

Enterprise Strategy Group | Getting to the bigger truth.™

Security Hygiene and Posture Management

Jon Oltsik, Senior Principal Analyst & ESG Fellow

OCTOBER 2021

© 2021 TechTarget, Inc. All Rights Reserved.





Research Objectives

Security posture management challenges are driven by the growing attack surface. Organizations have accelerated cloud computing initiatives and have been forced to support a growing population of remote users as a result of the pandemic. Firms are also deploying new types of devices as part of digital transformation initiatives, further exacerbating the growing attack surface, leading to management challenges, vulnerabilities, and potential system compromises. Meanwhile, security teams are also concerned about recent cybersecurity issues including MS Exchange vulnerabilities and the SolarWinds hack. As a result, organizations are further assessing security posture management processes, examining vendor risk management requirements, and testing security more frequently.

In order to gain insights into these trends, ESG surveyed 398 IT and cybersecurity professionals at organizations in North America (US and Canada) personally 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 hygiene and posture management today.



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



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



Highlight which actions cybersecurity professionals believe their organizations should take to improve security hygiene and posture management.









KEY FINDINGS

CLICK TO FOLLOW



Security Hygiene and Posture Management Remains One of the Least Mature Areas of Cybersecurity



Security Hygiene and Posture Management Opinions

Organizations understand that security hygiene and posture management is an essential element of an enterprise security program. The research reinforces this point. For example, 86% of organizations believe that they follow best practices for security hygiene and posture management, and 84% report that they prioritize security hygiene and posture management actions on business-critical assets.

Unfortunately, the research also uncovers numerous security hygiene and posture management obstacles. For example, 70% of organizations have more than ten security tools to manage security hygiene and posture management, which can only lead to data management issues and operations overhead. Furthermore, 73% of security professionals admit that security hygiene and posture management still depends on spreadsheets at their organization. Little wonder then why 70% of respondents say that security hygiene and posture management has become more difficult over the past 2 years.

practices for security hygiene and posture management."

Organizations' positions regarding security hygiene and posture management.



100%

5

Security Hygiene and Posture Management Metrics

The research indicates that organizations measure security hygiene and posture management success in numerous ways. For example, 38% of organizations point to vulnerability scanning coverage as a percentage of all internal/external IT assets as one of their most important security hygiene and posture management metrics, 36% cite cyber-risks calculated in monetary terms, and 32% believe that attack surface discovery coverage as a percentage of all internal/external IT assets is a valuable gauge.

While each of these metrics is important on its own, the data demonstrates that many organizations continue to address security hygiene and posture management tactically on a technology-bytechnology basis. ESG believes that CISOs should take a more holistic approach to security hygiene and posture management by adopting technologies and processes for discovering assets, analyzing data, prioritizing risks, automating remediation tasks, and continuously testing security defenses at scale. These requirements are driving a new security technology category: security observability, prioritization, and validation (SOPV).

Most important security hygiene and posture management metrics.





6



The External Attack Surface Is Vulnerable and Prone to Exploitation



External Attack Surface Discovery Drivers Include Regulations, Threats, and Attack Surface Dynamics

While nearly half (49%) of organizations undertake attack surface management for regulator compliance, they also recognize other reasons to do so. For example, 46% say they perform attack surface management to reduce the risk of a ransomware attack, 43% claim they need to discover external assets in order to calculate risk and apply the right security controls, and 40% do so because the attack surface if frequently changing. These are sound reasons, but CISOs must also understand that adversaries may be continuously scanning their organization's attack surface with automated tools as part of the reconnaissance phase of cyber-attacks. Therefore, attractive target organizations should strive to safeguard internetfacing assets and reduce their attack surface, thus increasing the work and needed resources for cyber-adversaries.

Drivers for external attack surface discovery.

We are required to perform external attack surface discovery as part of regulatory compliance We need to reduce risk of a ransomware attack We need to discover the external assets in order to calculate risk and apply the right security controls Our attack surface is expanding The assets in our attack surface are frequently changing We believe low priority assets are more susceptible to malicious attack We believe unknown assets are more susceptible to malicious attack We believe our organization's current asset inventory is incomplete None of the above 1%



G G CISOs must also understand that adversaries may be continuously scanning their organization's attack surface with automated tools as part of the reconnaissance phase of cyber-attacks.'



8

Reasons the Attack Surface Is Increasing

It's safe to assume that attack surface management is growing more difficult. Why? Two-thirds (67%) of organizations say that their attack surface has increased over the past two years. The research also revealed that the largest attack surfaces are growing fastest. From a security perspective, it's safe to conclude, "more assets, more problems."

Why is the attack surface growing so quickly? Nearly one-third (32%) pointed to three common reasons: more IT connections to third parties, increasing device diversity, and greater use of public cloud infrastructure. Additionally, 30% of organizations have increased their use of SaaS applications/services. To secure this growing attack surface, organizations need visibility and continuous monitoring across hybrid IT, third-party connections, remote worker devices, and all other types of internet-facing systems and services.



22%, The attack surface at my organization has increased substantially over the past 2 years

45%, The attack surface at my organization has increased slightly over the past 2 years

Primary reasons attack surface has increased.

My organization has increased user device type diversity

My organization has increased its IT connections with third parties My organization has increased its use of public cloud infrastructure

My organization has increased its use of SaaS applications/services

My organization has increased its remote worker population

My organization made changes to its technology infrastructure necessitated by privacy and security regulations

My organization has increased the use of IoT/OT devices

My organization has increased its number of users connecting to networks and applications

My organization has increased the amount of sensitive data that needs to be stored, monitored, and protected

> My organization has increased the pace of application development/deployment

My organization has grown through mergers/acquisitions



Back to Contents

Assets Exposed as Part of **Attack Surface Discovery**

Like other areas of security hygiene and posture management, organizations rely on an assortment of tools for attack surface management and monitoring. While extracting, normalizing, and analyzing data from different systems can be resource-intensive and introduce operational overhead, security professionals admit that their organizations have discovered many vulnerable internet-facing assets. Nearly one-third (31%) discovered sensitive data in a previously unknown location, 30% found websites with a path to their organization, 29% uncovered employee corporate credentials/misconfigured user permissions/ entitlements, and 28% exposed previously unknown SaaS applications. Other exposed assets included misconfigured SSL certificates, weak encryption ciphers, code fragments, unknown third-party connections, and forgotten subdomains.

Sensitive data in a previously unknown location Previously unknown SaaS applications Applications/systems with zero users Misconfigured SSL certificates Weak or outdated encryption ciphers Third-party connections we were previously unaware of Servers/workloads/APIs with open access Code fragments exposed on webpages Previously unknown cloud workloads Misconfigured systems Forgotten subdomains Compliance drift

Websites with a direct or indirect path to our organization Employee corporate credentials/misconfigured user permissions or entitlements SSL certificates used across multiple servers/applications Previously unknown assets connected to the corporate network Unmanaged corporate assets or assets with no known business purpose

Discoveries attributed to external attack surface monitoring.





Attacks Emanating from an Internet-facing Asset

ESG's research reaches an ominous conclusion: Attack surface vulnerabilities can open a door for cyber-attacks. Nearly seven in ten (69%) organizations admit that they have experienced at least one cyber-attack that started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset. Additionally, organizations with the most IT assets, and subsequently largest attack surfaces, were almost twice as likely to experience several of these cyber-attacks. This data alone should persuade CISOs to assess the effectiveness of their current attack surface management programs.

Have organizations experienced attacks tied to internet-facing assets?





Nearly 7 in 10

organizations admit that they have experienced at least one cyber-attack that started through the exploit of an unknown, unmanaged, or poorly managed internetfacing asset.



11

Asset Management Depends Upon Tools, Processes, and **Cross-department Cooperation**



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 (59%), endpoint security tools (50%), cloud security posture management (46%), network scanning (39%), and endpoint management systems (35%).

Nearly half (48%) of organizations claim that it takes more than 80 person-hours to conduct a full security asset inventory, and most organizations (79%) perform full security asset inventories once per month or less frequently.

ON AVERAGE, ORGANIZATIONS:





Devote 89

person-hours to generate an IT asset inventory.



Endpoint security Network scanning **Endpoint management** Network access controls General cloud logs Network directories Spreadsheets CMDB tools

IT asset management systems Vulnerability scanning/assessment tools Configuration and patch management Vendor-specific management systems

Cloud security posture management tools External attack surface management platform

Tools/systems used as part of organizations' IT asset inventory process.





Security Asset Management Challenges

The combination of multiple data sources and time-consuming processes results in numerous security asset management challenges. Forty-four percent of organizations claim that establishing an inventory of hybrid IT assets involves different organizations, which makes it difficult to coordinate activities, 40% say that conflicting data makes it difficult to get an accurate picture of assets, and 39% report that it is difficult to keep up with thousands of changing assets. It is also noteworthy that one-third of organizations depend on manual processes, making it difficult if not impossible to do security asset management at scale.

When asked to identify the types of assets to track and inventory, more than one-third (34%) of security professionals identified software (i.e., software misconfigurations, coding errors, vulnerabilities, etc.), 30% recognized cloud-based workloads, 30% acknowledged user accounts, 28% pointed to user entitlements, and 27% said loT devices.

Challenges understanding IT asset inventory.



Back to Contents

Actions for Improving Security Asset Management

Survey respondents were asked how their organizations could improve security asset management. Nearly one-third (31%) said this could be accomplished by automating security asset management processes, 28% suggested integrating security and IT tools, 27% recommended establishing business-centric KPIs, metrics, and reports, and 24% mentioned improving their organization's ability to analyze risk scores to help them determine which assets are truly at risk.

Overall, the data suggests that security asset management programs are likely informal, disorganized, and immature. Organizations would benefit from greater integration technology, advanced analytics, and process automation here. Actions likeliest to improve security asset management programs.

Automating tasks/processes associated with security asset management

Establishing KPIs, metrics, and reports that could help communicate the importance of security asset management to the business

Improving our ability to analyze and assign risk scores to asset attributes

Purchasing/deploying new types of tools designed for security asset management

Improving collaboration around security asset management between security and IT teams

Increasing the frequency of security asset management inventories

Increasing the staff dedicated for security asset management

Providing more asset management training to security and IT staff

Using managed services for some or all aspects of vulnerability management

Gaining visibility into security control performance

Establishing a dedicated budget for security asset management

Establishing more granular baselines and policies for asset integrity



Integrating security and IT tools

Formalizing policies/processes

15

Organizations Believe Their Vulnerability Management Programs Are Mature, but There Is Still Work to Be Done



Volume of Process Coordination Most Common Vulnerability Management Challenge

When asked to identify vulnerability management challenges, 30% said keeping up with the volume of open vulnerabilities, 29% said automating the process of vulnerability discovery, prioritization, dispatch to owner, and mitigation, 29% said coordinating vulnerability management processes across different tools, and 28% said coordinating vulnerability management processes across different teams.

Biggest vulnerability management challenges.

Keeping up with the volume of open vulnerabilities Coordinating vulnerability management processes across different tools Coordinating vulnerability management processes across different teams Analyzing the results of vulnerability scans Identifying all assets that need to be scanned mean time to patch) Prioritizing which vulnerabilities could be exploited and should be prioritized for remediation Tracking the cost and efficiency of the vulnerability management program Coordinating vulnerability scans across multiple scanning engines Tracking vulnerability and patch management over time Patching vulnerabilities in a timely manner Lack of understanding of business risk due to vulnerabilities Conducting/scheduling vulnerability scans

Automating the process of vulnerability discovery, prioritization, dispatch to owner, and mitigation

Tracking software vulnerabilities for which no patch is available or that cannot be patched (measuring Inability to understand asset exploitability, exposure, and impact on critical systems in our environment



Back to Contents



Determining Patching Priorities

Upon scanning and vulnerability identification, security teams analyze the data and then determine which vulnerabilities should be remediated first. How do organizations make these prioritization decisions? The research seems to indicate that individual organizations have multiple inputs for decision making. For example, 34% make patching priority decisions based on their use of specific vendor products, 31% do so based upon those vulnerabilities classified as "critical" by software vendors, and 30% use regulatory compliance guidelines. Interestingly, 20% say that they base prioritization and patching decisions on CVSS scores. While this seems to be a secondary consideration, ESG's experience is that CVSS scores are included in all vulnerability prioritization and patching decisions.

It is also noteworthy that 29% say that vulnerability prioritization and patching decisions are driven by risk scores from a dedicated risk-based vulnerability management system. These tools analyze vulnerability data as it relates to other factors like asset value, connections, threat intelligence on adversary TTPs, and whether vulnerabilities have a history of exploitation. Risk-based vulnerability management tools are gaining in popularity as they can help organizations streamline vulnerability and patch management operations while maximizing risk mitigation.



Approaches to vulnerability prioritization and patching.



Based on our use of specific vendor products

Based upon those vulnerabilities classified as "critical" by our software vendors

Based on regulatory compliance requirements

Based upon a risk score from a dedicated risk-based vulnerability management tool

Based on a risk score from an external attack surface management system

Based upon whether a vulnerable asset has a direct connection to business-critical applications or data

Based upon a risk scoring system within our vulnerability management tools

Based on an assessment of contextual security control performance data in our environment

Based upon where a vulnerable asset is located

Based upon vulnerabilities that have been exploited

Based on asset classification

Based on what attackers would find most attractive

Based on a vendor's patching schedule

Based on CVSS score

34%

Improving Vulnerability Management

How can organizations improve vulnerability management? Security professionals have a multitude of suggestions, including integrating VMs and other security/IT technologies (35%), establishing KPIs, metrics, and reports to help communicate VM performance to the business (30%), and providing VM training to security and IT personnel (28%).

Two other suggestions stand out: 28% recommend gaining insight into asset exploitability, exposure, and impact on critical systems to understand the underlying business risk posed by critical visibility. This means correlating VM and asset data with threat intelligence, a nod toward commercial risk-based vulnerability management technologies that provide this functionality. Additionally, 28% propose continuously updating the external attack surface inventory so they can perform more accurate and timely vulnerability scans. Once attack surface management tools discover and analyze unknown assets, VM tools should be triggered to immediately scan these assets, analyze cyber-risks, and provide suggestions for remediation prioritization.

Top five actions to improve vulnerability management programs.



35%

Integrating vulnerability management and other security and IT technologies



30%

Establishing KPIs, metrics, and reports that could help communicate the importance of vulnerability management to the business





28%

Providing more vulnerability management training to security and IT staff



28%

Gaining insight into asset exploitability, exposure, and impact on critical systems to understand underlying business risk posed by critical vulnerabilities



28%

Continuously update the external attack surface inventory so we can perform more accurate and timely vulnerability scans

Back to Contents

While the Value of Security Testing Is Well Understood, Frequency and Depth Remain Underserved



Why Conduct 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 the ESG data seems to indicate a change in motivation as nearly half (47%) of security professionals say that their organizations conduct penetration tests/red teaming as a best practice for risk assessment, 39% conduct penetration testing after a security incident, and 38% do so at the behest of executive management and/or the board of directors.

It is also noteworthy that over one-third (35%) of organizations conduct penetration tests after another firm in their industry has experienced a data breach. This is especially true in industries like education, financial services, healthcare, and the public sector that have been the primary targets of ransomware attacks.

F Nearly half (47%) of security professionals say that their organizations conduct penetration tests/red teaming as a best practice for risk assessment."

Primary reasons for conducting penetration tests and red team exercises.

We believe that penetration testing/red team exercises are a best practice for risk assessment and reduction

We conduct penetration testing after experiencing some type of security incident in order to assess risk

Executive managers/board of directors mandate that we do so

We are required to do so for regulatory compliance

We conduct penetration testing after another firm in our industry has experienced a data breach

We are required to do so as part of third-party contracts

Internal/external auditors mandate that we do so





21



Actions Taken as a Result of **Security Testing**

Security testing provides facts and feedback to security teams, so its value is well understood. For example, 46% of organizations use testing reports to reassess security and IT processes as well as cyber-risk. In other words, security tests uncover previously unknown blind spots and gaps that can then be addressed. Additionally, 38% use security testing to help them improve the efficacy of security controls, and 37% review testing reports with leadership teams.

It's also worth noting that 36% use testing to determine ineffective security controls for elimination. Over the years, many organizations accumulated dozens of security tools that may be redundant with one another or ineffective against modern threats. Security testing can uncover these inefficiencies, helping organizations simplify their security infrastructure while bolstering security efficacy.

By identifying outstanding cyber-risks and defense gaps, security testing can also help organizations pinpoint and prioritize security investments. This is precisely why 31% of organizations use security testing reports to justify security budgets and projects.

Actions the organization takes based on penetration tests and red team exercises.







BAS Technology Facilitates Purple Teams and Automated Testing

To make the best use of security testing benefits while minimizing management overhead, some organizations are considering breach and attack simulation (BAS), a technology that can emulate adversary behavior through automated testing. In fact, the ESG research seems to indicate that BAS is becoming increasingly attractive as 27% of organizations say they are already using BAS technology, 52% claim it is very likely they will purchase and utilize BAS technology in the future, and another 18% believe it is somewhat likely they will adopt a BAS solution.

Why are organizations open to BAS? More than one-third (38%) believe BAS presents a compelling option due to its ability to help them establish a "purple team" security methodology. In other words, BAS can help red teams (i.e., adversary emulators) and blue teams (i.e., security defenders) better understand each other and then work together on collaborative solutions.



Additionally, 38% believe BAS can provide automated testing to help them rationalize and consolidate existing security technologies. In this way, BAS can uncover which controls work best, helping organizations eliminate redundant or ineffective tools, thus engineering simpler yet stronger defenses. BAS can also help organizations identify coverage gaps (i.e., missing controls and data sources) (34%) and test the effectiveness of new security technologies (34%). BAS can also add value by integrating with attack surface management systems to help organizations understand whether exposed internet-facing assets could truly be used as part of a cyber-attack (33%). Finally, 30% of security professionals believe that BAS can help them map security testing with the MITRE ATT&CK framework. In other words, BAS can help organizations emulate known attack campaigns, assess controls as they relate to adversary TTPs, and build a threat-informed defense.

Top five reasons attack surface has increased.



34%

34%

33%



23



Organizations Will Move Toward Security Observability, Prioritization, and Validation (SOPV) Technologies



Security Hygiene and Posture Management Budget

How do organizations allocate funds for security hygiene and posture management budgets? The majority (65%) use funding from other areas like the IT budget, a vulnerability management budget, the regulatory compliance budget, or an application security budget. Alternatively, just more than one-third (34%) of organizations have created a dedicated budget for security hygiene and posture management. ESG believes that a dedicated security hygiene and posture management budget is a leading indicator of market behavior. As attack surfaces increase and organizations suffer more security incidents as a result, they will realize the need for a comprehensive and holistic strategy. This recognition will then serve as a tipping point from tactical and haphazard actions to a strategic security hygiene and posture management program.

Source of budget for security hygiene and posture management.



25

Following the Security Hygiene and Posture Management Money

In addition to the creation of a dedicated budget, this research indicates that CISOs are already focused on improving cyber-risk identification and mitigation through security hygiene and posture management. In fact, 80% of organizations plan to increase security hygiene and posture management spending 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 data security tools (i.e., data discovery, classification, DLP controls, digital rights management, etc.) (31%), cyber-risk quantification tools (30%), cloud security posture management (i.e., CSPM) (28%), security asset management (21%), and external attack surface management technology (20%).

6 6 80% of organizations plan to increase spending for security hygiene and posture management over the next 12-18 months."

Spending priorities for security hygiene and posture management.

Data security tools Cyber-risk quantification tools 30% Cloud security posture management 28% Security asset management 21% External attack surface management 20% Vulnerability scanning 19% Application security 16% Third-party risk management 16% Penetration testing tools/services 16% Identity and access management tools 16% Breach and attack simulation tools 16% Training 13% Red teaming tools/services 12% Asset management 11% **Deception technology** 10% Personnel 10% Crowdsourcing services 9%



Actions for Improving Security Hygiene and Posture Management

Aside from increased budgets, security professionals offered several suggestions for how their organizations can improve security hygiene and posture management. Consistent with the interest in BAS technology, 38% recommend performing continuous security controls validation to discover gaps in existing security tools and perform prompt remedial actions to harden security posture. Furthermore, 36% suggest automating security hygiene and posture management processes, 35% propose deploying a dedicated tool for security/ IT asset management, and 31% advocate for increasing the staff dedicated to security hygiene and posture management.

Top ten steps to improve security hygiene and posture management.

Performing continuous security control validation to discover gaps in existing security tools and

Automating processes associated with security hygiene and posture management Deploying a dedicated tool for security/IT asset management that can interoperate and pull data

Increasing the staff dedicated to security hygiene and posture management

Deploying attack surface management technology that can discover and test internet-exposed assets and can alert/prioritize associated cyber-risks

Taking a more adversarial/offensive approach to cybersecurity so we can adjust our defenses as countermeasures to modern attack TTPs

Increase executive awareness of the value of security hygiene and posture management

Increasing integration of the MITRE ATT&CK framework into our cybersecurity strategy

Consolidating all security hygiene and posture management data into a single repository as a single source of truth



from other existing systems

Identify and engage cyber-risk owners



JupiterOne

JupiterOne is a cyber asset management and governance solution company, providing visibility and security into your entire cyber asset universe. JupiterOne creates a contextual knowledge base using graphs and relationships as the single source of truth for an organization's cyber asset operations. With JupiterOne, teams can discover, monitor, understand, and act on changes in their digital environments. Cloud resources, ephemeral devices, identities, access rights, code, pull requests, and much more are collected, graphed, and monitored automatically by JupiterOne.

LEARN MORE

ABOUT ESG

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.

© 2021 TechTarget, Inc. All Rights Reserved.



Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between August 3, 2021 and August 14, 2021. To qualify for this survey, respondents were required to be IT or cybersecurity professionals 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. 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 398 IT and cybersecurity professionals.



RESPONDENTS BY INDUSTRY





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

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



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.

© 2021 TechTarget, Inc. All Rights Reserved.