The State of Attack
Surface Management
2022
Table of Contents

Executive Summary ..............................................................................................................03
Introduction ..........................................................................................................................05
Attack Surface Expansion Continues While Visibility Remains Poor ................................07
Tomorrow’s Threats, Yesterday’s Technology ................................................................. 11
External Attack Surface Management Is the Top Priority for 2022 ................................. 14
Why Are Enterprises Starting with EASM? ........................................................................ 16
Conclusion ............................................................................................................................ 17
About Randori .......................................................................................................................18
Executive Summary

Randori recently partnered with ESG to gain a more complete picture of the current state of Attack Surface Management. We surveyed 398 IT and security decision-makers in the US and Canada, the better to have perspectives from real practitioners on how companies currently manage their attack surfaces, how they adapt their programs for evolving threats, and the biggest hurdles to effective attack surface management.

A Few of Our Key Findings

**ATTACK SURFACES CONTINUE TO EXPAND, BUT VISIBILITY REMAINS POOR**

- 2 out of 3 organizations say their external attack surface has expanded in the past 12 months.
- 7 in 10 organizations have been compromised via an unknown, unmanaged, or poorly managed internet-facing asset in the past year.

**TEAMS CAN’T KEEP PACE, EXISTING PROCESSES ARE SLOW & INEFFECTIVE**

- It takes more than 80 hours for the average organization to update their attack surface inventory.
- Nearly 3 out of 4 organizations still rely out of 4 on spreadsheets to manage their attack surface.

**EXTERNAL ATTACK SURFACE MANAGEMENT IS A TOP INVESTMENT FOR 2022**

- Less than 1 in 3 organizations have a formal external attack surface management solution.
- External attack surface management is the number one investment priority for large enterprises in 2022.
Our findings show that in order to resolve the attack surface management challenges facing organizations, IT and security teams need to invest in solutions that automate and centralize monitoring of internet-facing assets and provide greater insight into vulnerabilities. To stay ahead of attackers, organizations must be able to accurately monitor their attack surfaces, maintain fully updated asset inventories, and truly judge which vulnerabilities to patch for the greatest risk reduction.
Introduction

Having a clear view of which assets are exposed and the risk they pose has long been recognized as foundational to an effective security program (CIS 1, 2, and 7). However, investigations into recent data breaches have shown that despite increased investment, enterprises continue to struggle with managing their attack surface effectively.

To uncover more about the issues holding security teams back and understand the current state of attack surface management, Randori 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 attack surface management.

The joint ESG/Randori research shows an industry fighting to keep pace with the rapid expansion of and constant shifts in the digital landscape, but lacking the tools and processes required to do so effectively. The result is a growing gap between what’s truly exposed to attackers and the risks known to security teams.

Based on our research, there are three forces driving growing demand for solutions that offer a more continuous approach to attack surface management:
ATTACK SURFACE EXPANSION CONTINUES WHILE VISIBILITY REMAINS POOR

67% of organizations saw their external attack surface expand 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.

69% of organizations have been compromised via an unknown, unmanaged, or poorly managed internet-facing asset in the past year. This reality underscores the risk of shadow IT, and the importance of building an accurate picture of your attack surface.

EXISTING PROCESSES ARE SLOW AND INEFFECTIVE

80+ hours
It takes more than two weeks for the average organization to get an updated view of their attack surface.

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.

Nearly 3 in 4
organizations still rely on spreadsheets to manage their attack surface.

EXTERNAL ATTACK SURFACE MANAGEMENT IS A TOP INVESTMENT FOR 2022

Less than 1 in 3
organizations have a formal external attack surface management solution.

#1
External attack surface management is the number one investment priority for large enterprises in 2022.
This report looks into the data and dives deeper into each of these three forces and the factors behind them, as well as providing actionable recommendations. The goal of these findings is to inform you what others are doing to close the gap between what attackers see and what your team knows to protect.

Attack Surface Expansion Continues While Visibility Remains Poor

7 in 10 Organizations Have Been Compromised By Shadow IT

Over the past two years, the known attack surface – the sum of all internet-connected assets known to security – has increased at 67% of organizations. This shouldn’t come as a surprise; between the rise of work-from-home employees and the increased usage of internet-accessible assets in the form of cloud applications and other solutions, it is a foregone conclusion that companies now have more internet-exposed cyber assets than before.

On its face, larger attack surfaces are not a cause for concern. The world is becoming more connected and distributed, which creates a natural increase in the number of assets connected to the internet. Driving this expansion, beyond increased cloud adoption and greater use of SaaS applications and services, companies have increased their reliance on third-party providers as well introducing new risks and blindspots. The problem? Visibility into these assets remains poor.

“67% of organizations have seen their attack surface increase in the past two years.”
The result: more breaches. Sixty-nine (69) percent of organizations have been compromised by an unknown, unmanaged, or poorly managed internet-facing asset in the past 12 months. The preponderance of shadow IT is not an unusual problem. Randori finds that organizations, on average, have 30% more exposed assets than tracked by traditional asset management programs. Inside that 30%, organizations most frequently find they have unknowingly exposed sensitive data, unknown or third-party hosted web assets, and unknown misconfigurations and vulnerable systems.

These areas: exposed sensitive data, misconfigurations, and previously unknown web assets are also among those into which enterprises have the least visibility overall. Given the commonality of attacks using unknown or unmanaged assets, it’s absolutely critical for organizations to improve their attack surface visibility.

On the plus side, enterprises largely acknowledge the need to improve attack surface monitoring. Unfortunately, this acknowledgement has not resulted in technology adoption. A significant number of organizations still rely on traditional IT asset management systems (40%) for discovery and broad cyber threat intelligence (41%) for alerts on new threats.
While certainly valuable, asset management systems only cover assets that your IT and security team already know about and cyber threat intelligence solutions only inform you about known threats. Neither tool will automatically discover unknown or unmanaged facets of your attack surface – the key vector driving breaches today.

By contrast, a dedicated attack surface management solution provides automated monitoring and continuous discovery that heightens visibility into your attack surface. Only 34% of organizations surveyed currently have that dedicated solution in their security stack. This puts 66% of companies at a disadvantage when it comes to visibility into their attack surface – almost the same percentage of organizations who’ve experienced a cyberattack because of unmanaged or unknown assets.

Visibility into the attack surface must increase for enterprises to, at the very least, quantify their cyber attack risk. The data show that increasing one’s ability to quantify cyber risk is seen as one of the most effective ways of reducing attack surface risk. Without the visibility and continuous discovery of a dedicated ASM tool, organizations are far more likely to experience attacks for which they are unprepared. As attack surfaces continue to increase, visibility will continue to remain a significant concern.

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

- ESG
CASE STUDY

Armellini Logistics Experiences Shadow IT’s Impact

In December of 2019, Armellini Logistics was the target of a sophisticated ransomware attack. They quickly recovered, but their IT team adopted a more proactive approach to cybersecurity following that incident. They quickly zeroed in on poor internet-facing asset visibility as a key gap and acquired Randori Recon to resolve the issue.

As IT director Eric McManis said, “We had no way of knowing which of our assets an attacker would target first until we worked with Randori.”

Critical for Armellini was not only visibility, but Randori’s Target Temptation scores, which proactively help flag exploitable or at risk systems for Armellini’s team. This unique approach provides Armellini with a daily prioritized list of risks from which they can take action.

“We had no way of knowing which of our assets an attacker would target first until we worked with Randori.”

– ERIC MCMANIS, IT DIRECTOR
ARMELLINI LOGISTICS
Tomorrow’s Threats, Yesterday’s Technology

3 in 4 Organizations Still Rely on Spreadsheets for Attack Surface Management

In December 2021, the Log4j vulnerability sent security teams scrambling to understand their exposure. Within five hours, the Randori Hacker Operations Center had developed a working exploit and it didn’t take malicious attackers much longer than that to start widespread exploitation of Log4j.

What started off as homogenous spray-and-prey has quickly become active targeting of specific app applications.

– REMY, GREYNOISE INTELLIGENCE

Within 48 hours, firms such as GreyNoise intelligence observed widespread attempts at exploitation. This proved what many had long feared: attackers are getting faster. Unfortunately, while attackers were already running, most organizations were still trying to understand if they were even exposed.
As attackers increasingly become more agile and aggressive, our research suggests most organizations are already behind when it comes to staying ahead of attackers. The average organization takes more than 80 hours to compile an updated inventory of their attack surface, compared to 48 hours for attackers to develop a working exploit.

In the case of Log4j, that means the average organization was exposed and potentially under active attack for five days before they even knew if they were exposed. From this perspective, it is clear that the tools organizations rely on to manage their attack surfaces are not keeping pace. When 73% of organizations admit to still using spreadsheets to manage their attack surface, it's no surprise that large enterprises have named external attack surface management their number one investment priority for 2022.
### Top Things That Would Improve Attack Surface Management

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31%</td>
<td>Increasing the frequency of vulnerability scanning dedicated to discovering and assessing the posture of externally facing assets.</td>
</tr>
<tr>
<td>29%</td>
<td>Improving our ability to analyze and assign risk scores to assets in our external attack surface based on threat intelligence about their exploitability.</td>
</tr>
<tr>
<td>25%</td>
<td>Providing more attack surface management training to security and IT staff.</td>
</tr>
</tbody>
</table>

External attack surface management solutions eliminate the scramble associated with compiling an updated asset inventory. By continuously monitoring for exposed assets and alerting organizations when new risks arise, understanding your exposure to issues like Log4j is as simple as checking your email or logging into the console. This saves hundreds of hours of work a year and eliminates the risk of burnout.

“In the case of Log4j, Randori’s real-time visibility was the difference between being ahead of attackers or having to react attacks. That first weekend, we saw 4,000 Log4j related attacks against our environment... that we were already ahead of and had mitigated. Continuous monitoring and real-time alerting was the key here.”

- Philip Keibler, CISO, Meijer
External Attack Surface Management Is the Top Priority for 2022

31% of Enterprises Say EASM is #1 Investment Priority for 2022

What’s clear in our research is that organizations recognize that what they are doing today is not working. They take security hygiene seriously and are planning to increase investments in 2022 to improve their results. From the data, there is much room for improvement in this area, with 73% of organizations relying on spreadsheets to manage their dynamic attack surfaces. Meanwhile, just 34% of organizations have a dedicated external attack surface management solution.

When asked what’s needed to move the needle, organizations were consistent on the biggest challenges they face – with better intelligence on exploitability and need for more continuous visibility being the most common areas of concern.

TOP THINGS THAT WOULD IMPROVE ATTACK SURFACE MANAGEMENT

1. Ability to Use Latest Intelligence to Assign Risk Scores & Prioritize by Exploitability
2. Increase Frequency of Discovery & Scanning
3. Increase Awareness and Training Around Attack Surface Management

Just 1 in 20 vulnerabilities are ever exploited in the wild
In 2022, organizations plan to get serious about maturing their attack surface management programs and are taking real steps to achieve them. The most common actions organizations are taking include increasing investments in external attack surface management (EASM) solutions, establishing formal KPIs & metrics around their attack surface management programs and beginning to leveraging EASM solutions to derive greater value out of their penetration testing and red teaming efforts.

### TOP INVESTMENTS ORGANIZATIONS ARE MAKING TO IMPROVE THEIR ATTACK SURFACE MANAGEMENT PROGRAMS

**#1** prioritizing investments in EASM

**#2** Establishing formal KPIs & metrics for attack surface management

**#3** Leveraging EASM to improve their penetration testing and red team effectiveness
Why Are Enterprises Starting with EASM?

There are a few reasons why enterprises have decided to start with external attack surface management as their first step. Primary among these is that the attack surface is the first line of defense against attack. If you have a high number of unknown or unmanaged assets in your attack surface, then you are open to an attack that you may not see coming. IT and security leaders understand this, and enterprises by and large will spend 2022 focusing on enumerating their internet-facing assets and ensuring they monitor their attack surface.

The next major issue is continuous visibility into the attack surface, which remains one of the biggest gaps. Visibility into your attack surface helps determine exposure risk; continuous visibility allows you to accurately evaluate and re-evaluate that risk. The average enterprise’s attack surface changes all the time, which is why the continuous component is key for visibility. In this way, you ensure the long-term viability of your EASM program.

Lastly, it’s important to understand that EASM is only the beginning. As the attack surface of the average enterprise expands, organizations can’t stop with just identification, discovery, and monitoring. They must also improve their security controls through continuous testing and validation to ensure that their assets are protected and their infrastructure secure.
Conclusion

Based on these findings, it’s clear that the current state of attack surface management has a long way to go. As organizations continue to recognize the importance of a robust and effective attack surface management program, we expect to continue to see high demand for solutions and expertise that help organizations take a more proactive approach to attack surface management for years to come.

Organizations need to resolve their challenge with visibility into their growing attack surface, while also fixing the issue with slow and ineffective processes to move forward with a more secure architecture. EASM is the top priority for enterprises to resolve those issues, and gain the continuous visibility and streamlined processes necessary for the modern security landscape.
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 →