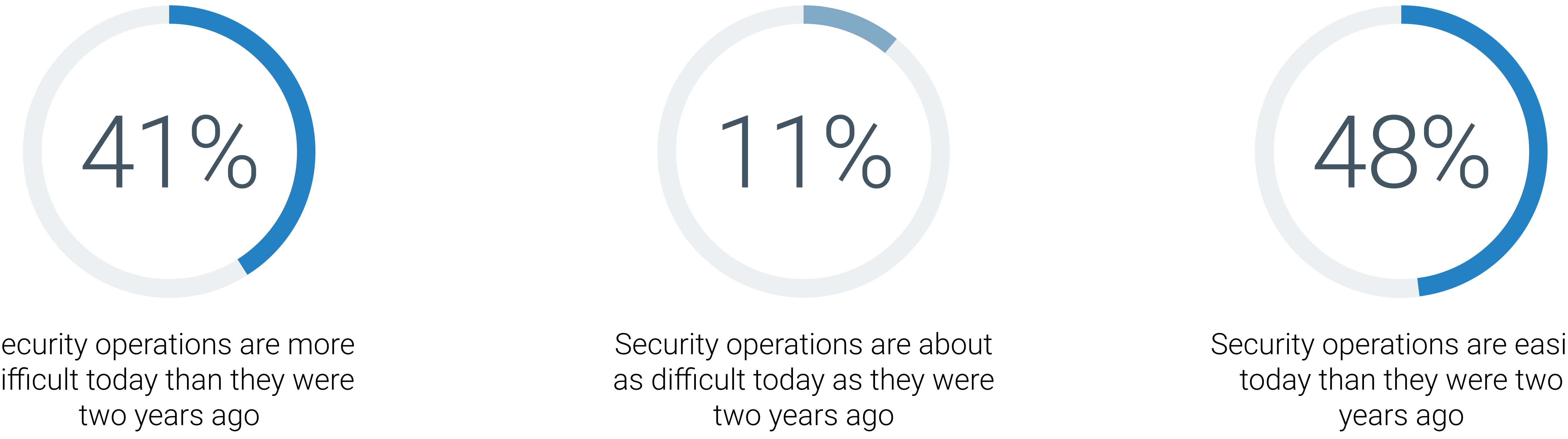
Drivers That Tip the SecOps Scales in a Positive Direction

Almost half (48%) of organizations believe SecOps has gotten *easier* over the past two years, compared with the 41% that think it has become more difficult. This is an improvement from past years, when 49% and 45% reported increased difficulty within SecOps in 2022 and 2023 respectively.

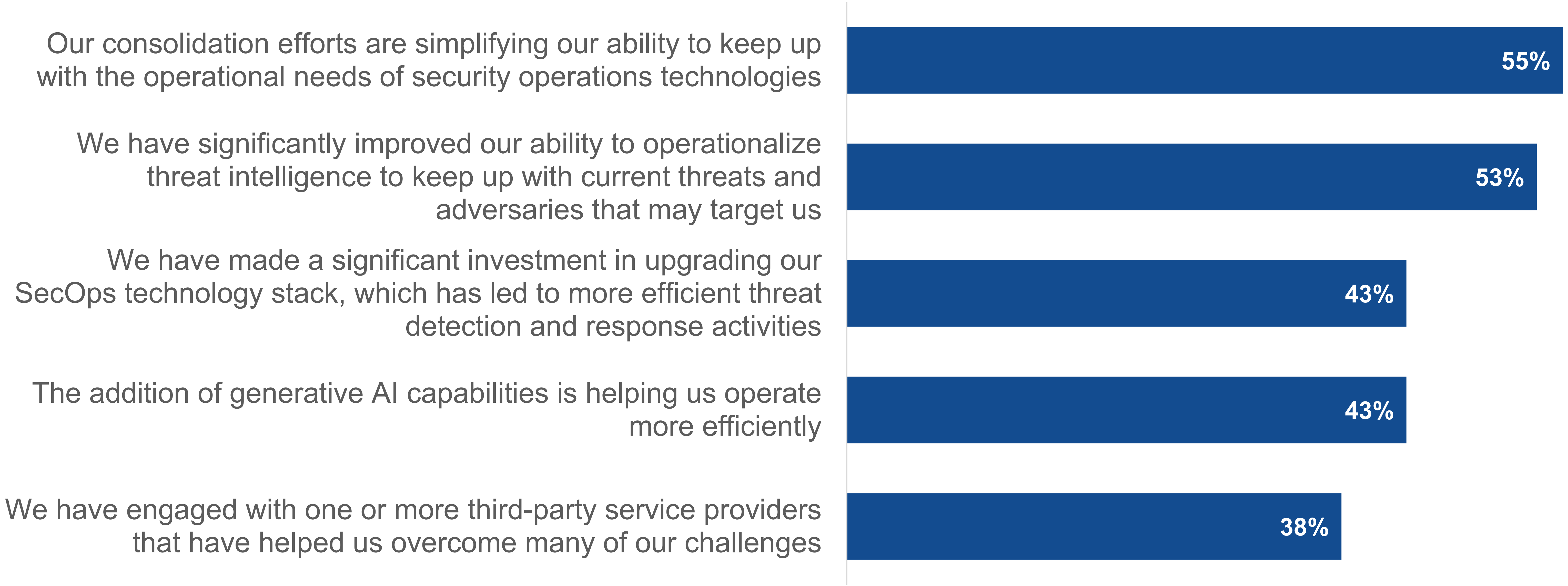
So what's happening to help simplify SecOps? More than half (55%) of organizations report that consolidation efforts are streamlining the management and operations of the many security tools and processes in use. Leveraging GenAI and machine learning, organizations further report that they are finally improving their ability to operationalize threat intelligence to keep up with current threats and adversaries that many target them. This improvement reverses a historical key challenge that had previously seen better operationalizing threat intelligence as a top-five *challenge*. Other commonly cited reasons included more efficient threat detection and response enabled by upgrades to the SecOps technology stack (e.g., extended detection and response [XDR], security information and event management [SIEM], and automation), as well as the addition of GenAI capabilities resulting in more efficient operations.

It's worth noting that the use of third-party services providers remains high on the list of solutions helping teams overcome many of their security operations shortcomings.

Assessing the change in the security operations landscape.



Top five reasons SecOps has become easier over the last two years.

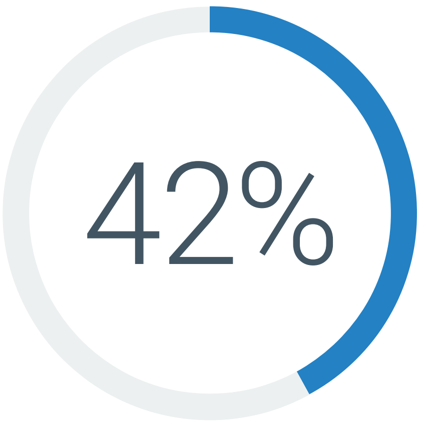


General SecOps Challenges

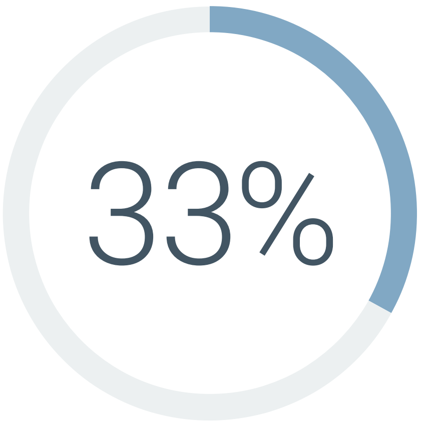
Despite significant improvement, challenges still exist across the many aspects of security operations. Topping the list is the pace of growth and change in the attack surface, as security teams struggle to keep up. And despite improvements reported from tool consolidation and better operationalizing threat intelligence, many still face challenges in this area as they work to carry out improvements.

Notably, firefighting to address high-priority or emergency issues is less commonly cited this year. Also notable, and less positive, is that gaining appropriate levels of security oversight with cloud-based workloads, applications, and SaaS moved up in terms of the number of organizations prioritizing it as an issue, reflecting continuing growth and change in cloud infrastructure and applications.

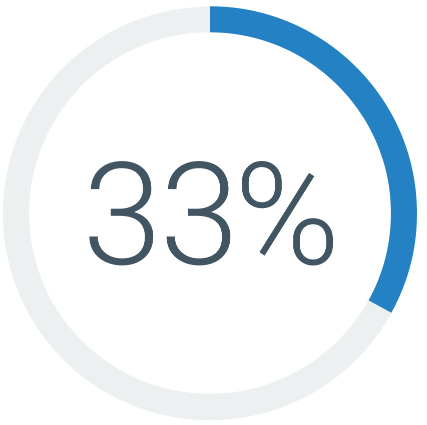
Top six SecOps challenges.



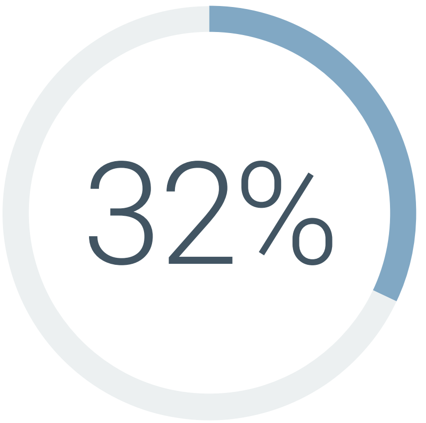
Monitoring security across a growing and changing attack surface



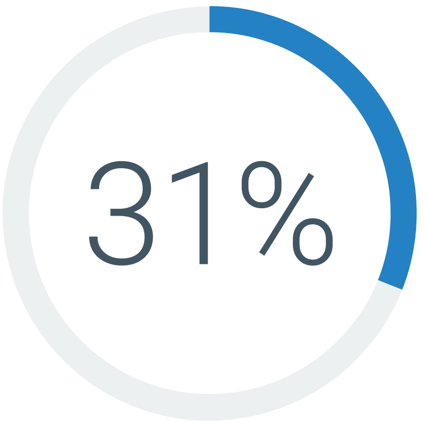
Managing too many disconnected point tools for security analytics and operations, making it difficult to piece together a holistic strategy and investigate complex threats



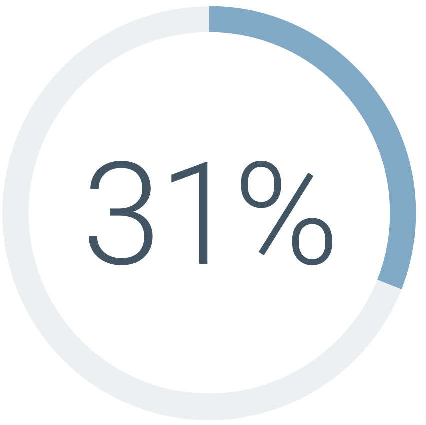
Operationalizing cyberthreat intelligence



Spending too much time on high-priority or emergency issues and not enough time on strategy and process improvement



Detecting and/or responding to security incidents in a timely manner



Gaining the appropriate level of security oversight with cloud-based workloads, applications, and SaaS

Nearly a third (31%) believe actively improving their security hygiene and posture management to reduce the attack surface will **improve both security efficacy and operational efficiency.**

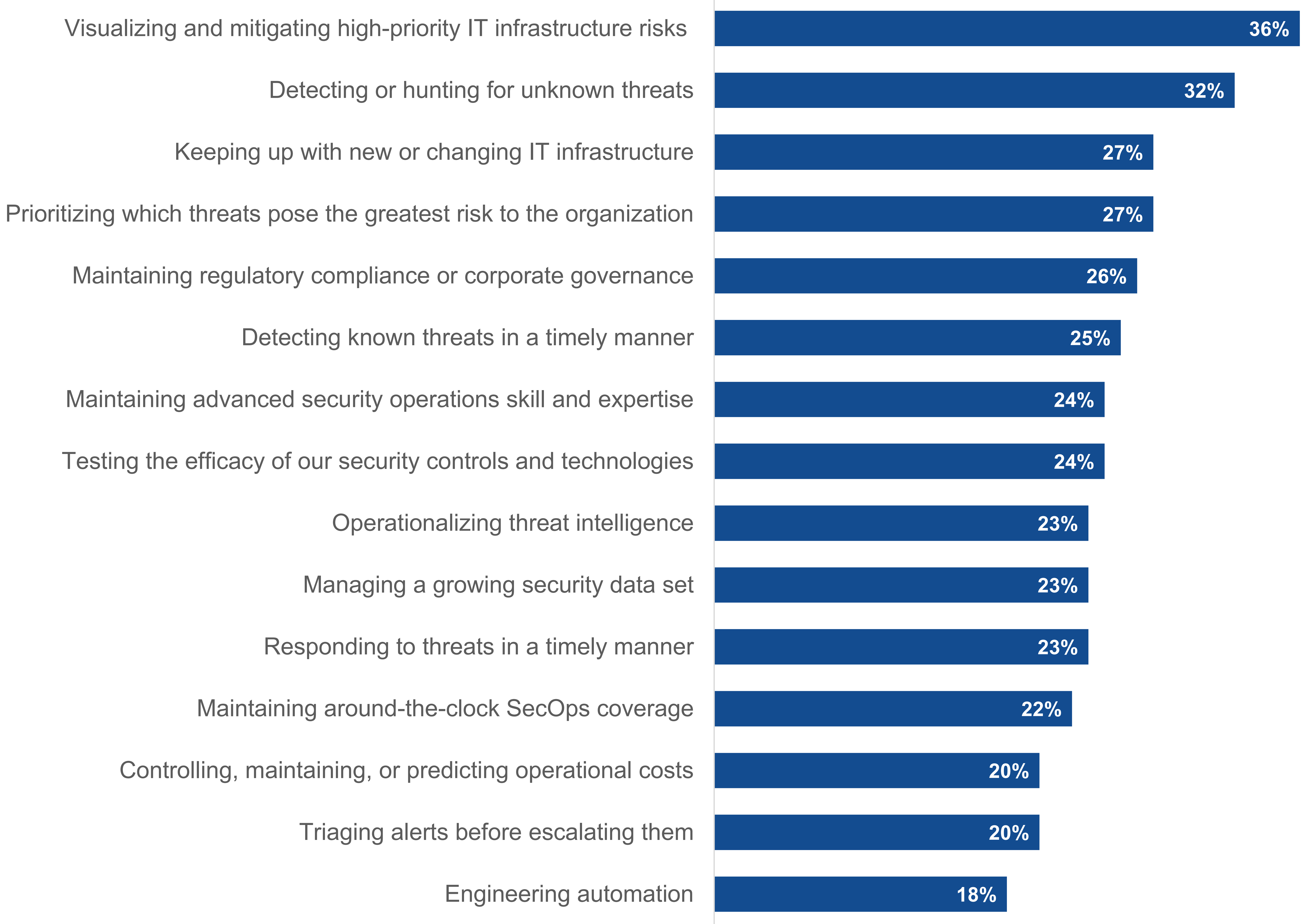
SecOps Program Weaknesses

The risk agenda has finally landed within SecOps, as the risk-driven security strategies have rapidly evolved over the past three years. This key takeaway from the research shines a light on the new proactive focus within SecOps as security posture management takes on a mainstream role in the prioritization and mitigation of threats.

The bad news is that many see weaknesses here (both in visualizing and mitigating high-priority IT infrastructure risks and prioritizing which threats pose the greatest risk to the organization) as they focus on areas of improvement for 2025.

Accordingly, actively improving security hygiene and posture management to reduce the attack surface tops the list of what organizations think would be most beneficial to improving security efficacy and operational efficiency.

Weakest areas of security operations.

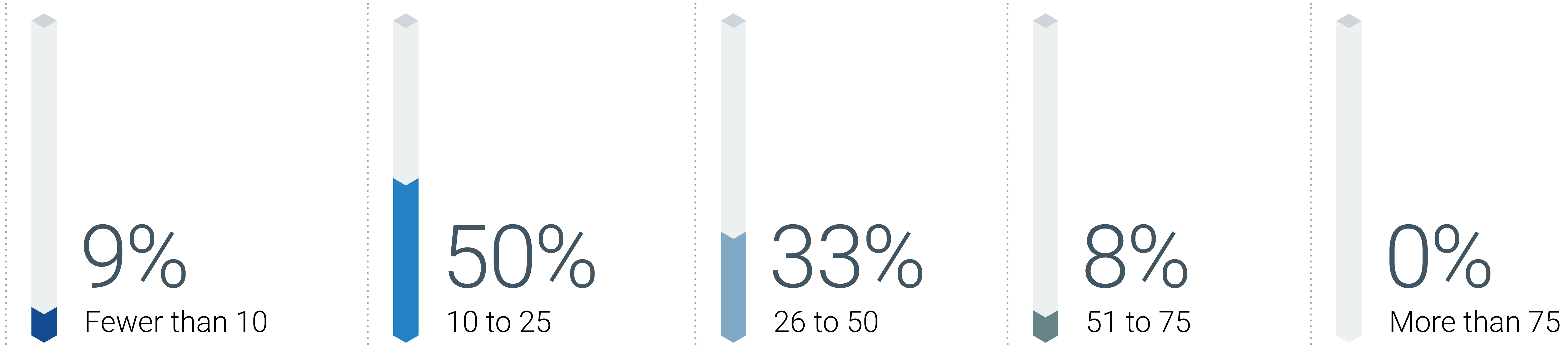


Consolidation and Platformization Are Increasingly Common for Security Tools and the Data Stack

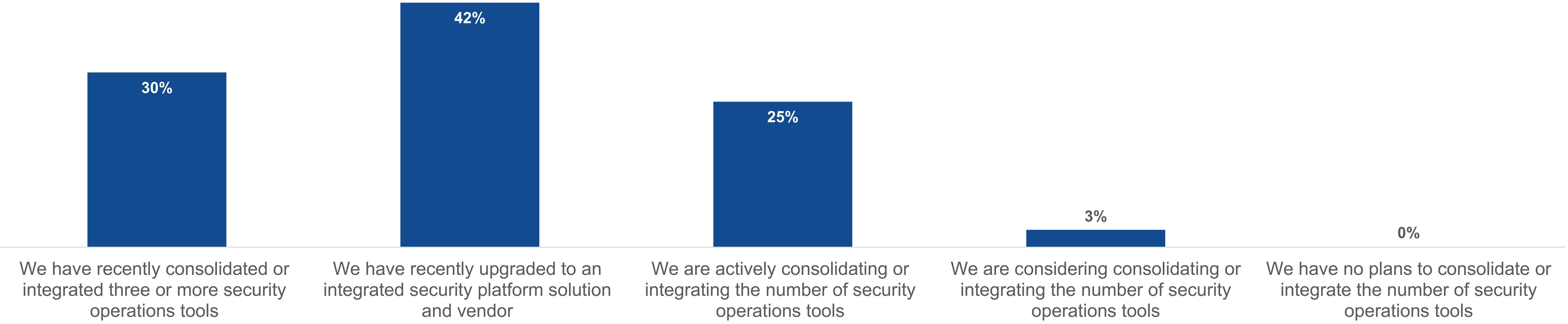
Adoption of Security Platforms Is a Priority

The march to consolidation continues, with measurable progress resulting in positive outcomes. Currently, with 91% of organizations indicating the usage of at least 10 SecOps tools, complexity is the enemy, driving consolidation as a priority once again. Indeed, more than half have recently consolidated (30%) or are actively consolidating (25%) their SecOps tools.

Number of SecOps tools in use.



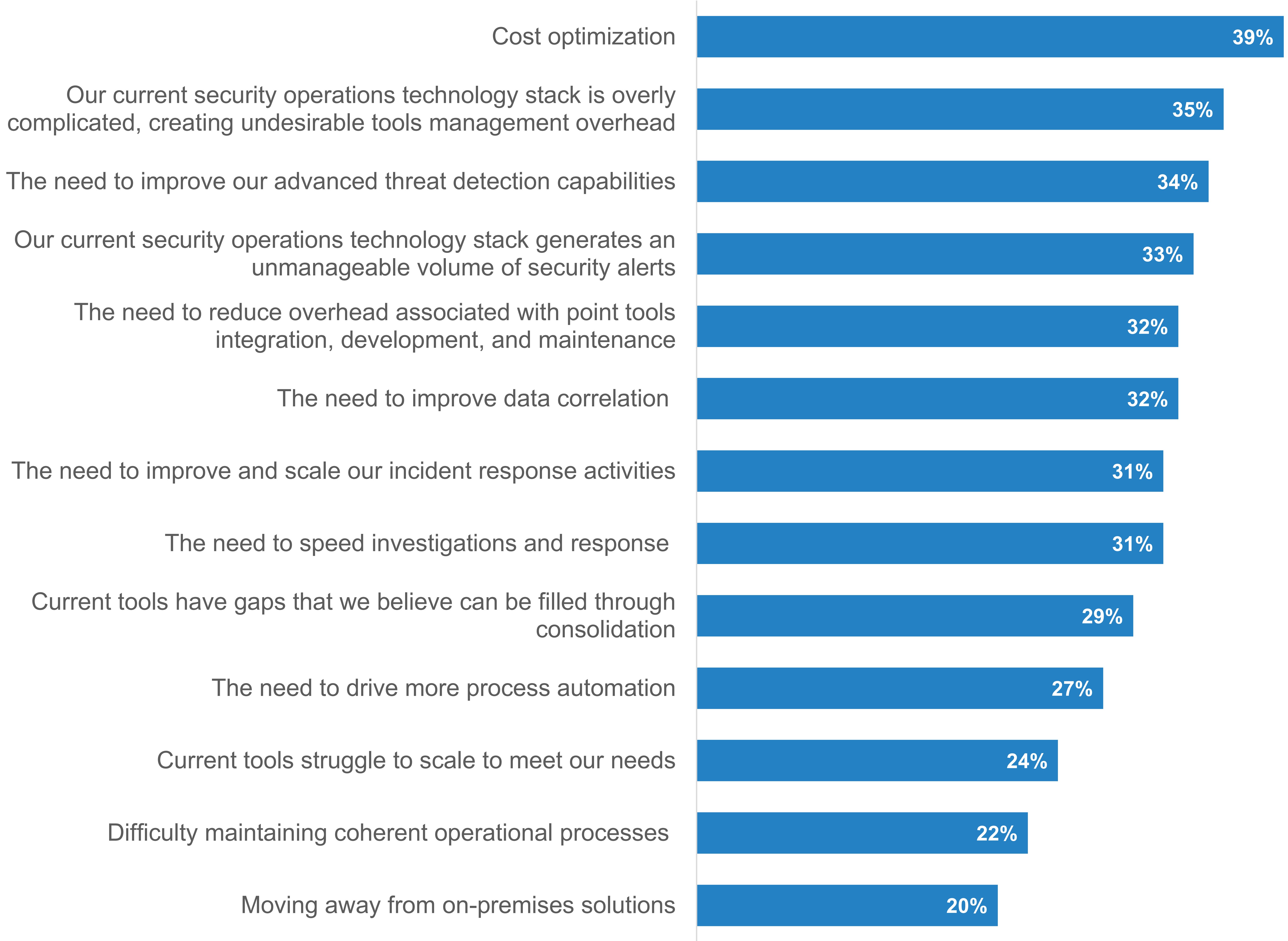
Position on consolidation of SecOps tools.

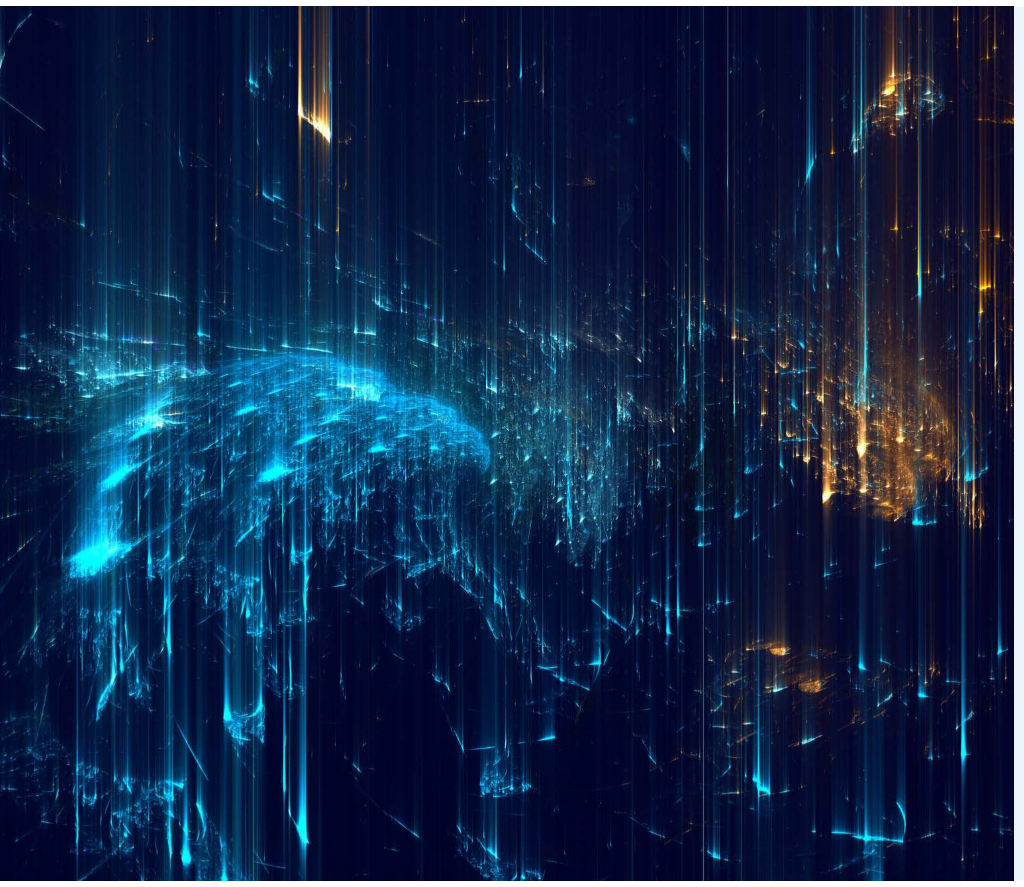


SecOps Tool Consolidation Drivers

Interestingly, the objective of consolidation efforts has shifted slightly from complexity to cost, as budgets stay tight in a tough economy. In addition to tools management overhead costs, the shear number of alerts generated by the many tools continues to challenge teams. A further consolidation motivator is the need for better data correlation, and the desire to improve advanced threat detection capabilities is likely driving many to explore how XDR and SIEM improvements can help.

Drivers behind SecOps tool consolidation efforts.

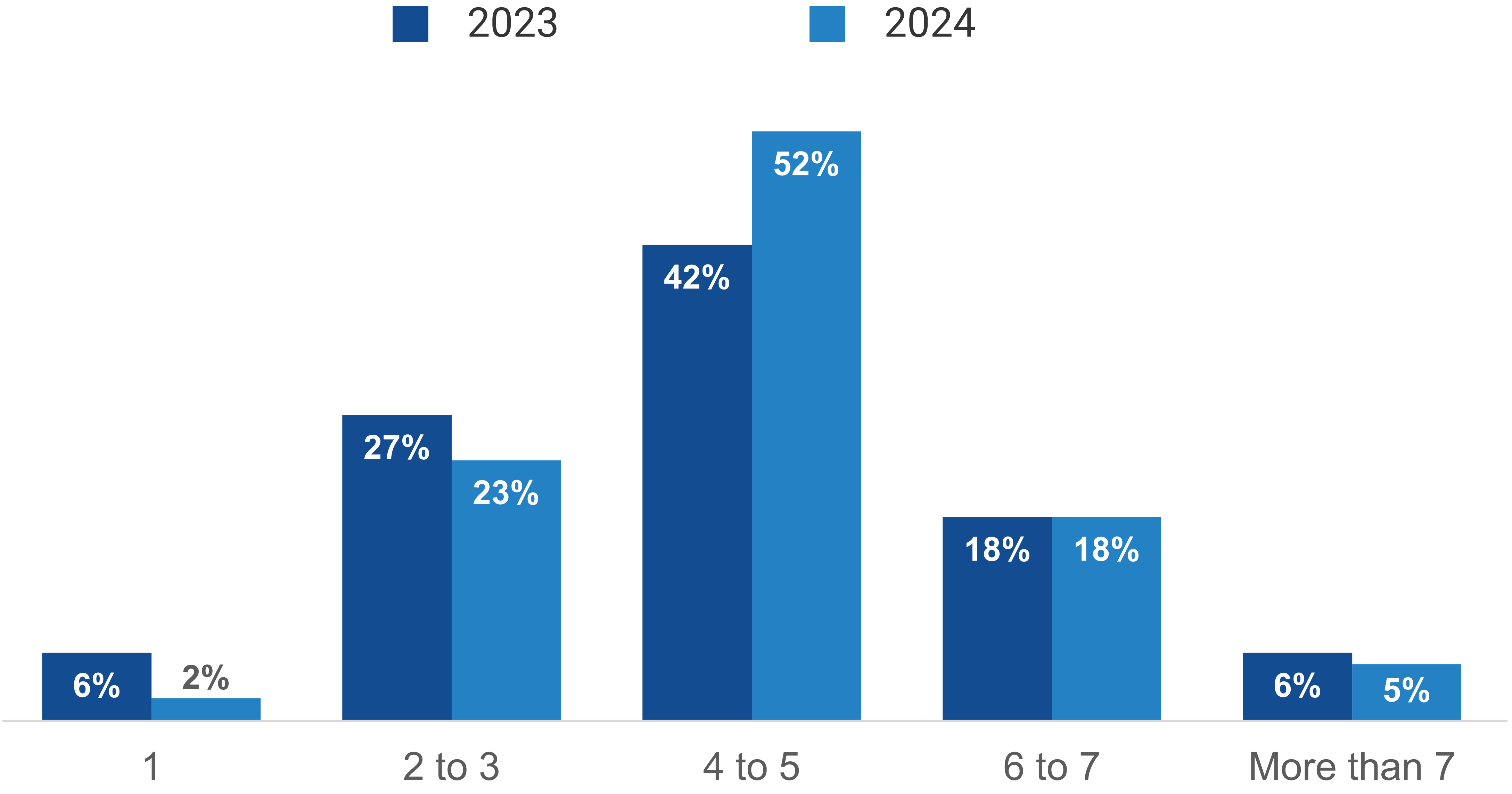




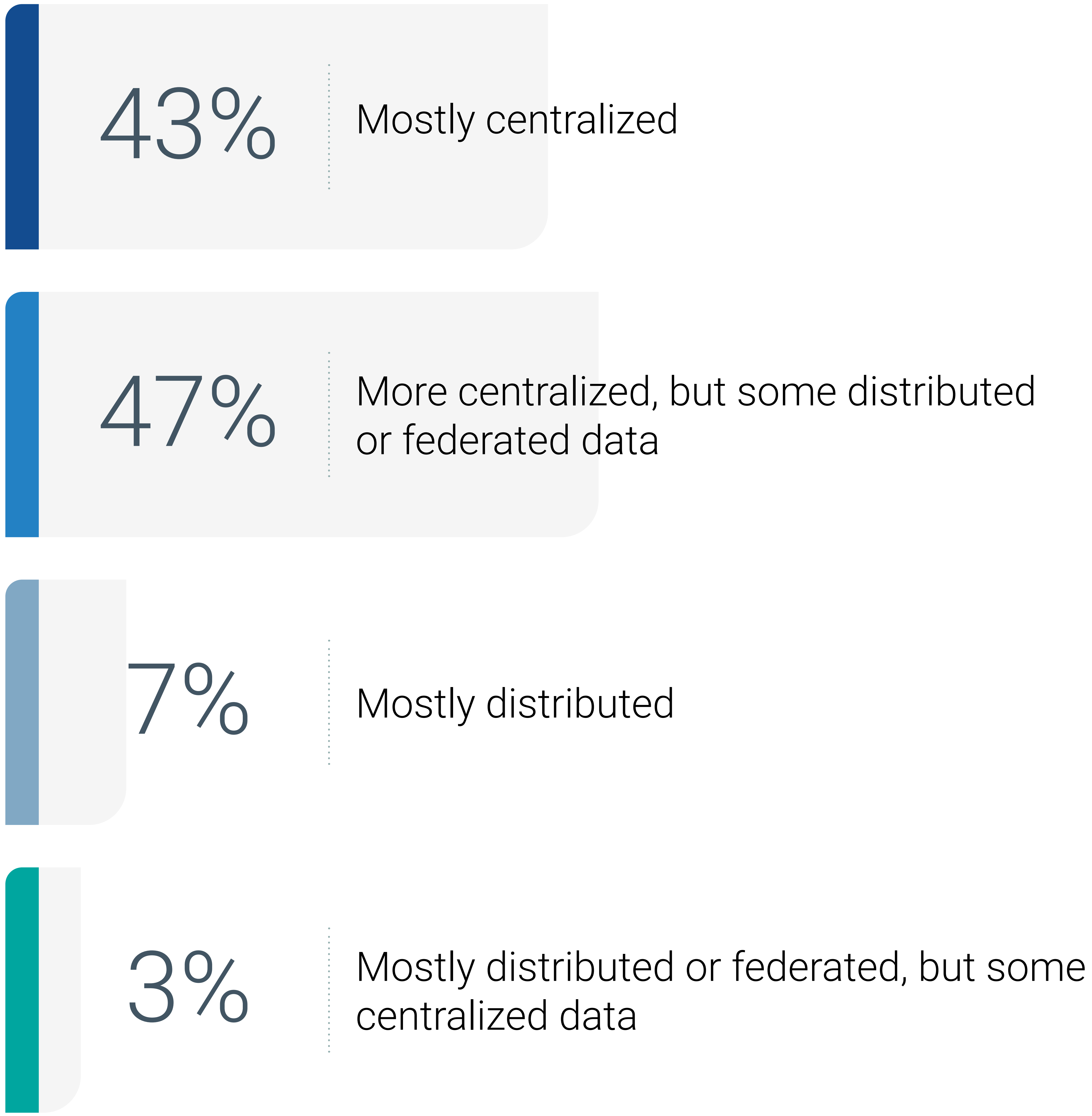
Security Data Repositories: Consolidation Is Underway

Aligned with security tool consolidation initiatives, a more centralized security data strategy is the vision for most, though progress is slow. Despite consolidation efforts, multiple repositories persist, with slight year-over-year increases in repositories in use.

Number of security data repositories.



Current security data strategy.



43% Mostly centralized

47% More centralized, but some distributed or federated data

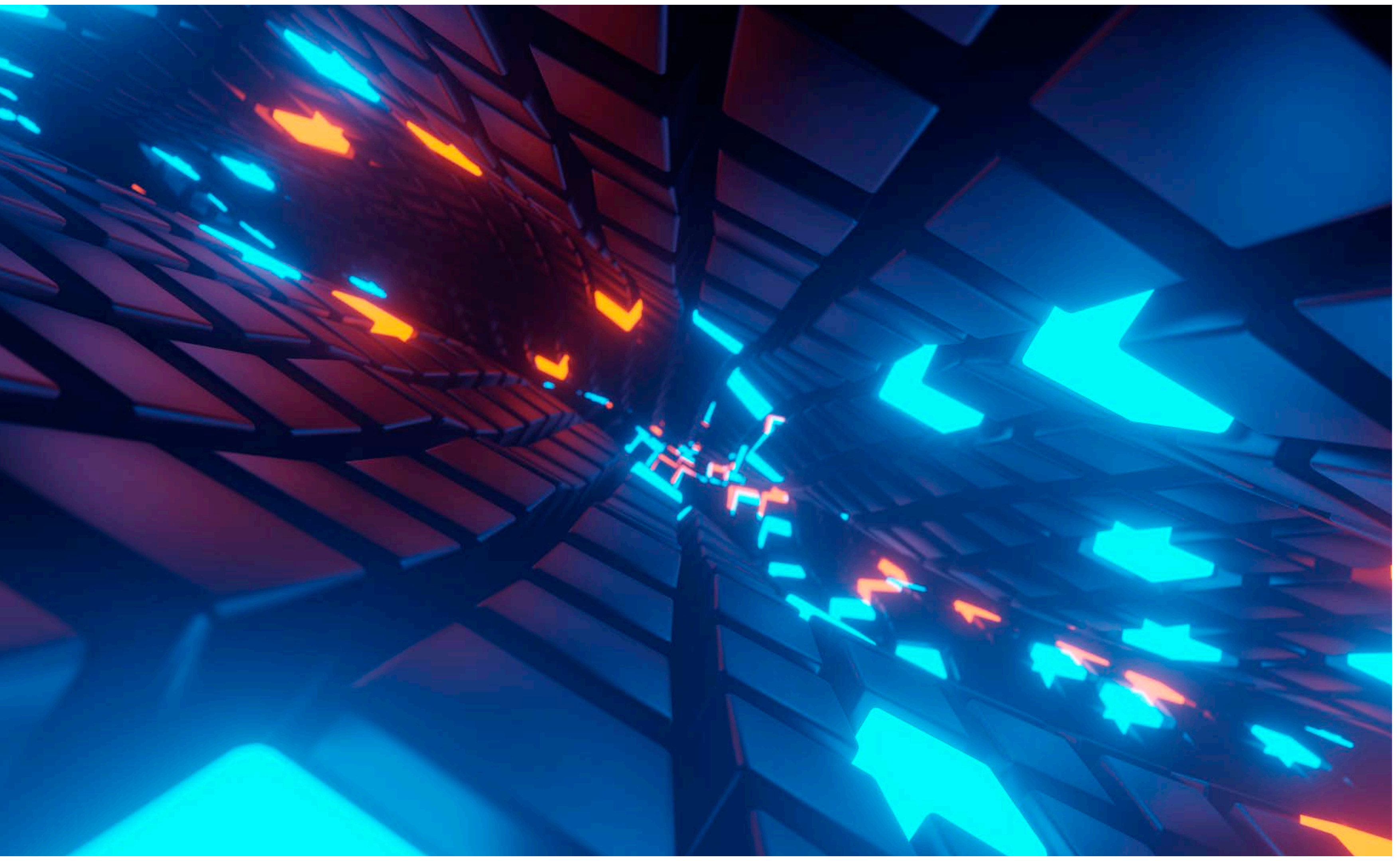
7% Mostly distributed

3% Mostly distributed or federated, but some centralized data

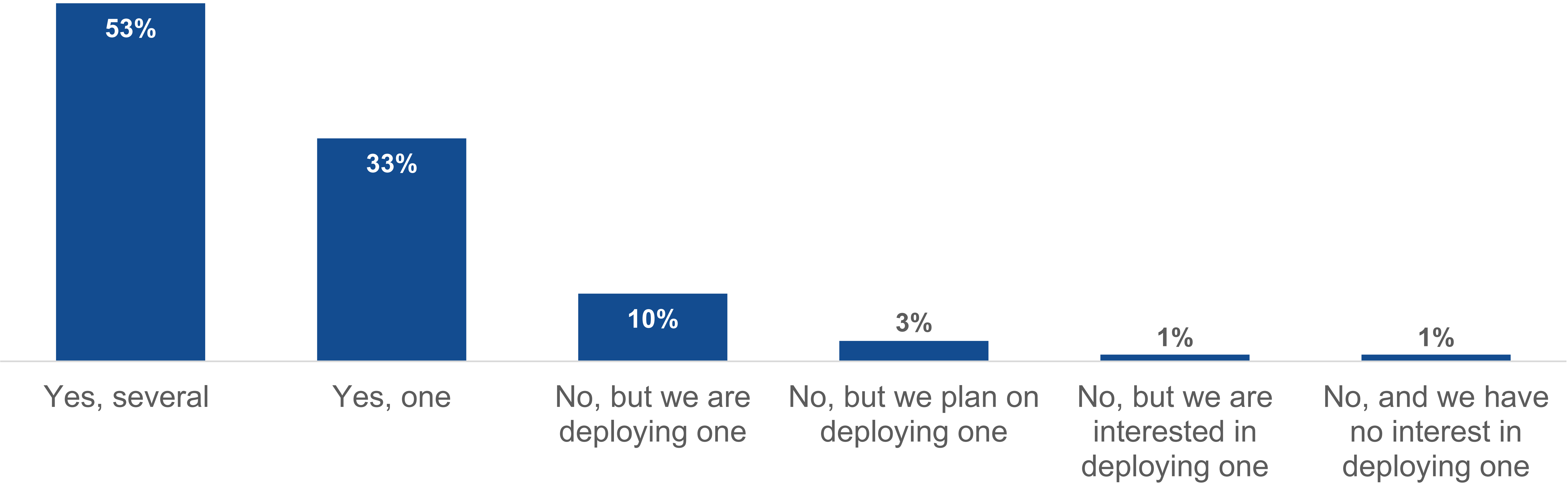
XDR and SIEM Are Both Providing Measurable Value, but XDR May Still Replace SIEM Someday

SIEM Usage Continues To Be Strong, but Change Is in the Winds

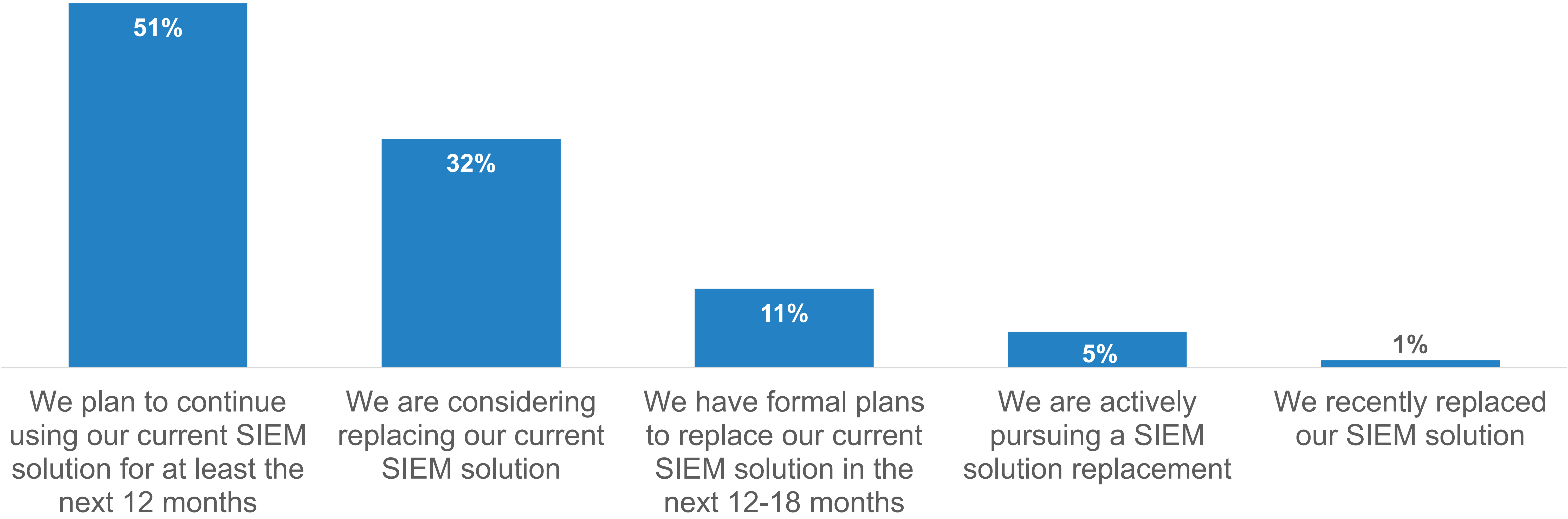
Despite widespread continued usage of SIEM technology (86%), organizations are paying significant attention to improving the security data layer, with nearly half (48%) of organizations either considering replacing one or more of their current SIEM solutions or planning to. Pressure is coming from next-generation SIEM, XDR, and platform providers—all with “new and improved” solutions for operationalizing security data for SecOps. Despite this focus, Enterprise Strategy Group believes that SIEM will continue to play a key role in the SecOps security stack for the foreseeable future, supporting many use cases.



Do organizations have SIEM solutions deployed?

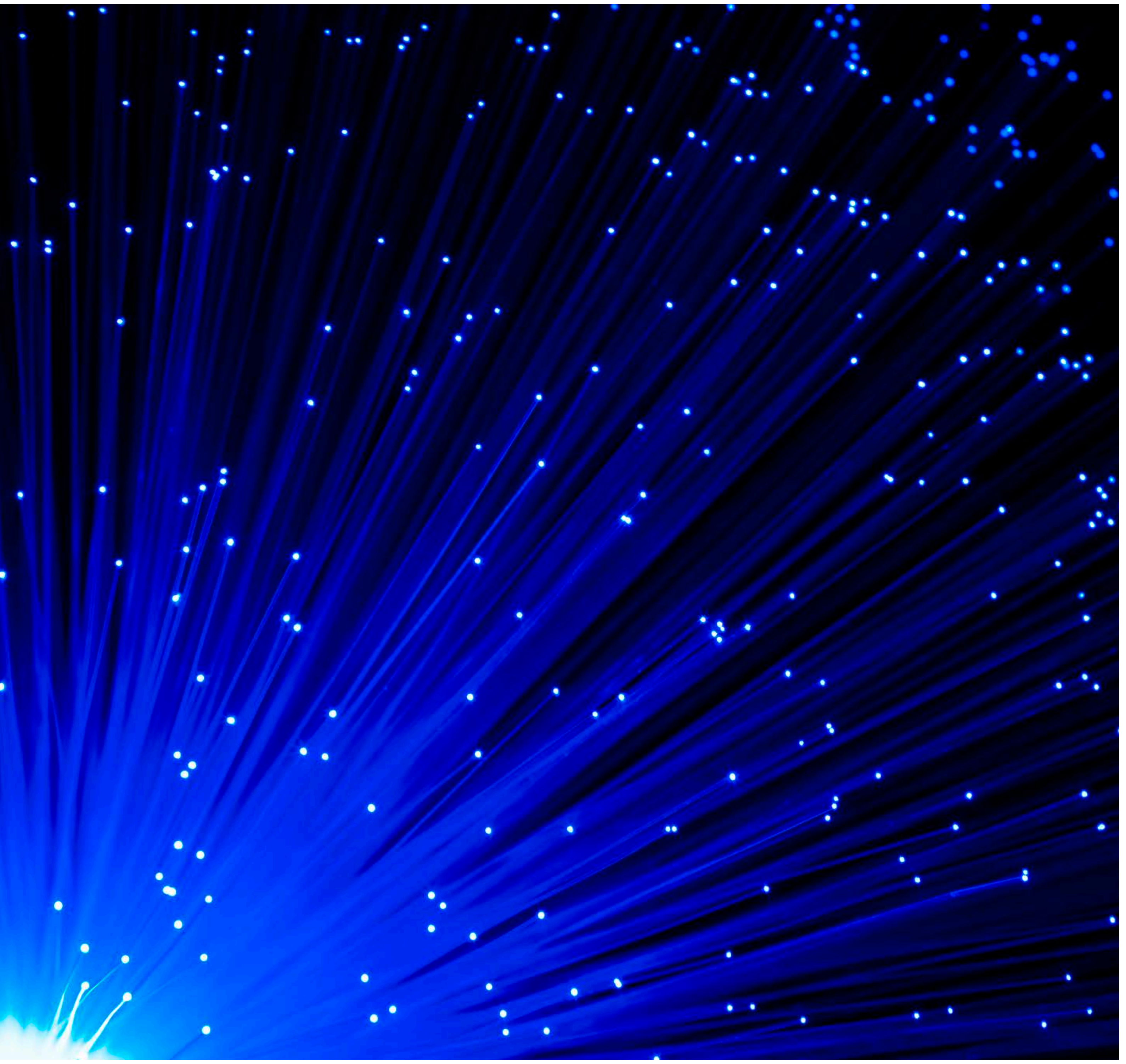


Current SIEM strategy.

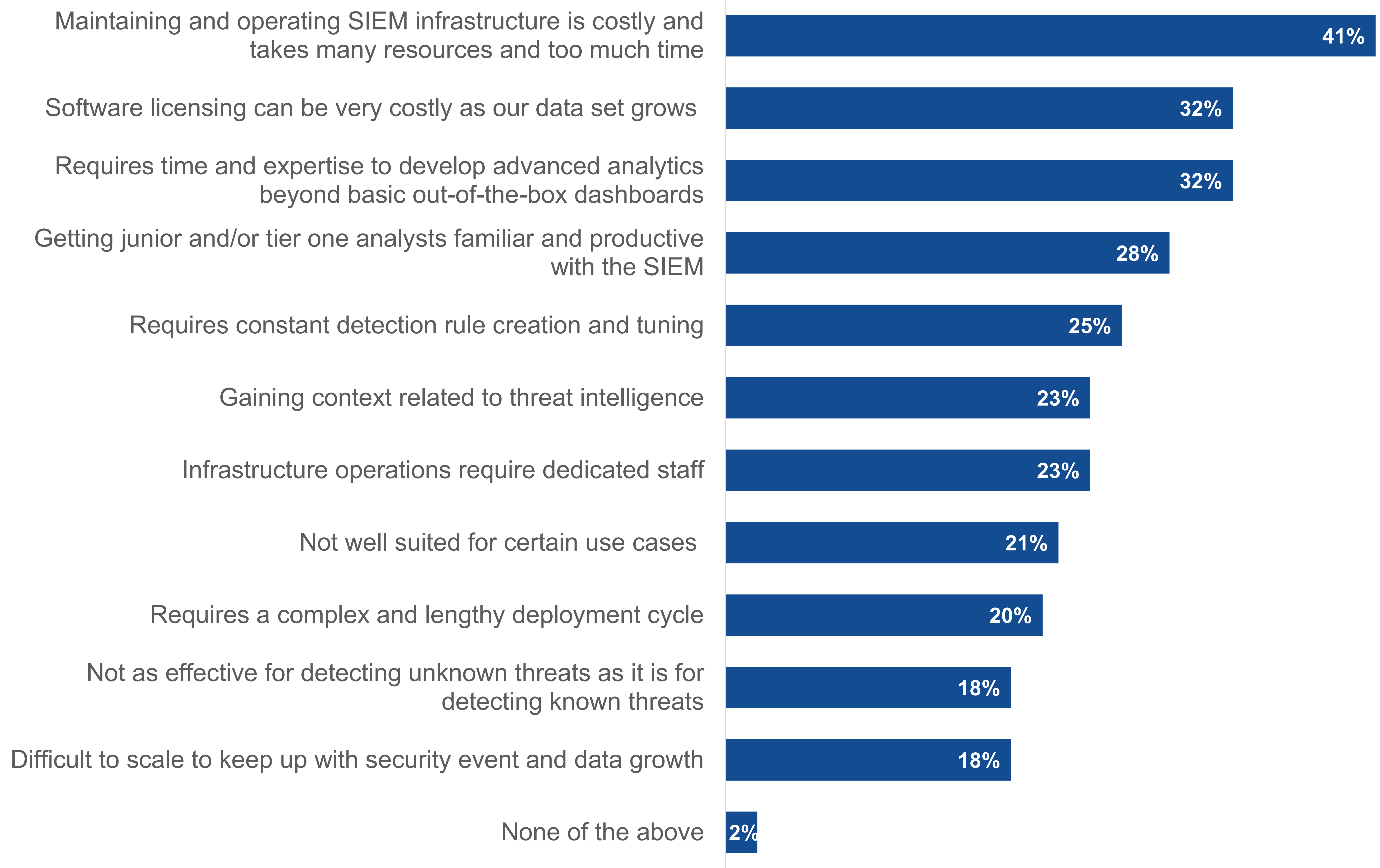


SIEM Challenges Persist

But SIEM challenges persist, explaining why many are exploring alternative options. These challenges remain consistent with the prior year's research, focusing on operating costs and the need for specialized talent.



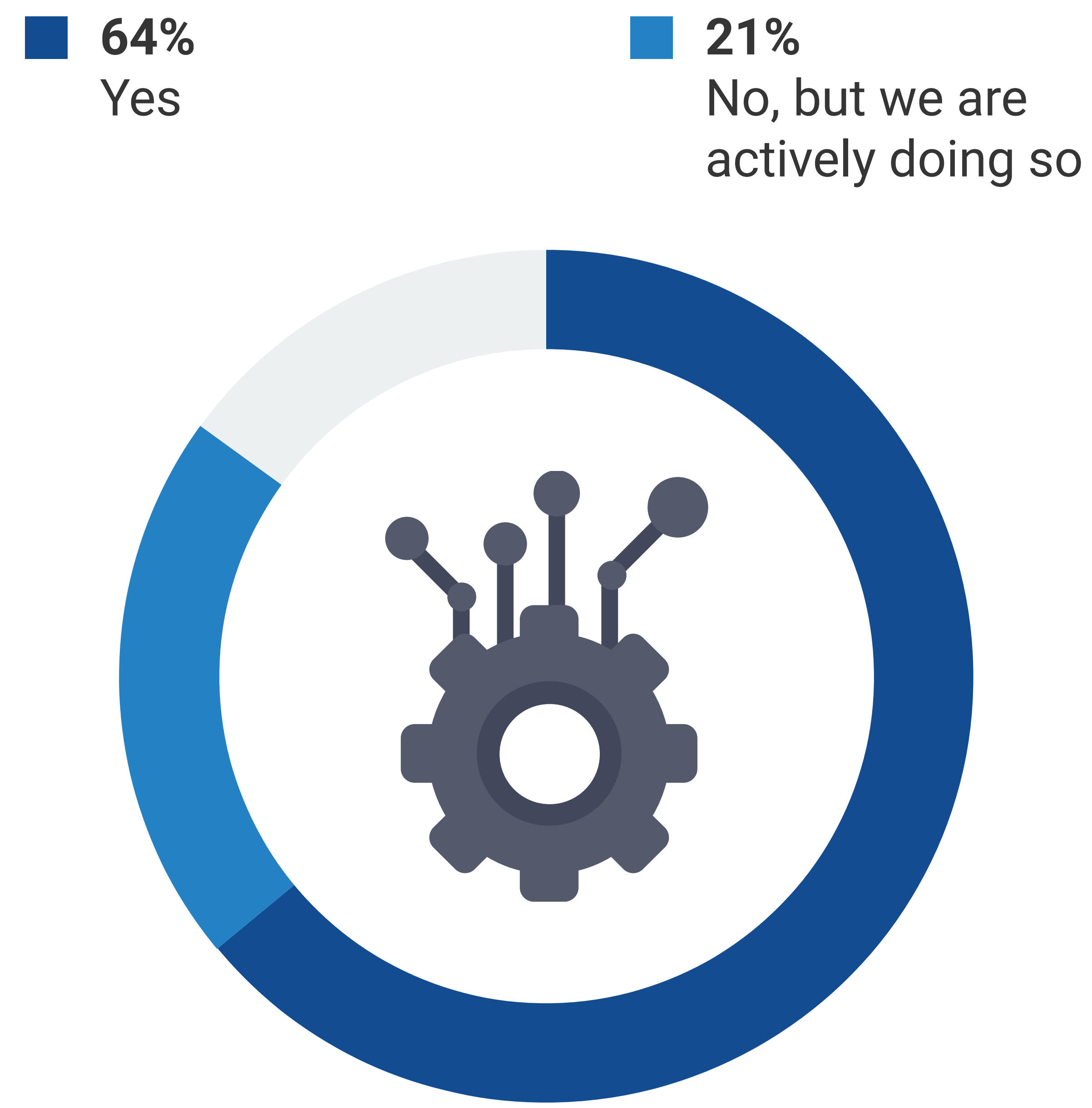
Most challenging attributes of a SIEM solution.



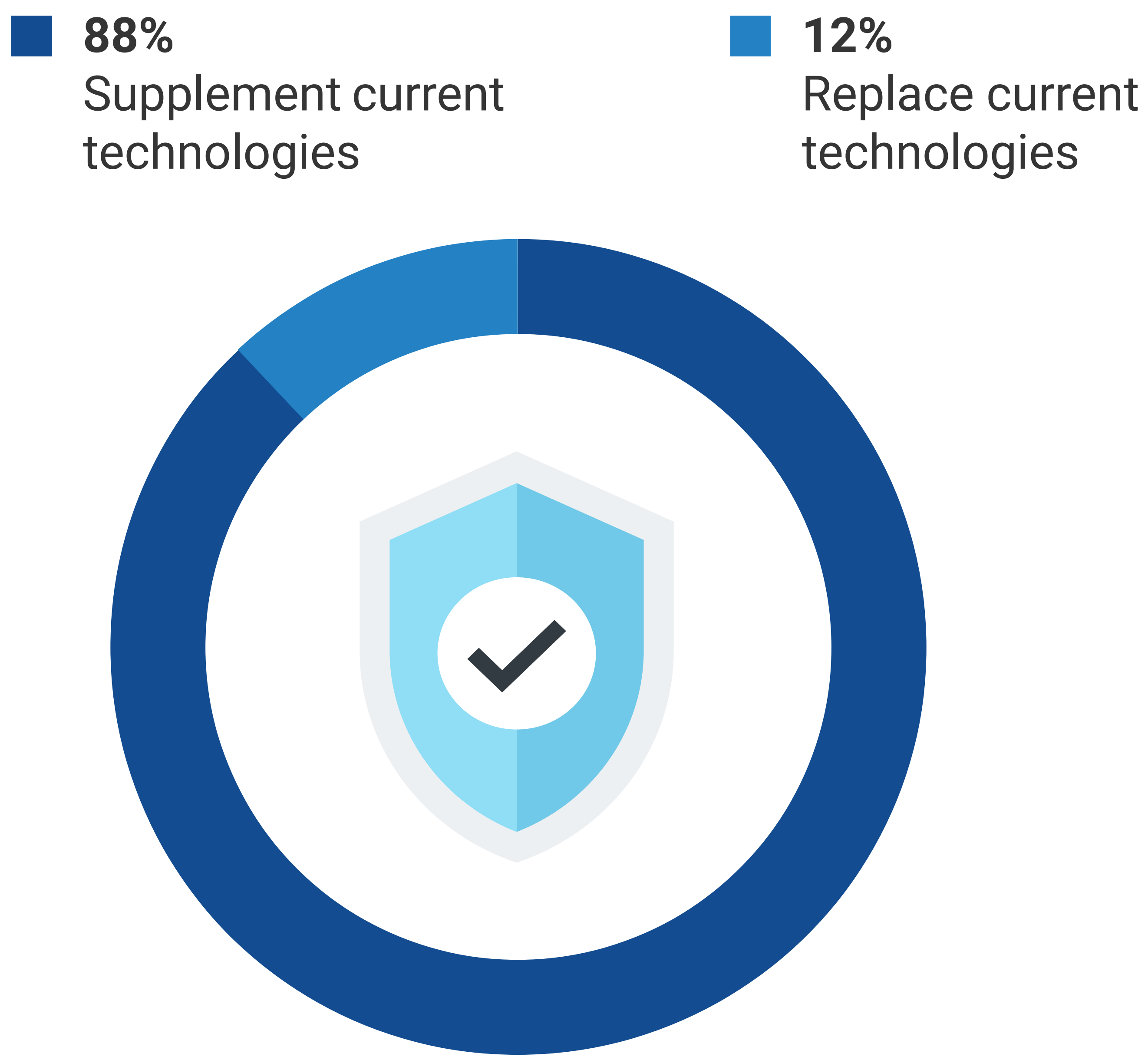
XDR Solutions Are Widely Deployed as a Supplement to Other Threat Detection and Response Tools

Despite the wide use of SIEM for threat detection and response, security teams want better advanced threat detection, integration, and response support, as well as solutions to plug gaps in cloud detection and response capabilities. This is clearly motivating the nearly two-thirds (64%) of organizations that have already deployed an XDR solution, as well as the 21% actively doing so. However, among these XDR first movers, nearly nine in ten expect XDR solutions to supplement SIEM and other SecOps tools. While once considered a possible panacea for SecOps, XDR has settled in as a supplement to other technology in the SecOps stack, including SIEM.

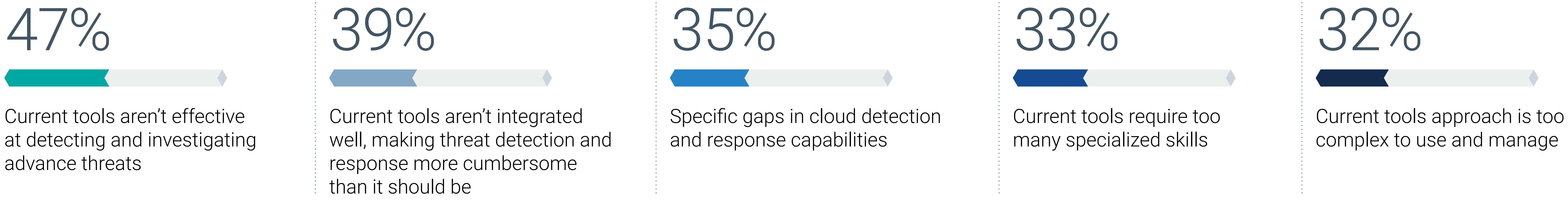
Have organizations deployed XDR solutions?



Effect of XDR on security operations environment.



Top five threat detection and response challenges driving usage of or interest in XDR solutions.

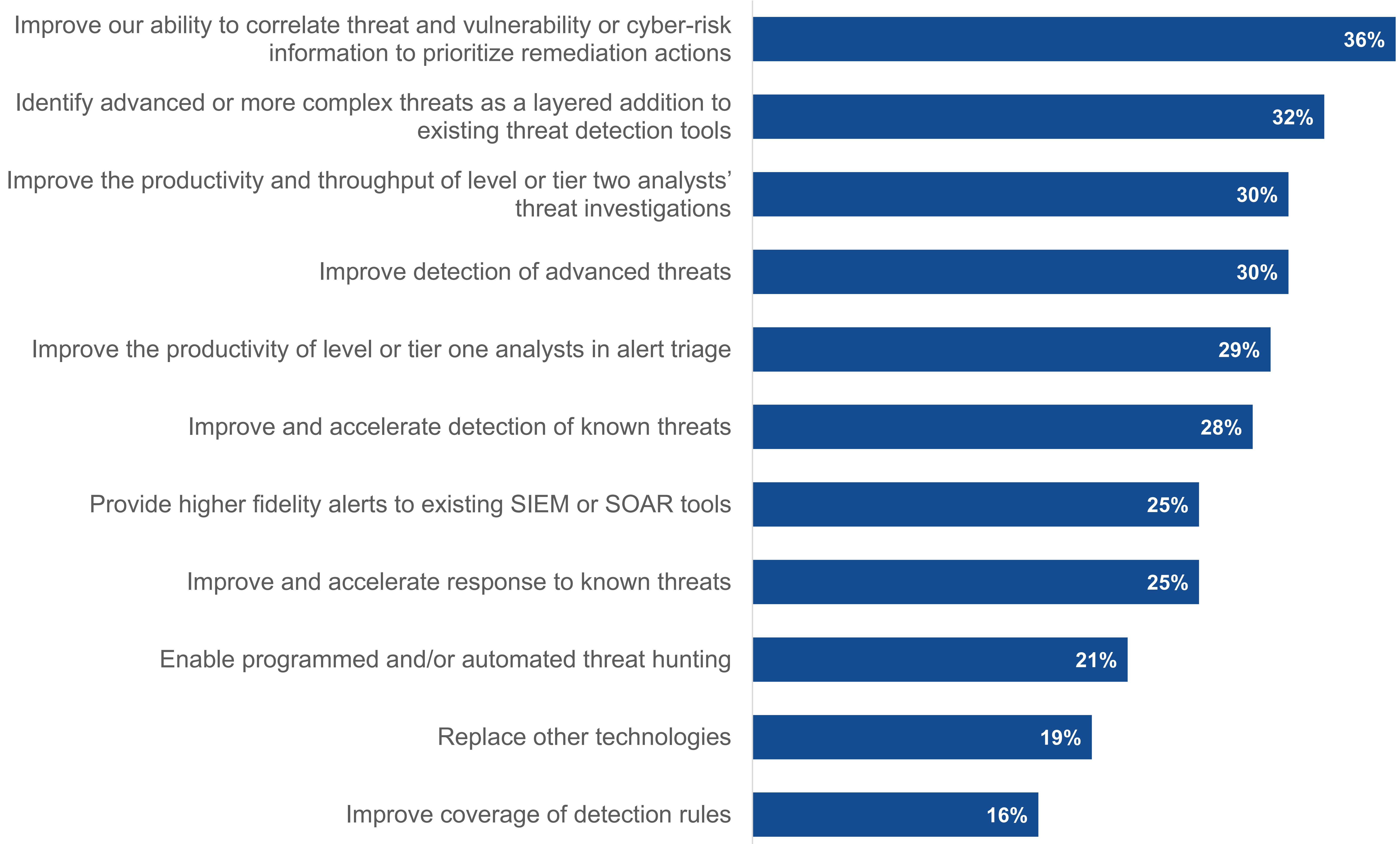


BACK TO CONTENTS

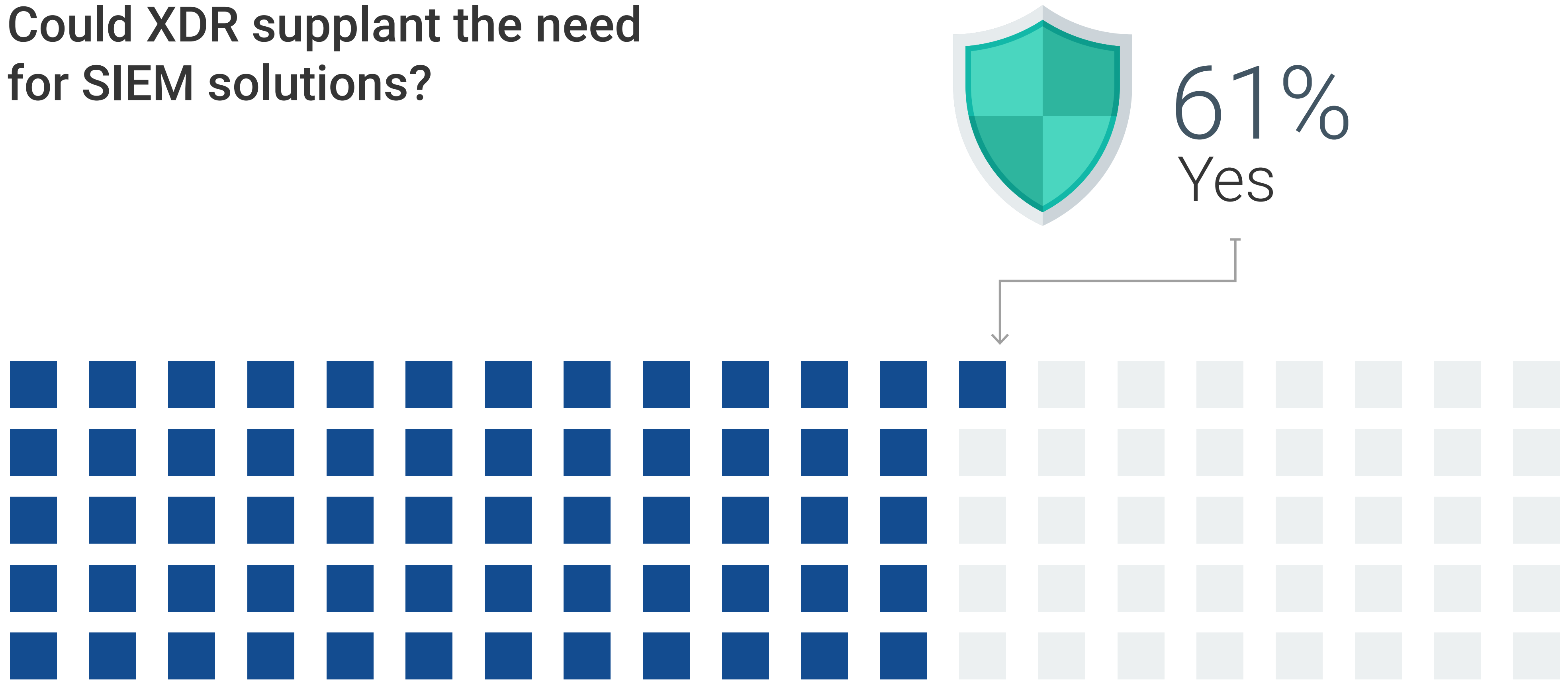
XDR Use Cases

And something new is expected from XDR solutions: the ability to correlate threat and vulnerability risk information to prioritize remediation. This new requirement reflects the inclusion of security posture management within SecOps, and the need for a better understanding about risk and posture management. This is especially noteworthy as it was not a factor in the earliest years of the general availability XDR.

Highest priorities when considering use cases for XDR.



Could XDR supplant the need for SIEM solutions?

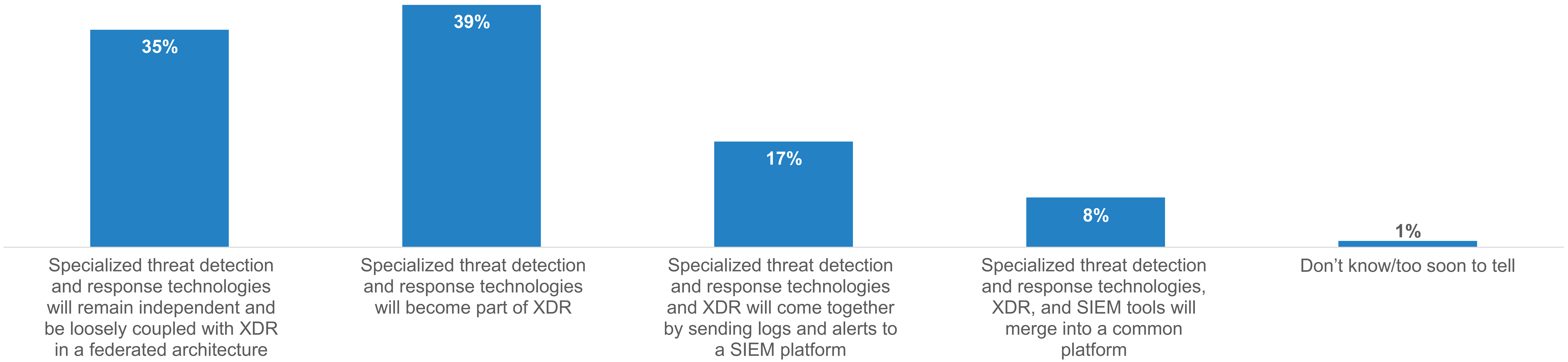


The Future of Threat Detection, Investigation, and Response (TDIR): Teams Will Still Need Specialized Detection and Response Solutions

While the jury is still out on where XDR fits into the future of TDIR, it seems clear that XDR is here to stay. However, what XDR will supplement is still unclear. Just more than one-third (35%) say specialized detection and response solutions will continue to be needed, 39% say specialized threat detection and response will become part of XDR, and another 25% say other threat detection and response solutions will merge into a common platform.

Despite all this, many (61%) still can see a time when XDR could replace their SIEM solution.

How specialized threat detection and response technologies will likely integrate over time.



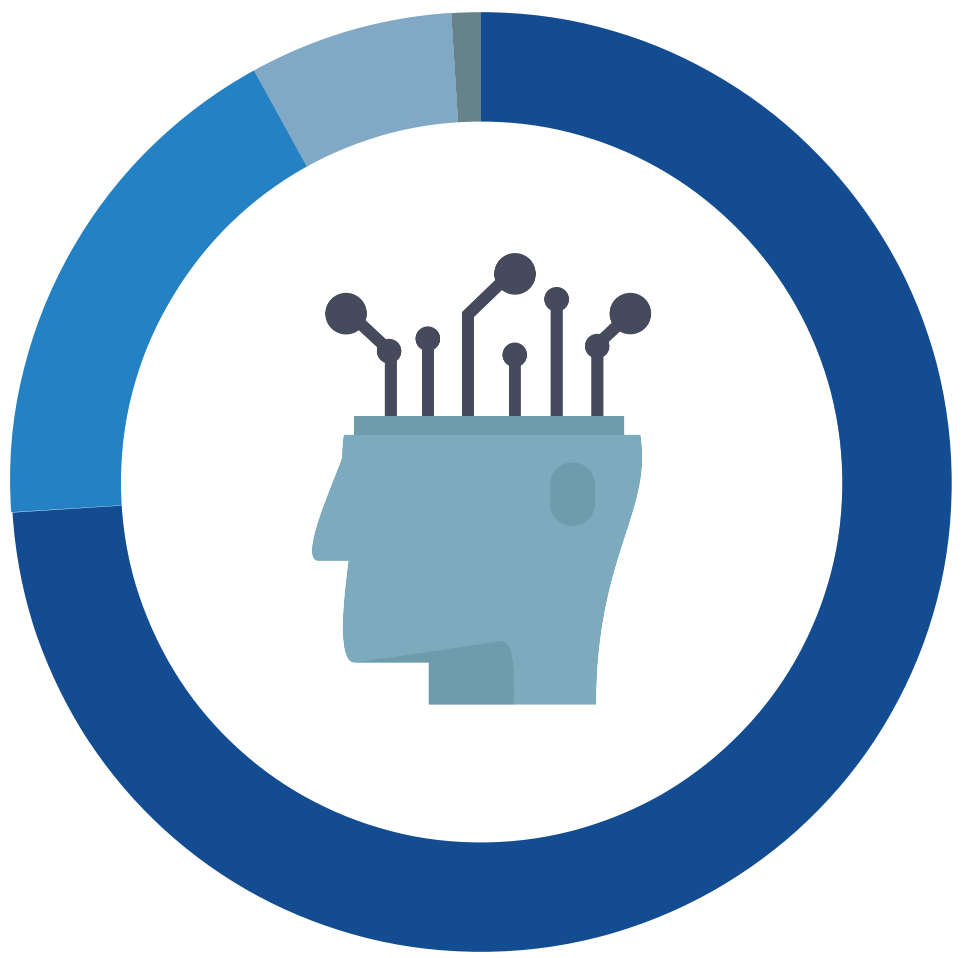
BACK TO CONTENTS

GenAI Use Cases for SecOps Are Limited at This Point but Poised for Significant Contribution

Generative AI (GenAI)-enabled Security Solution Usage

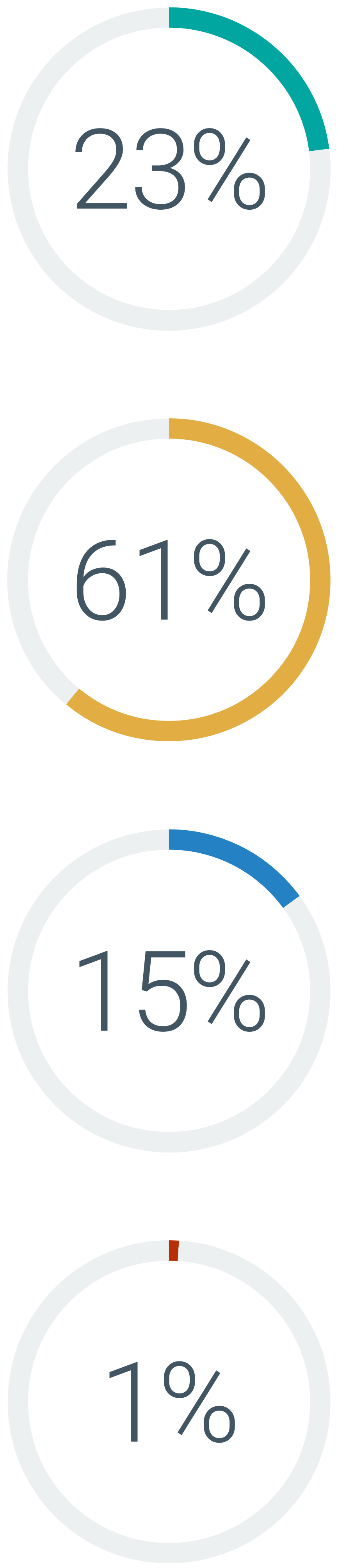
Security leaders continue to display cautious attitudes about how widely GenAI will seep into security use cases. Despite nearly three-quarters (74%) of organizations already using GenAI-enabled security solutions in their SOC, 61% of these early adopters believe that it will only support a few use cases over the next 12-18 months. This reflects ongoing caution in the speed of GenAI assimilation, especially when it comes to supporting security operations.

Are GenAI-enabled security solutions used to support SOCs?



- **74%** Yes, solutions already in daily use
- **18%** No, but currently implementing solutions
- **7%** No, but we are considering future use
- **1%** No

Will GenAI play a role within security operations over the next 12 to 18 months?



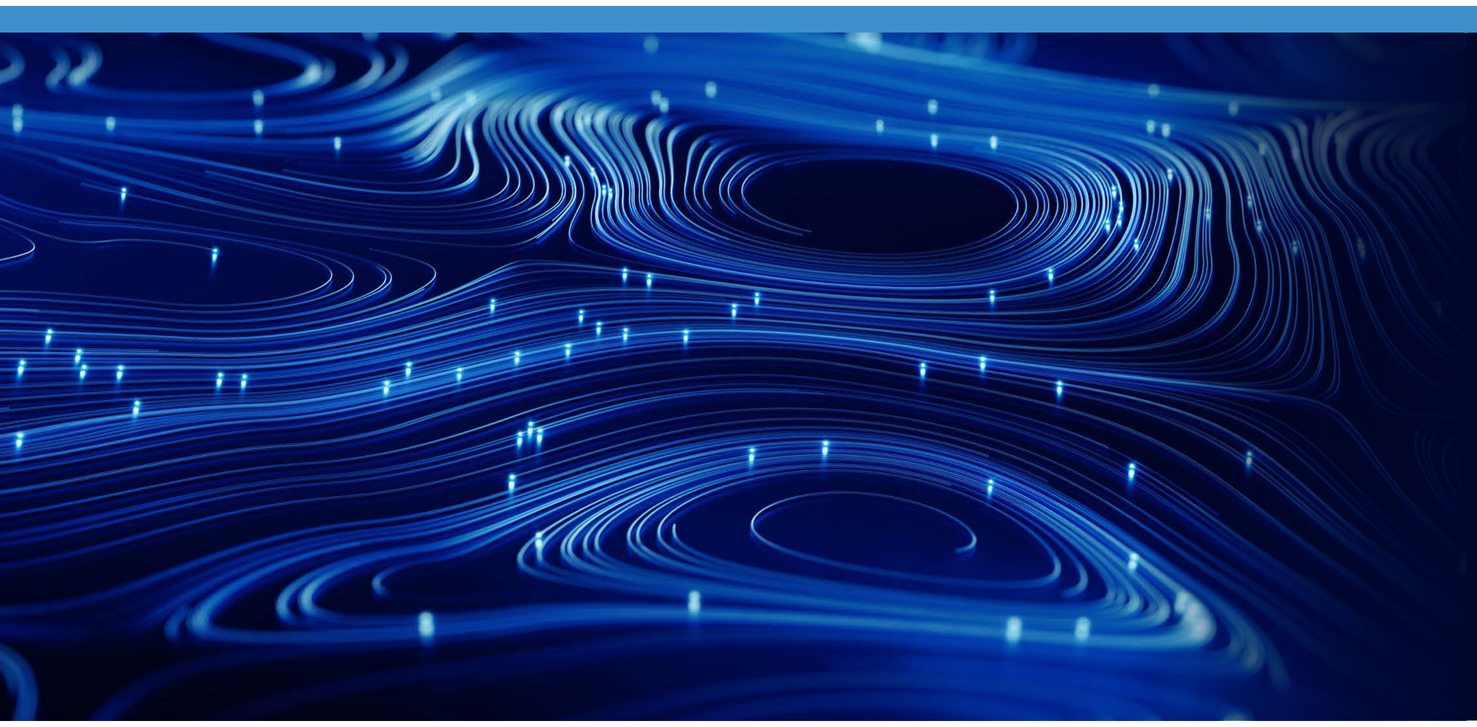
23% Yes, I believe generative AI will be used for many security operations use cases over the next 12 to 18 months

61% Yes, I believe generative AI will be used for a few security operations use cases over the next 12 to 18 months

15% No, my organization plans to test generative AI for security operations, but I don’t anticipate that it will become part of our security operations in that timeframe

1% No, my organization has no plans to adopt generative AI for security operations in that timeframe

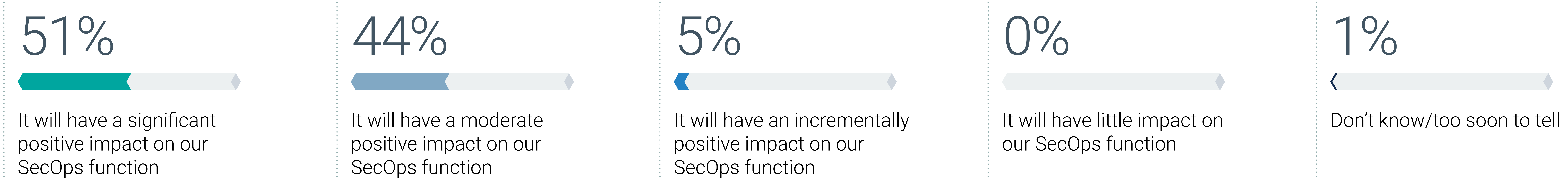
BACK TO CONTENTS



Half Think GenAI Will Have a Significant Positive Future Impact

What does the future hold for GenAI and SecOps? The vast majority of organizations believe GenAI will have a positive impact. But security professionals are cautious by nature, so maybe it shouldn't be a surprise that just slightly more than half (51%) think GenAI will have a significant positive future impact.

Anticipated outcome of adoption and utilization of GenAI within SecOps over the coming 24 months.



51% It will have a significant positive impact on our SecOps function

44% It will have a moderate positive impact on our SecOps function

5% It will have an incrementally positive impact on our SecOps function

0% It will have little impact on our SecOps function

1% Don't know/too soon to tell

BACK TO CONTENTS

CORTEX®

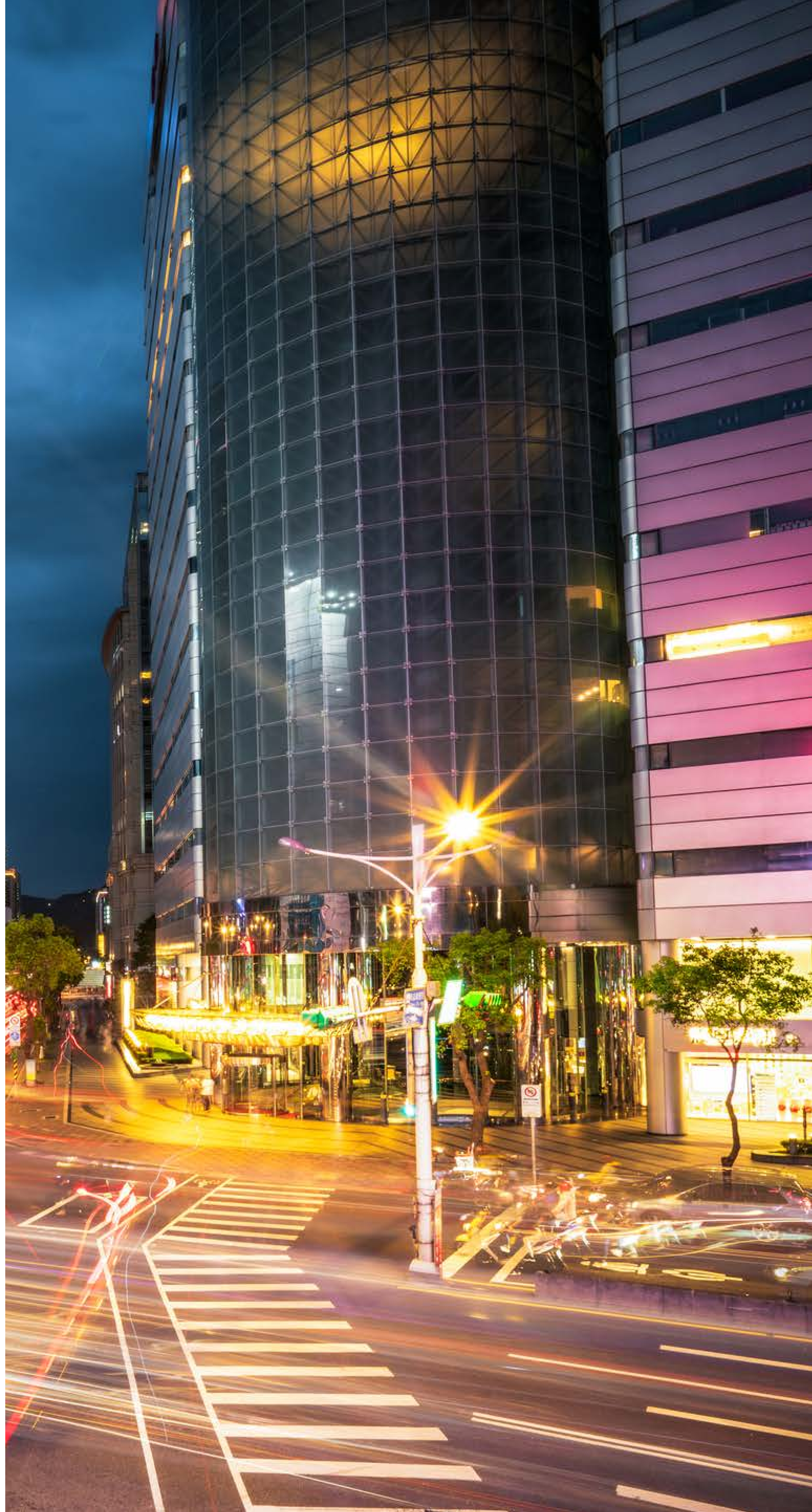
BY PALO ALTO NETWORKS

ABOUT

Cortex® by Palo Alto Networks has redefined solutions for security operations to help organizations deliver the modern security operation center (SOC) experience. Cortex delivers best-in-class threat detection, prevention, attack surface management, and security automation in an integrated platform powered by machine learning and Unit 42 threat intelligence. Trusted by companies around the world and recognized by leading analyst firms, Cortex XDR®, Cortex XSOAR®, Cortex Xpanse®, and Cortex XSIAM® provide proven protection as standalone solutions and also work seamlessly together as a force multiplier across the SOC.

EXPLORE CORTEX

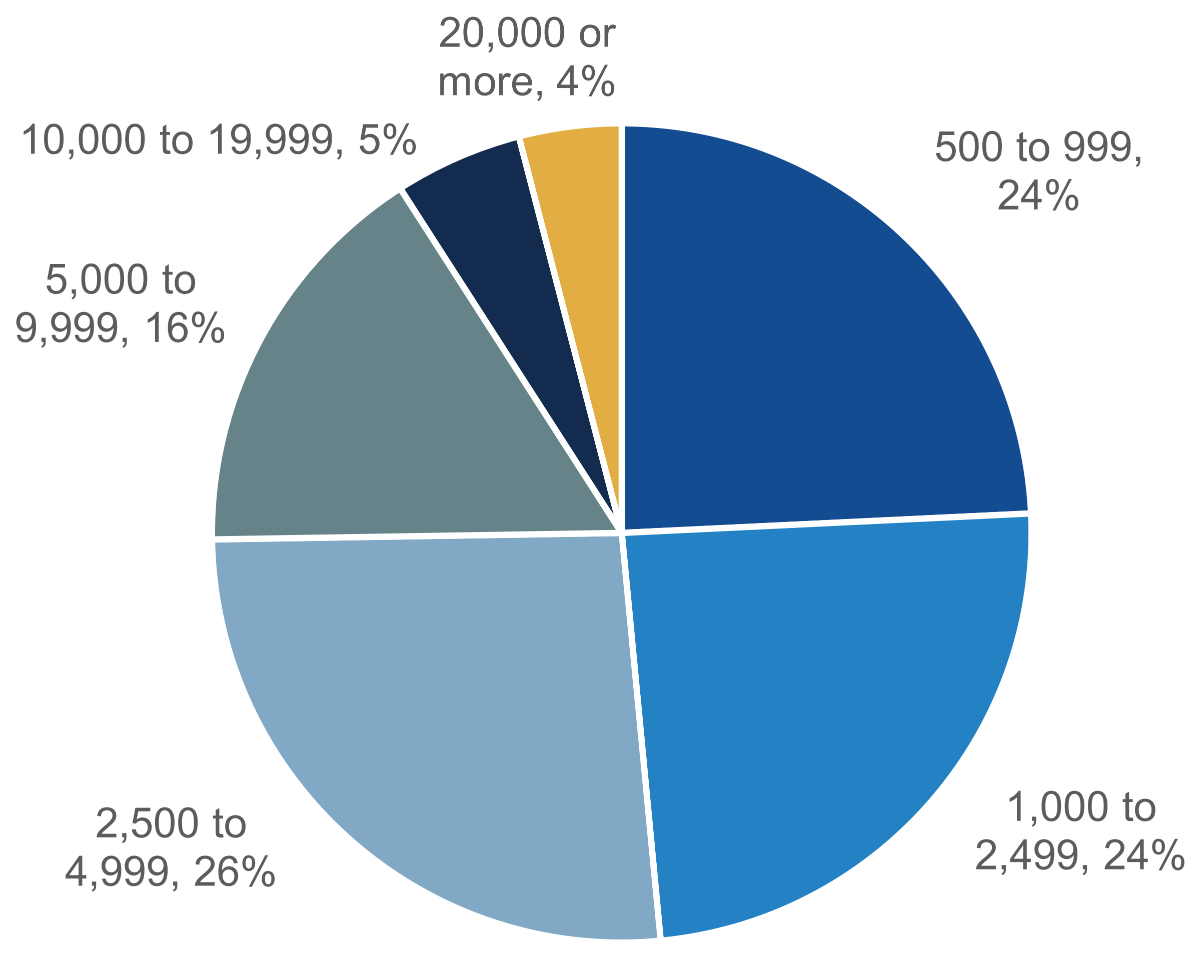
REQUEST A DEMO



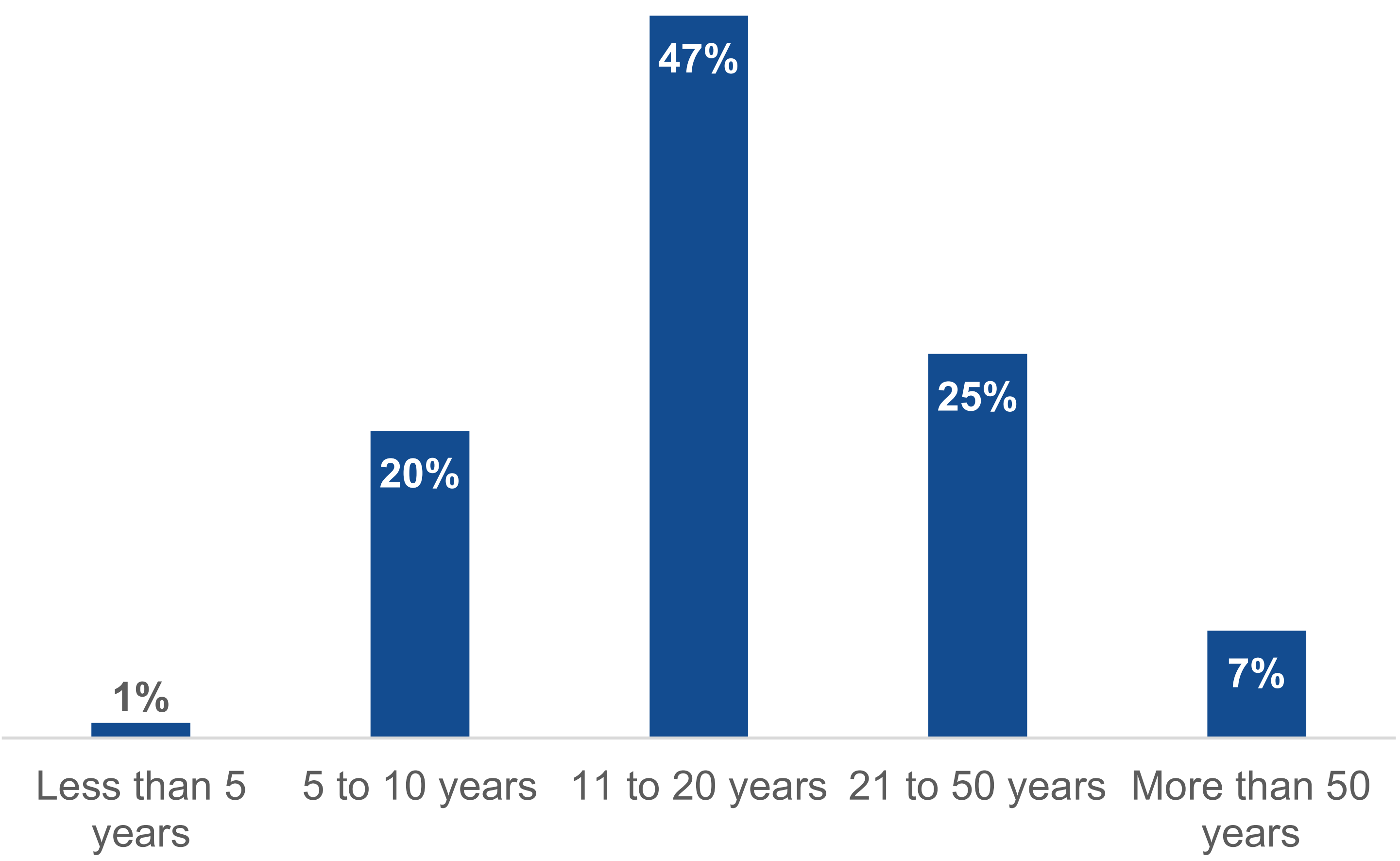
RESEARCH METHODOLOGY AND DEMOGRAPHICS

To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across the globe between November 7, 2024 and November 26, 2024. To qualify for this survey, respondents were required to be involved with security operations technology and processes at 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 366 IT and cybersecurity professionals.

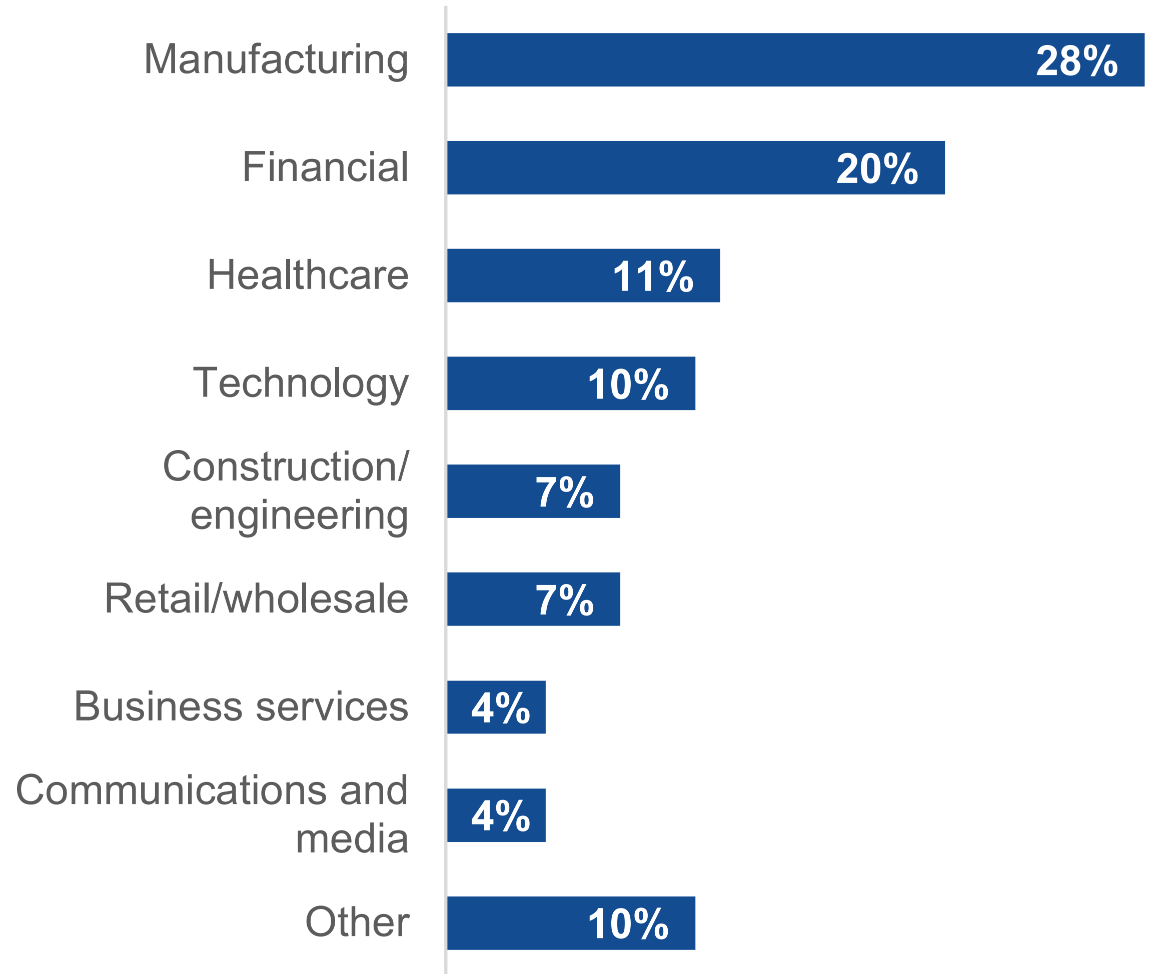
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



Enterprise Strategy Group™
by 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.