Enterprise Strategy Group™

# **The Evolution of Risk Reduction:** Contextual Analysis and Automated Remediation in Threat and Exposure Management

**Tyler Shields** | Principal Analyst

ENTERPRISE STRATEGY GROUP

JULY 2025

# Research Objectives

Threats, exposures, and assets are growing exponentially, leaving security operations and threat and exposure management capabilities behind. Technology to support continuous cybersecurity data collection, AI-driven analysis of complete cybersecurity context, and issue remediation via autonomous agents are all mandatory for security organizations that want to stay ahead of their growing risk profile.

Risk reduction is difficult, and homegrown technology solutions to this problem are becoming unmanageable. Security teams must move beyond continuously finding more issues that they don't have the capability to fix and instead focus on creating automated and scalable remediation systems. To continue to improve, teams must build automated security programs while breaking down the silos that exist between isolated tools and multiple security and technology owners.

To gain further insight into these trends, Enterprise Strategy Group surveyed 400 IT and cybersecurity decision-makers at organizations in North America (US and Canada) involved with or responsible for discovering and reducing threats and vulnerabilities in their organizations.

This study sought to:

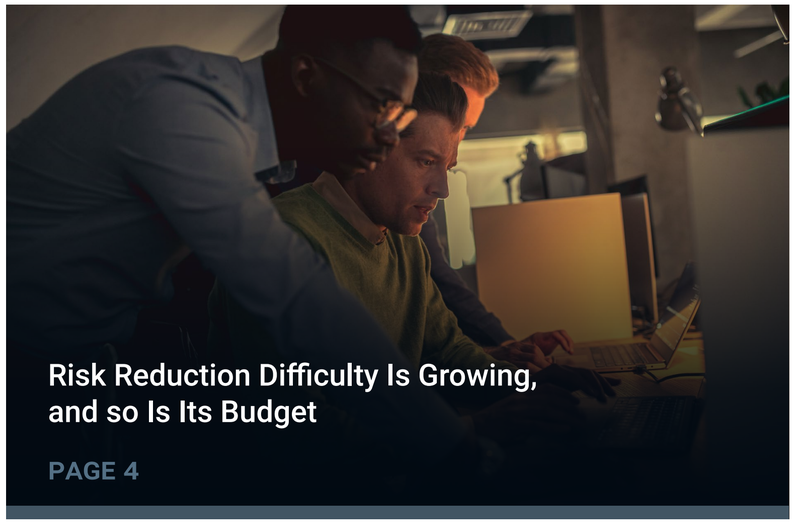
**Identify** the current state of threat and exposure management capabilities.

**Guide** vendors and practitioners to an improved state of risk reduction.

**Determine** the market demand for specific capabilities and features.

**Understand** ways of breaking down the silos between IT and security to rapidly reduce risk.

# **Key** Findings



## Risk Reduction Difficulty Is Growing, and so Is Its Budget

PAGE 4

## DIY Threat and Exposure Management Poses Risks

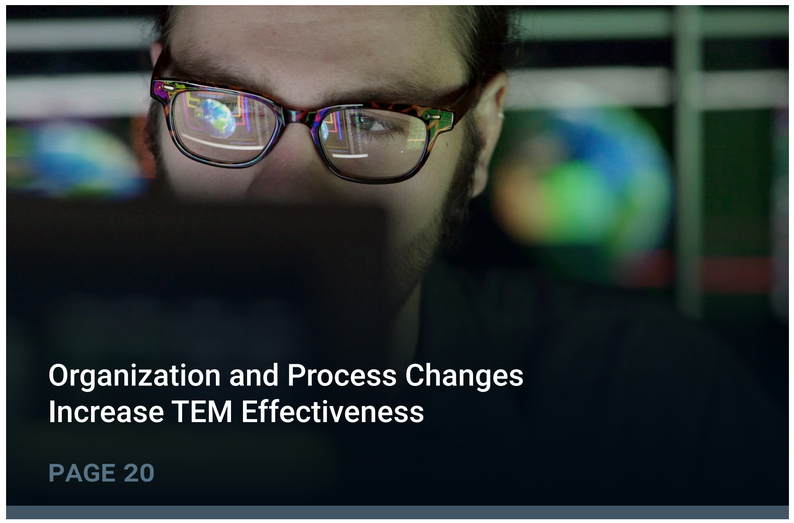
PAGE 9

## Modern Threat and Exposure Management Moves Beyond Simply ‘Showing Issues’

PAGE 12

## Risk Reduction Requires Automated Remediation and Agentic AI

PAGE 17



## Organization and Process Changes Increase TEM Effectiveness

PAGE 20



BACK TO CONTENTS

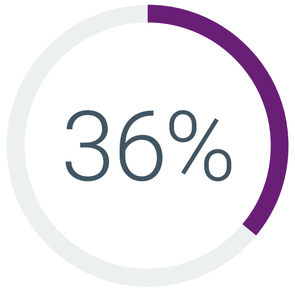
# Risk Reduction Difficulty Is Growing, and so Is Its Budget

# Reducing Risk Isn’t Getting Any Easier

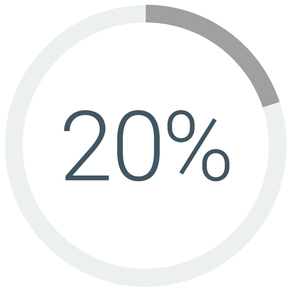
Risk reduction in the cloud infrastructure and application era is more difficult than ever before. Security operations are increasing in difficulty, and traditional vulnerability management offerings are incapable of keeping up with the pace of change. Indeed, nearly three-quarters (71%) of those surveyed say that the process of reducing risk and exposures has not improved or has actually become more difficult over the past two years. Increased cloud adoption and piles of cyberthreat data are making exposure management more challenging. Security operations teams are buried in alerts, with limited resources and outdated processes available to them. Security organizations need change now to reduce security debt and improve their risk posture.

**Change in difficulty level of reducing risk and exposures.**


Risk reduction is
significantly more difficult
today than it was two years ago




Risk reduction is
slightly more difficult
today than it was two years ago




Risk reduction is
about as difficult
today as it was two years ago


Risk reduction is
slightly less difficult
today than it was two years ago


Risk reduction is
significantly less difficult
today than it was two years ago



BACK TO CONTENTS

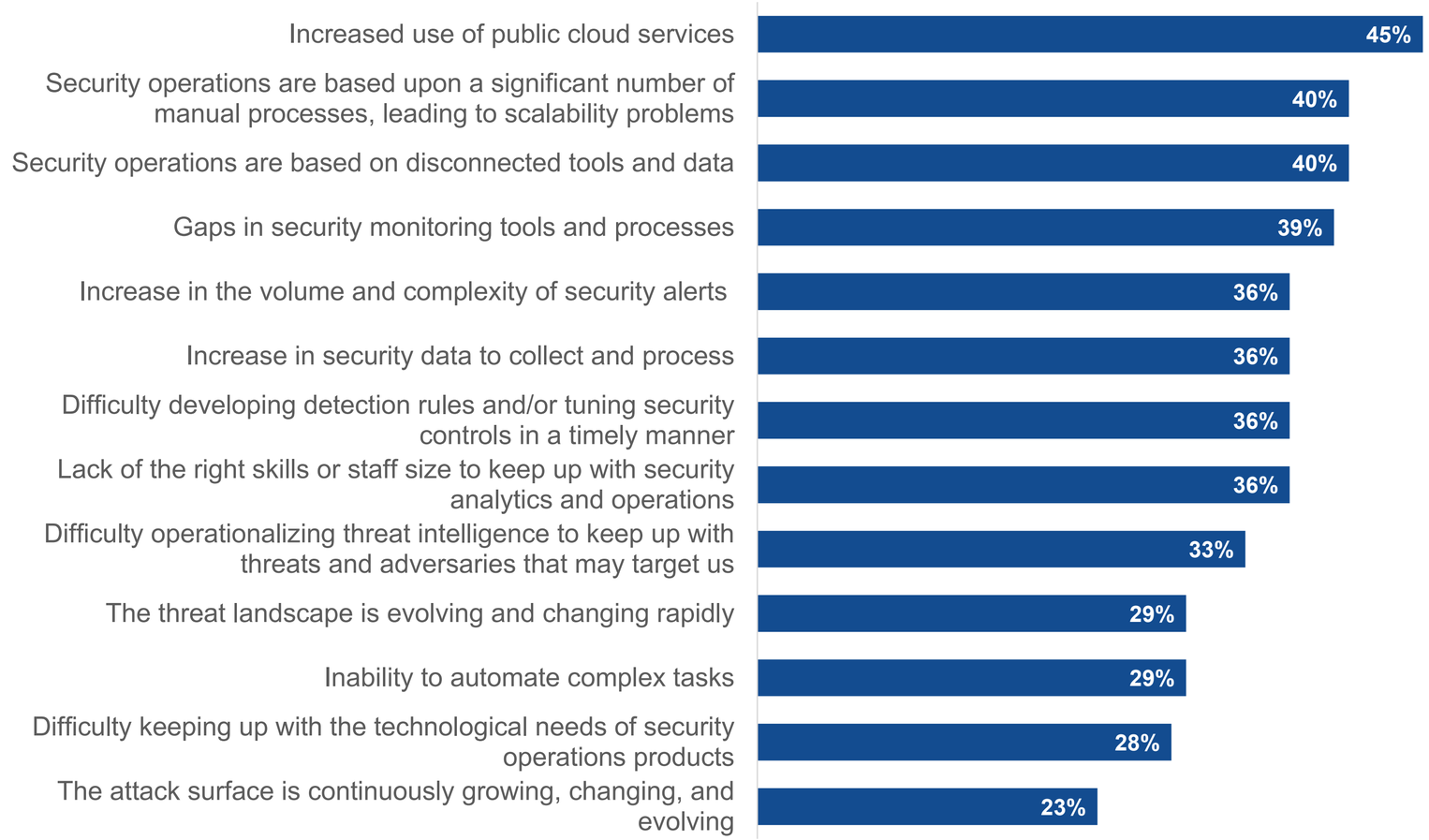
# Cloud Usage, Cybersecurity Data Growth, and Tool Gaps Fuel Risk Reduction Difficulty

Modern cloud-native infrastructure and applications are a primary driver of complexity in threat and exposure management. Public cloud platforms can cause issues with security team processes as the cloud asset landscape continues to grow. Cloud application and infrastructure components are ephemeral, making them more complex to secure.

Inadequate, disconnected, or nonexistent tools and data are common causes of difficulty in risk reduction. Current risk reduction processes rely upon siloed technologies that each have their own bespoke contextual data set. These silos make it complex for security analysis to occur at a holistic and contextual level.

The quantity and complexity of security data and alerts are causing fatigue and overload. Security teams are tired of manually fixing numerous vulnerabilities, many of which are false positives, when automation and AI should be helping to scale.

**Primary reasons reducing risk is more difficult than it was two years ago.**



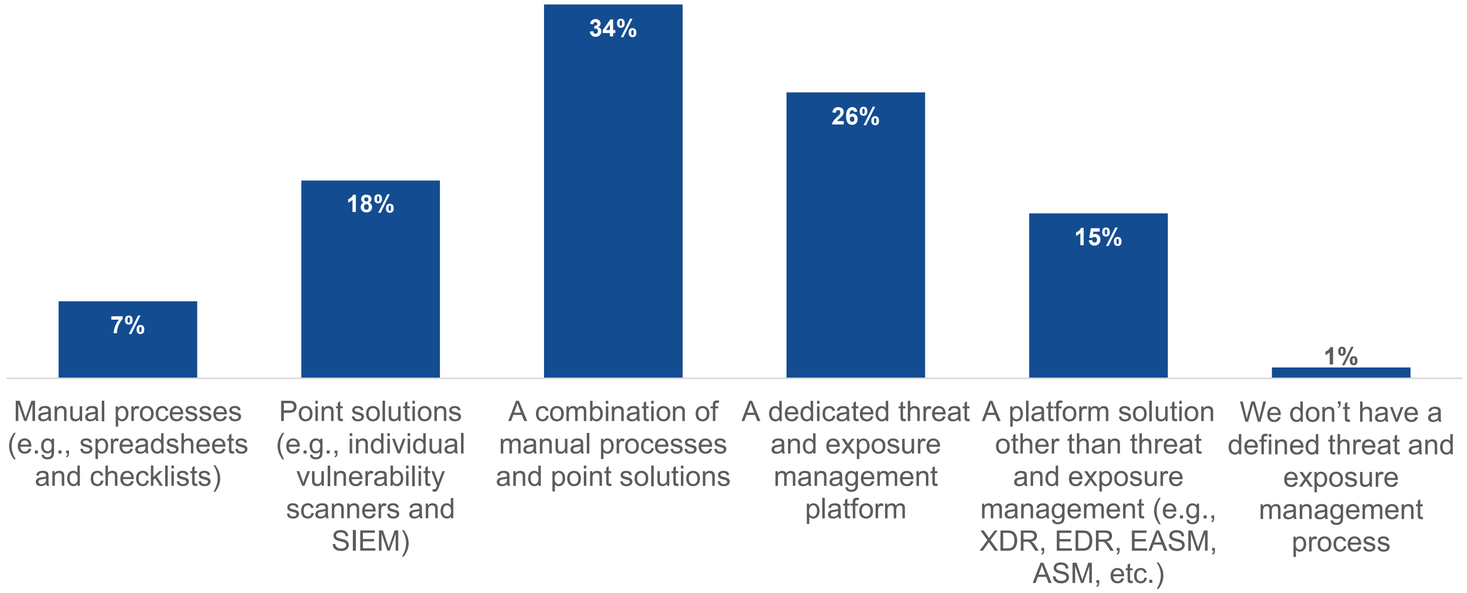



BACK TO CONTENTS

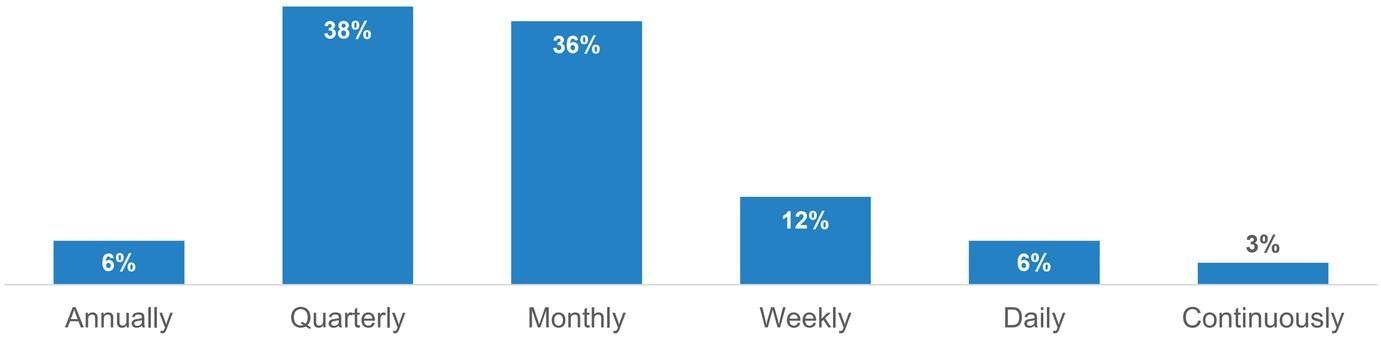
# Threat and Exposure Management Remains Manual and Infrequent

Threat and exposure management processes cannot keep up with the constant pace of change in today's cloud-driven environment. Manual threat and exposure processes remain the most common approach to risk reduction today, with 34% of respondents using a combination of manual and point solutions. Inefficiencies resulting from the use of multiple point tools and manual processes make scaling security operations arduous. Yet the majority of those surveyed have not progressed toward technology unification, with only 26% stating that they use a dedicated threat and exposure management platform. As long as manual processes and tool sprawl persist, threat and exposure management will remain an uphill battle.

**How organizations primarily identify and assess threats and exposures.**




**Frequency with which organizations assess environment for security vulnerabilities, threats, and exposures.**




Along similar lines, audit-based cybersecurity results in point-in-time assessments that are almost always immediately outdated. Risk reduction processes cannot rely on one-off snapshots of risk with a long time to remediation for security exposures. Attackers are moving faster than ever as they leverage AI and automation, continually decreasing the time before an exposure becomes weaponized. Today, 80% of organizations conduct a threat and exposure assessment analysis no more frequently than once per month. Today's threats move significantly faster than once a month, leaving exposure gaps and increasing time to discovery for vulnerabilities. Security teams must focus on decreasing the time that risk exists in their environments by moving toward a programmatic model in which security data collection, analysis, and automated remediation happen continuously.

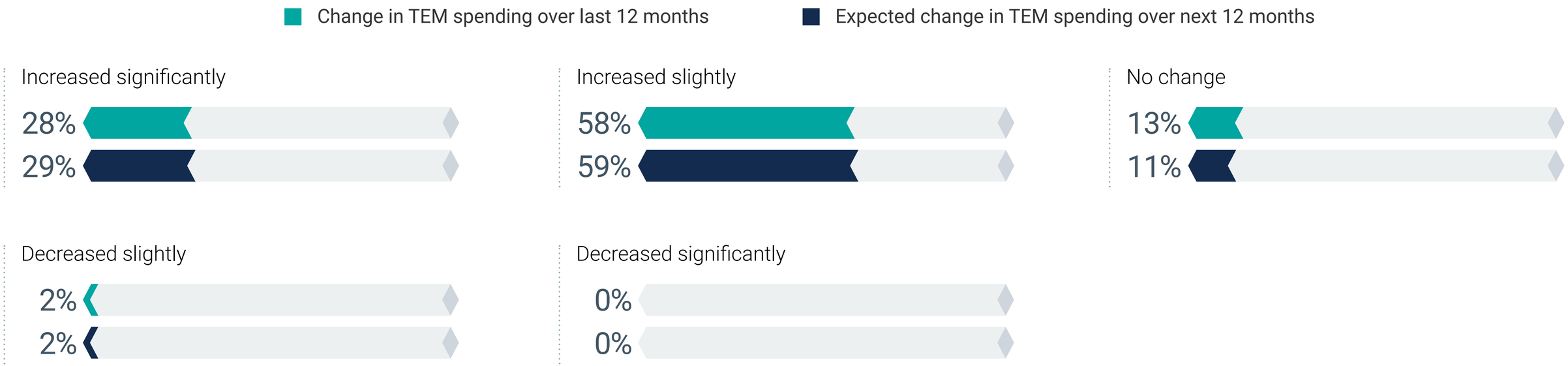


BACK TO CONTENTS

# Threat and Exposure Budgets Are Growing, Which Is Expected to Continue

However, there is a silver lining in the story of increasing risk and cybersecurity's inability to scale. Organizations have begun to recognize the value of a more complete and automated threat and exposure management (TEM) program and are growing their budget to match. Vendors are also embracing a new approach to risk reduction by taking a more holistic and contextual view of the data they collect and the value propositions that they offer to their customers. With 88% of those surveyed stating that their budgets are increasing year over year, there is a positive outlook for potential improvement over time.

**Change in spending for threat and exposure management technology.**






BACK TO CONTENTS

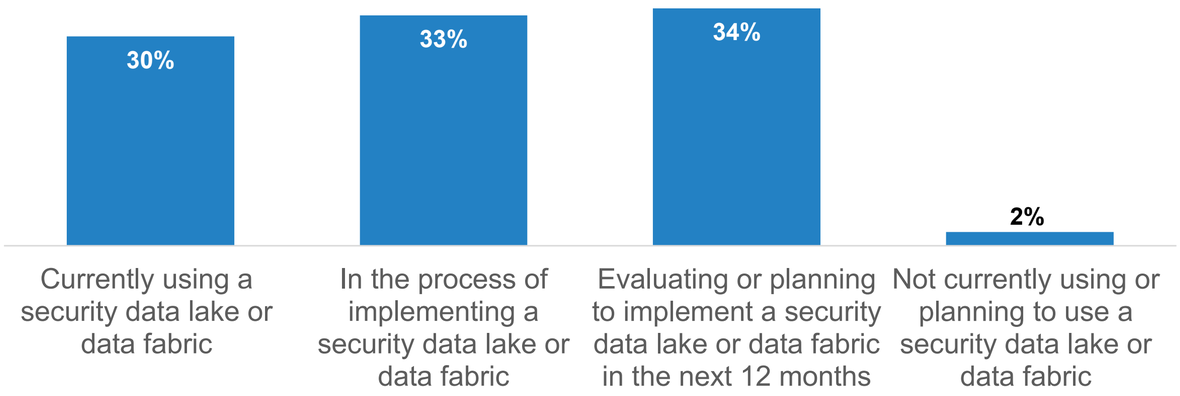

# DIY Threat and Exposure Management Poses Risks

# Security Teams Look to Deploy DIY Solutions First

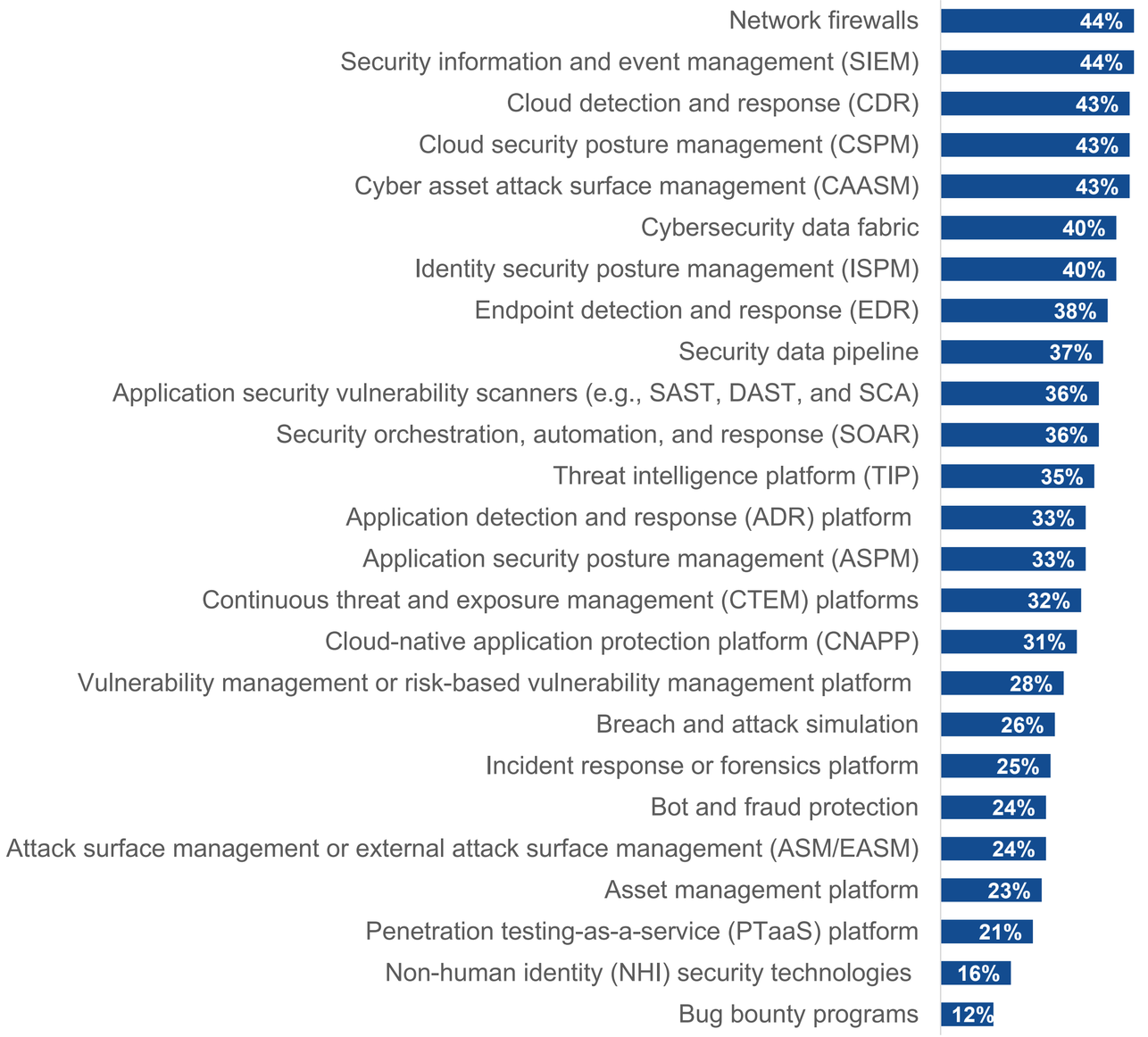
Current generation threat and exposure management platforms are built upon a broad cybersecurity and asset data consumption and analysis approach. A security data fabric is required to store, deduplicate, and analyze large quantities of threat, asset, and exposure data.

As threat and exposure management platforms have been slow to innovate from the ashes of traditional vulnerability management, security organizations have been attempting to solve their problems with do-it-yourself (DIY) risk reduction systems. Survey data shows that only 2% of security teams are not currently using or planning to use a security data fabric or lake. With both “cybersecurity data fabric” and “security data pipeline” being among the top third of deployed technologies, it’s clear that organizations today are looking to manage the deluge of cybersecurity data required to make informed security operations decisions and are willing to build something themselves if they must.

**Current usage status of a security data lake or data fabric.**




**Security tools and technologies organizations currently use.**



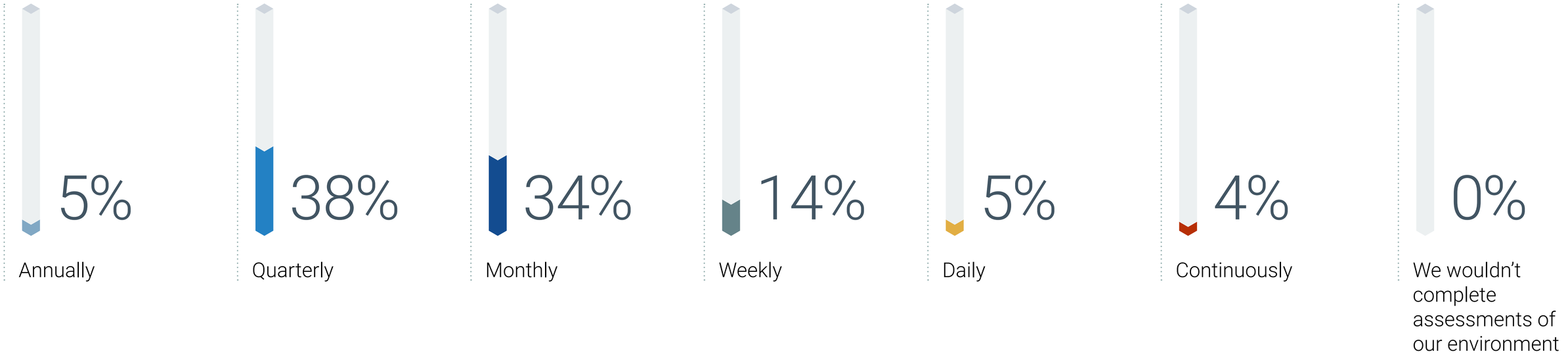



BACK TO CONTENTS

# TEM Platform Expectations for Analysis Cadence Are Low

Cybersecurity cannot operate as a point-in-time inspection model. Instead, it must be continuous and complete in its analysis approach. Security teams aim to enhance security operations metrics, such as mean time to resolution (MTTR) and mean time to detection (MTTD); however, they are still relying on the outdated approach of periodic risk assessments. Respondents indicate that security teams anticipate minimal improvement in threat and exposure management processes with the deployment of a platform. Indeed, current assessment frequency expectations for platforms are low, leaving ample opportunity to educate and empower the security team with significant value, including improvement in security metrics.

**Expected frequency with which organizations analyze their environment for security vulnerabilities, threats, and exposures with TEM platform.**





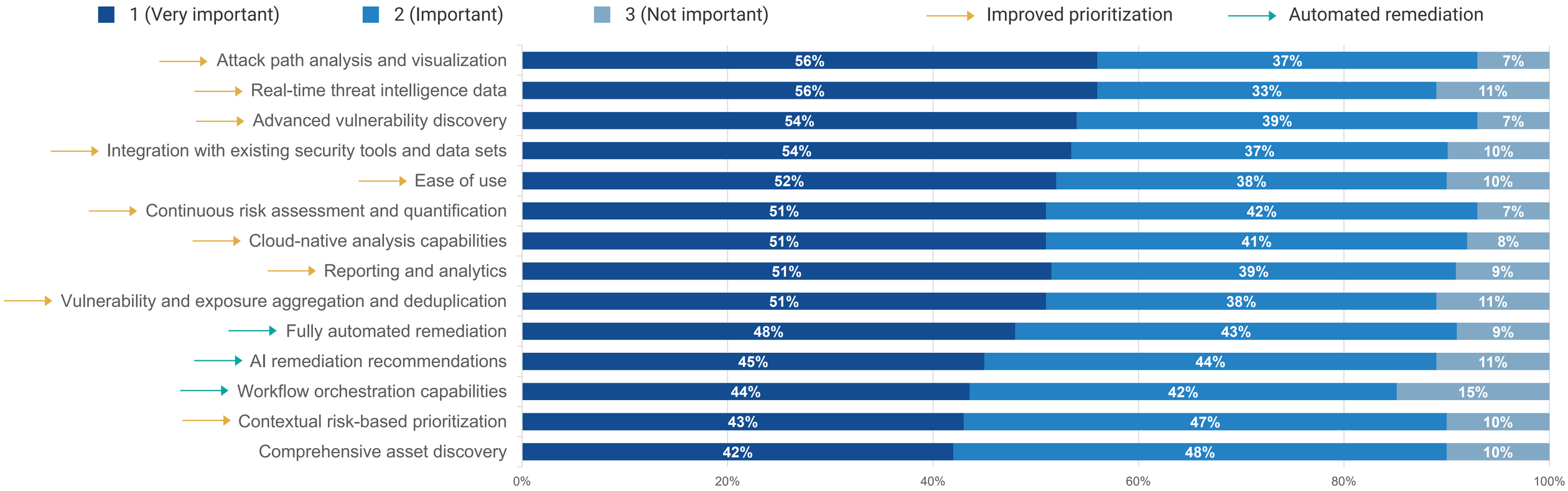

BACK TO CONTENTS

# Modern Threat and Exposure Management Moves Beyond Simply ‘Showing Issues’

# Threat and Exposure Features Must Go Beyond ‘Showing Issues’

Cybersecurity teams want risk reduction, not just to find more vulnerabilities. Organizations are already burdened with issues that require repair; they aren’t interested in uncovering more exposures to add to the pile of problems that their current processes can’t handle. They are seeking threat and exposure management tools that enhance their prioritization and risk reduction capabilities through automated remediation and deeper analysis. What matters most to security teams is fixing the most important issues first and doing it as quickly as possible at scale.

**Prioritizing features and capabilities of continuous threat and exposure management solutions.**



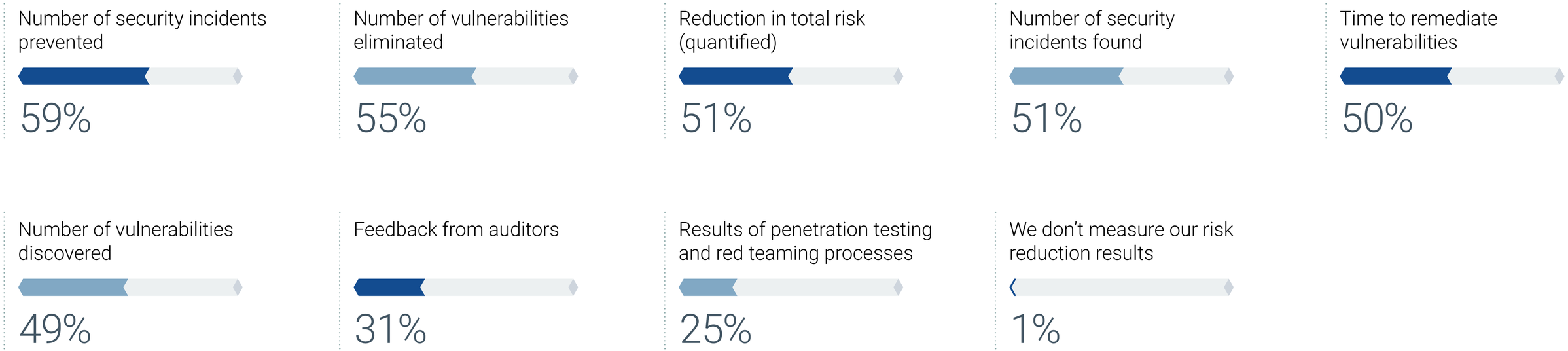



BACK TO CONTENTS

# Eliminating Security Exposures Is the Top Requirement

The most commonly cited metrics organizations use to assess the effectiveness of their threat and exposure management and risk reduction processes are focused upon risk reduction, while metrics that focus on vulnerability discovery and enumeration are further down in priority. Risk and exposure reductions remain the most important metrics of success. Discovery of issues is less important than remediation.

**How organizations assess the effectiveness of threat and exposure management and risk reduction processes.**



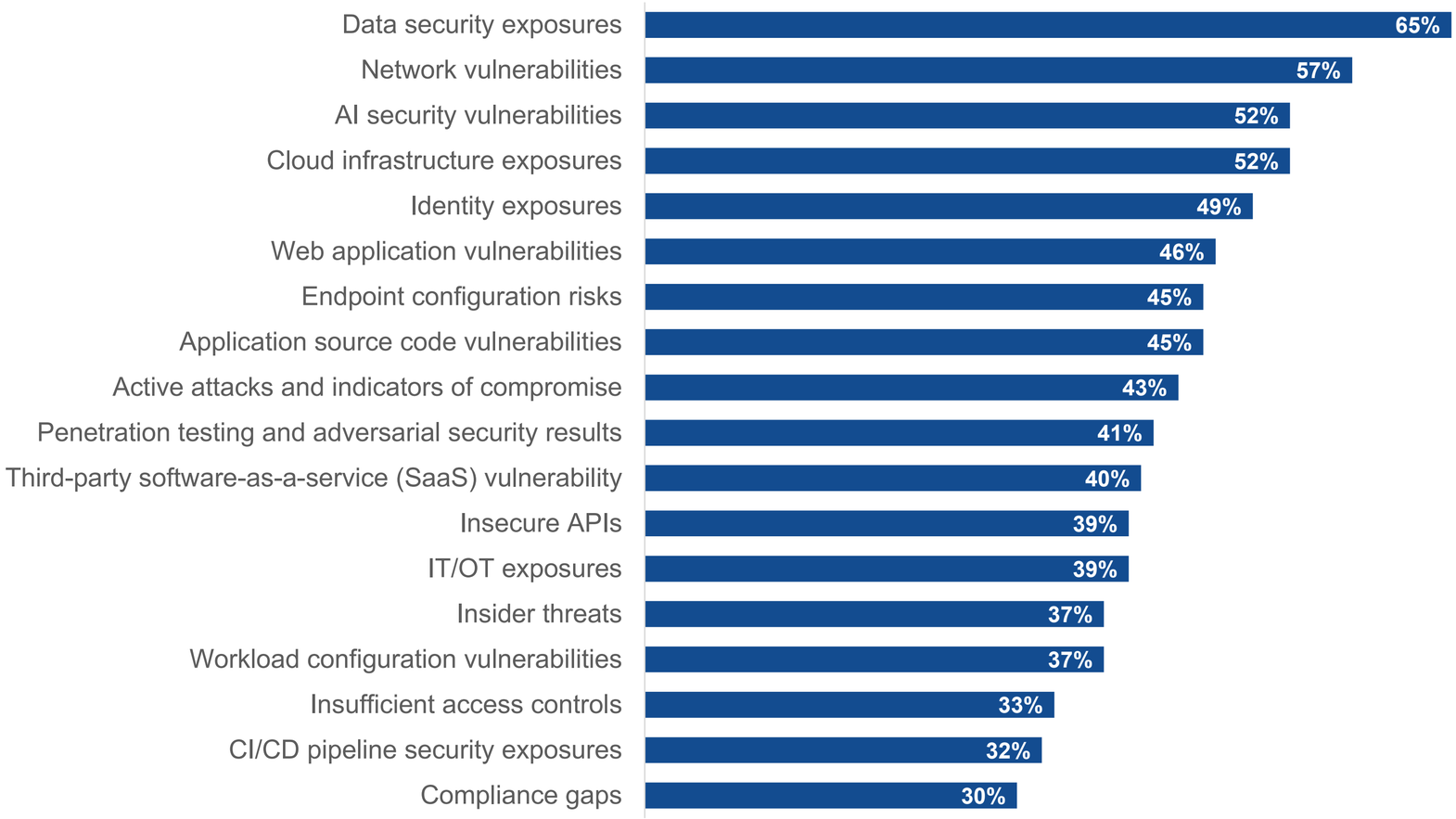



BACK TO CONTENTS

# Continuous Threat and Exposure Management Platforms Must Offer Detection, Reduction, and Response

Traditional risk reduction platforms have focused on enumerating and prioritizing vulnerabilities with limited context regarding the broader technology ecosystem of the organization. Today, security teams are demanding improvements in prioritization and processes that require a complete contextual understanding of exposure, threats, risks, and all mitigating factors. Organizations are seeking a threat and exposure management platform that offers comprehensive coverage of various exposure and threat classes, including those not supported by legacy vulnerability management technologies. Identity, application, infrastructure, cloud, web application, and endpoint exposures must all be tracked, prioritized, and remediated. The most advanced threat and exposure management platforms are even extending beyond vulnerabilities and exposures to contribute to threat intelligence, incident response, and post-incident cleanup efforts. In the eyes of buyers, exposure reduction is often intermingled with detection and response, creating an opportunity for innovative vendors to redefine the traditional market understanding of threat and exposure management.

**Types of vulnerabilities, exposures, and risks organizations expect a continuous threat and exposure management platform to discover, prioritize, and/or help remediate.**





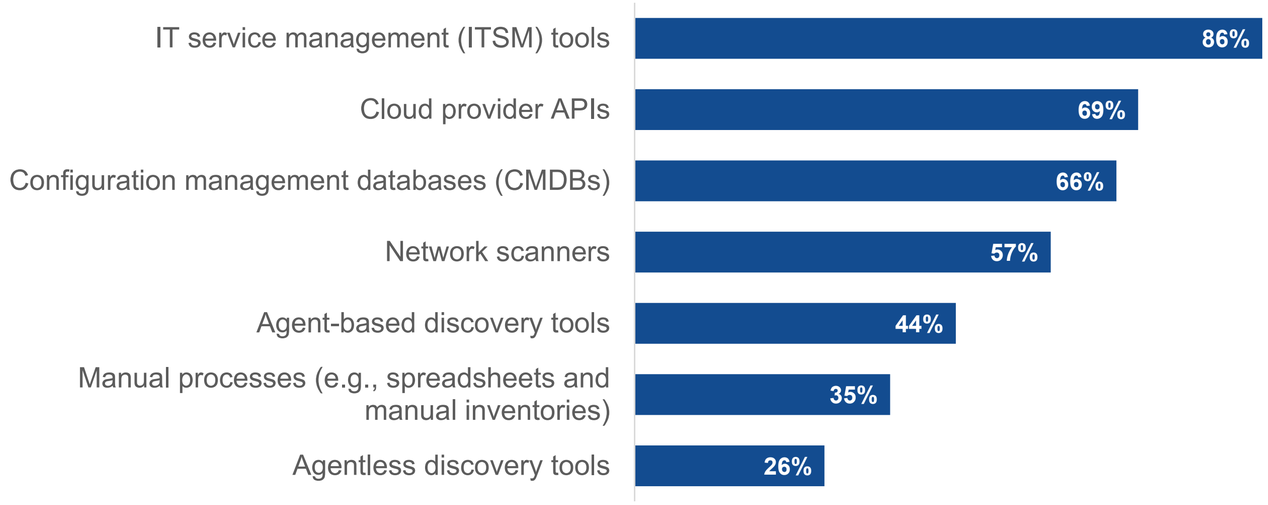

BACK TO CONTENTS

# Asset Discovery Remains an IT Process While Security Teams Are Deprioritizing Valuable Contextual Data

The foundation of a modern threat and exposure management platform is contextual knowledge about all assets present in the environment. However, asset discovery remains the responsibility of the IT team. Today, ITSM tools, along with cloud provider APIs, represent the most common methodology for asset data collection. Cybersecurity tools, network scanners, and both agent and agentless discovery solutions are frequently used as well, but the system of record for asset knowledge is generally maintained within CMDB or ITSM systems.

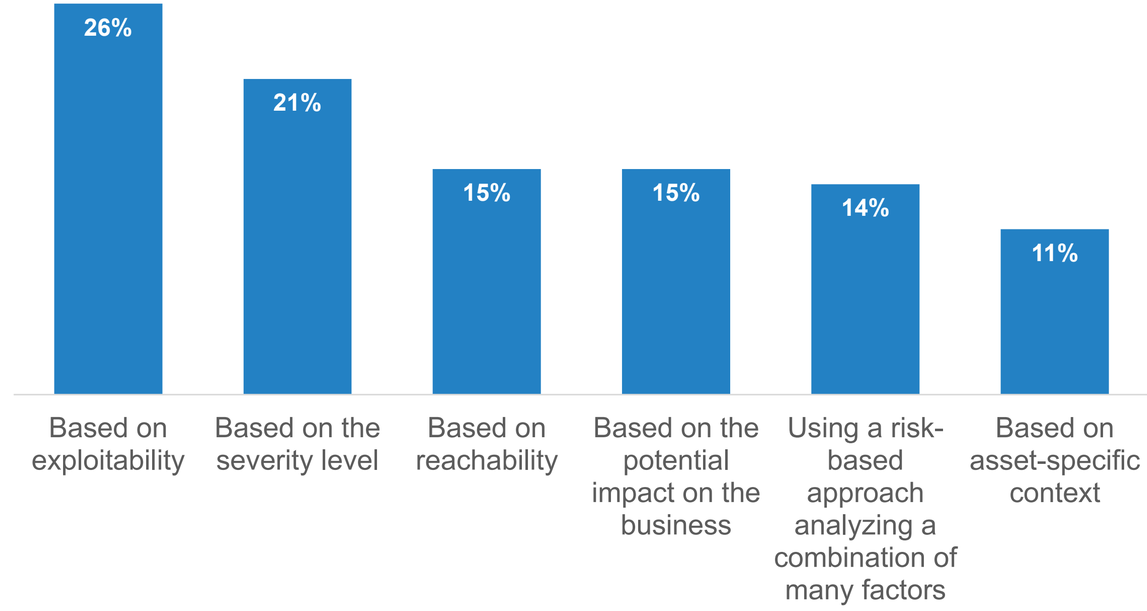
As organizations continue to progress toward a continuous threat and exposure management model, the silos and barriers separating IT and security must be dismantled. Cybersecurity and IT tools must collaborate and share data for optimal scale and efficiency for both teams.

**How organizations currently conduct asset discovery and management activities.**




There is also a significant opportunity for improvement within current threat and exposure management processes. Exploitability and severity are the primary factors in prioritization used by cybersecurity teams today. While this data is crucial for prioritizing exposure remediation, security teams are not considering more meaningful data, such as reachability, business impact, and asset-specific context, as much today. This results in a shallow depth of analysis and lowered accuracy of prioritization recommendations. Without understanding the deeper context of the business, assets, threats, and risks, vulnerability and exposure scoring remains based solely on the technical context of the vulnerability itself. This is inadequate and leads to glaring issues when considering the deployment of limited remediation resources.

**How organizations most commonly prioritize vulnerabilities and exposures for remediation.**






BACK TO CONTENTS

# Risk Reduction Requires Automated Remediation and Agentic AI

# Demand for Automated Remediation Is High, and One-third of Organizations Are Willing to Provide Free Rein

The main goal of threat and exposure management is to reduce risk in the most efficient way possible. This reality drives the need for improvement in prioritization, as well as the ability to incorporate automation into remediation processes, helping to scale the limited resources of the security operations team. Enhancements in automation serve as a fertile ground for agentic AI features, and vendors are rapidly announcing innovations in agentic AI for threat and exposure management. Ninety-four percent of security organizations report feeling comfortable with their threat and exposure management platform automatically remediating issues on their behalf. The primary goal for customers is to resolve exposures and vulnerabilities as quickly as possible, and they are willing to accept the risks associated with automated remediation and agentic AI if it results in a significant improvement to the security posture of the business.

**Are organizations comfortable with threat and exposure management platforms automatically remediating issues?**

94% **YES**

Fully automated remediation with agentic AI is a scary proposition to many security practitioners. Many have lived through the days when fixing security issues would often lead to outages, damaging the security team's reputation within the greater organization. Today, 63% of security organizations want automation to be limited while 37% desire complete autonomy of remediation. In the case of agentic AI and automated remediation, trust is earned over time. As agents execute without mistake and with humans in the loop for oversight, the comfort level with automated security remediation should continue to increase.

**Organizations' preferred approach to automating issue remediation.**

37%

We are willing to allow the engine to run **fully autonomously right now**

34%

We are willing to allow the engine to run **only on certain devices and systems for now**

29%

We will **review each fix before** we tell the automation to execute for now

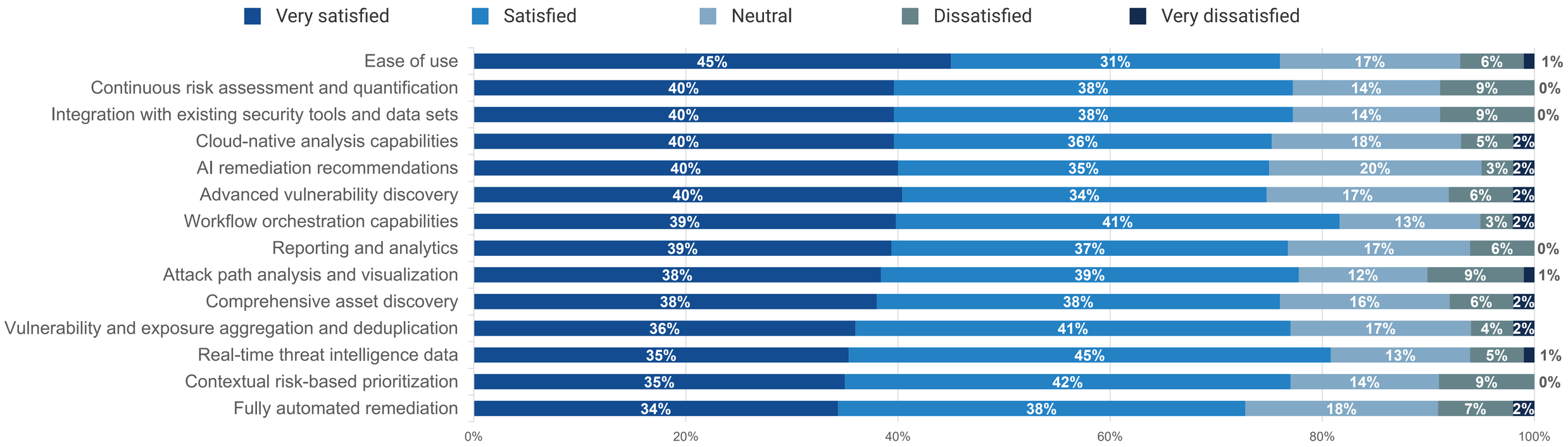


BACK TO CONTENTS

# Next-generation Innovation Requires Improved Feature Sets

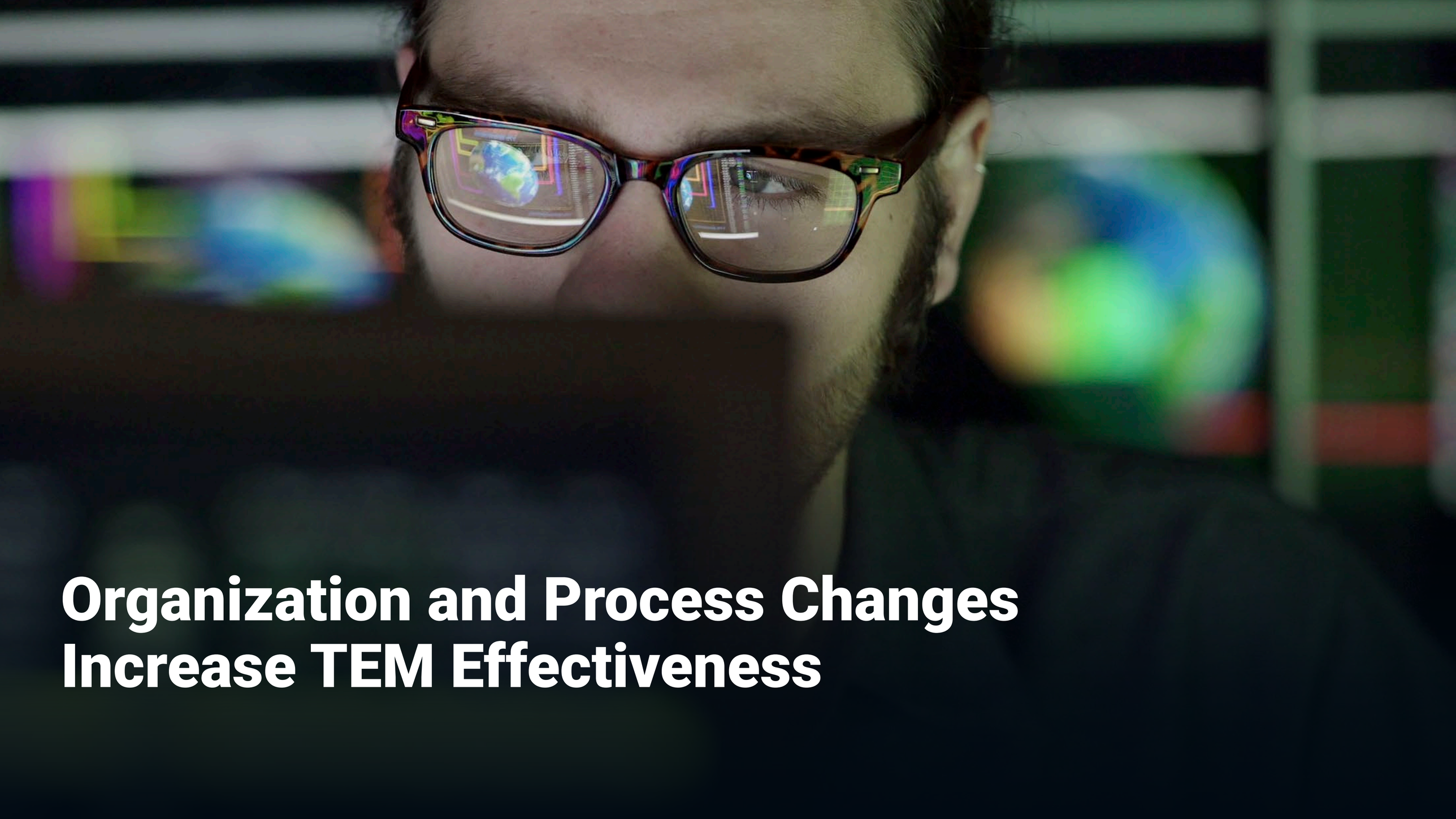
The next generation of threat and exposure management innovation will focus on AI-driven remediation and advanced prioritization through AI analysis. In terms of current levels of satisfaction, the three largest areas for potential improvement within threat and exposure management solutions today are all connected to AI. AI remediation recommendations, advanced vulnerability discovery, and fully automated remediation are the areas where security teams are most dissatisfied, presenting an opportunity for innovative vendors to create value. These three areas will benefit from a data-driven security framework integrated into the platform, equipping them with the context to make informed, AI-driven decisions.

**Level of satisfaction with features and capabilities in current continuous threat and exposure management solution.**






BACK TO CONTENTS



# Organization and Process Changes Increase TEM Effectiveness

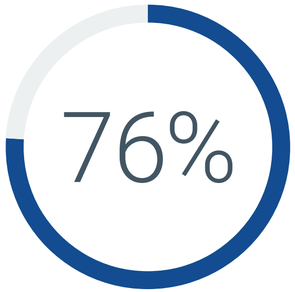
# IT Still Leads Threat and Exposure Management

The daily operations of threat and exposure management processes should be led by individuals with security expertise; however, threat and exposure management is often perceived as an IT operations team issue. Ironically, teams responsible for vulnerability or exposure management are less common than the general IT team in terms of ownership of threat and exposure management.

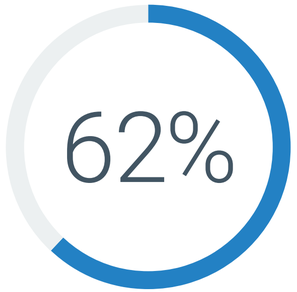
The problem stems from the fact that many organizations lack the available expertise to staff dedicated vulnerability or exposure management teams and thus rely on a general IT organizational structure to fulfill the need.

Security operations must dismantle the barriers between their expertise in vulnerability and exposure management and the general IT organization to enhance efficacy.

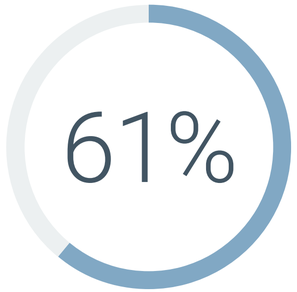
**Teams and roles responsible for managing threats and exposures.**



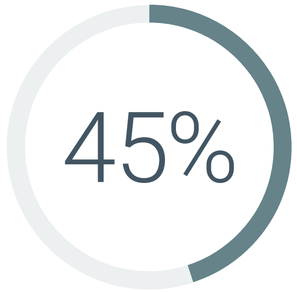

IT operations team



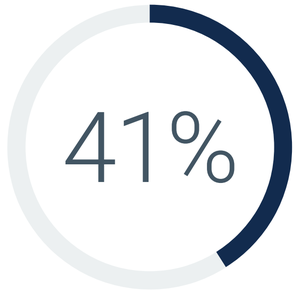

Cloud security team




Security operations center (SOC)




Threat intelligence team




Vulnerability or exposure management team


DevOps team



BACK TO CONTENTS

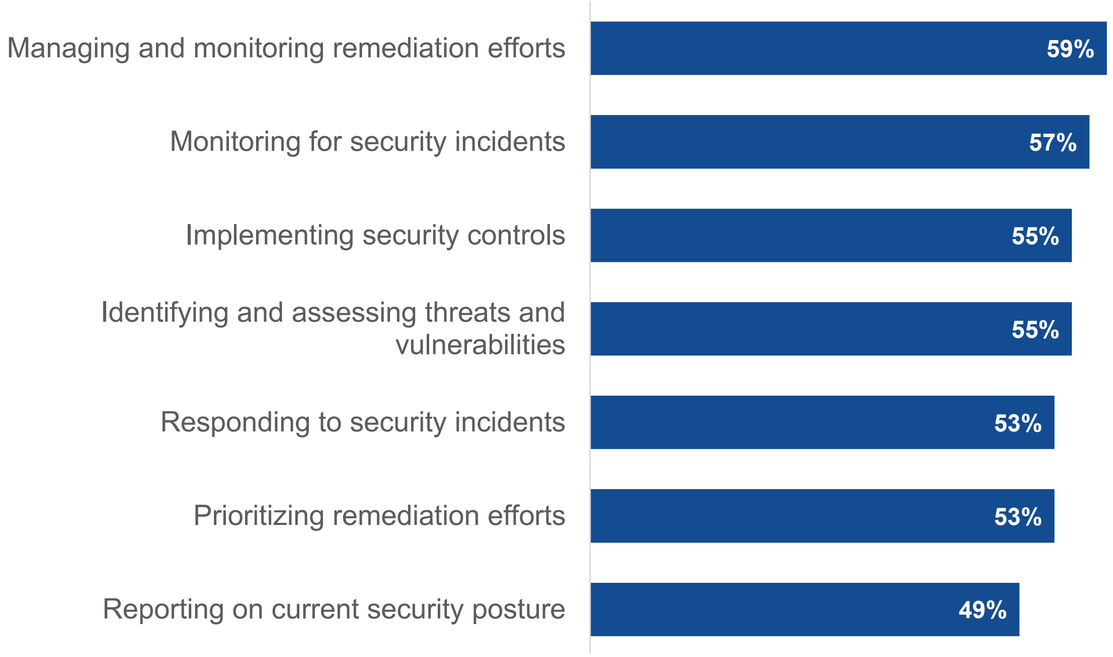
# The Catch-all Team of Cybersecurity

The team that manages threats and exposures often oversees the entire security stack. The efficiency of threat and exposure management relies on a set of skills that covers diverse areas of cybersecurity. Capabilities around remediation, incident handling, security control optimization, and reporting all fall within the scope of threat and exposure management.

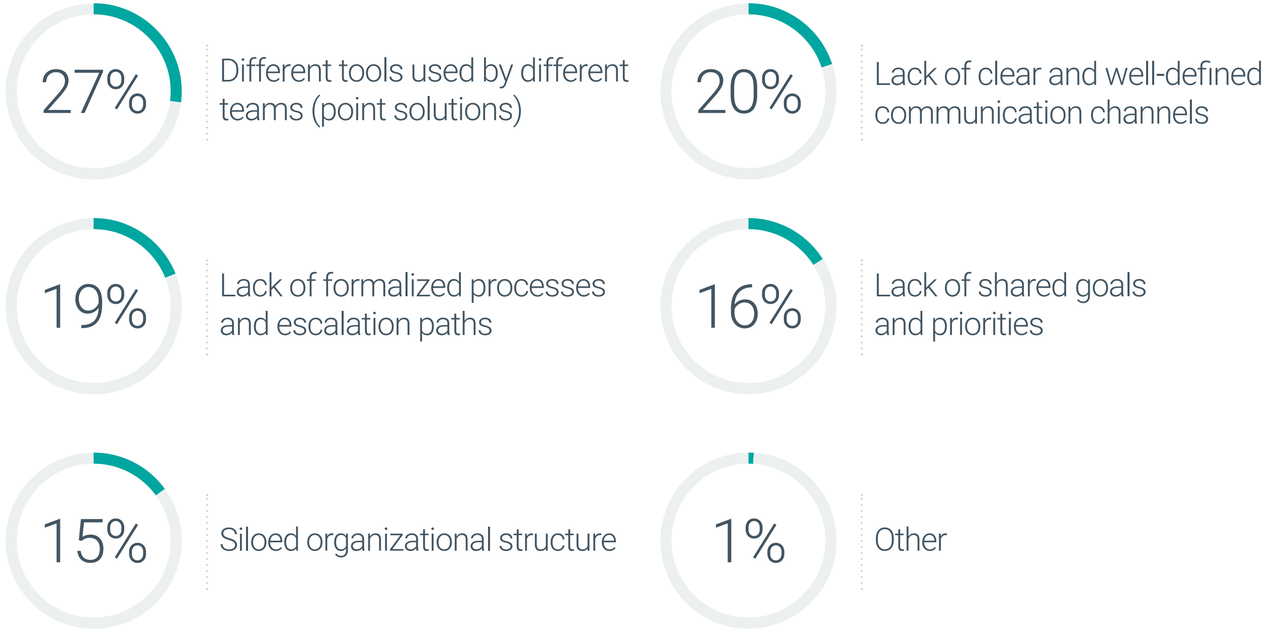
Detection, response, remediation, monitoring, security control implementation, prioritization, and reporting must be consolidated under one management umbrella if security teams are to maximize efficiency.

Due to this extensive knowledge requirement, teams that are overwhelmed must look to break down silos that exist between both tools and team structures for maximum risk reduction results.

**Primary responsibilities for team that owns threat and exposure management.**




**Primary challenge to communication and effective collaboration between teams responsible for threat and exposure management.**






BACK TO CONTENTS

The Zscaler Security Operations portfolio simplifies the flood of exposure and alert data from disjointed tools, allowing teams to reduce critical risk and minimize threats efficiently. With solutions built on the industry's first Data Fabric for Security, SecOps teams can transform limitless security data into actionable insights to identify critical gaps and vulnerabilities, group and prioritize active threats, and streamline response workflows to close the window on attackers. Reimagine SecOps with a unified approach to managing exposures and reducing threats.

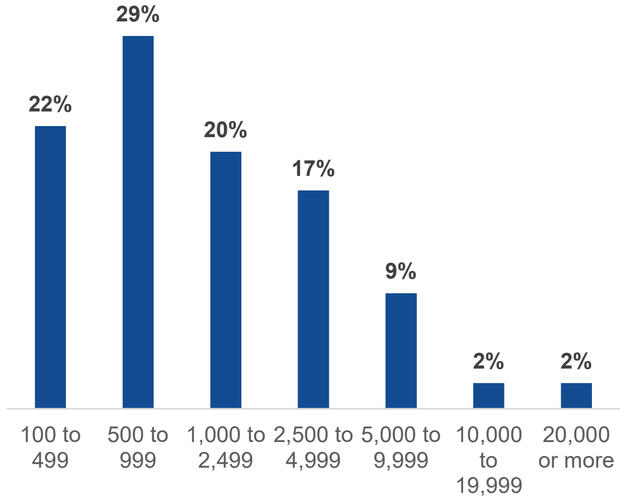
LEARN MORE

## RESEARCH METHODOLOGY AND DEMOGRAPHICS

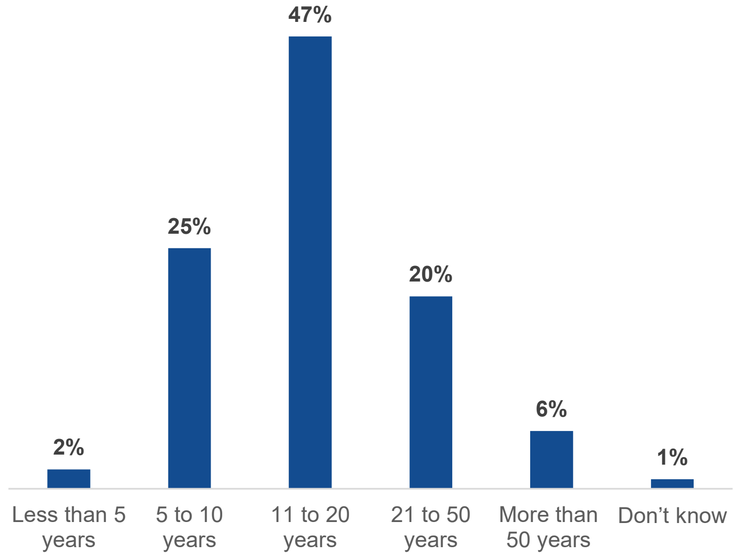
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between April 18, 2025 and May 12, 2025. To qualify for this survey, respondents were required to be involved with discovering and reducing threats and vulnerabilities in 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 IT and cybersecurity professionals.

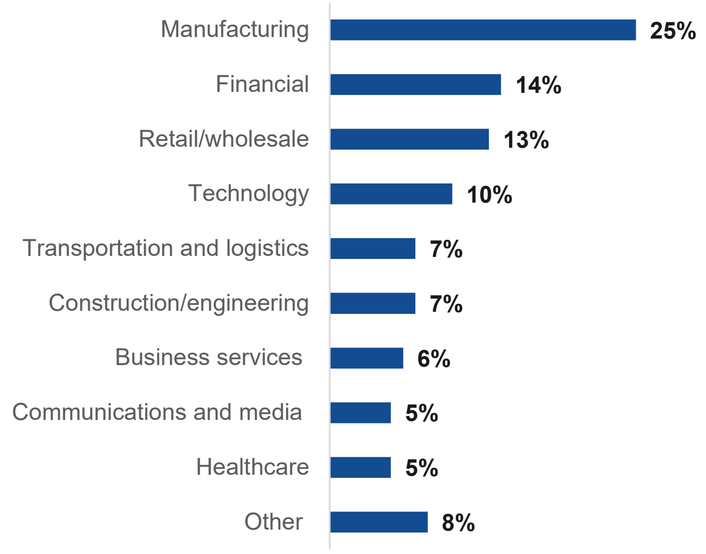
**Respondents' organizations by number of employees.**




**Respondents' organizations by years in operation.**




**Respondents' organizations by industry.**






BACK TO CONTENTS


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.