Enterprise Strategy Group™ by TechTarget

Security Hygiene and Posture Management Remains Decentralized and Complex

Jon Oltsik, Distinguished Analyst and Fellow

APRIL 2023

Research Objectives

Security hygiene and posture management has become increasingly difficult because of factors like a growing attack surface, the increased use of cloud computing, and the need to support a remote workforce. These factors can create security vulnerabilities that lead directly to cyber-attacks. Indeed, a majority of organizations have experienced at least one cyber-incident due to the exploit of an unknown, unmanaged, or poorly managed internet-facing asset. Unfortunately, this pattern will likely persist as most organizations continue to approach security hygiene and posture management with point tools, spreadsheets, and manual processes. Organizations are prioritizing spending on security hygiene and posture management, focusing on areas like continuous security testing, process automation, and increasing staff. Security professionals also aspire to consolidate disparate point tools into a security observability, prioritization, and validation (SOPV) architecture to gain a holistic perspective across all aspects of security hygiene and posture management.

To gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 383 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for evaluating, purchasing, and utilizing products and services for security hygiene and posture management, including vulnerability management, asset management, attack surface management, and security testing tools, among others.

This study sought to:

Assess how organizations approach security hygeine and posture management today.

Evaluate how organizations test the efficacy of their security controls and what this testing accomplishes.

Understand coverage gaps, why these gaps exist, and whether these gaps lead to security incidents.

Highlight what cybersecurity professionals believe their organizations should do to improve security hygiene and posture management.

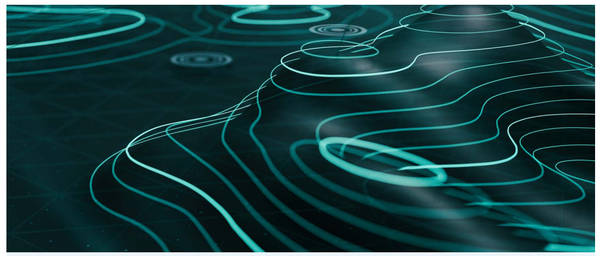
BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW

Security Hygiene and Posture Management Remains Immature but Is Garnering More Attention

PAGE 4

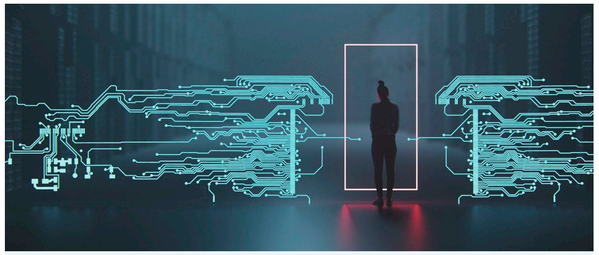


The External Attack Surface Is Growing and Represents a Consistent Vulnerability

PAGE 9

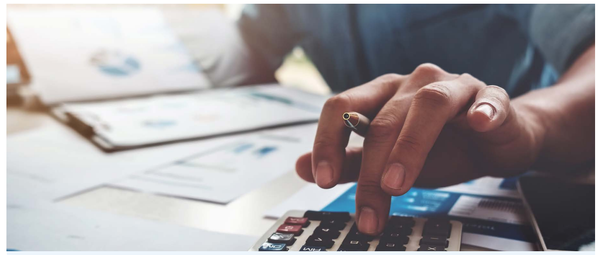
Asset, Vulnerability, and Patch Management Depend Upon Tools, Processes, and Cross-department Cooperation

PAGE 15



Security Testing Is Valuable but Mismanaged

PAGE 23



SHPM Spending Will Continue Despite Macroeconomic Pressure

PAGE 27

Research Methodology and Demographics

PAGE 31

Security Hygiene and Posture Management Remains Immature but Is Garnering More Attention

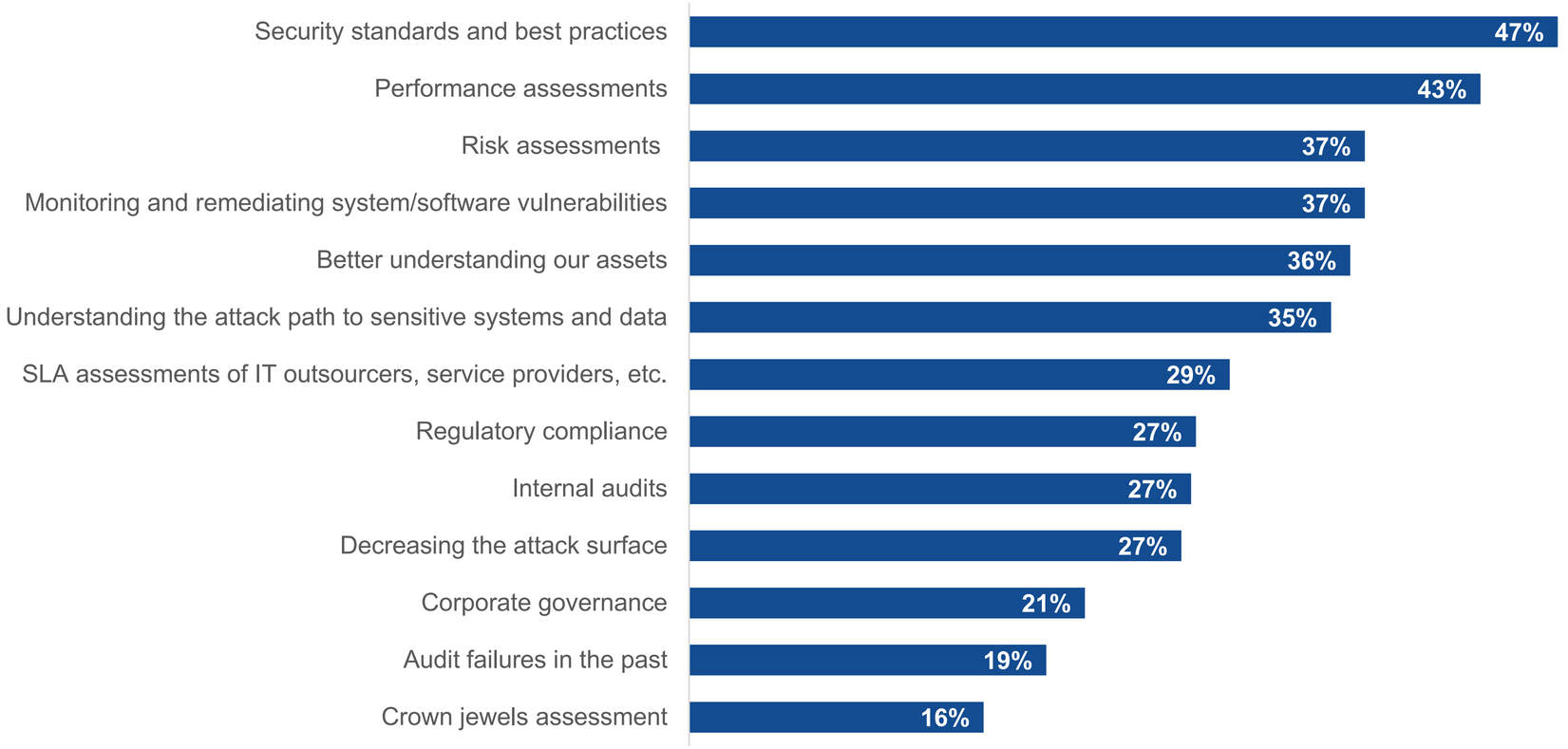
Biggest Security Hygiene and Posture Management Drivers

Security hygiene and posture management (SHPM) is a cybersecurity fundamental. Safeguarding any organization demands a thorough understanding of all assets, user identities and entitlements, how everything is configured, and the relationships between all the piecemeal parts.

Security professionals point to SHPM drivers like adhering to security standards and best practices (i.e., CIS critical security controls, ISO, NIST, etc.), risk assessments, vulnerability monitoring, and gaining a better understanding of assets. More recently, security teams have focused on attack path mapping. This helps them truly understand an adversary mindset and prioritize risk mitigation actions that could expose sensitive systems and data.

> “Security professionals point to SHPM drivers like **adhering to security standards and best practices.”**

Biggest drivers for security hygiene and posture management policies.



BACK TO CONTENTS

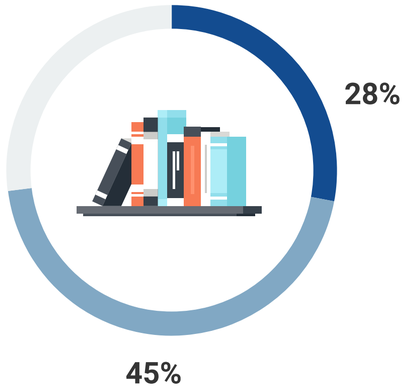
Security Hygiene and Posture Management Is Decentralized and Challenging

As organizations focus on initiatives like customer self service, digital transformation, remote worker support, and IT systems have become increasingly business-critical. This has also triggered greater oversight of cyber-risk and associated components like SHPM. Unfortunately, security hygiene and posture management isn't easy: More than one-third (36%) of organizations say that security hygiene and posture management is more difficult today than it was two years ago.

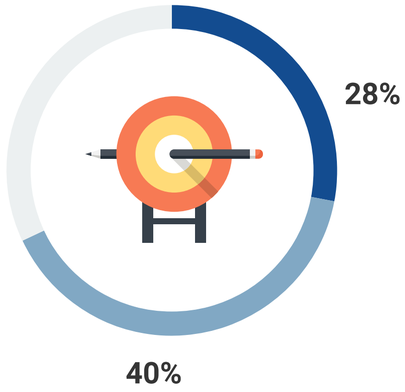
Why is security hygiene and posture management growing more difficult? Because it touches nearly all assets and activities across hybrid IT (i.e., user access and entitlements, asset configurations, network connections, application settings, etc.). The distributed nature of SHPM leads inevitably to a series of challenges. More than half (56%) of organizations claim that they sometimes struggle to understand which assets are business-critical, and similarly, 68% say that while they understand the importance of security hygiene and posture management, it's difficult to prioritize the actions that can have the biggest impact on risk reduction. Nearly three-quarters (73%) admit that they only have strong awareness of less than 80% of all assets, and another 56% report that determining asset ownership is difficult when a vulnerability is discovered. These issues hamper SHPM effectiveness, increase cyber-risk, and could open a door to a devastating cyber-attack.

Opinions on security hygiene and posture management. Strongly agree Agree

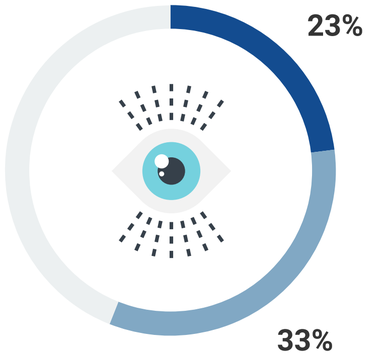
We have strong awareness of less than 80% of all assests



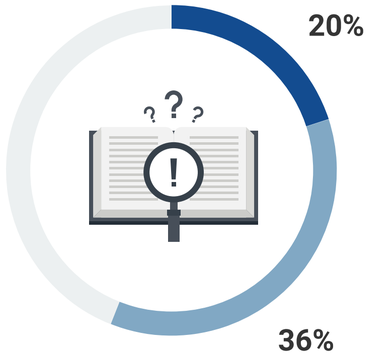
While my organization understands the importance of security hygeine and posture management, it's difficult to prioritize the actions that can have the biggest impact on risk reduction



It can be difficult to determine asset ownership when a vulnerability or misconfiguration is discovered



My organization sometimes struggles to understand which assets are business-critical



BACK TO CONTENTS

Who Owns SHPM?

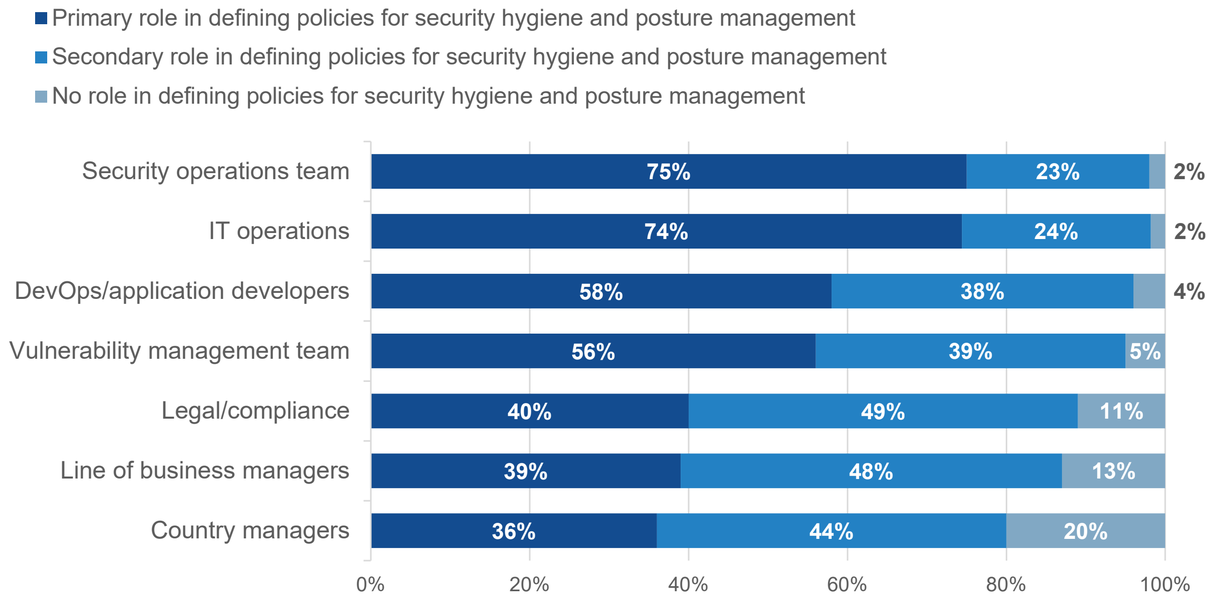
Due to the preponderance of assets across hybrid IT infrastructure, security hygiene and posture management depends upon cooperation across multiple teams, including DevOps, IT operations, regulatory compliance, risk management, security, software developers, and more. Since each team uses its own tools and processes to manage its piece of the pie, and given that SHPM spans on-premises, cloud-based, and even business partner IT applications and infrastructure, it's not surprising that different organizations manage it with different models. Specifically, 42% of organizations claim that SHPM is **completely centralized** with a single team having ultimate SHPM oversight. Other organizations take a more decentralized approach, with 41% saying SHPM is partially centralized where one team is responsible for coordinating activities across disparate groups and locations, while SHPM is completely decentralized at 17% of organizations (i.e., different teams are responsible for monitoring and managing the security hygiene and posture of individual areas such as endpoints, servers, and the cloud).

Does anyone own SHPM? Not really. The data reveals that more than half of organizations depend upon security operations, IT operations, DevOps/application developers, and vulnerability management teams to define SHPM policies. CISOs must take an active role here to ensure that collective efforts align with organizational goals of mitigating cyber-risk and maintaining resilience of business applications.

Personnel approach to security hygiene and posture management.

- 42% Completely centralized (i.e., a single team is responsible for security hygiene and posture management across all technologies)
- 41% Partially centralized (i.e., a single team is responsible for coordinating security hygiene and posture management with the help of endpoint, server, cloud, and other teams)
- 17% Completely decentralized (i.e., different teams are responsible for monitoring and managing the security hygiene and posture of individual areas such as endpoints, servers, cloud, etc.)

Groups responsible for defining security hygiene and posture management policies.



BACK TO CONTENTS

SHPM Process Automation

Security hygiene and posture management can be time consuming and resource intensive, so process automation is critical to improving threat prevention and operational efficiency. Consequently, 91% of organizations are automating SHPM processes like generating SHPM reports, testing the value of remediation actions, continuously scanning assets, and patching vulnerable software.

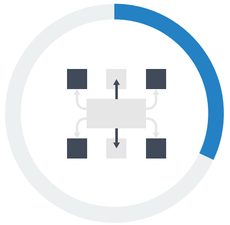
Since SHPM tends to be a decentralized, shared responsibility across multiple teams, organizations should look for opportunities to automate processes across security and technology domains to achieve maximum velocity and usefulness.

Five most commonly automated security hygiene and posture management activities.

36%
Generation of reports for security, IT, management, etc.

35%
Security testing to validate remediation actions

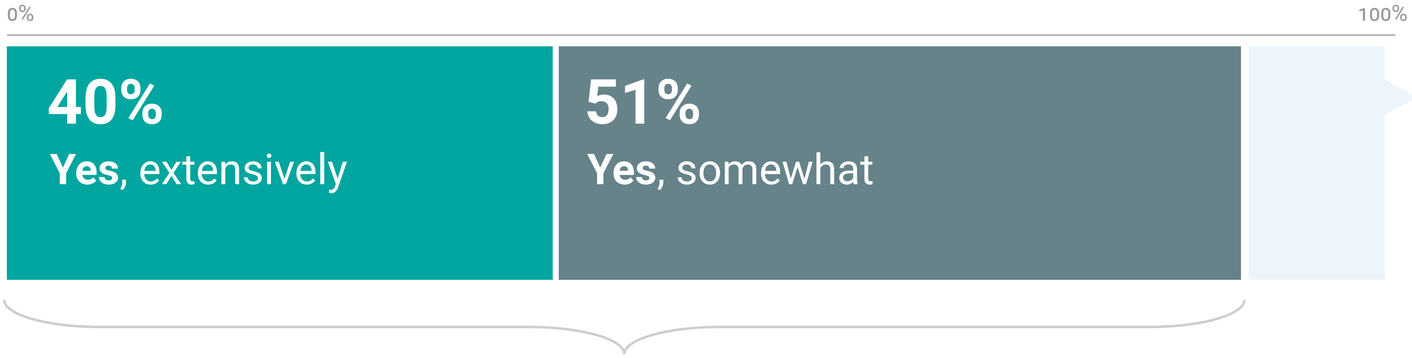
33%
Continuous asset scanning



32%
Application of software patches

30%
Analytics to help prioritize remediation actions

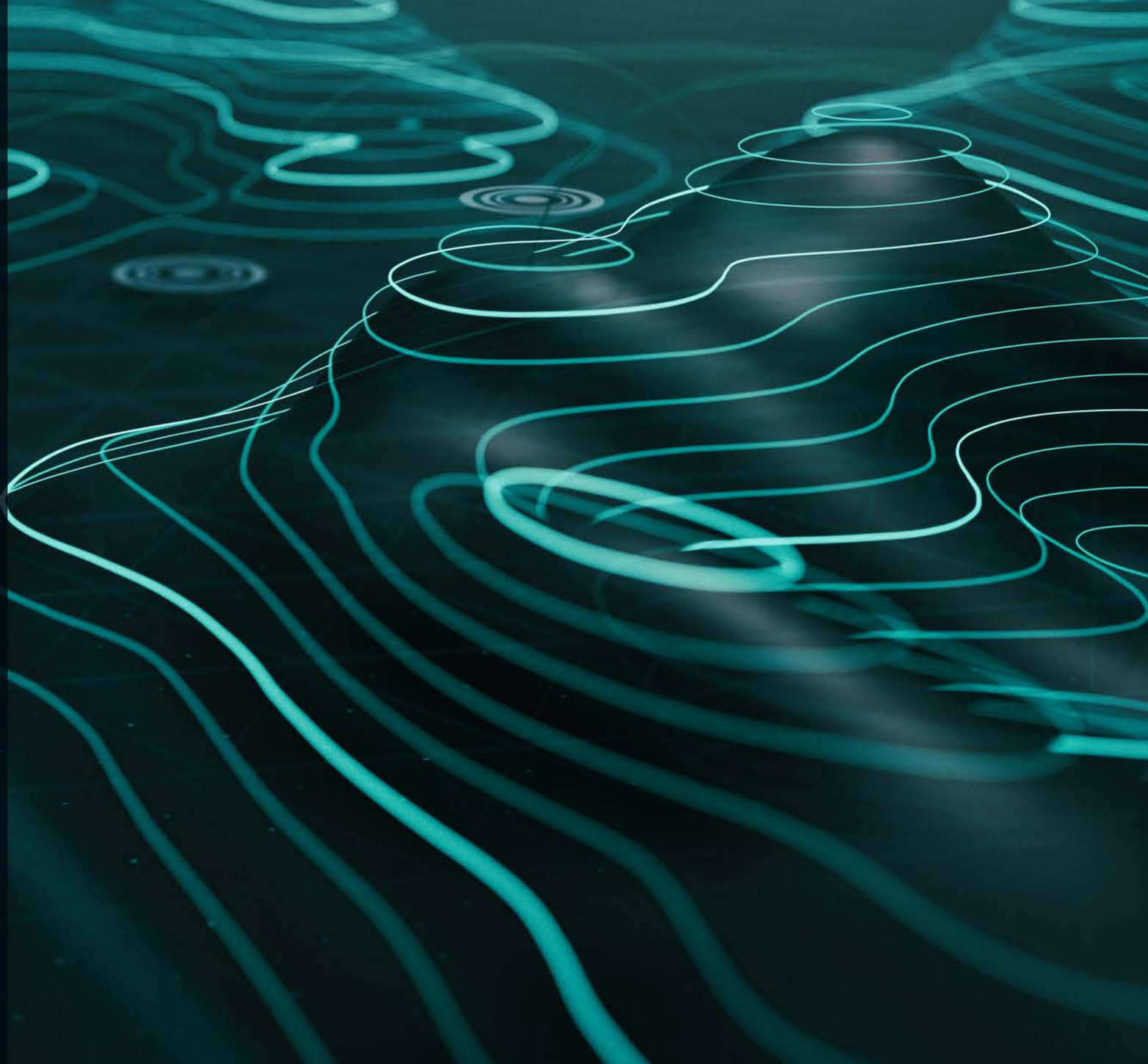
Has your organization automated security hygiene and posture management activities?



91% of organizations are automating SHPM processes.

BACK TO CONTENTS

The External Attack Surface Is Growing and Represents a Consistent Vulnerability



Proactive and Reactive Reasons for Performing Attack Surface Discovery

Two years ago, the primary reason why organizations did attack surface discover was for regulatory compliance. While this is still one of the common drivers, organizations seem more concerned with calculating cyber-risk and applying the right security controls and reducing the risk of a ransomware attack. Clearly, attack surface discovery is important, but CISOs must understand that hybrid IT infrastructure is always changing while cyber-adversaries are continuously scanning their organization's attack surface with automated tools as part of the reconnaissance phase of cyber-attacks. CISOs must continually scan and safeguard the attack surface, assess attack surface risks, and mitigate high-priority issues.

Reasons external attack surface discovery is performed.

48%
To calculate risk and apply the right security controls

45%
To reduce risk of a ransomware attack

43%
Regulatory compliance requirement

40%
To complete our asset inventory

39%
The assets in our attack surface are frequently changing

35%
Our attack surface is expanding

34%
Unknown assets are more susceptible to malicious attack

31%
Low-priority assets are more susceptible to malicious attack

BACK TO CONTENTS

Attack Surface Accelerants Include Third Parties, IoT, and Cloud

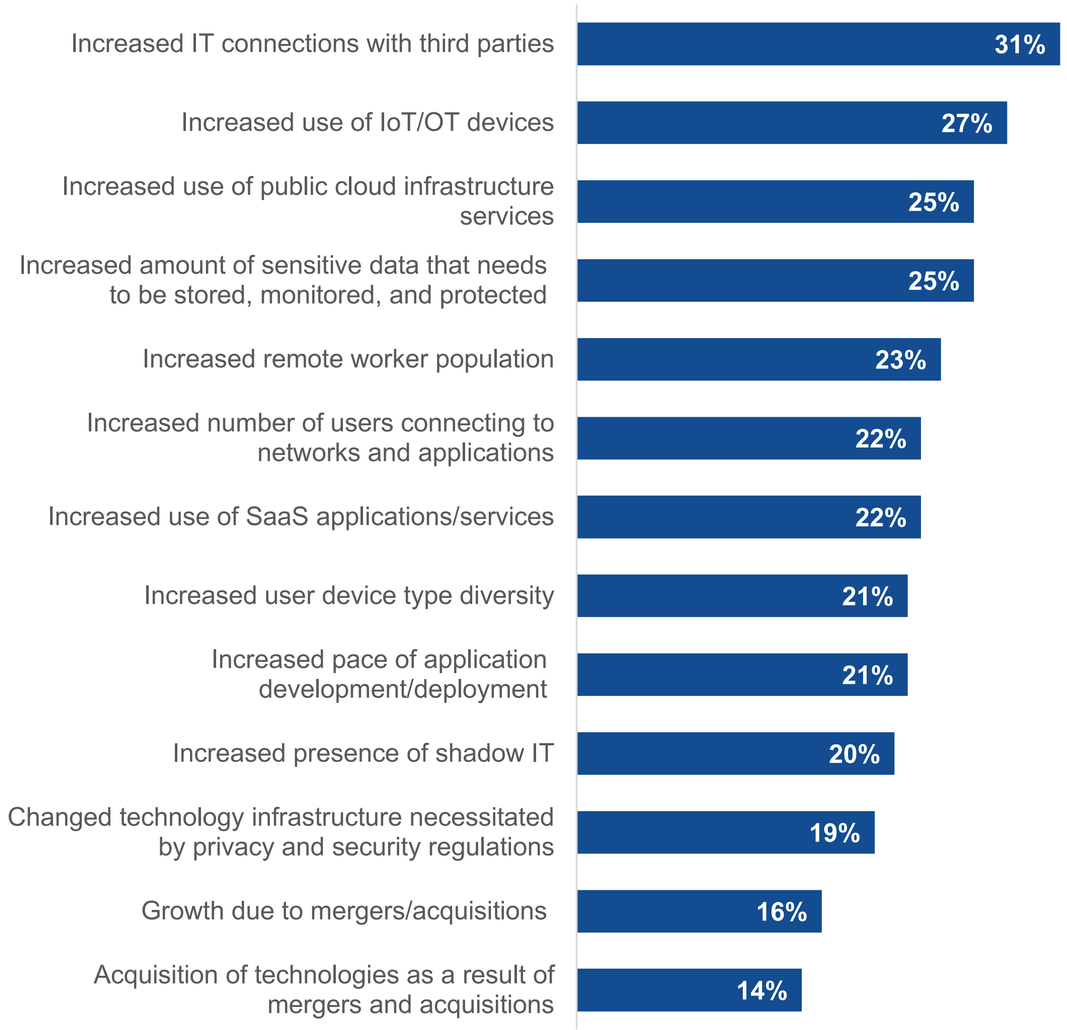
While reducing attack surface risk should be a universal goal, it can be difficult to achieve this due to continuous attack surface growth. Nearly two-thirds (62%) of organizations claim their attack surface has grown over the past two years, driven by increasing connections with third parties, growing use of IoT/OT devices, increasing use of public cloud infrastructure services, and growth in the amount of sensitive data.

How organizations characterize the change in their attack surface over the past two years.

20%
The attack surface has increased substantially over the past two years

42%
The attack surface has increased slightly over the past two years

Reasons the attack surface has increased over the last two years.



BACK TO CONTENTS

Actions taken to reduce the attack surface over the past 12 to 18 months.

34%

Established and implemented more secure configuration requirements for endpoints, servers, cloud workloads, etc.

34%

Implemented zero trust policies, processes, and technologies

33%

Implemented policies and technologies for multi-factor authentication

31%

Assessed and confirmed that protocols are robust and secure

30%

Eliminated or reinforced overly permissive rules and accounts

29%

Implemented policies and processes for software supply chain security

29%

Tightened access controls for critical applications and services

29%

Employed network segmentation technologies

29%

Removed administrator account privileges from endpoints

27%

Reduced the number of internet access points

26%

Used tokens, encryption, and/or signatures to secure APIs

25%

Removed unneeded code, applications, and/or services

Actions to Reduce Attack Surface Growth

Many organizations are addressing attack surface growth with proactive actions to reduce their attack surface. More than one-third of organizations have established and implemented more secure asset configurations for reducing cyber-risk and/or implemented zero trust. Another 33% use multi-factor authentication, and 31% are assessing their use of secure protocols. It is worth noting that 30% have eliminated/reinforced overly permissive rules and accounts. This is especially important for reducing risks associated with cloud administration accounts that are often shared among developers.

BACK TO CONTENTS

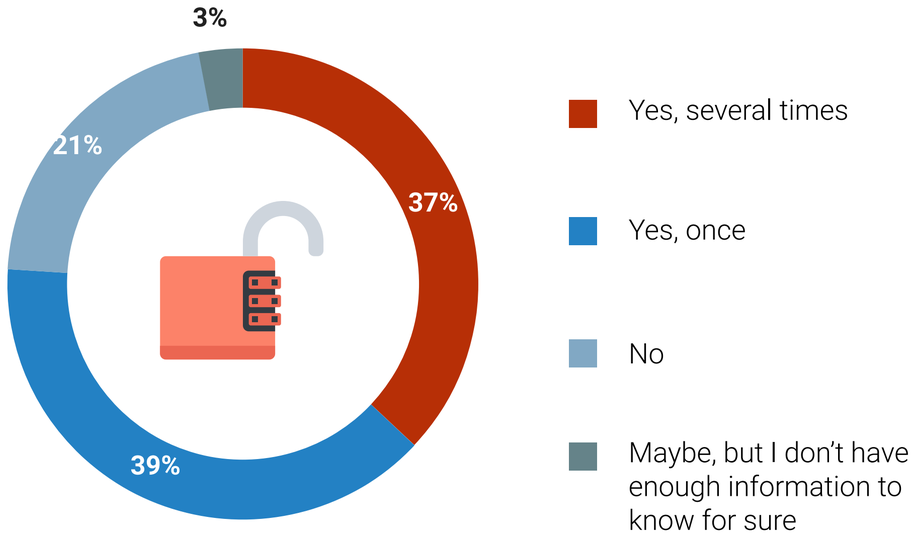
Cyber-attacks Emanating from an Exposed Asset

Attack surface management isn't easy. Responsibilities are spread across different IT and security teams using an assortment of specialized tools. Twenty-six percent of organizations perform some aspects of attack surface management (ASM) continually, but the majority (68%) find time for ASM weekly or monthly. Just performing attack surface discovery alone can be time consuming and resource intensive; nearly three-quarters (72%) of organizations say attack surface discovery takes more than 40 person hours to complete, and only starts the ASM process. Upon discovery, security teams still need to analyze the data, prioritize actions, and work with IT and development teams to mitigate risks.

While ASM is undoubtedly cumbersome, it is also a necessary cyber-defense requirement. This point is reinforced by the fact that more than three-quarters (76%) of organizations have experienced some type of cyber-attack due to an unknown, unmanaged, or poorly managed internet-facing asset, which is up from 69% in 2021. For example, ransomware attacks often exploit known CVEs with available patches, but unknown, mismanaged, and vulnerable assets on the attack surface probably aren't patched regularly.

Frequency with which attack surfaces are typically scanned.

Has your organization experienced some type of cyber-attack in which the attack itself started through an exploit of an unknown, unmanaged, or poorly managed internet-facing asset?



"72% of organizations say attack surface discovery takes more than 40 person hours to complete, and only starts the ASM process."

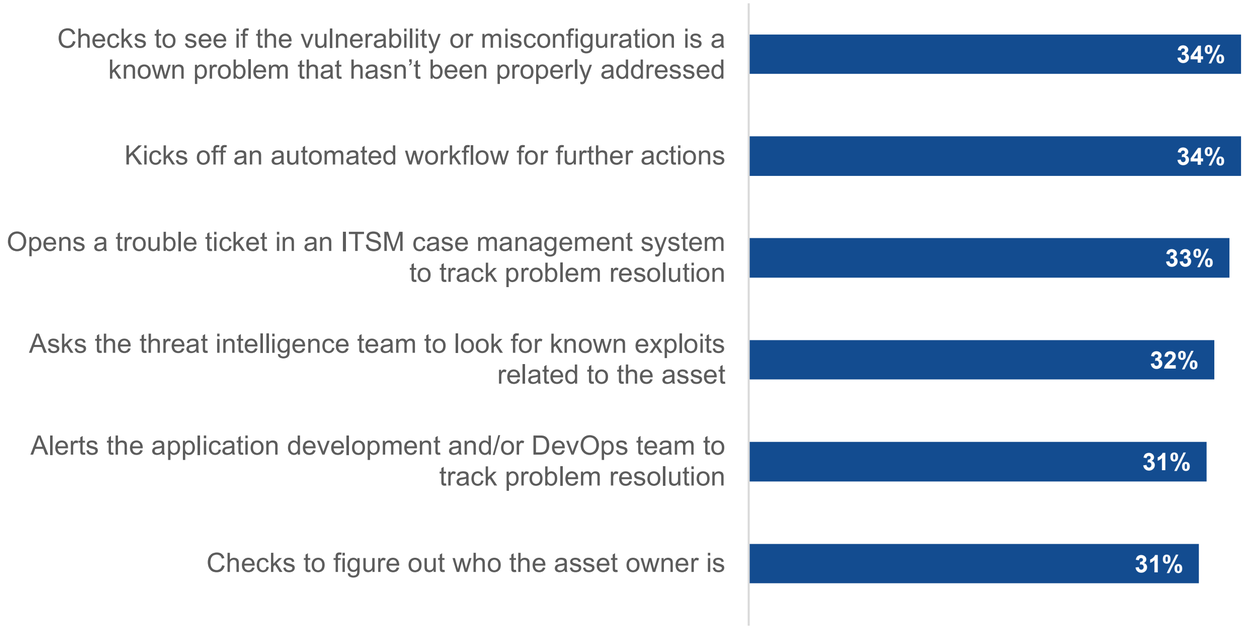
BACK TO CONTENTS

Remediating and Managing the Attack Surface

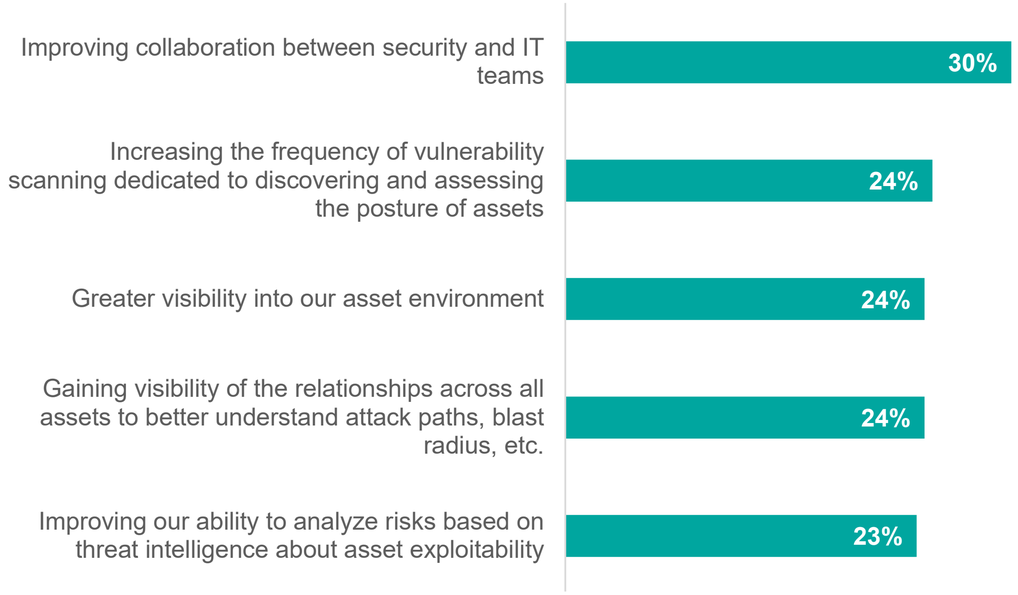
When an attack surface problem is discovered, more than one-third (34%) check to see if the vulnerability or misconfiguration is a known problem that hasn't been properly addressed, 34% use automated workflows for remediation actions, 33% open an ITSM trouble ticket, 32% correlate attack surface vulnerabilities with threat intelligence, and 31% alert application developers or DevOps teams for fixes while they track their progress.

Beyond what organizations are doing today, what actions could they take to improve their ASM programs? Organizational enhancements top the list as 30% say their ASM programs would benefit from improving collaboration between security and IT teams. Beyond teamwork, nearly one-quarter say their ASM program could be improved by increasing the frequency of vulnerability scans, gaining greater visibility into their asset environment, and/or achieving visibility into the relationships across all assets (to understand the attack path and blast radius of an attack). In aggregate, ASM programs could be improved through greater visibility, continuous automated processes, and organizational changes.

Actions the organization takes upon discovering a vulnerable asset on the attack surface.

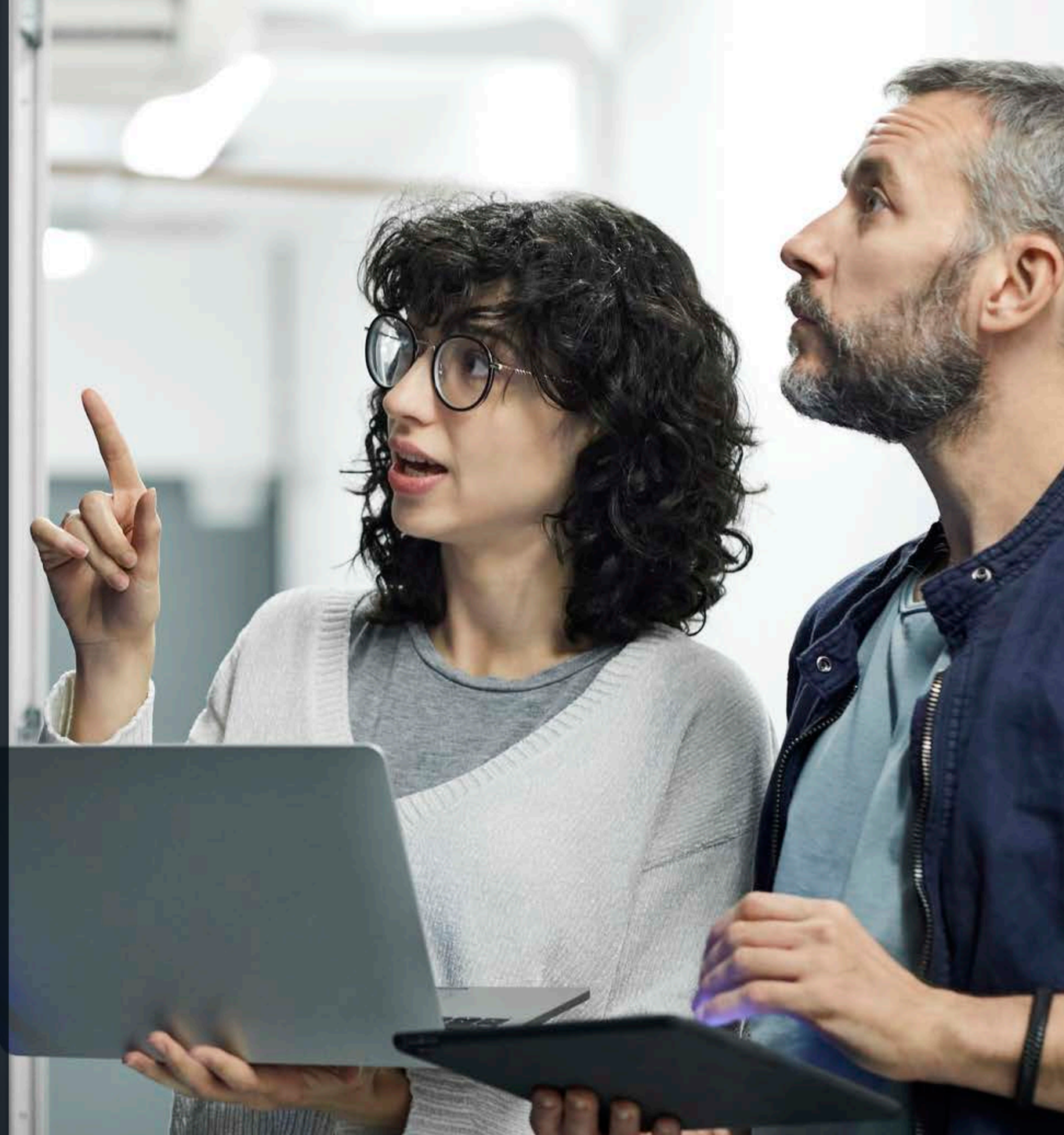


Actions that would **most improve** attack surface management programs.

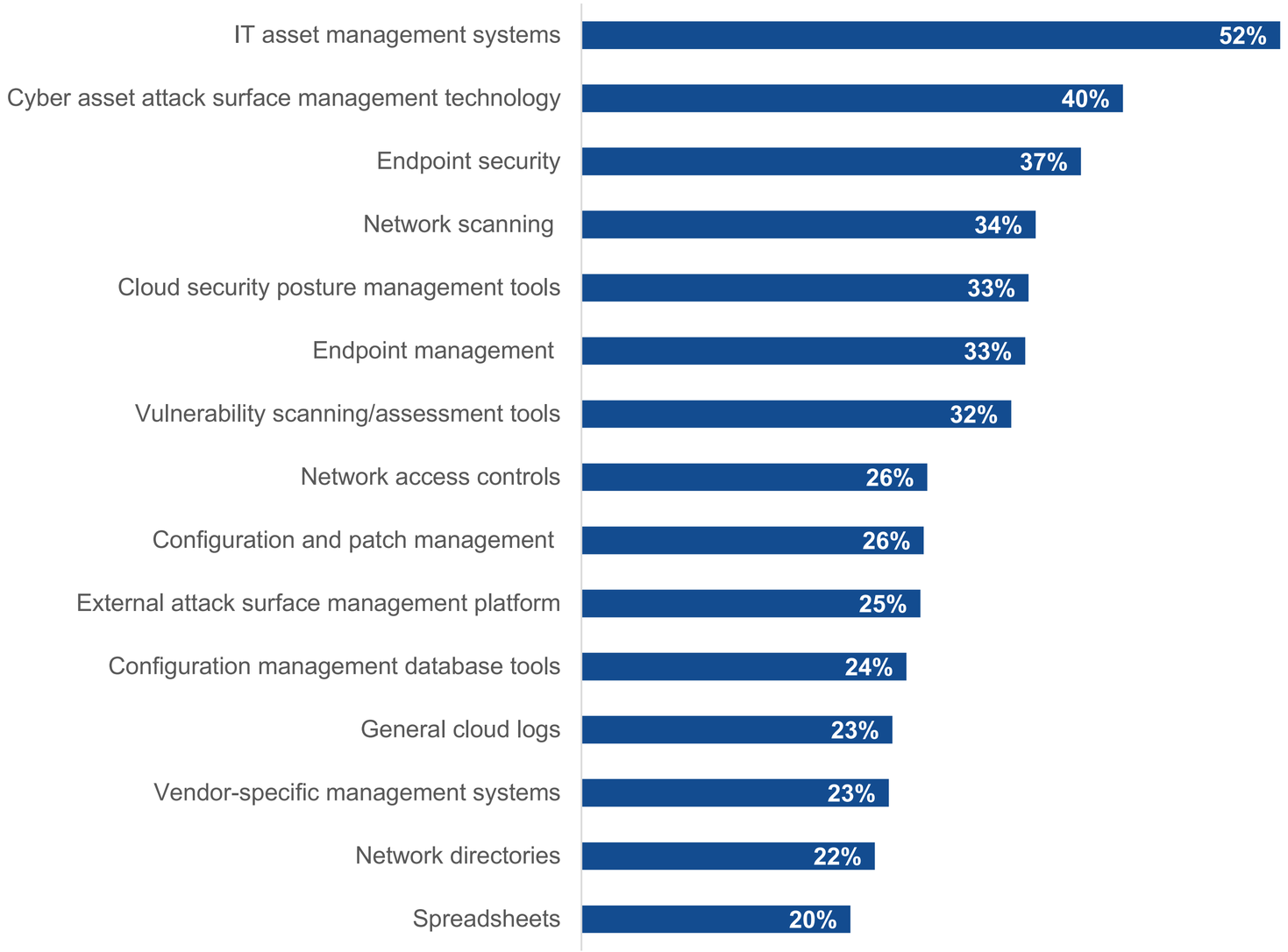


BACK TO CONTENTS

Asset, Vulnerability, and Patch Management Depend Upon Tools, Processes, and Cross-department Cooperation



Types of databases/systems/tools currently in use as part of IT asset inventory processes.



Security Asset Management by the Numbers

Nearly one-third (32%) of organizations collect, process, and analyze data from more than 10 sources for security asset management. The most common data sources used include IT asset management systems (52%), endpoint security tools (32%), network scanning (34%), and cloud security posture management (33%). It is worth highlighting that 40% are using cyber-asset attack surface management (CAASM) technologies for security asset management. These tools consolidate security asset data by connecting with other tools' APIs, collecting all asset data, analyzing the data, assigning risk scores, and suggesting remediation priorities. CAASM systems were fairly new in 2021 when ESG last researched SHPM. The data suggests that CAASM has gained broad deployment since.

Number of databases/systems/tools currently in use as part of IT asset inventory processes.

- **27%** actively use 1 to 5 tools
- **40%** actively use 6 to 10 tools
- **23%** actively use 11 to 20 tools
- **9%** actively use 20+ tools

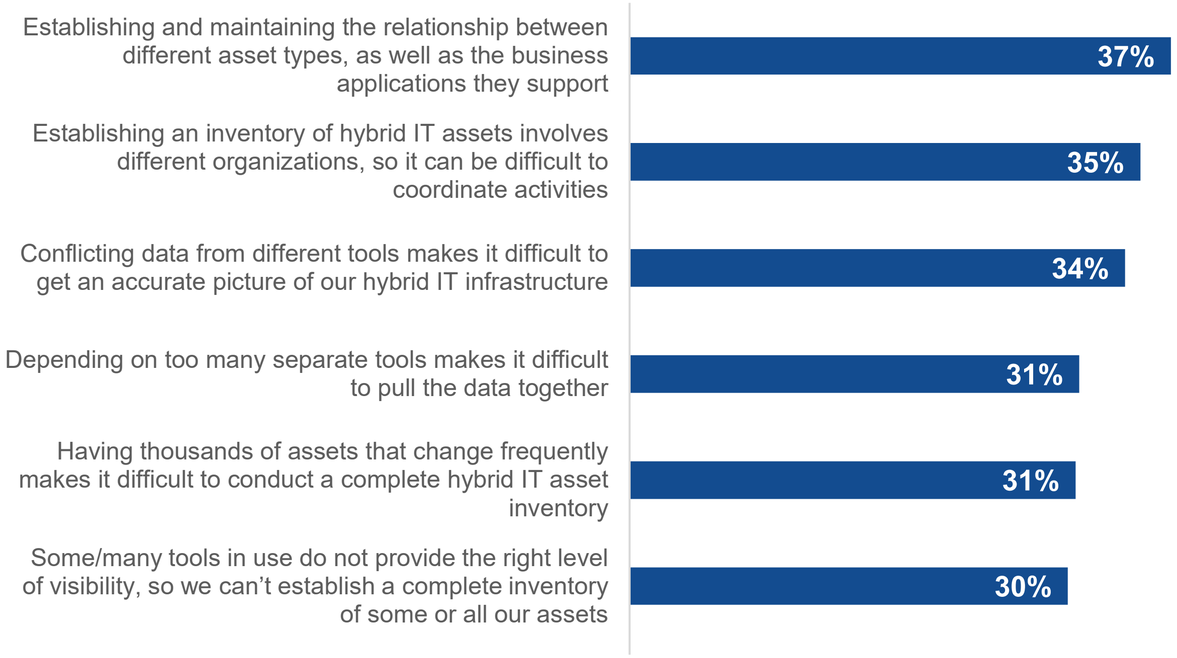
BACK TO CONTENTS

Security Asset Management Challenges

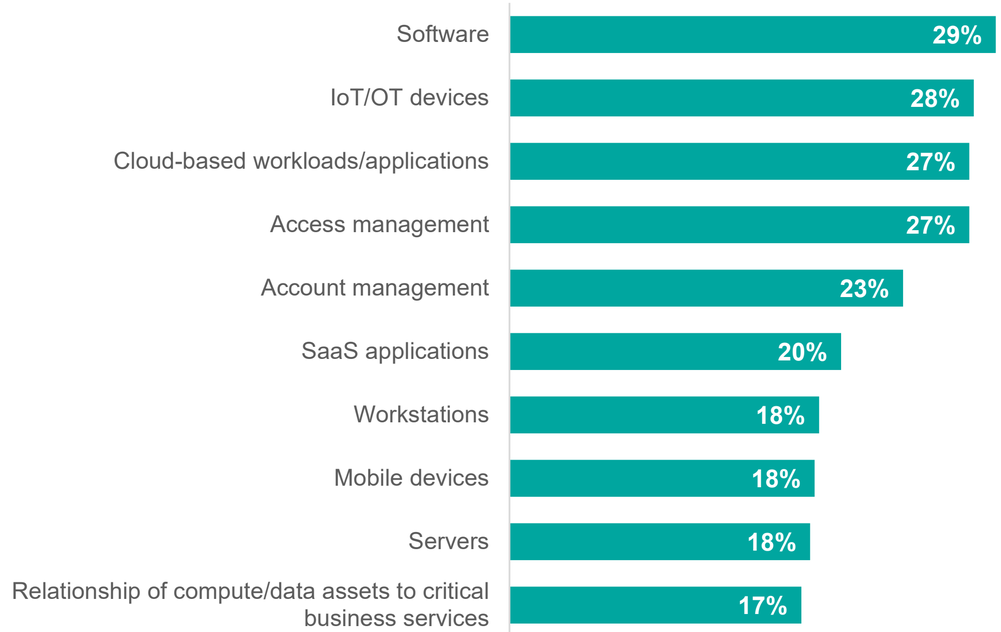
With thousands of IT assets across a hybrid IT infrastructure, security asset management is fraught with challenges. Indeed, 37% of security professionals find it challenging to establish and maintain the relationships between different asset types (as well as the business applications they support). Lack of knowledge here makes it difficult to know which remediation actions to prioritize. Additionally, 35% find it challenging to coordinate security asset management across different organizations, 34% are challenged by conflicting data from different tools, 31% are challenged to pull data together from separate tools, and 31% are challenged by the sheer volume of assets.

When asked to identify the types of assets most difficult to track and inventory, 29% of security professionals identified software (i.e., software misconfigurations, coding errors, vulnerabilities, etc.), 28% pointed to IoT/OT devices, 27% recognized cloud-based workloads, 27% acknowledged access management, and 23% said account management. IoT/OT devices represent the biggest change since 2021, rising from the fifth to the second most difficult asset type for maintaining an accurate inventory.

Challenges fully understanding the total inventory of IT assets.



Most difficult assets to maintain a timely and accurate inventory for.



BACK TO CONTENTS

Actions to Improve Security Asset Management

Survey respondents were asked how their organizations could improve security asset management. More than a quarter said this could be accomplished by integrating security and IT tools (28%) and/or automating security asset management processes (26%), while 24% recommended establishing business-centric KPIs, metrics, and reports. Another 22% mentioned improving their organization's ability to analyze risk scores to help them determine which assets are truly at risk and/or bolstering the collaboration on security asset management between IT and security teams.

Similar to 2021, the data suggests that security asset management programs tend to be informal, disorganized, and immature, but the adoption of CAASM technology seems to be a positive development as it supports tools integration, advanced analytics, risk scoring, and suggestions for remediation prioritization. It's likely these systems will continue to proliferate.

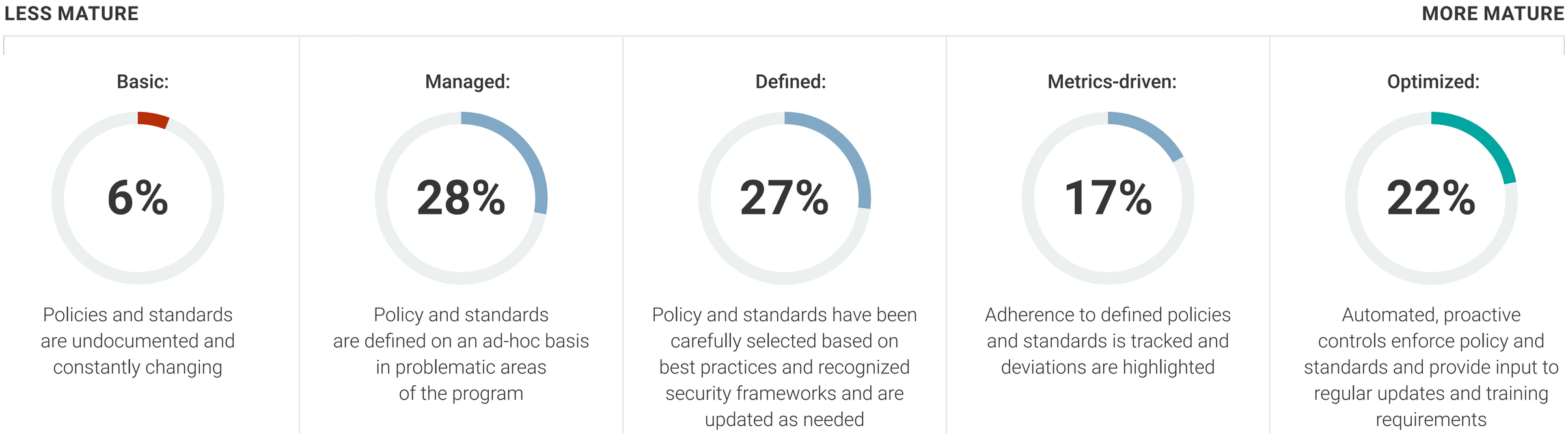
Actions that would most improve security asset management program.

BACK TO CONTENTS

Vulnerability Management Maturity

This year, ESG asked respondents to rank the status of their vulnerability management program. One might think that since vulnerability management processes have been in place for over 20 years, most organizations would have reached a state of program maturity, but that's not the case. While 22% believe they have reached the most mature vulnerability management level (**optimized**), more than half (55%) are stuck at either the **managed** or **defined** levels. The remaining organizations fall into either the **basic** level, meaning policies and standards are undocumented and constantly changing, or **metrics-driven** level, meaning adherence to defined policies and standards is tracked and deviations are highlighted. Based on the research, best practice adherence acts as a foundation for vulnerability management. Mature organizations build on top of best practices with metrics, adjustments, and automation.

Vulnerability management program self-assessment.



BACK TO CONTENTS

Biggest Vulnerability Management Program Challenges

While optimized vulnerability management programs include process automation, this seems to be beyond many organizations. When asked to identify the most challenging aspects of these programs, more than one-quarter (28%) pointed to automating the process of vulnerability discovery, prioritization, dispatch to owner, and mitigation. These steps encompass the entire vulnerability management lifecycle, so it's safe to assume there is a lot of work ahead. Another program challenge is tracking software vulnerabilities for which no patch is available (28%). This is often true for organizations with lots of IoT/OT devices. Like other areas of SHPM, vulnerability management programs are challenged by coordinating processes across different tools (28%) and coordinating processes across different teams (27%).

Biggest challenges associated with vulnerability management.

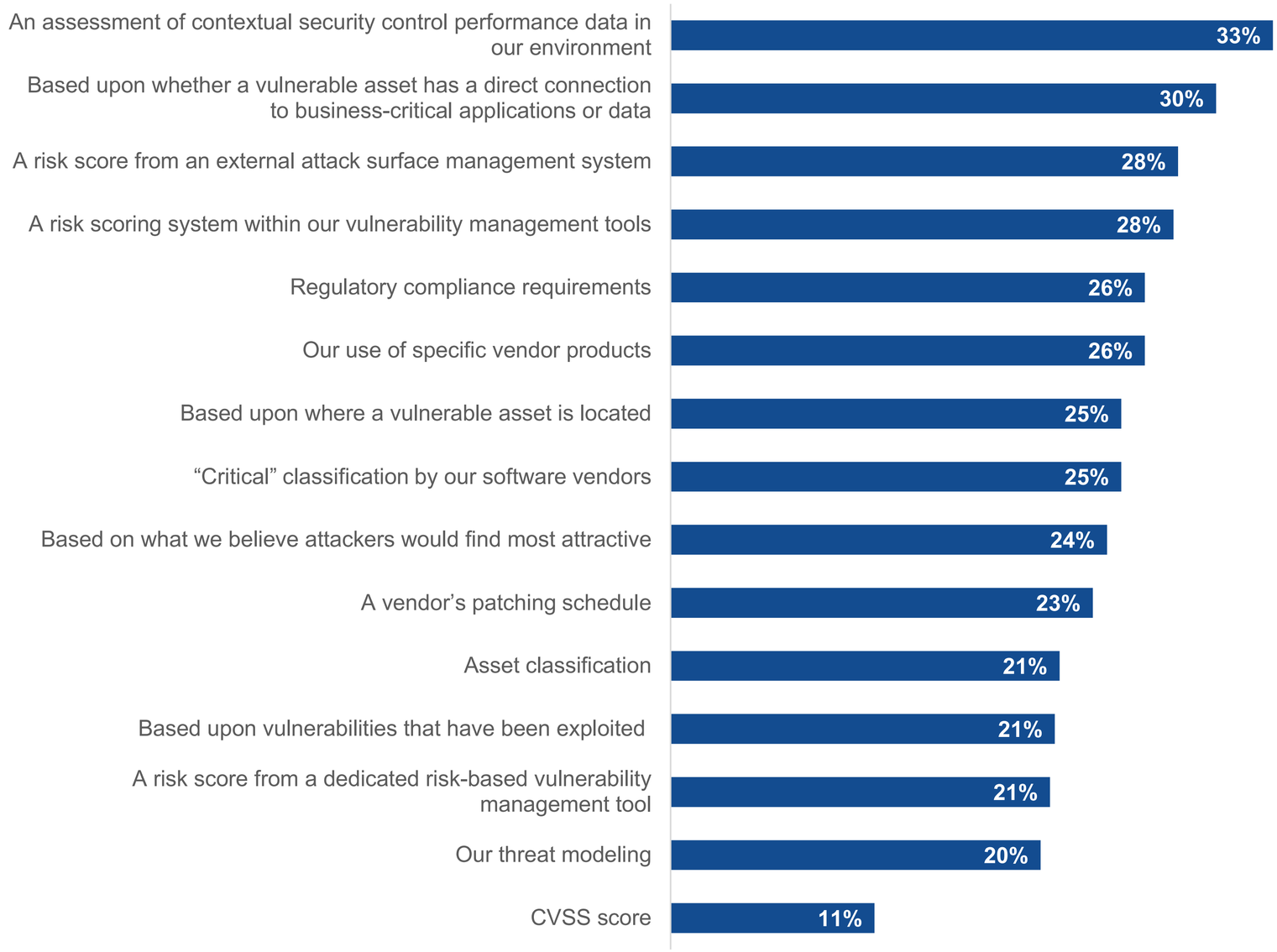
BACK TO CONTENTS

Vulnerability Patching Priorities

After scanning, security teams analyze data and then determine which vulnerabilities should be remediated first. How do organizations make these prioritization decisions? As was the case in 2021, the research indicates that organizations have multiple inputs for decision making. For example, one-third make patching priority decisions based on an assessment of contextual security control performance data. In other words, decisions are made based on the efficacy of controls or gaps in security defenses. Other priority inputs include whether vulnerable assets have a direct connection to business-critical applications (30%), a risk score from an ASM system (28%), or a risk score from a vulnerability management tool (28%).

Interestingly, CVSS scores seem like a secondary consideration as only 11% use them for prioritization. Certainly, they assess this input as some compliance regulations require that organizations patch vulnerabilities with baseline CVSS scores, but it seems like analytics and context have become far more important considerations than static rankings.

How vulnerabilities are prioritized and patched.



BACK TO CONTENTS

Actions to Improve Vulnerability Management

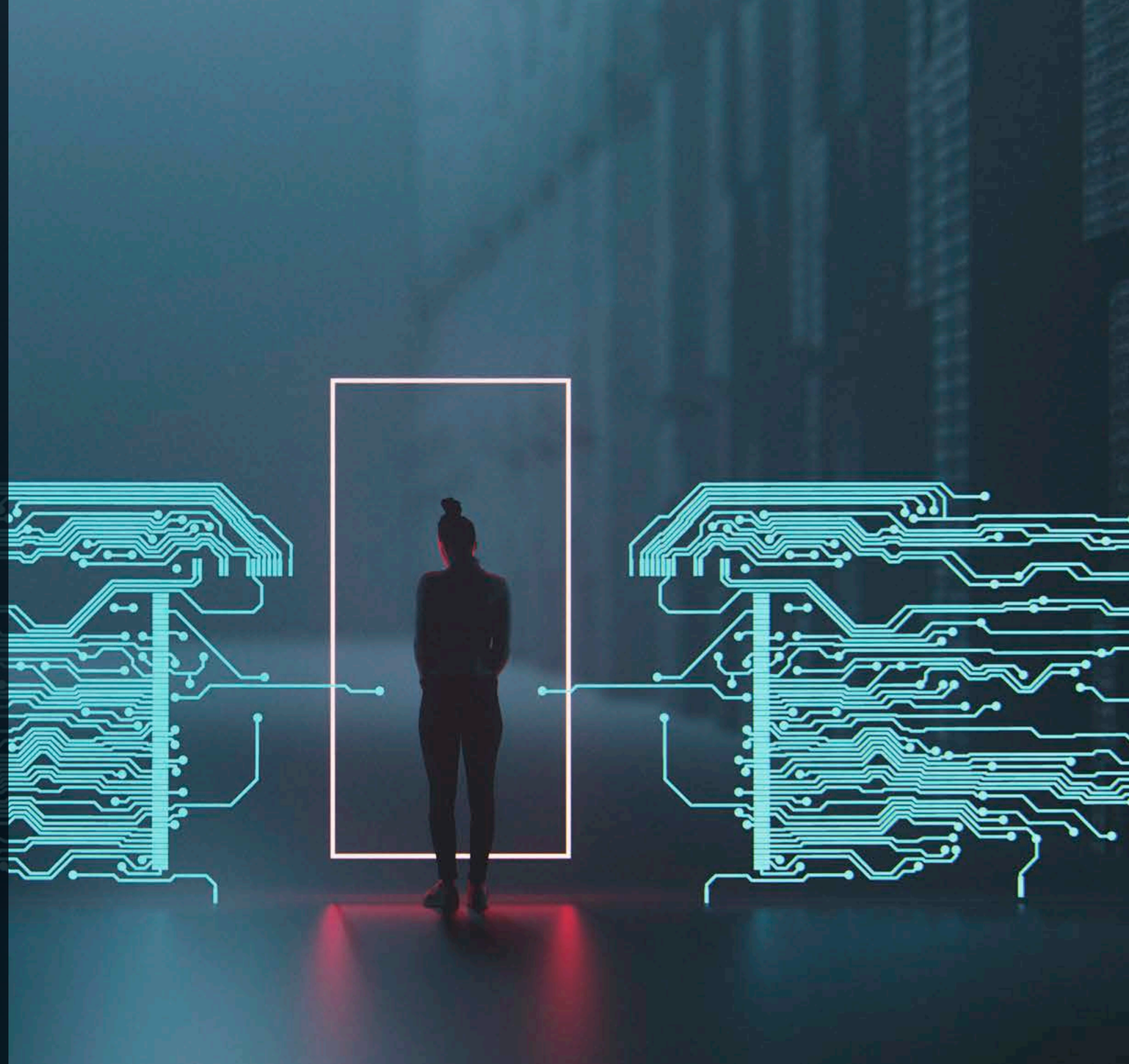
How can organizations improve vulnerability management? Security professionals have a multitude of suggestions, including establishing KPIs, metrics, and reports to help communicate performance to the business; integrating vulnerability management and other security/IT technologies; getting insight into asset exploitability, exposure, and impact on critical systems; and/or continuously updating attack surface discovery to trigger vulnerability scans.

It is also worth noting that more than one-quarter (26%) of organizations believe that automating vulnerability and patch management processes would help improve their vulnerability management programs. This is consistent with the level 5 maturity description presented previously (i.e., optimized: automated proactive controls enforce policy and standards and provide input to regular updates and training).

Actions that would most improve vulnerability management programs.

BACK TO CONTENTS

Security Testing Is Valuable but Mismanaged



Reasons for Conducting Security Testing

While some organizations perform frequent security testing, many periodically do formal penetration testing or red teaming exercises on a quarterly or biannual basis. In the past, security testing was driven by regulatory compliance or governance requirements, but like 2021, ESG's data indicates a change in motivation: Nearly half (49%) of security professionals say that their organizations conduct penetration tests/red teaming as a best practice for risk assessment, 42% conduct penetration testing after a security incident, and 41% do so at the behest of executive management and/or the board of directors.

Business partners also influence security testing as 39% of organizations conduct penetration tests to comply with third-party contracts. Finally, testing is common after another firm in the same industry has experienced a data breach (39%). This is especially true in industries like education, financial services, healthcare, and the public sector that have been the primary targets of ransomware attacks.

Primary reasons penetration tests and red teaming exercises are conducted.

49%
As a best practice for risk assessment and reduction

42%
To assess risk after a security incident

41%
Executive manager/board of director mandate

41%
Regulatory compliance requirements

39%
Third-party contracts requirements

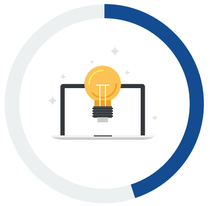
39%
To assess risk after another firm in our industry has a data breach

37%
Internal/external auditor mandate

> "In the past, security testing was driven by regulatory compliance or governance requirements, **but like 2021, ESG's data indicates a change in motivation**."

BACK TO CONTENTS

Actions the organization takes based on results from penetration tests and red teaming exercises.



45%
Uses the reports to reassess security and IT processes and cyber-risk

40%
Reviews all reports with the business, technology, and security leadership

39%
Uses the reports to help us determine if we are using any ineffective security technologies that may be candidates for elimination

37%
Creates a priority list of remediation actions

36%
Integrates with operational and software development tools to automate responses

35%
Uses the reports to justify security budgets and projects

34%
Uses the reports to help improve the efficacy of security controls

34%
Works with the development team on remediation/ engineering plans

29%
Shares all reports with third-party partners

Actions Taken Based Upon Security Testing Results

Security testing provides facts and feedback to security teams, so its value is well understood. In 2023, 46% of organizations use testing reports to reassess security and IT processes as well as cyber-risk (note: this was also the top response in 2021). In other words, security tests uncover blind spots and coverage gaps that can then be analyzed and addressed.

Additionally, 40% use security testing reports for reviews with business, technology, and security leaders. These reports can help CISOs communicate cyber-risks to executives and boards, determine priorities, and justify budgets. Beyond reinforcing security defenses, 39% use security testing to help them determine which controls can be eliminated. Finally, 37% say security testing can help them create a priority list of remediation actions.

All in all, security testing can be seen as a “Swiss Army knife,” with utility for assessing cyber-risks, prioritizing investments, and fine-tuning defenses.

BACK TO CONTENTS

Actions to Improve Security Testing

In the past, security testing was often based on advanced skills and tribal knowledge. A few senior penetration testers and/or red teamers used their own tools and methodologies to attack networks and then piece together reports and recommendations. These efforts were generally effective, but manual processes and “lone wolf” staff members can’t scale to meet today’s needs for continuous testing.

This situation is reflected in the research results. When asked how their organizations could improve security testing, 35% said by improving their ability to analyze test results and prioritize actions. It is safe to assume that these two outputs take too much work and time. Just more than one-third (34%) believe that testing could be improved by purchasing, deploying, and operationalizing attack surface management solutions. This makes sense as understanding attack surface assets and vulnerabilities is often a starting point for ethical hackers. Other suggestions include quantifying cyber-risks in monetary terms, likely as inputs for business managers, and increasing testing budgets.

Somewhat down the list, one-quarter believe that testing could be improved by creating a “purple team” model. Based on qualitative interviews conducted as primary research for this project, leading organizations are adopting this type of strategy, as it improves collaboration, knowledge, and cooperation between offensive and defensive security teams, promoting the concept of a threat-informed defense.

Actions that would most improve penetration tests and red teaming programs.

BACK TO CONTENTS

SHPM Spending Will Continue Despite Macroeconomic Pressure

SHPM Spending Priorities

Due to macroeconomic conditions, many CISOs are focused on improving foundational security requirements like SHPM. This is reflected in the fact that 85% of organizations plan to increase spending on SHPM over the next 12 to 18 months. While security hygiene and posture management spending will be sprinkled across hybrid IT infrastructure, security professionals believe the biggest increases will be in cyber-risk quantification tools (27%), security testing tools (25%), security asset management technology (e.g., CAASM, 24%), and data security tools (24%).

33% My organization will increase its spending on security hygiene and posture management significantly

54% My organization will increase its spending on security hygiene and posture management slightly

Areas of security hygiene and posture management expected to have greatest spending increase.

BACK TO CONTENTS

Actions for Improving SHPM

Finally, security professionals were asked which actions would improve security hygiene and posture management most. The results are far ranging, representing the scale and scope necessary for SHPM improvement. Nearly half (49%) suggest performing continuous security control validation, 45% recommend SHPM process automation, 42% advise increasing the staff dedicated to security hygiene and posture management, 38% propose establishing a dedicated security hygiene and posture management budget, and 37% advocate for consolidating all security hygiene and posture management data into one repository as a single source of truth.

Based on these recommendations, it seems clear that there is no silver bullet for SHPM excellence. Rather, CISOs must take a "people, process, and technology" approach with some suggestions as follows:

- **People:** Appropriate training; improved collaboration and communication across organizations; common goals, objectives, and metrics; and services for skills/staff augmentation.
- **Process:** Best practices, continuous improvement, and process automation.
- **Technology:** ASM, CAASM, risk-based vulnerability management (i.e., with threat intelligence integration), continuous automated security testing, and operationalizing the MITRE ATT&CK framework.

Actions that would most improve security hygiene and posture management.

BACK TO CONTENTS

CORTEX®
BY PALO ALTO NETWORKS

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021)and HRC Best Places for LGBTQ Equality (2022).

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

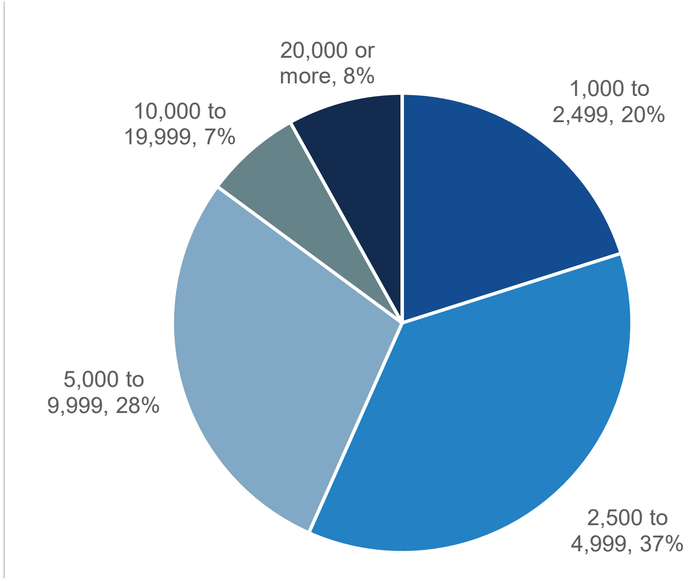
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

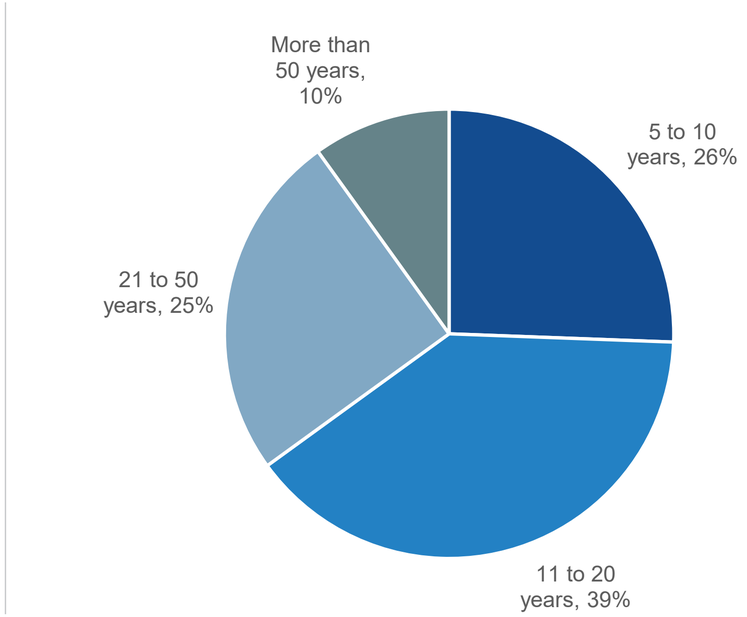
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between February 10, 2023 and February 23, 2023. To qualify for this survey, respondents were required to be responsible for evaluating, purchasing, and utilizing products and services for security hygiene and posture management, such as vulnerability management, asset management, attack surface management, security testing tools, etc. 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 383 IT and cybersecurity professionals.

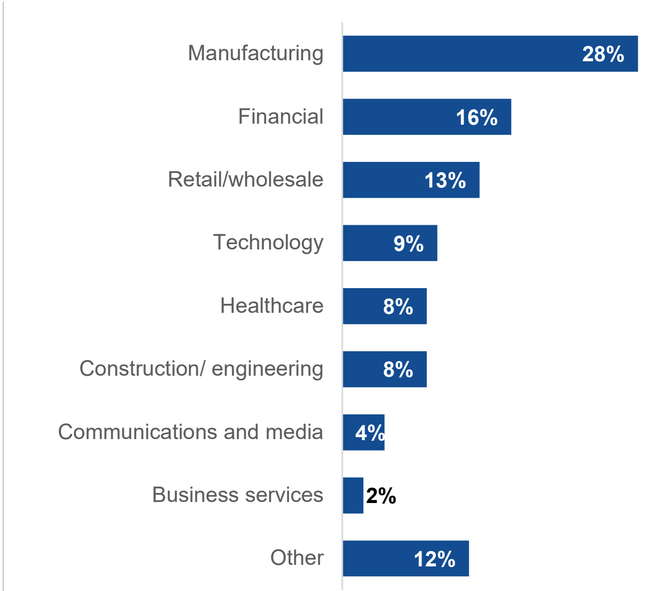
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF ORGANIZATION



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

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.