CYCOGNITO

RESEARCH REPORT

The State of External Attack Surface and Risk Management

How Modern EASM Technology Closes the Gap between Attackers and Defenders

IT ecosystems continue to evolve towards greater complexity. As they do, discovering and remediating the highest-risk vulnerabilities becomes more and more difficult. How are today's IT and security teams meeting the challenge?

Introduction

For all the talk about how insider threats are devastating, the reality is that the vast majority of today's data breaches are perpetrated by external attackers — at least 80% of them, according to the Verizon Data Breach Investigations Report (DBIR).[1] What's more, many of these attacks target the external attack surface — those IT systems and applications that are accessible via the internet. Often, these are the least visible and protected parts of an organization's IT ecosystem: nearly 70% of organizations have experienced at least one cyberattack that began with the compromise of an unknown, unmanaged or poorly managed internet-exposed asset.[2]

To learn more about the challenges organizations face in monitoring and managing the external attack surface to reduce these risks, we recently surveyed 329 IT and security professionals in the US, UK and Canada. All respondents had significant hands-on experience triaging, remediating and validating the remediation of Common Vulnerabilities and Exposures (CVEs) and/or supervising teams responsible for doing so. We wanted to learn about participants' attitudes and perceptions regarding their organizations' attack surface and their ability to manage it.

Key Takeaways

- **Increased visibility into externally exposed risk is a critical requirement.** More than nine out of ten respondents reported that their organization had experienced at least one incident in the past year resulting from the exploitation of an unpatched vulnerability. Ninety-eight percent (98%) of survey participants agreed that increased investment in attack surface reduction would significantly improve their organization's security and risk posture.

- **Organizations struggle to uncover vulnerabilities in a timely fashion.** When presented with a list of vulnerability management capabilities, survey participants rated their ability to discover vulnerabilities lowest of all the available options. More than nine in ten survey participants (92%) believe that there's significant room for improving their use of automated technologies to discover and test for vulnerabilities.

- **Web application security testing is underutilized in many organizations.** When asked which vulnerability and attack surface management technologies they were planning to implement, organizations were most likely to indicate that they had plans to add dynamic application security testing (DAST) (21% of respondents).

- **Remediation prioritization is often misguided.** Most survey participants are using the simplest techniques — counting and timing — to set their vulnerability remediation priorities.

- **Remediation validation remains a challenge.** A large majority of respondents (89%) believe that increasing automation would improve their ability to verify that vulnerability remediation efforts were successful.

- **External attack surface management (EASM) investments are growing.** Security leaders are planning to invest in technologies to improve this situation. Sixty-two percent (62%) of respondents plan to add an external attack surface management (EASM) solution or upgrade what they currently have in place; 63% plan to add or upgrade dynamic application security testing (DAST).

[1] Verizon, 2022 Data Breach Investigations Report.
[2] Enterprise Strategy Group, Security Hygiene and Posture Management, 2022.

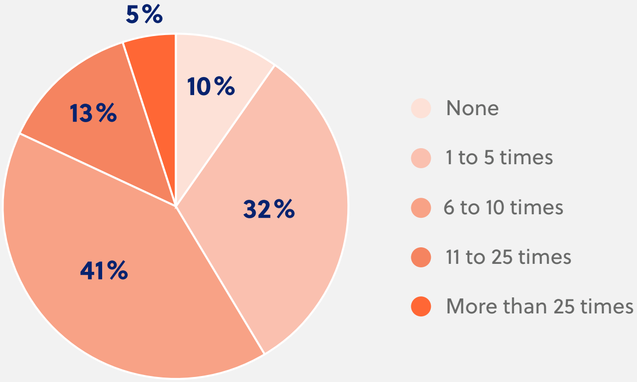
Results and Analysis

Results from this survey reveal how IT and security teams are approaching external attack surface management today.

How many organizations are experiencing breaches or security incidents because of poor management of their external attack surface?

Unfortunately, breaches related to poor management of the external attack surface are all too common. More than 90% of survey participants experienced an incident or compromise due to an unpatched vulnerability.

Figure 1: Occurrence of incidents resulting from known, unremediated vulnerabilities



In the past 12 months, how many security incidents at your organization were the result of a known, open vulnerability (i.e., one that had not yet been remediated)?

It's clear that open vulnerabilities create significant security risks for today's organizations and attackers are actively exploiting these vulnerabilities. More than nine out of ten survey participants had experienced at least one incident in the past year that resulted from a known vulnerability that had not been patched.

In addition, nearly six out of every ten respondents (59%) had experienced more than five security incidents resulting from open vulnerabilities over the past year. This finding is in line with those of other industry researchers. The Verizon DBIR, for instance, noted that the number of breaches attributable to vulnerability exploitation had doubled in the past year, growing to seven percent of the 20,000 breaches examined in the study.[3]

Verizon also found that breached organizations had an average of 50 known but unpatched vulnerabilities per host within their IT ecosystem. For attackers, it's simply a numbers game — they'll keep scanning internet-facing assets until they can find one through which they can obtain some sort of access. It's just a matter of time until they succeed.

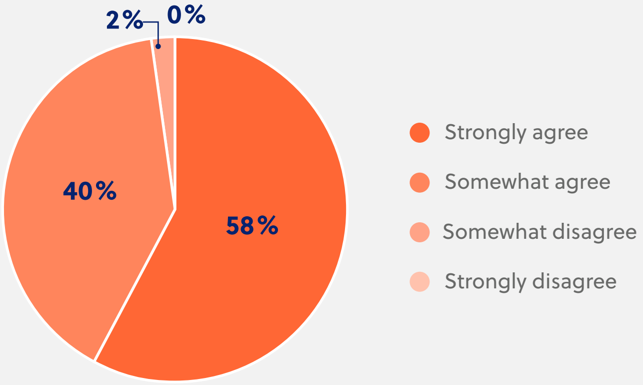
[3] Verizon, 2022 Data Breach Investigations Report.

How important is attack surface risk reduction to today's stakeholders?

Nearly all survey participants agree that investments in attack surface reduction would benefit their enterprises. As we'll see as we move deeper into this report, however, there's no universally agreed-upon solution that promises to achieve this aim.

Figure 2: Reducing attack surface risk matters

Describe your agreement with this statement: "Increased investment in attack surface reduction — for example, by finding and remediating open vulnerabilities — would significantly improve my organization's security and risk posture."



Improving their ability to manage the attack surface is important to survey participants. The vast majority (98%) generally agreed that reducing their organization's attack surface would significantly improve its security and risk posture.

It's clear that respondents in organizations of all sizes feel that there's significant value to be gained from attack surface reduction.

What is external attack surface management?

Attack surface management is the process of discovering, classifying and assessing the security of an IT ecosystem. This can incorporate activities performed to discover and manage internet-exposed assets, a process known as external attack surface management (EASM) or it can include activities performed on assets only accessible from within the organization, or both.

Many organizations use an assortment of tools and manual processes to secure their attack surface. This leads to operational complexity, human error and best-guess analyses. Today, better solutions exist.

Attack Surface Management Processes, Technologies and Challenges

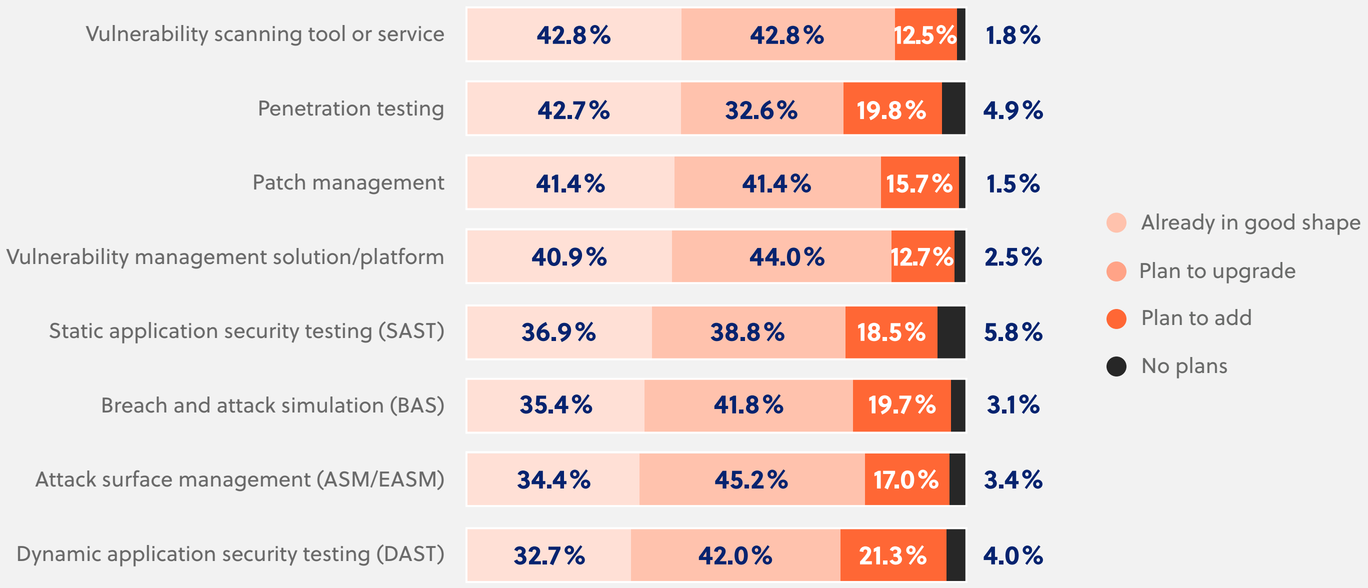
Far too many enterprise security teams continue to rely on manual processes and legacy vulnerability scanners to discover open vulnerabilities. Even more of them lack consistent, automated tools for remediating these vulnerabilities — and validation and testing to make sure their efforts were successful.

What tools are today's organizations using to find vulnerabilities and manage the attack surface?

It's no surprise that different companies rely on different solutions. What *is* eye-opening, though, is how wide the assortment of strategies and solutions is across various organizations, and how many still rely on inefficient manual processes in this area — especially considering how often attackers are leveraging automation.

Figure 3: The vulnerability and attack surface management technologies that enterprises rely on

Which of the following vulnerability and attack surface management technologies are currently in use, or planned for upgrade or initial use by your organization within the next 12 months?



Security programs currently rely on a broad array of technologies to identify and remediate vulnerabilities and verify whether these efforts were successful. The most commonly-employed technologies include vulnerability scanners, penetration tests, patch management solutions and vulnerability management platforms.

In none of the above-listed areas, however, did a majority of respondents say that they were already "in good shape." Even with vulnerability scanning, the most widely-implemented technology, more than half of survey participants (57%) said that they were not yet "in good shape." 43% said they planned to upgrade their vulnerability scanning tool or service (presumably meaning that they have a solution in place but aren't satisfied with its performance) and 13% said they plan to add a new vulnerability scanning solution.

Among the solutions we asked about, organizations were most likely to say that they were planning to add dynamic application security testing (DAST) (21% planning to add), breach and attack simulation (BAS) (20% planning to add), static application security testing (SAST) (19% planning to add) and attack surface management (ASM) (17% planning to add).

However, many of these solutions fall within emerging market categories, and it's not clear whether or not all respondents' understanding of what the solutions actually encompass — and how they stack up in terms of capabilities — are similar.

It's also noteworthy that survey respondents said the technology solution they were most likely to upgrade was attack surface management (ASM). It's possible that significant numbers of respondents are interested in moving away from legacy tools and outdated manual processes, and towards modern, automated solutions for managing the external attack surface.

Vulnerability and attack surface management technologies

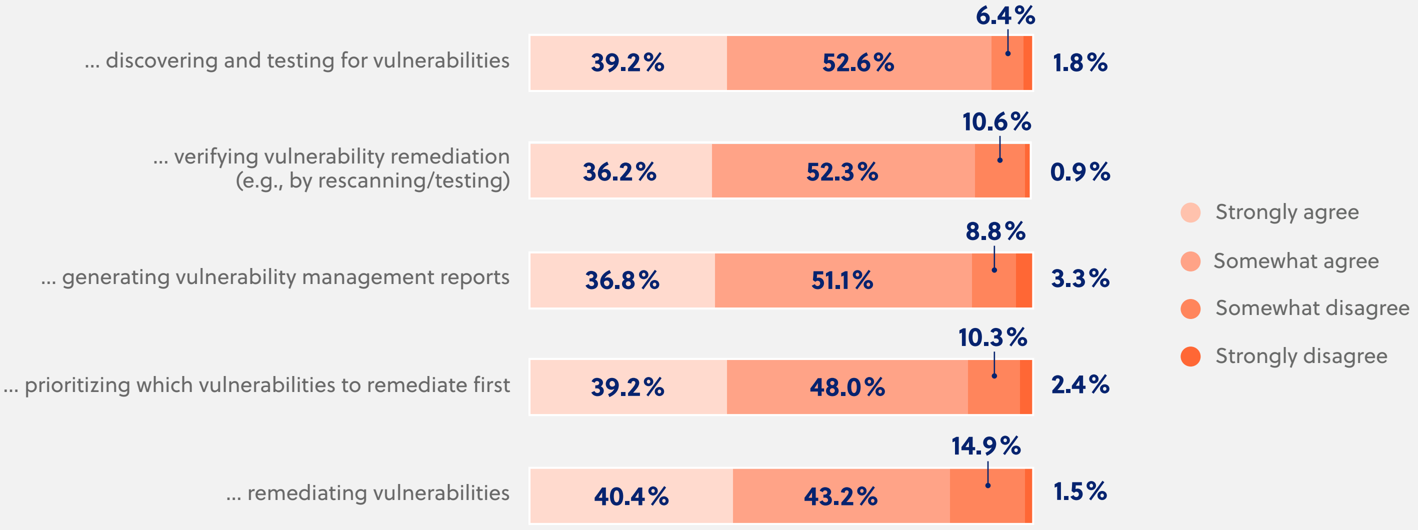
- **Vulnerability scanning.** A vulnerability scanning solution or service compares details about a target's attack surface with information about known vulnerabilities in software, services and ports. In some cases, the scanner may attempt to exploit each vulnerability that it discovers.
- **Vulnerability management solutions/platforms.** A vulnerability management platform goes beyond vulnerability scanning or merely applying software patches. Depending on the solution in question, it might scan to discover vulnerabilities, rank them according to some measure of risk (typically CVE scores), remediate some or all of them and report on the results.
- **Penetration testing.** One of the oldest and best-known tools used by security teams, penetration tests (also known as pen tests) are attack simulations carried out by ethical hackers, who mimic the tactics and strategies an attacker might use to compromise an organization's systems, network or applications.
- **Patch management.** Many organizations rely on automated tools to help them acquire, install and test the patches (software updates) that the systems and applications in their environment require on a regular basis.
- **Breach and Attack Simulation (BAS).** These tools enable enterprises to simulate cyberattacks (including insider threats, lateral movement and data exfiltration) targeting security-related assets such as web application firewalls, secure email gateways and web gateways.
- **External Attack Surface Management (EASM).** Solutions in this emerging market category continuously survey and test the entire attack surface, performing ongoing reconnaissance across it from an attacker's point of view, identifying and prioritizing risks across all assets in your environment — even ones you might not have known about beforehand.
- **Static Application Security Testing (SAST).** This is a commonly-used development tool that scans an application's source code in order to identify the root causes of vulnerabilities and help developers remediate them.
- **Dynamic Application Security Testing (DAST).** This is a methodology for analyzing web applications to find vulnerabilities within them by performing simulated attacks on their front end. This method does not require access to the application's source code.

How well are today's security programs leveraging automation to manage attack surfaces?

There's room for improvement. Most respondents agree that more automation would be beneficial across all aspects of vulnerability management.

Figure 4: Attitudes towards increasing the use of automation in vulnerability management

Describe your agreement with the following statements as they pertain to your organization: "There is significant room for improvement when it comes to the degree of automation we have for..."



Respondents broadly agree that more automation is needed throughout all parts of the vulnerability management process. More than nine in ten survey participants (92%) believe that there's significant room for improving their use of automated technologies to discover and test for vulnerabilities.

However, over 85% also believe that increasing automation would improve their ability to verify that vulnerability remediation was successful (89%), report on vulnerability management (88%), and prioritize which vulnerabilities to remediate first (87%). Even for the least-frequently cited use case for automation, remediating vulnerabilities, more than eight in ten respondents (84%) agreed that there was significant room for improvement in their organization's capabilities.

Automating attack surface management

Today's attackers are increasingly making use of automation in their reconnaissance techniques. A modern external attack surface management solution that leverages the same techniques can quickly and efficiently discover assets that IT/security teams would otherwise miss. Automation also enables ongoing and continuous attack surface testing, which is critical in today's dynamic and ever-changing IT ecosystems. Point-in-time scans can no longer keep pace. Automation can also facilitate and streamline information exchange between the teams responsible for assessing and prioritizing risks (typically SecOps) and those responsible for applying software patches (typically IT operations).

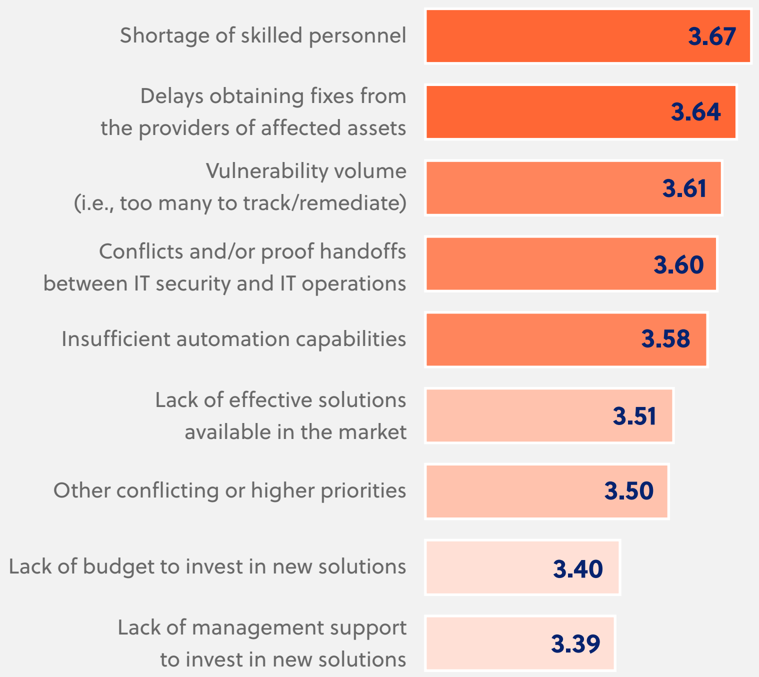
In general, the benefits of automation are well understood by today's security stakeholders, who know that it can help them operate efficiently in the face of talent shortages (which remain a perennial problem) and the need to accomplish more in less time.

What other challenges do security programs face in decreasing attack surfaces?

In this, as in all areas of cybersecurity, the skills shortage is a perennial problem. But delays in obtaining fixes from software vendors also slow vulnerability management teams down, and the fact that an enormous number of vulnerabilities continue to be discovered on an ongoing basis makes it difficult to prioritize.

Figure 5: Obstacles to reducing the attack surface

On a scale of 1 (not at all) to 5 (very significantly), rate how each of the following inhibits your organization's ability to effectively reduce its attack surface by finding and remediating open vulnerabilities:



It's unsurprising that staffing shortages were the inhibitor that was most often cited by survey participants. After all, the most recent Cybersecurity Workforce Study conducted by (ISC)² revealed that more than 2.7 million positions in the field remained unfilled worldwide as of late 2021.[4]

But other inhibitors were also prominent. Software vendors are notoriously slow to release patches for known vulnerabilities in their products as well, with vendors particularly likely to delay release of fixes for vulnerabilities that have not been disclosed to the public. Plus, the sheer volume of disclosed vulnerabilities remains a problem. Over the past ten years, the number of CVEs published annually has more than doubled, from 4,819 in 2011 to 11,463 in 2021.[5] In addition, the percentage of vulnerabilities assigned a CVSS score of 9 or 10 has continued to climb as well.[6]

Many organizations also struggle with internal allocation of responsibilities. Poor handoffs between security and IT operations teams often slow vulnerability remediation and impede attack surface management.

[4] (ISC)², (ISC)² Cybersecurity Workforce Study, 2021.

[5] Kenna Security, Kenna Research: A Decade of Insights, 2020.

[6] CVE Details, Current CVS Score Distribution for All Vulnerabilities.

Attack Surface Management Metrics

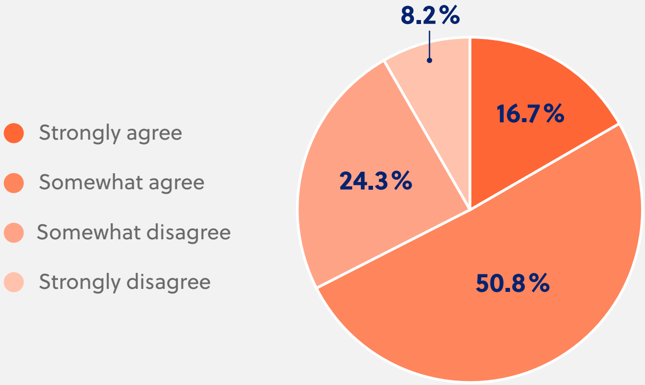
Many organizations struggle to report on risk exposure due to open vulnerabilities in a timely fashion, while they're also challenged to find the right metrics to use in this type of reporting.

Could organizations be doing a better job of reporting on risk exposure due to unpatched vulnerabilities as well as remediation progress?

It certainly seems that they could.

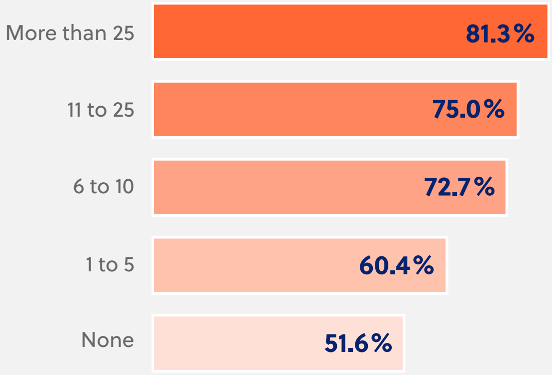
Describe your agreement with this statement: "We struggle to provide meaningful and/or timely reports regarding the organization's risk exposure from open vulnerabilities and the progress being made to remediate them."

Figure 6: Number of organizations that struggle to report on risk exposure



It seems that there's a need for improvement in reporting capabilities across the board, with more than two-thirds of respondents (68%) indicating general agreement with the statement that they struggle to provide meaningful and/or timely reports on their vulnerability remediation and attack surface management efforts.

Figure 7: Number of organizations that struggle to report on risk exposure, by organization size



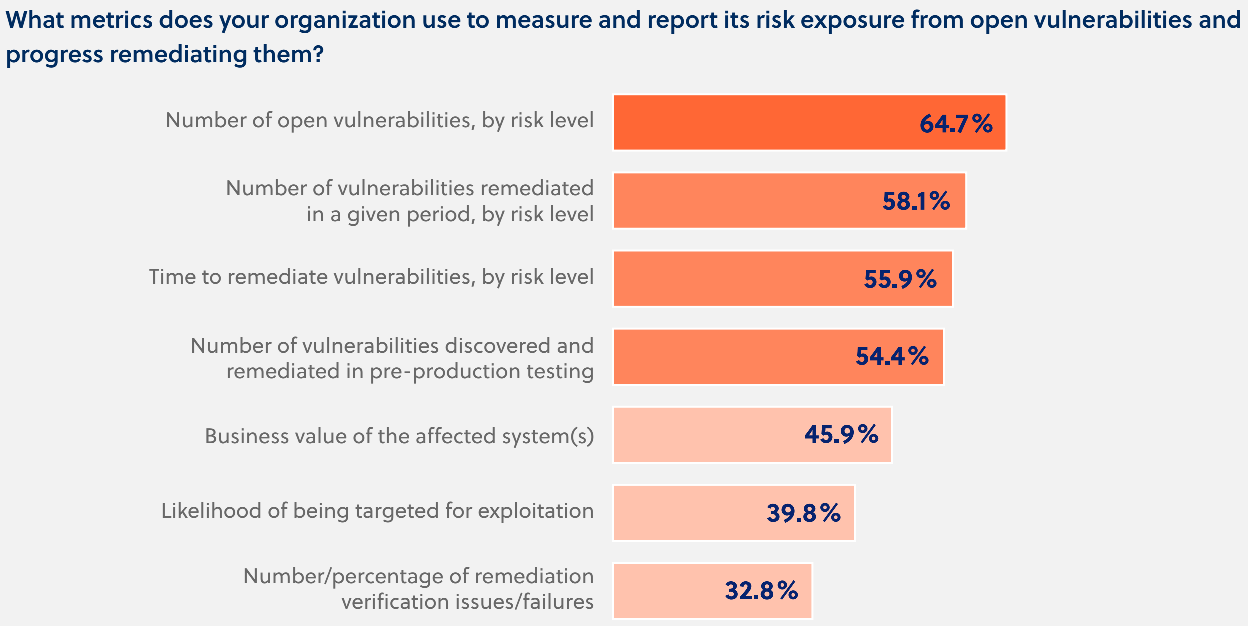
Meaningful, timely reporting is particularly challenging for the midsized organizations that we surveyed. Among those with between 2,500 and 9,999 employees, approximately 75% of respondents agreed with the above statement. It may be that while maintaining visibility over remediation progress is far simpler in the smallest organizations (because their IT environments are so much less complex) and the very largest enterprises have implemented more technologies to automate reporting (helping them compensate for the greater complexity of their ecosystems), those in the middle fall into the opposite of a "sweet spot" — with enough complexity to make visibility challenging, but not enough investment in the automated tools and solutions that can help.

Midsized organizations especially struggle with meaningful and timely reporting on risk exposure, because their IT environments have enough complexity to make visibility challenging, but often there's not enough investment in the automated tools and solutions that can help.

How do organizations measure — and understand — their risk exposure due to open vulnerabilities and gaps in attack surface management?

All too often, in terms that are too simple. Most are just counting the number of open vulnerabilities, or how many vulnerabilities they were able to remediate within a particular time period.

Figure 8: Metrics used to measure risk exposure due to open vulnerabilities


What metrics does your organization use to measure and report its risk exposure from open vulnerabilities and progress remediating them?

The majority of survey participants are using the simplest techniques — counting and timing — to assess their progress in remediating vulnerabilities.

The largest group (65%) said that they're simply reporting on the number of open vulnerabilities by risk level. We did not ask respondents to specify which factors they used to determine "risk level," though Common Vulnerability Scoring System (CVSS) scoring is the most commonly-employed method in the U.S.

A slightly smaller group (58%) of survey participants said that they reported on this metric over time, assessing the number of vulnerabilities remediated per a given time period by risk level. A group that was smaller still (56%) calculated their organization's average time to remediate vulnerabilities by risk level.

Taken together, these findings imply that organizations may lack the data or insights needed to measure their risk exposure in terms of more complex and potentially ambiguous factors — such as the business value of the affected assets or a particular vulnerability's likelihood of exploitation. Ultimately, however, these less clear-cut elements have much more to do with real-world risks.

Why CVSS scores aren't enough

CVSS is an open framework articulating the severity of a threat according to the vulnerability's technical characteristics. It's used worldwide as a standard measurement system across industries, organizations and governments. To be sure, CVSS scoring has value.

However, it provides a weak foundation for assessing the severity of a real-world risk. Few vulnerability management and security teams have the available resources to patch *all* known vulnerabilities in their environment promptly, especially since 15,000 to 20,000 CVEs are published per year.[7] Compounding the problem is the fact that more than 10% of disclosed vulnerabilities are given CVSS scores of 9 or 10 (indicating the very highest-possible degree of severity).[8]

The good news is that only a small subset of vulnerabilities (approximately 2.5%, according to one recent study) is actively being exploited by threat actors in the wild. Focusing remediation efforts on that select group of vulnerabilities, rather than all those with high CVSS scores, has the potential to make vulnerability management efforts far more effective at reducing risk.

[7] CVE.org, Metrics.
[8] CVE Details, Current CVS Score Distribution for All Vulnerabilities.

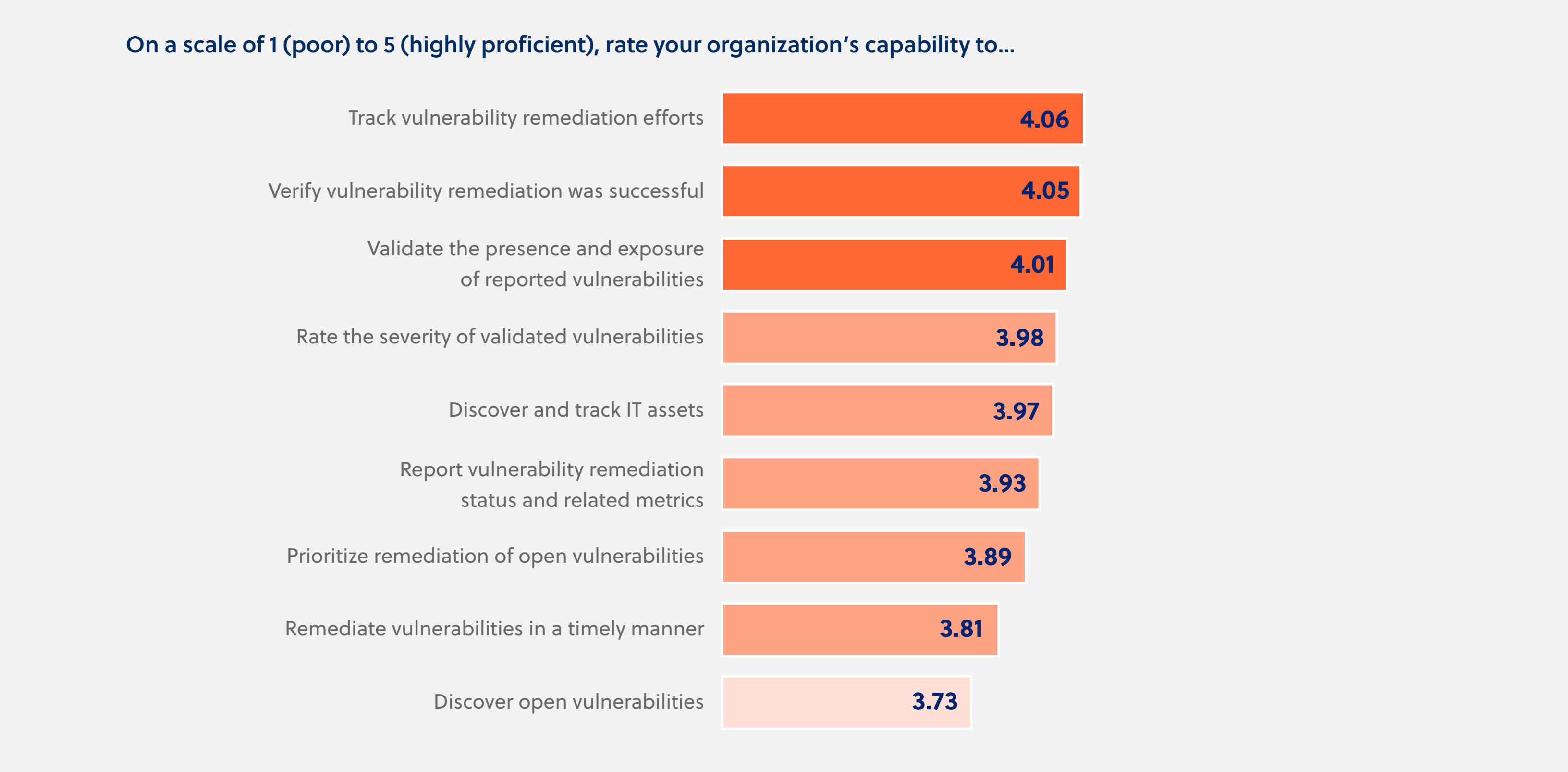
Capabilities and Confidence

Overconfidence bias is a near-universal part of human nature. Most people believe that they're more attractive, smarter and better drivers than they actually are. The same phenomenon may impact IT and security leaders, who tend to believe they're better at discovering and remediating open vulnerabilities than industry research (and breach reports) indicate.

Are security leaders able to accurately assess their own proficiency in vulnerability and attack surface management?

Perhaps not. Participants rated their organization's employees' ability to discover open vulnerabilities and manage the remediation lifecycle higher than industry statistics or breach data suggest is actually the case.

Figure 9: Organizations' vulnerability management capabilities



Among survey participants, there's a surprising — and perhaps excessive — amount of confidence in their organizations' ability to manage vulnerabilities effectively. Respondents rated their abilities in all areas above 3.5 and below 4.5 on a five-point scale, suggesting that they believe themselves to be almost equally good at all aspects of the vulnerability management lifecycle.

Respondents are most confident in their ability to track their remediation efforts, verify that remediation was successful and validate the presence and exposure of reported vulnerabilities. They're least confident in their ability to accurately discover open vulnerabilities — an important point that qualifies all other responses, since all the other activities listed occur *after* discovery in the vulnerability management lifecycle. This means that if organizations are missing key vulnerabilities — perhaps because they're unaware of the existence of the assets that they impact — other efforts to prioritize vulnerabilities, track remediation efforts or remediate those vulnerabilities in a timely fashion won't have the hoped-for impact on the organization's overall risk levels.

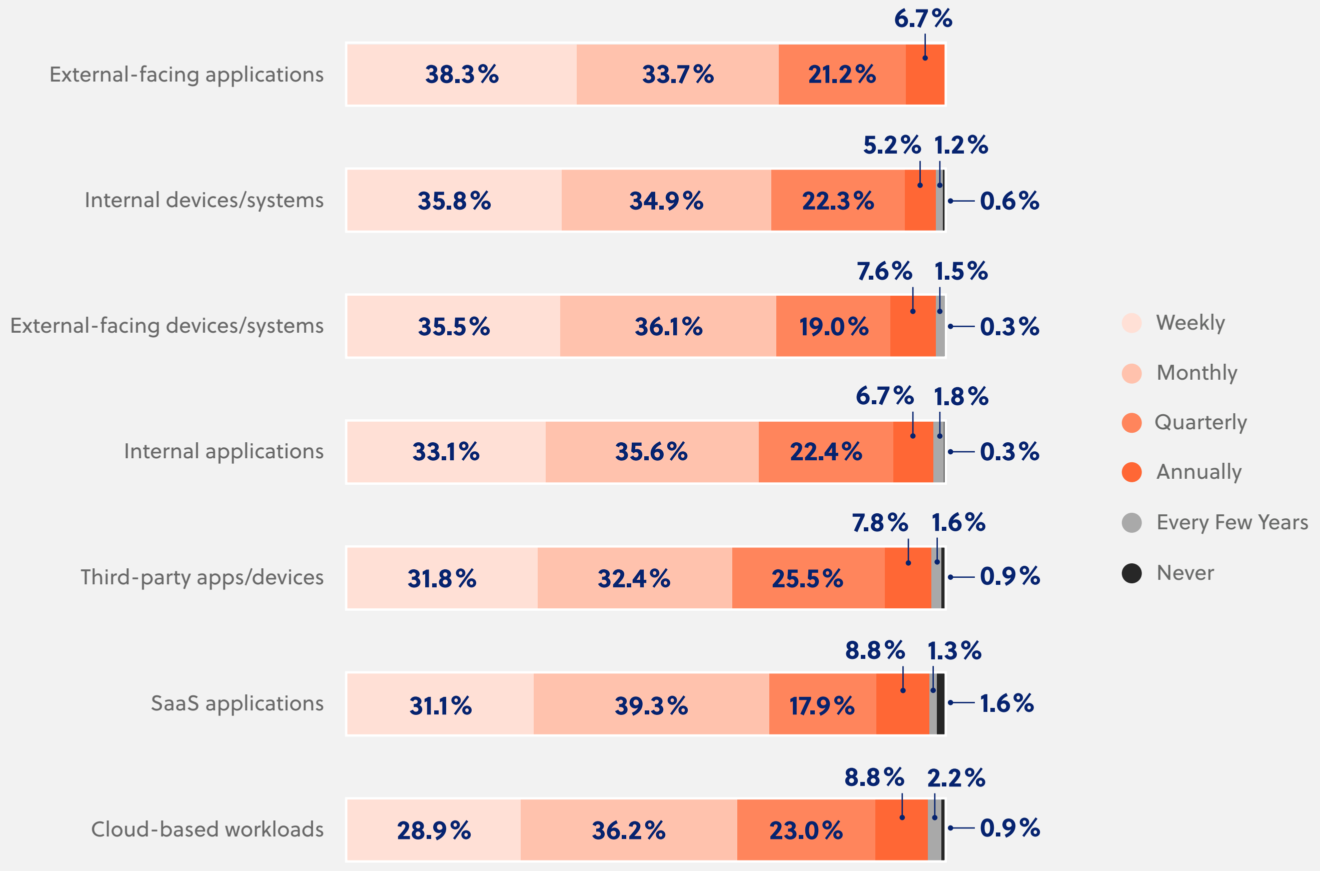
This fact is reflected in the high incidence of vulnerability-related incidents that we observed elsewhere in this survey. More than 90% of respondents' organizations, after all, had experienced such an incident within the past year (see p. 3). It may also help to explain organizations' struggles to provide meaningful and timely reports on risk exposure (see p. 9).

How well are organizations maintaining visibility across the entirety of the attack surface?

This is another area when overconfidence bias may have had some degree of impact upon responses.

Figure 10: Vulnerability scanning frequency, by asset type

How often does your organization typically scan for vulnerabilities for each type of asset listed?



We were surprised to see higher-than-expected vulnerability scanning frequencies across all asset types and categories.

More than one quarter (29%) of respondents stated that they were scanning cloud workloads on a weekly basis, and nearly one-third (31%) stated that they were scanning Software-as-a-Service (SaaS) applications just as frequently. In addition, nearly one-third (32%) said they were scanning third-party applications and devices every week.

All told, nearly two-thirds of respondents (65%) claimed to be scanning their cloud workloads at least once a month, almost three-quarters (70%) said they were scanning SaaS apps at least once a month, and 64% of respondents said they were scanning third-party apps and devices at least once each month.

Participants did not specify, however, how thorough or comprehensive these scans were. Given the challenges in maintaining ongoing visibility over today's dynamic cloud environments and the difficulties of being granted access to third-party environments (including SaaS), we wonder if these results reflect partial scans that are limited in scope.

One in every ten organizations are scanning their cloud apps and workloads (including SaaS) and third-party apps/devices only once per year or even less often. And, more than one-quarter of respondents are scanning all of their assets (including external-facing applications) only once per quarter or even less often.

How Modern Attack Surface Management Changes the Game

External attack surface management (EASM) is an emerging market category that Gartner created in March 2021 to describe a set of products that support organizations in identifying risks coming from internet-exposed systems and assets that they may be unaware of.[9]

By definition, the external attack surface includes all of an organization's IT assets that can be uncovered during attacker reconnaissance efforts. Attackers continuously survey and test the attack surface to find the path of least resistance into an environment. The most advanced EASM solutions approach it the same way, performing comprehensive ongoing reconnaissance across the entire IT ecosystem from an attacker's point of view. In this way, industry-leading EASM technologies can close the gap between attackers and defenders, making it possible for defenders to prevent breaches and be more effective.

Because the most advanced EASM solutions conduct automatic external organizational business mapping and asset discovery, rather than scanning a catalog of known assets for missing patches or misconfigurations, they can provide full attack surface visibility — even across assets that IT and security teams didn't know about. Together with continuous security testing of these assets and a threat intelligence overlay, this makes it possible for security teams to focus on the few critical security gaps that their real-world adversaries are actually targeting.

The very best EASM solutions can also perform continuous automated and active security testing on all externally-exposed assets in the organization's IT ecosystem to identify changes in its risk posture. Such solutions can automatically prioritize the risks that need to be remediated immediately. Being able to complete the full process, automatically, with a single end-to-end solution, is critical because it enables scalability. Covering a mere ten percent of assets, while creating significant noise and a great deal of manual work — as most of today's vulnerability management solutions do — is not success.

Modern EASM solutions include five core elements:

- **Discovery:** Modern EASM uses machine learning, natural language processing and other advanced technologies to investigate all business and IT relationships between your organization and other entities, including acquired companies, joint ventures and shared cloud environments. Modern EASM then discovers all of the internet-exposed assets of your business and those entities, identifying connections between them, even ones that aren't obvious or known.

- **Attribution and classification:** Modern EASM technology automatically determines who owns assets and what data resides on them. This means it can classify assets according to business context, so that stakeholders can understand which data and assets belong to which departments or subsidiaries within the organization, and which risks and attack paths those assets might expose.

- **Security testing:** Modern EASM performs automated security testing that goes far beyond identifying CVEs to instead reveal all the attack vectors that real-world threat actors could use to compromise your most critical assets. This automated, smart vulnerability assessment uncovers risks across your entire external attack surface, not just the assets or IP ranges your teams have identified for scanning.

- **Threat intelligence:** Modern EASM incorporates relevant threat intelligence so that it can identify the handful of attack vectors (out of hundreds or thousands of possibilities) that account for the vast majority of your risk. By understanding attackers' current priorities, and what exploits are weaponized, the solution helps you see where to focus your efforts.

- **Remediation prioritization guidance:** A modern EASM platform can provide detailed and actionable remediation guidance to give your security and IT teams a clear sense of what to do next. Extensive integrations with the most commonly-used IT and security technologies make it easy to share the findings with your remediation team.

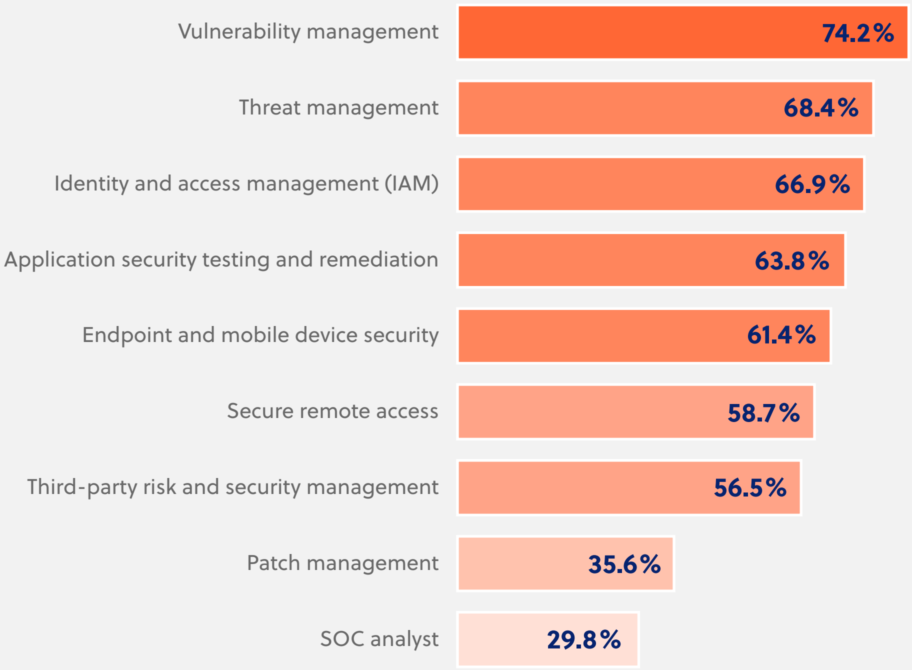
[9] Gartner, Emerging Technologies: Critical Insights for External Attack Surface Management, March 2021.

Demographics

This report is based on a survey of 329 qualified respondents from three countries: Canada, the UK and the US. The largest group, 59%, were from the United States. Each participant was required to have a full-time role in some aspect of IT or security operations, and all had to have significant hands-on experience triaging, remediating and validating the remediation vulnerabilities and/or supervising teams responsible for doing so. Survey participants held a variety of hands-on and managerial roles in security operations center (SOC) analyst, secure remote access, application security testing and remediation, endpoint and mobile device security, identity and access management (IAM), third-party risk and security management, and threat and vulnerability management.

Figure 11: Survey participants by area of responsibility

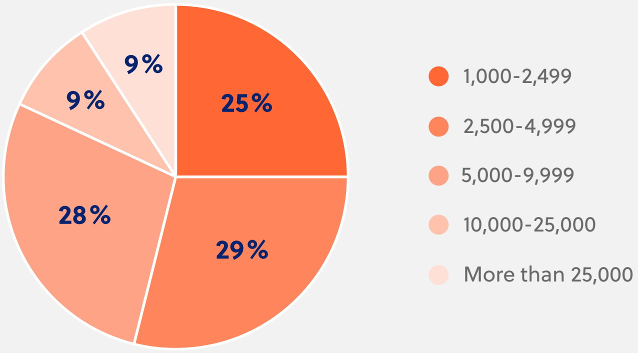
Which of the following areas of your organization's cybersecurity and IT operations are you regularly involved with on a hands-on basis or in a managerial capacity? Select all that apply.



All participants in this survey were working within enterprises with 1,000 or more employees. The largest group (29%) came from organizations with 2,500-4,999 employees. However, 18% came from organizations with 10,000 or more employees, and 46% came from organizations with more than 5,000 employees.

Figure 12: Survey participants by organization employee count

How many employees are in your organization worldwide?



Methodology

CyCognito and the AimPoint Group worked together to develop a 15-question survey. The survey was promoted via email to 329 security and IT operations professionals in the US, UK and Canada, and administered via a web-based survey instrument. The global survey margin of error for this research study (assuming a standard 95% confidence level) is five percent.

All respondents were required to meet three filter criteria: (1) they must have a full-time role in an organization's IT department, (2) their job responsibilities must include hands-on experience triaging, remediating and/or validating the remediation of CVEs and/or supervising teams responsible for doing so, and (3) they must be employed by an organization with a minimum of 1,000 employees.

A Word from the Sponsor

CyCognito solves one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization. CyCognito automatically discovers and tests an organization's internet-facing assets, identifies gaps and weak points attackers can leverage, and provides clear steps on how an organization can analyze, monitor, and eliminate those risks.

CYCOGNITO