

The State of Offensive Security **2022**

Toward a More Resilient Enterprise

Randori

Executive Summary

In the second half of 2021, Randori partnered with ESG to better understand the current state of offensive security. They surveyed 398 IT and security decision-makers in the U.S. and Canada, and discovered that enterprises are struggling to keep up with a rapidly changing threat landscape due to process challenges that are overwhelming security staff. This state of affairs creates a dangerous gap between what attackers can see and what defenders think they're defending.

Ultimately, the struggle defenders face comes down to a few core topics:

- Security hygiene is harder than it should be
- A growing attack surface adds more frustrations
- Asset inventory processes are broken with too many gaps
- Vulnerability management teams are overwhelmed
- Continuous security testing is the new imperative

KEY FINDINGS

69%

of organizations have been compromised due to an unknown, unmanaged, or poorly managed external asset

67%

of organizations have seen their attack surface increase in the past two years

80%

hours on average for organizations to perform an asset inventory

31%

of organizations have found sensitive data in a previously unknown location after adopting attack surface management solutions

73%

of organizations still use spreadsheets to manage their attack surface

30%

of organizations struggle to keep up with the volume of new vulnerabilities

To resolve the challenges facing organizations, IT and security teams need to deploy solutions that monitor assets and scan for changes on a continuous basis. They also need to prioritize vulnerabilities based on the actual risk of exposure. It's only with the help of automation that organizations can accurately monitor the attack surface, maintain fully updated asset inventories, and truly judge which vulnerabilities to patch for the greatest risk reduction. This may be one of the reasons external attack surface management solutions, such as Randori, are the no. 1 offensive security investment large enterprises plan to make in 2022.

Table of Contents

INTRODUCTION 05

SECURITY HYGIENE IS HARDER THAN IT SHOULD BE 09

A GROWING ATTACK SURFACE ADDS MORE FRUSTRATIONS 12

ASSET INVENTORIES ARE INCOMPLETE, DRIVING UP BREACH RISK 16

VULNERABILITY MANAGEMENT TEAMS CAN'T PATCH EVERYTHING 20

CONTINUOUS SECURITY TESTING IS THE NEW IMPERATIVE 23

WHAT IT MEANS TO BE SECURE HAS SHIFTED.....26

CONCLUSION: THE FUTURE OF OFFENSIVE SECURITY.....29

ABOUT RANDORI 31



Introduction

Offensive security as a discipline focuses not on building defenses around your critical assets, but rather on proactively seeking out weaknesses and closing them. This has the knock-on effect of reducing the risk of a breach occurring and enhancing the overall resilience of the enterprise. By its nature, offensive security is proactive as opposed to reactive. What this means in practice is that security teams seek out ways to test their defenses against trusted adversaries as opposed to deploying more defensive tools and waiting for threat actors to try to break in.

Spending on
cybersecurity is
expected to reach
**\$221 billion
in 2025**

– GARTNER

Breach and attack simulation, penetration testing, red teaming, vulnerability management, and attack surface management are just a few of the areas that can fall under this umbrella. All of these sectors

fundamentally focus on proactive discovery of internet-exposed assets and validation of security controls. Performing this discovery and validation, despite the attention it has received in the market, has never been harder. This is evident from the reality that spending on cybersecurity is expected to [reach \\$221 billion in 2025](#) and yet, the cost to businesses from cybercrime continues to increase; annual estimates of [damages now topping \\$1 trillion](#).

While having a clear and comprehensive inventory of what's exposed and the risk they represent has long been recognized as foundational to an effective security program ([CIS 1, 2, and 7](#)), investigations into recent data breaches show that despite continued investment organizations continue to struggle with the basics. This creates an organizational culture that struggles to adopt the offensive approach necessary to reduce risk in the face of the rising tide of cyberattacks.

THE CORE COMPONENTS OF THIS OFFENSIVE, PROACTIVE APPROACH ARE:

Strong security hygiene

Security hygiene is the foundation of offensive security, empowering organizations with a core baseline from which to build in their goals of adopting a proactive approach.

Comprehensive insight into the attack surface

The external attack surface is the key risk vector for a breach. Enterprises should have detailed insight into their attack surface to ensure they know where best to reduce risk.

An updated inventory of their assets

Understanding the assets attached to your organization means that you can more accurately ascertain possible pathways for a threat actor.

Intelligence around the most relevant vulnerabilities

Not every vulnerability matters to the enterprise; intelligence on the most relevant ones is the most impactful when it comes to reducing risk.

Regular testing of defenses

An offensive approach to security is nothing without validating controls. Defenses must be constantly tested against attacks, and it's unlikely malicious hackers will tell defenders how they broke in.

At Randori, we talk to a lot of organizations deploying an offensive approach. We became curious about how the wider market was doing, and sought to understand the specific challenges holding back security teams and what steps security leaders are taking to proactively reduce risk in their organizations. To find out the answer, we partnered with ESG to survey 398 IT and security decision-makers on what their enterprises are doing today to provide a broad assessment on the current state of offensive security.

The results show an industry doing their best to keep pace with a rapidly expanding and ever changing digital landscape but lacking the tools and processes required to do so effectively. The reality on the ground is thus a growing gap between the assets and risks security teams see and the reality of what's truly exposed to attackers.

FIVE MAIN FACTORS DRIVE THE KNOWLEDGE GAP BETWEEN ATTACKERS AND DEFENDERS

1

Security hygiene is harder than it should be

Strong cybersecurity hygiene is fundamental to an offensive security strategy, and creates a firm foundation that empowers enterprises to be proactive. Fully 70% of organizations use at least 10 solutions to manage their security hygiene — a recipe for data quality and management issues if ever there was one.

2

A growing attack surface adds more frustrations

Two-thirds of respondents (67%) have experienced at least a slight increase in their attack surface in the past two years. The rising use of cloud solutions, SaaS applications and services, third-party providers, and remote workers have all contributed to expansions in the attack surface.

3

Asset inventories are incomplete, driving up breach risk

Asset management practices are haphazard at best, with 73% of organizations still using spreadsheets as part of their asset inventory work, and 69% having experienced some type of cyberattack that started through an exploit of an unknown, unmanaged, or poorly managed internet-facing asset.

4

Vulnerability management teams can't patch everything

More than 20,000 vulnerabilities were reported in 2021, the highest year ever, with growth every single year since 2004. The growing number of vulnerabilities overwhelms already stretched IT and security teams and the traditional find-and-fix method of vulnerability management.

5

Continuous security testing is the new imperative

Enterprises need to test their security architectures regularly to ensure that their defenses perform as expected. Companies recognize this, and yet they persist in testing their defensive architectures only infrequently. Only 45% of organizations test their systems at least weekly, leaving substantial room for improvement in security testing.

This report dives into these major offensive security challenges, while also providing guidance for how enterprises can close the gap between what attackers see and what defenders think they're protecting.

Security Hygiene Is Harder Than It Should Be

At its core, an offensive approach to security means adopting a forward-thinking methodology. In the military, the concept is called “defending forward,” and describes a more proactive approach to cybersecurity. This contrasts with the classic reactive strategy where defenders deploy tools and then wait for a new vulnerability to be released or for an attack to occur before they make additional changes. Enterprises that adopt a defend-forward mentality, by contrast, actively seek out the weaknesses in their technology architecture and build resilience to reduce the risk of a breach occurring.

This proactive approach to security starts with a solid foundation in the form of security hygiene. If you attempt to deploy an offensive strategy when, for example, there are massive blind spots in your organization, then the strategy will ultimately fail. That’s what security hygiene is at its core: the foundation that allows enterprises to deploy a proactive, offensive approach to securing their infrastructure.

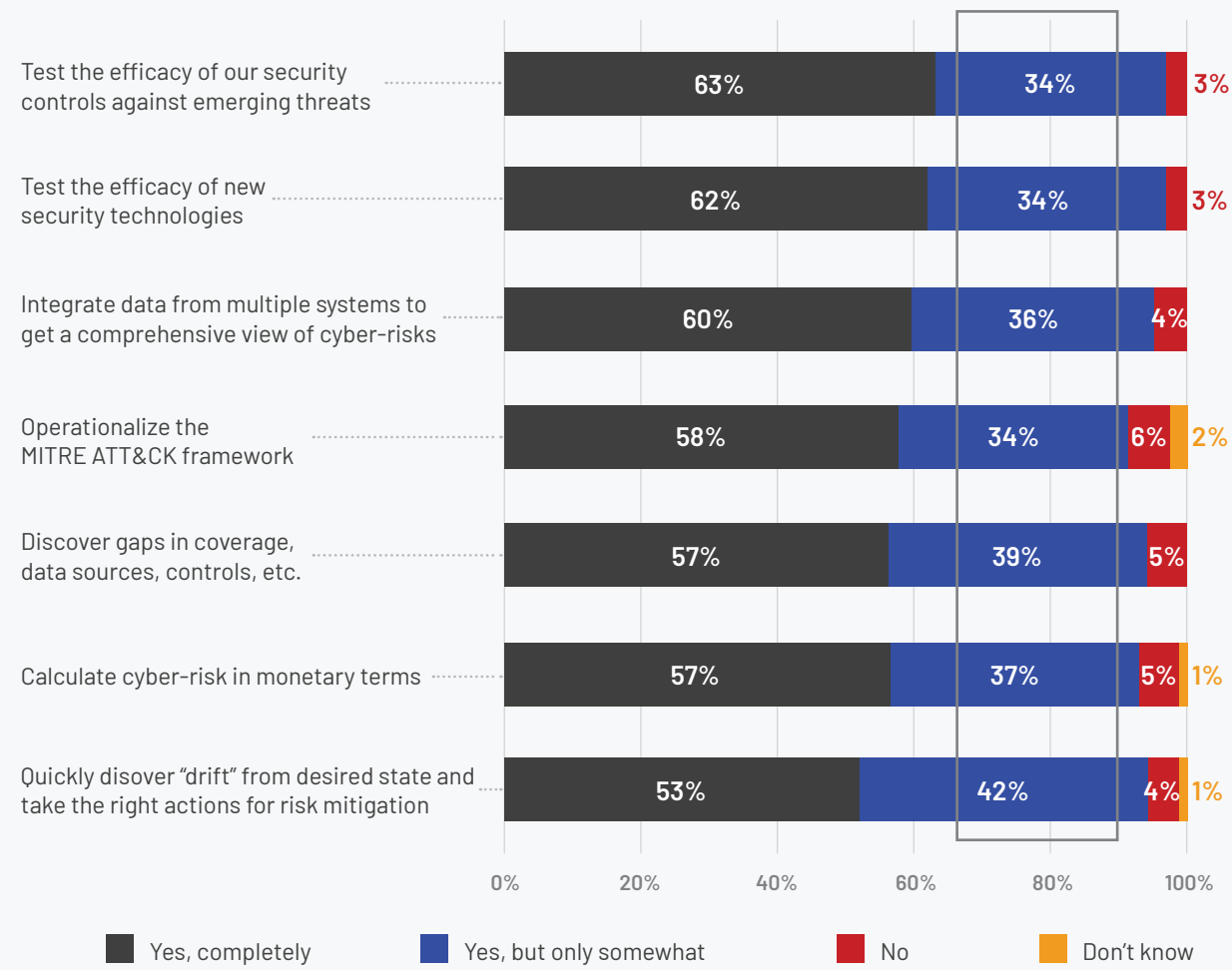
70% of organizations
have more than 10 security tools to manage security hygiene and posture management



With the way most enterprises have designed their security stacks, it's very difficult to have that firm foundation. After all, our research with ESG found that 70% of organizations have more than 10 tools to manage their security hygiene and posture management. It's impossible to truly have good security hygiene with that many tools trying to manage the space for a few reasons. The primary issue is that data from those tools needs to be heavily integrated and cross-checked before it can be actioned, and there are no guarantees that those 10 tools interact with your SIEM or have data that can easily be analyzed.

Organizations recognize the complexity of security hygiene, with 31% acknowledging that hygiene-related tasks have become more complex in the last two years. Moreover, about a third of organizations achieve only partial success with their security hygiene work today. Although 60% say they can integrate data from multiple systems, doing so takes a substantial amount of time and there is no telling how effective that data integration truly is.

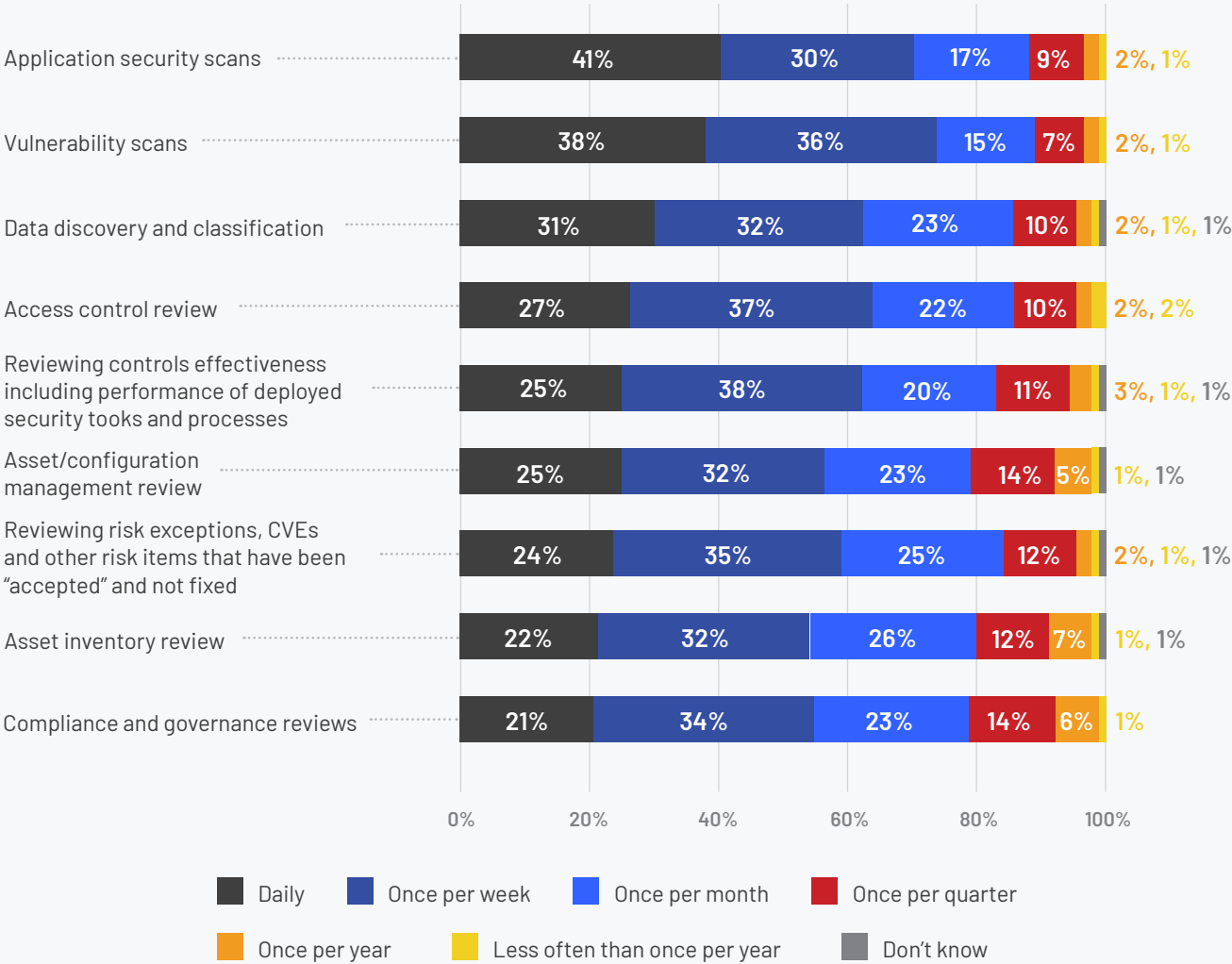
MANY ORGANIZATIONS CAN'T PERFORM BASIC SECURITY HYGIENE AT A HIGH ENOUGH LEVEL



Most concerning, however, is that 39% of organizations only have partial success at discovering gaps in coverage, data sources, and controls. Understanding where the holes are in your security infrastructure is key to good security hygiene. A proactive approach to security necessitates this forward-thinking methodology, especially as attackers become more efficient at discovering holes in security architectures.

Broadly speaking, organizations also appear to struggle with building a holistic security hygiene program. Many security hygiene tasks, such as application security scans, are performed weekly at most organizations, with only a few enterprises performing daily activities designed to improve their security hygiene and allow them to implement a proactive strategy.

MOST ENTERPRISES PERFORM BASIC SCANS TOO INFREQUENTLY



It's a reality that security hygiene has become more difficult, and infrequent tasks performed to ensure a strong foundation do not help streamline these processes. Nor, for that matter, does a security stack composed of multiple disconnected solutions with data that needs to be merged. Although multiple protection solutions are necessary to secure the entire IT infrastructure, data unification creates its own problems when trying to determine the state of your security hygiene.

How to Solve the Problem

Security hygiene is the foundational aspect of offensive, proactive cybersecurity. Enterprises face the challenge of multiple solutions that don't interact well, from which they need to pull data and unify it to determine the true state of their security hygiene. This is overtly a manual process, and one fraught with difficulty.

To get a true baseline picture of security hygiene, enterprises need to find a way to programmatically judge the risk of a breach in their infrastructure. **Adopting an attack surface management (ASM) solution, like Randori Recon, that combines continuous discovery and authentic and proactive validation can reduce the burden on overworked security staff.** Although this could seem like adding yet more technology to the stack, the reality is that an ASM tool that provides asset discovery and automated risk scoring can streamline the security hygiene process and empower IT and security teams to move to a proactive approach faster.

A Growing Attack Surface Adds More Frustrations

The average attack surface has
55,000
internal and external assets

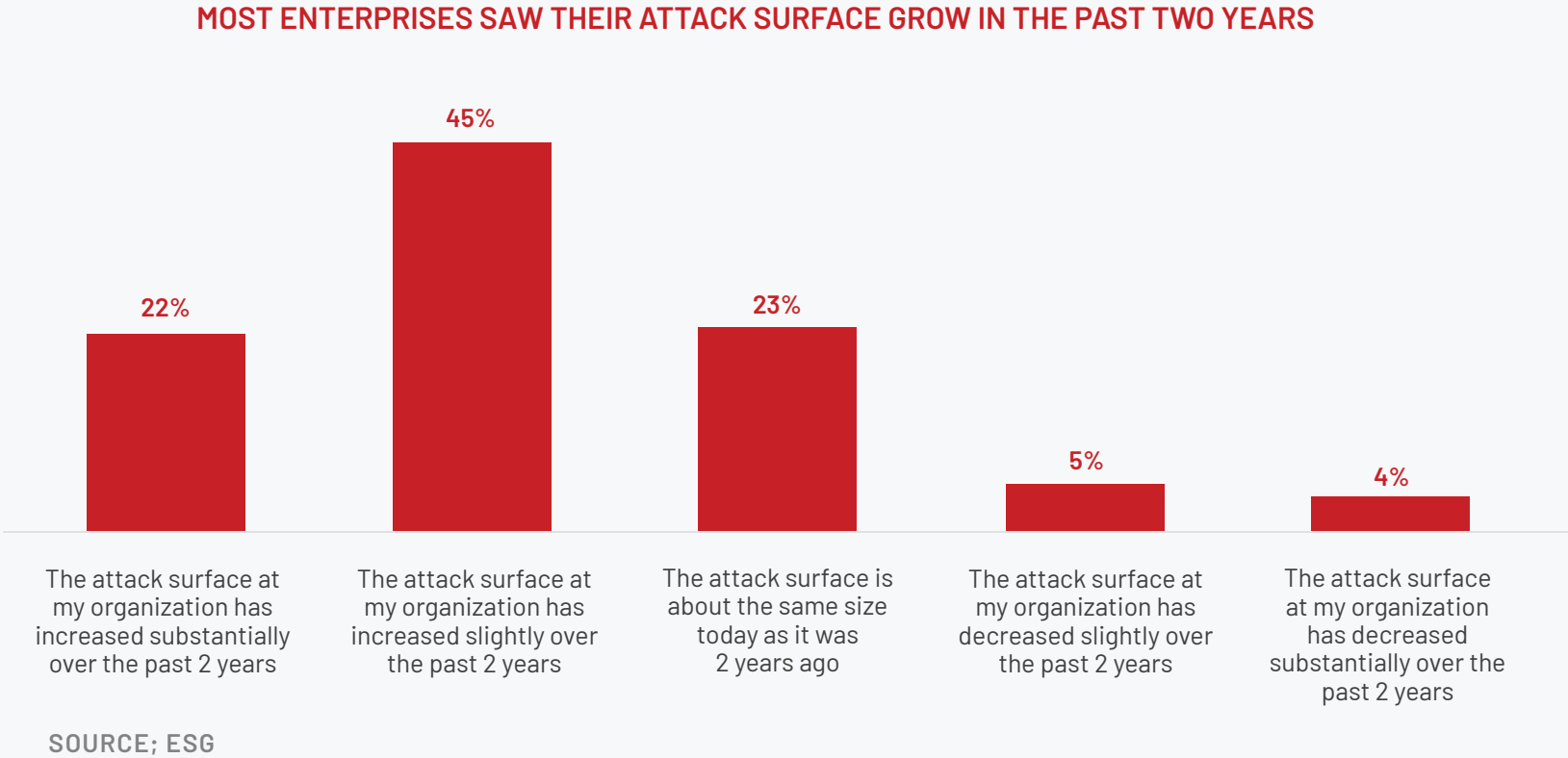
The attack surface of the average organization is the sum of all software assets, regardless of whether they are exposed to the internet or not. Effective management of your attack surface is about minimizing the risk of exposure for any one of these cyber assets. When done properly, this means that attackers have as few ways as possible to infiltrate your systems and achieve their goals.

Attack surfaces are already large, with the average enterprise having an attack surface of 55,000 internal and external assets. It should be noted that these are the assets enterprises *actually know about*. The true attack surface could be much larger; traditional asset management tools by some estimates miss 30% of internet-exposed assets. Complicating the problem is that it's increasingly easy for business units to stand up their own technology outside the purview of central IT, creating more risk and a broader attack surface.

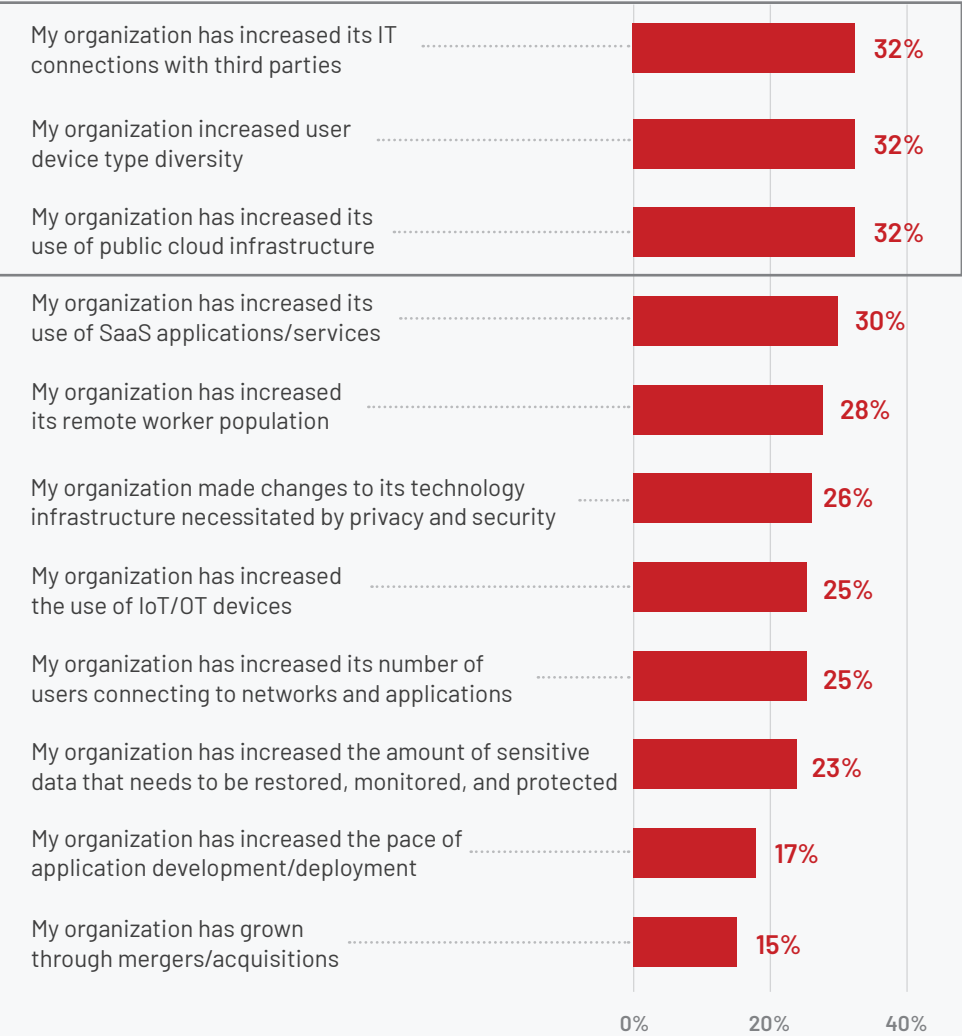
Even without shadow IT, the attack surface continues to grow. Over the past two years, 67% of organizations have experienced an increase in their attack surface. These additional assets and larger attack surface means that these organizations are at greater risk of exposure today than they were two years ago, and attackers see on average more pathways to possible exploitation.

Between digital transformation and the rise of the remote worker, it's almost a given that the average attack surface has increased. With this higher number of failure points, there is more exposure risk at the average company than at practically any other time. A few of the reasons for this attack surface growth are outlined in the chart below.

67% of organizations
have seen their attack surface increase in the past two years
- ESG



ATTACK SURFACES HAVE INCREASED FOR A NUMBER OF REASONS



No matter the reason, the most important thing to know is that attack surfaces are growing larger. This creates more complexity in monitoring for changes, which is the major sticking point for exposure risk. If you can't accurately monitor your attack surface for changes, then there is a substantial chance of a cyberattack slipping through your defenses. This rise in attack surface can be said to be a root cause for the knowledge gap between attackers and defenders. With a larger attack surface, the gap between what attackers see and what defenders think they're protecting grows more substantial.

How to Solve the Problem

To close this knowledge gap, organizations should implement an **attack surface management solution** that continuously monitors for changes and includes regular scanning. This level of automation allows you to uncover changes more readily, and ensure that even a growing attack surface can be accurately monitored for alterations. Leaving attack surface monitoring to manual effort creates too much risk, especially as the number of assets in the attack surface continues to grow at an exponential rate.



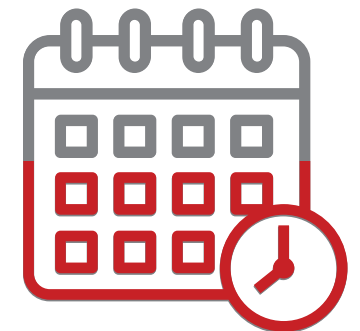
Asset Inventories Are Incomplete, Driving Up Breach Risk

Cyber asset management is a core capability of IT and security teams. Central IT needs to know which software assets are deployed in the enterprise, and this understanding helps inform the vulnerability management strategy to ideally ensure the company's security.

In fact, the first step in understanding your cyber risk is to create an accurate catalog of all the cyber assets attached to your organization. This list could include IP addresses, cloud platforms, and SaaS applications, along with other assets leveraged throughout your organization. Creating this asset inventory allows you to gain a full understanding of possible risk exposure by ensuring you understand precisely what is attached to your systems and where.

Creating this asset inventory is a significant undertaking for many organizations, with most enterprises taking an average of 80 person-hours to build an asset inventory. This is a major time commitment for any IT and security team, equal to two FTEs spending a full workweek on inventorying all the company's cyber assets. Realistically, this inventory is unlikely to be completed all at once. It's more plausible that the asset inventory is performed around other tasks, which could result in it taking many weeks.

It takes
80 hours
on average
to build an asset inventory

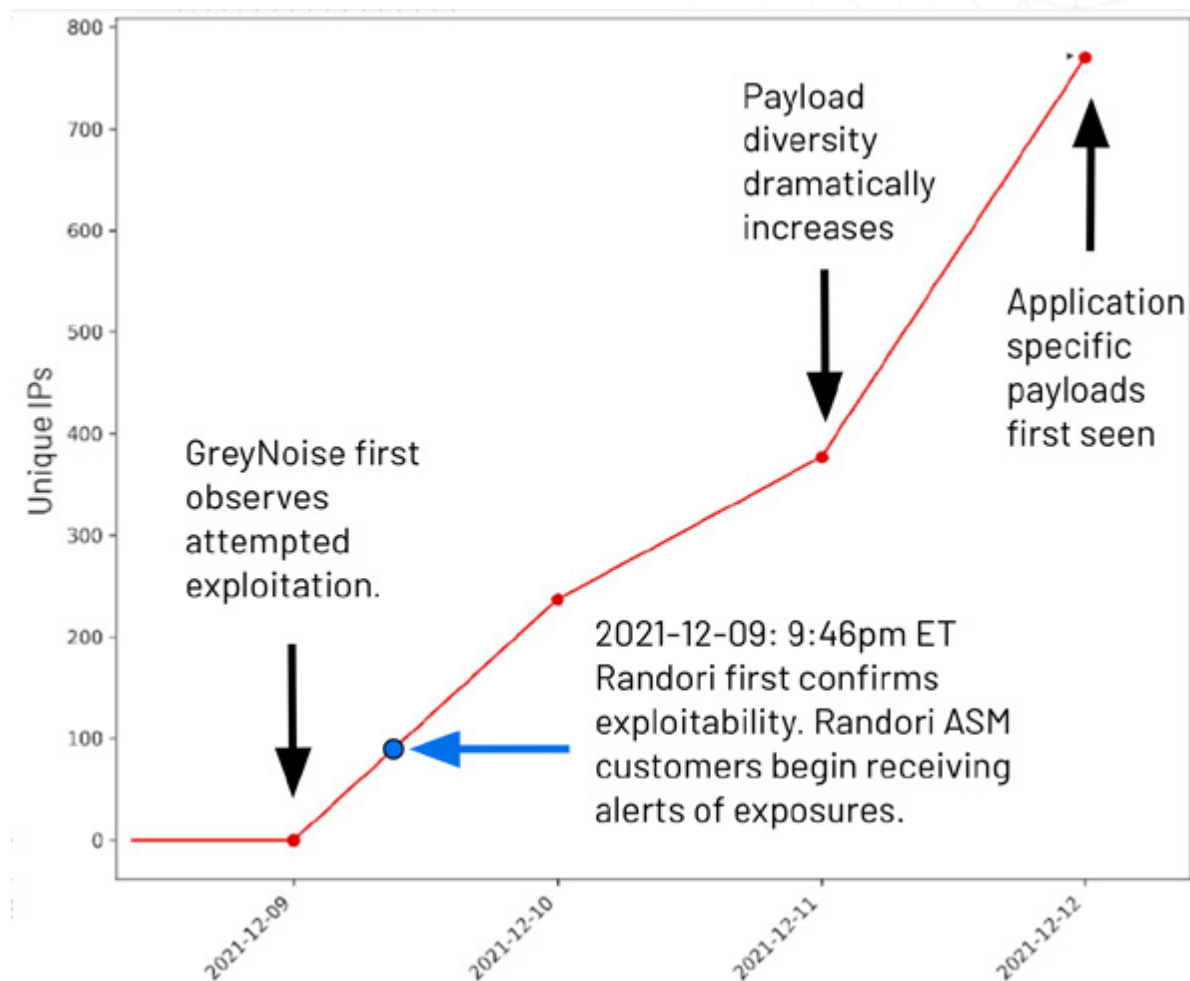


Often these asset inventories, once finished, aren't even entirely accurate. The rise of "shadow IT," where employees install applications or services without the knowledge or guidance of central IT, means that organizations typically don't have the full picture of their asset landscape. These unknown, unmanaged, or poorly managed assets, in fact, are frequently at the core of successful cyberattacks.

Consider that it took Randori's Hacker Operations Center about five hours to develop a working exploit based around the [Log4j vulnerability unveiled in early December 2021](#). It didn't take malicious attackers much longer than that to do the same. By December 11, according to data from our partner GreyNoise Intelligence, the diversity of payloads using Log4j increased dramatically.

This shows how easy it is for attackers to develop working exploits once they receive word of a vulnerability. As shown in the chart from GreyNoise above, it takes two days for attackers to develop working exploits leveraging a vulnerability. Contrast this with the up to three weeks of person-hours it takes most enterprises to inventory their assets. This gap could result in an organization not knowing their exposure for the equivalent of three days. The time gap between when attackers have a working exploit and when defenders can fully enumerate their exposure is a significant risk factor.

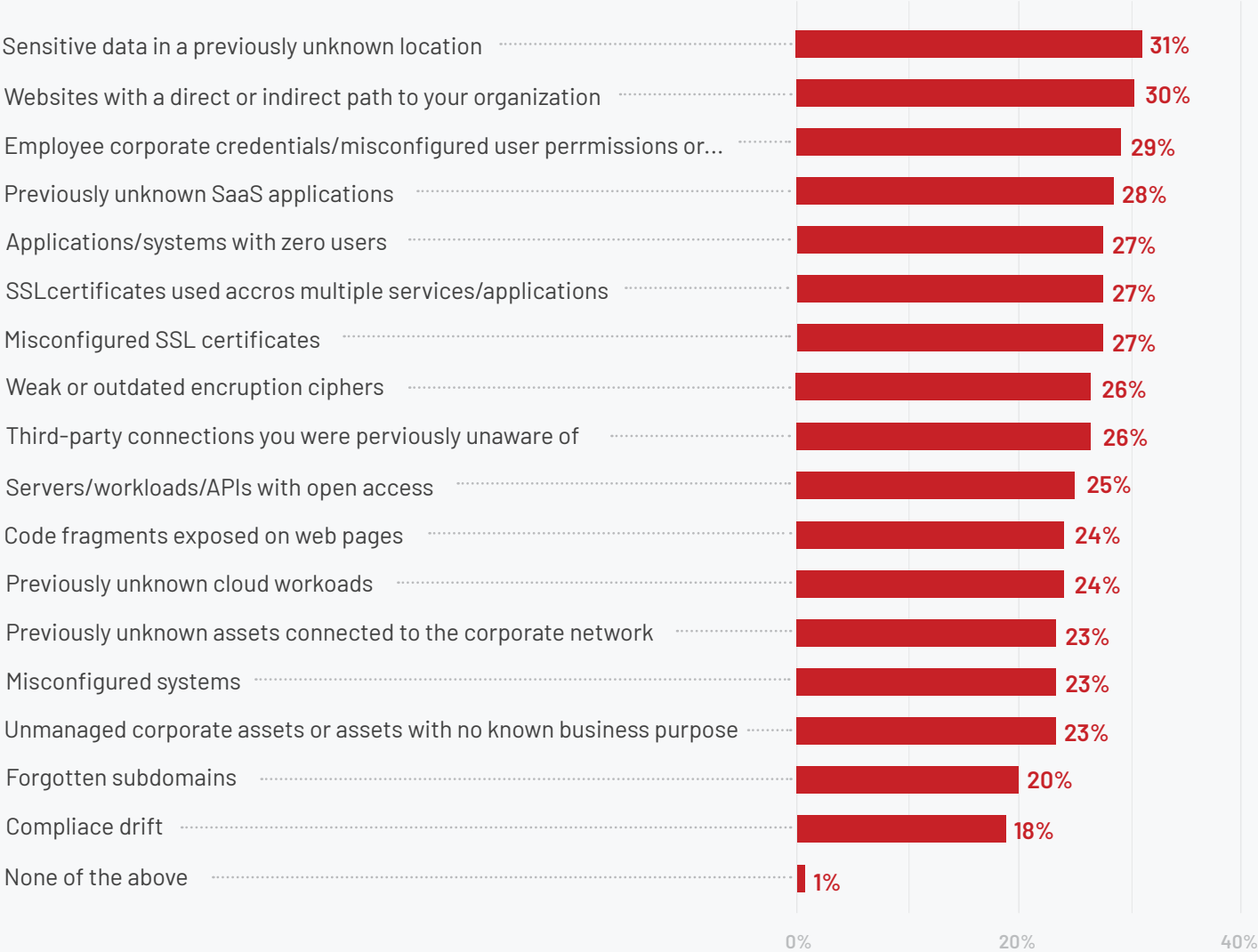
ATTACKERS STARTED EXPLOITING LOG4J IN 48 HOURS



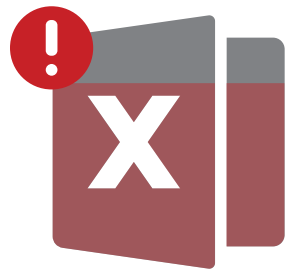
69% of organizations have experienced some type of cyberattack in which the attack itself started through an exploit of an unknown, unmanaged, or poorly managed internet-facing asset – ESG

Shadow IT isn't the only reason that organizations lack a full picture of their assets, but it is one of the most significant. There could also be applications with zero users assigned, or software that was purchased and brought inside the corporate perimeter but never fully deployed. Because of the issues around asset discovery, it's common once a scan of the attack surface is completed, to find assets that were previously unknown. The most frequent discovery, at 31%, is sensitive data in a previously unknown location. Previously unknown SaaS applications are only a few points behind at 28% of respondents stating that's what they found upon scanning their external attack surface.

ENTERPRISES REGULARLY FIND PREVIOUSLY UNKNOWN ASSETS OR DATA SOURCES



Once assets are discovered, that inventory needs to be managed and updated. Unfortunately, managing the asset inventory is similarly fraught with manual processes; 73% of organizations still use spreadsheets as part of their asset management. This is concerning, given how easy it is for unknown assets to persist within the corporate perimeter. Any time there are manual processes involved, the chance of missing a key piece of information increases. With shadow IT such a persistent risk, a spreadsheet-based asset management practice will quickly fall out of date.



73% of organizations still use spreadsheets as part of their asset management

This opens up additional exposure risk, practically ensuring that something will be missed or someone will forget to update the asset inventory. When something is missed, you get more unknown or unmanaged assets attached to the organization, which grows the attack surface and increases the risk of exposure.

How to Solve the Problem

The time commitment of inventorying assets and the rise of unknown assets necessitates a new approach to asset management. This starts with automation. Organizations need to implement automated, continuous scanning that can uncover new assets and keep the inventory updated. This is the baseline for reducing the time commitment of asset inventories, and countering the rise of unknown or poorly managed assets that add exposure risk. Only with deploying a continuous scanning solution can you be confident that the asset inventory is up to date with everything attached to your systems.

Vulnerability Management Teams Can't Patch Everything

Traditional vulnerability management involves tracking CVEs and the associated severity score against your list of cyber assets. The goal is to ensure that you're aware of all the reported issues with the assets attached to your organization, and can then more accurately decide what patches to deploy and where.

This worked when the attack surface was smaller and fewer vulnerabilities reported each year. The problem is that the number of vulnerabilities has exploded. In 2004, there were [1,677 vulnerabilities reported to the National Vulnerability Database](#); 772 of which were rated at high severity. In 2021, 20,136 total CVEs were reported; 4,062 were rated at high severity. This is a growth of 994% over the course of 16 years in the raw number of CVEs, and a 426% growth in the number of high-severity vulnerabilities.



**20,136 CVEs
were reported in 2021**

—NATIONAL VULNERABILITY DATABASE

Traditional vulnerability management no longer scales in this environment. IT and security teams are already overworked; adding in the multitude of high-severity vulnerabilities that must be analyzed just adds to that burden. Each reported vulnerability also can't necessarily be immediately resolved. These CVEs need to be judged against your asset inventory to determine whether there is any impact on your systems, and then potential patches tested, and then deployed. Doing this for more than 4,000 high-severity vulnerabilities per year is simply not possible with any sort of alacrity.

Organizations have noticed the burden, with 30% saying that keeping up with the volume of open vulnerabilities is their biggest challenge in vulnerability management. At 29% each, automating vulnerability discovery/prioritization and coordinating processes across different tools are the next biggest barriers facing VM teams.

VULNERABILITY MANAGEMENT TEAMS FACE SUBSTANTIAL CHALLENGES



Furthermore, 28% of organizations struggle to analyze the results of vulnerability scans and 26% face issues identifying all the assets that need to be scanned. These challenges, more than anything, make clear that the traditional find-and-fix approach to vulnerabilities simply does not work anymore.

The sheer scale of reported vulnerabilities makes it functionally impossible to patch all the CVEs in your systems, especially when faced with the reality that you might not know about everything. Further, a high CVSS doesn't mean that an attacker will necessarily use that particular vulnerability as part of their attack chain.

Ultimately, however, there are far too many vulnerabilities for the average IT team to triage using traditional VM methods. Given that the average time to patch a vulnerability remains between 60 and 150 days, [according to Infosec Institute](#), and the number of reported weaknesses constantly creeping upward, it's clear that there is a strong need for a new approach.

How to Solve the Problem

30% of organizations

struggle to keep up with the volume of open vulnerabilities

– ESG

Risk-based vulnerability management (RBVM) is a far more efficient and effective method of managing your patching process. RBVM takes into account different factors, such as how critical the application in question is to your business and how likely it is that attackers will use that vulnerability as part of their attack. Focusing on actual risk to your organization with regards to managing vulnerabilities has the added benefit of saving you time and money while also minimizing the risk of a successful attack.

Adopting an RBVM approach means that you emphasize applying patches for the vulnerabilities that will have the most impact on your systems. Other applications will be patched as well, but they end up being lower priorities for the IT and security team. This could mean that you patch your production server before resolving issues on your marketing website, for example. Both may have vulnerabilities, but an attack on your production server would have a far larger impact to your organization.

Continuous Security Testing Is the New Imperative

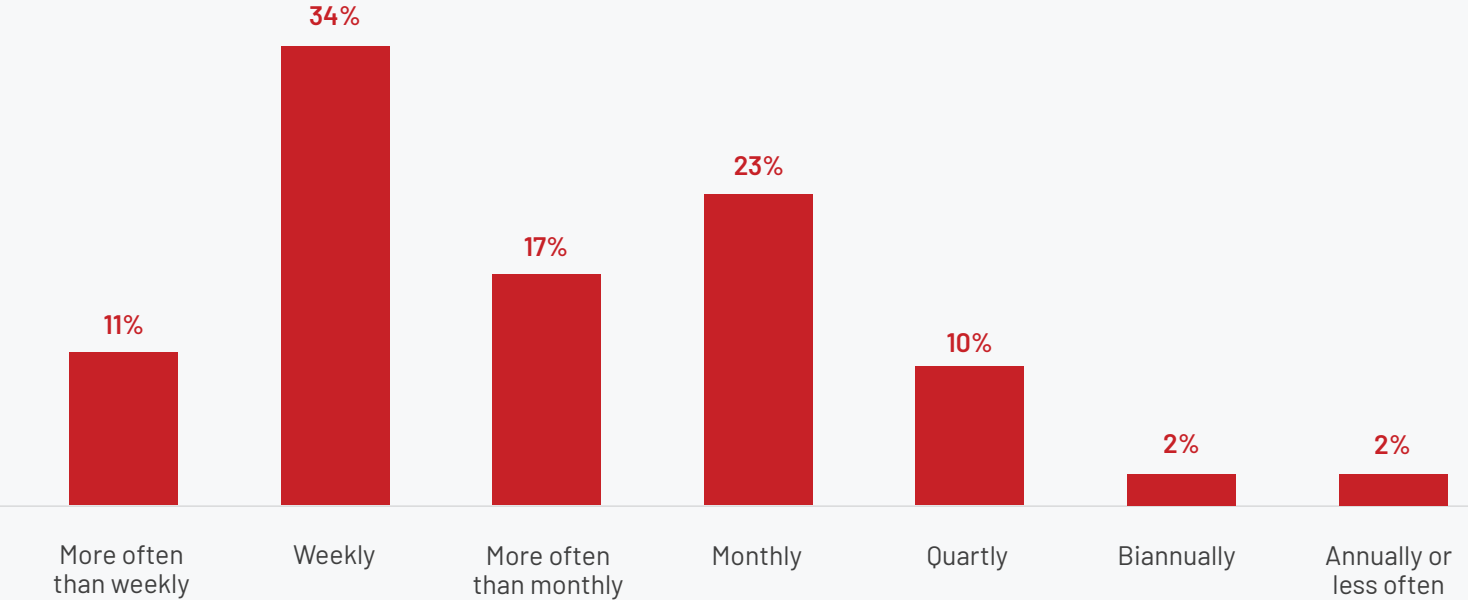
Testing your security infrastructure is a key aspect of a strong offensive security strategy. There are dozens of security tools available to protect every category of technology, including containers, cloud instances, endpoints, servers, networks, and other components of enterprise technology.

Without a strong testing program, however, there is no way to judge the effectiveness of this strategy short of experiencing an actual attack. No enterprise wants to find any flaws in their security in the midst of an active cyberattack. By conducting a security test, you're able to find the flaws — if any — in your protection strategy ahead of time.

Penetration testing is the traditional way to fulfill this need to test security setups, and many organizations do conduct such tests. Forty-four (44) percent of organizations conduct security testing at least weekly, and 86% conduct such tests at least monthly. This is a good starting point, and its prevalence is supported by the rise in market size for penetration testing. The global penetration testing market size, according to Markets and Markets, will grow from \$1.6 billion in 2021 to \$3.0 billion by 2026, at a compound annual growth rate (CAGR) of 13.8% from 2021 to 2026.

47% of respondents view penetration testing and red teaming as a best practice for risk reduction

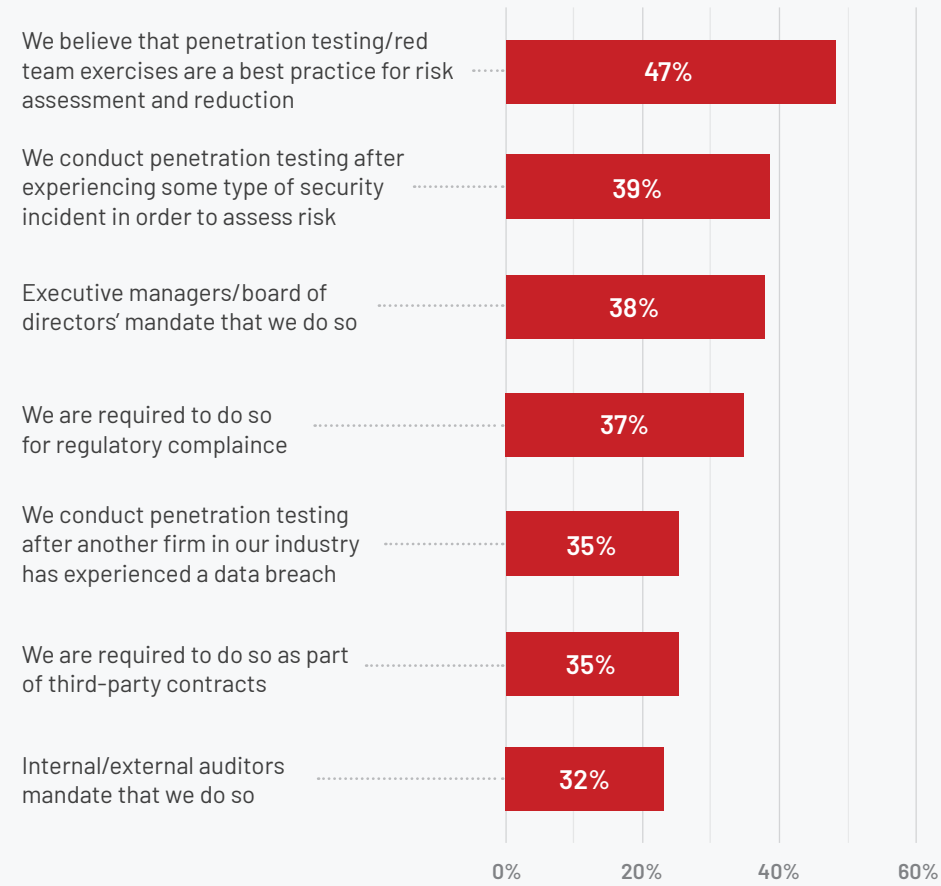
MOST ENTERPRISES CONDUCT SECURITY TESTING ON A ROUGHLY WEEKLY BASIS



According to ESG data, the top reason is that regular security tests such as red teaming engagements are viewed as a best practice for risk assessment and reduction (47% of respondents). The second most common reason is to assess risk after some type of security incident (39%). While it's understandable to conduct tests following a breach or incident, security testing should instead be performed prior to a breach ever occurring to ensure that your enterprise's defenses are effective. Ultimately, conducting red team exercises on a regular basis should really be the best practice. Penetration tests are too episodic and too limited in scope to truly validate security controls.



WHY DO ENTERPRISES CONDUCT PENETRATION TESTS?



How to Solve the Problem

At issue, however, is that pentesting is ultimately a snapshot of a moment in time. Even when pentests are conducted more than weekly, they are often limited in scope. Moreover, when changes are made following pentests, there's a need to schedule another testing engagement to ensure that appropriate new controls function correctly. Further, that only 46% of enterprises leverage the results of these tests to reassess security and IT processes makes clear that security testing isn't being fully leveraged. A new, continuous approach to testing, validation, and reassessment is needed.

Traditional security testing is episodic and highly manual. Enterprises hire skilled pentesting firms on a monthly, quarterly, or annual basis, and then receive reports afterward that they can decide to take action on or not. These are expensive engagements, and available typically to only those enterprises with significant budget. Moreover, these tests are a moment in time and lose value very quickly, especially when they must be re-performed once changes are made.

A more efficient and cost-effective approach is to deploy an automated, continuous red teaming solution. Automated red teaming tools can be run continuously, surfacing weaknesses and empowering IT and security teams with the knowledge of how best to reduce risk on a far more frequent basis. This also streamlines repeated testing and validation, and helps enterprises push forward on a proactive, offensive approach to security.



What It Means to Be Secure Has Shifted

Cybersecurity has traditionally focused on responding to attacks and vulnerabilities. When a new attack appears in the wild, IT and security teams work to ensure their defenses are strong. When a CVE is announced and a patch released, that same group works to deploy the patch in their environment and ensure that it's stable with the rest of their stack. At a very fundamental level, this turns cybersecurity into a reactive discipline that waits to perform defensive operations until they've been attacked.

The reactive approach has not made enterprises safer. The cost of a breach increased from \$3.86 million in 2020 to \$4.24 million in 2021, [according to IBM data](#), despite the expectation of firms like Gartner that enterprises will spend \$172 billion on information security in 2022 – an increase from \$155 billion the year before.

In addition, the growing number of vulnerabilities worldwide and changes in the composition of the modern workforce, has magnified the scale of the problem. In 2021, the [National Vulnerability Database](#) registered more than 20,000 CVEs, with more than 4,000 marked as critical. Moreover, 60% of knowledge workers now work remotely. This figure is unlikely to decline that much even after the environment of COVID-19 changes enough to allow more in-person working.

60%
of knowledge workers
were working remotely
by Spring 2020

Given the realities of the threat environment and digital transformation, enterprises are starting to rethink what it means to be secure. In terms of patching specific vulnerabilities, the attitude toward reacting to every security issue has already pivoted. Today, 34% of enterprises determine what to patch based on specific vendor products in their stack. Only 20% consider the CVSS score when determining what software vulnerability to patch.

HOW DO ENTERPRISES DECIDE WHICH VULNERABILITY TO PATCH FIRST?



Moreover, that 29% of enterprises decide what to patch based on a risk score is similarly crucial. Only one in 20 vulnerabilities are ever actually exploited, so a risk-based approach to patching is a critical viewpoint to take. CVSS score is theoretically important, but if a CVE with a high criticality can only be exploited in very specific circumstances, then it may still be lower risk than a vulnerability that scored low but is trivially easy to use in a real attack. The Log4j event is the rare counterexample of a critical vulnerability also being easy to exploit that proves the rule.

That enterprises recognize relying on CVSS scores is no longer effective is a sign that the measure of what it means to be secure has already begun to shift. Rather than resolving the most software vulnerabilities or reacting to attacks, the new methodology is to take a risk-centric approach to defense with a more proactive bent. This bodes well for the continued evolution of cybersecurity and its elevation to the pantheon of business risk where it belongs.

Only 1 in 20
vulnerabilities are ever
actually exploited, so a risk-
based approach to patching
is a critical viewpoint
to take.

Conclusion

The Future of Offensive Security

Offensive techniques in cybersecurity aren't new. Penetration testing, red teaming, vulnerability scanning, and asset management as concepts have all existed for the past 20 years. To this point, however, these processes and solutions have operated episodically. Pentesting and red teaming firms, for example, are often engaged on an annual or quarterly basis for security testing. Once the testing is complete and the reports written, the client firm decides whether or not to implement the recommendations.

Asset management systems and vulnerability scanners are similar episodic tools. The asset inventories are often updated on a specific cadence, and vulnerability scanners notify IT and security teams when there is a new CVE or security risk on one of their owned assets. These are fundamentally periodic events that still support the fundamental reactive nature of traditional cybersecurity.

The future of offensive security, however, lies in unifying these different components into a cohesive strategy. External attack surface management (EASM) solutions play a key role here. EASM offerings can be leveraged to support asset management tools with continuous discovery, ensuring that unmanaged or poorly managed assets are included in the asset inventory. Similarly, EASM empowers enterprises to shift from a maturity-based model of security to a risk-based one.

“Where enterprises operating on a maturity-based model try to protect everything, risk-based companies decide to focus their tightest security on their most critical cyber assets.”

The risk-based method of security, according to McKinsey, “means that to decrease enterprise risk, leaders must identify and focus on the elements of cyberrisk to target.” Said another way, it means that IT and security teams should focus on reducing the risk of a cyberattack in the most crucial areas of the business. Where enterprises operating on a maturity-based model try to protect everything, risk-based companies decide to focus their tightest security on their most critical cyber assets. This could result in a production server for a software application having better security than the marketing website, for example.

A breach on the marketing website is not remotely desirable, but it’s not nearly as impactful at an existential level as an attacker locking up the production server. Integrating continuous security testing into this strategy is crucial. Enterprises need to know that their security stacks are functioning properly, and the only way to do it at the necessary pace is through continuous automated testing.

IT and security teams are overworked. They face a growing attack surface of more internet-connected assets that create greater risk of exposure every year. The pain of this attack surface growth compounds with the amount of time it takes to create an accurate asset inventory, and the increasing volume of software vulnerabilities. All these factors combine to create an environment where IT and security professionals falter in managing their attack surface through no fault of their own.

Blending all this together enables richer prioritization of assets within the enterprise. Once you have an understanding of the real risk of a cyberattack on your systems, then and only then can you make an accurate decision on how to protect yourself. Building this starts with understanding your foundation with security hygiene, composing a true picture of your attack surface, adopting a risk-based approach to vulnerability management, and testing your security controls in a continuous and automated manner. Only then can enterprises truly defend forward and adopt a proactive, offensive approach.

About Randori

Randori attacks to protect. Recognized by Gartner & IDC as a leader in offensive security, the Randori Platform unifies Attack Surface Management (ASM) and Continuous Automated Red Teaming (CART) to provide enterprises the visibility, actionable insights and validation they need to proactively prevent breaches. Customers like VMWare, Greenhill Inc, FirstBank, NOV, Lionbridge and many more, trust the Randori platform, which was designed by the world's foremost offensive security practitioners at nation-state levels.

Connect with Randori to discover what's exposed on your attack surface and learn more about the tempting targets on your perimeter.

LEARN MORE →

