

The state of attack surface management 2022

IBM

Randori
an IBM Company

Table of contents

3	Executive summary
4	Introduction
6	Attack surface expansion continues while visibility remains poor
8	Case study: Armellini Logistics experiences shadow IT’s impact
9	Tomorrow’s threats, yesterday’s technology
11	EASM is the top priority for 2022
12	Why are enterprises starting with EASM?
12	Conclusion
12	Why IBM?

Executive summary

Randori, an IBM Company, partnered with ESG to gain a more complete picture of the current state of attack surface management (ASM). We surveyed 398 IT and security decision makers in the US and Canada to gain perspectives from real practitioners on how companies manage their attack surfaces, how they adapt their programs for evolving threats, and the biggest hurdles to effective ASM.[1]

Key findings[1]

Attack surfaces keep expanding, 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 by an unknown, unmanaged or poorly managed internet-facing asset in the past year.

Teams can't keep pace, and existing processes are slow and ineffective.

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

External ASM is a top investment for 2022.

- Less than 1 in 3 organizations have a formal external ASM solution.
- External ASM is the number one investment priority for large enterprises in 2022.

Our findings show that to resolve the ASM 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. 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 ASM, 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 ASM.

The joint ESG/Randori research shows an industry fighting to keep pace with the rapid expansion 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 the growing demand for solutions that offer a more continuous approach to ASM:

1. **Attack surface expansion continues while visibility remains poor.**

67%

of organizations saw their external attack surface expand in recent 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.[1]

69%

of organizations have been compromised by an unknown, unmanaged or poorly managed internet-facing asset in recent years. This reality underscores the risk of shadow IT and the importance of building an accurate picture of your attack surface.[1]

2. Existing processes are slow and ineffective.

80+ hours

or more than two weeks are what it takes for the average organization to get an updated view of its attack surface.[1]

70%

of organizations use at least 10 solutions to manage their security hygiene—a recipe for data quality and management issues if ever there were one.[1]

Nearly 3 in 4

organizations still rely on spreadsheets to manage their attack surface.[1]

3. External ASM is a top investment for 2022.

Fewer than 1 in 3

organizations have a formal external ASM solution.[1]

#1

External ASM is the number one investment priority for large enterprises in 2022.[1]

This report looks into the data and dives deeper into each of these three forces and the factors behind them, as well as provides 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

Seven 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's a foregone conclusion that companies now have more internet-exposed cyberassets 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 while introducing new risks and blind spots. The problem? Visibility into these assets remains poor.

The result: more breaches. Sixty-nine 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.[1]

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 cyberthreat intelligence (41%) for alerts on new threats.[1]

67%

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

What do companies find with an EASM solution?

31%

find unknowingly exposed sensitive data[1]

30%

have unknown or third-party hosted web assets[1]

29%

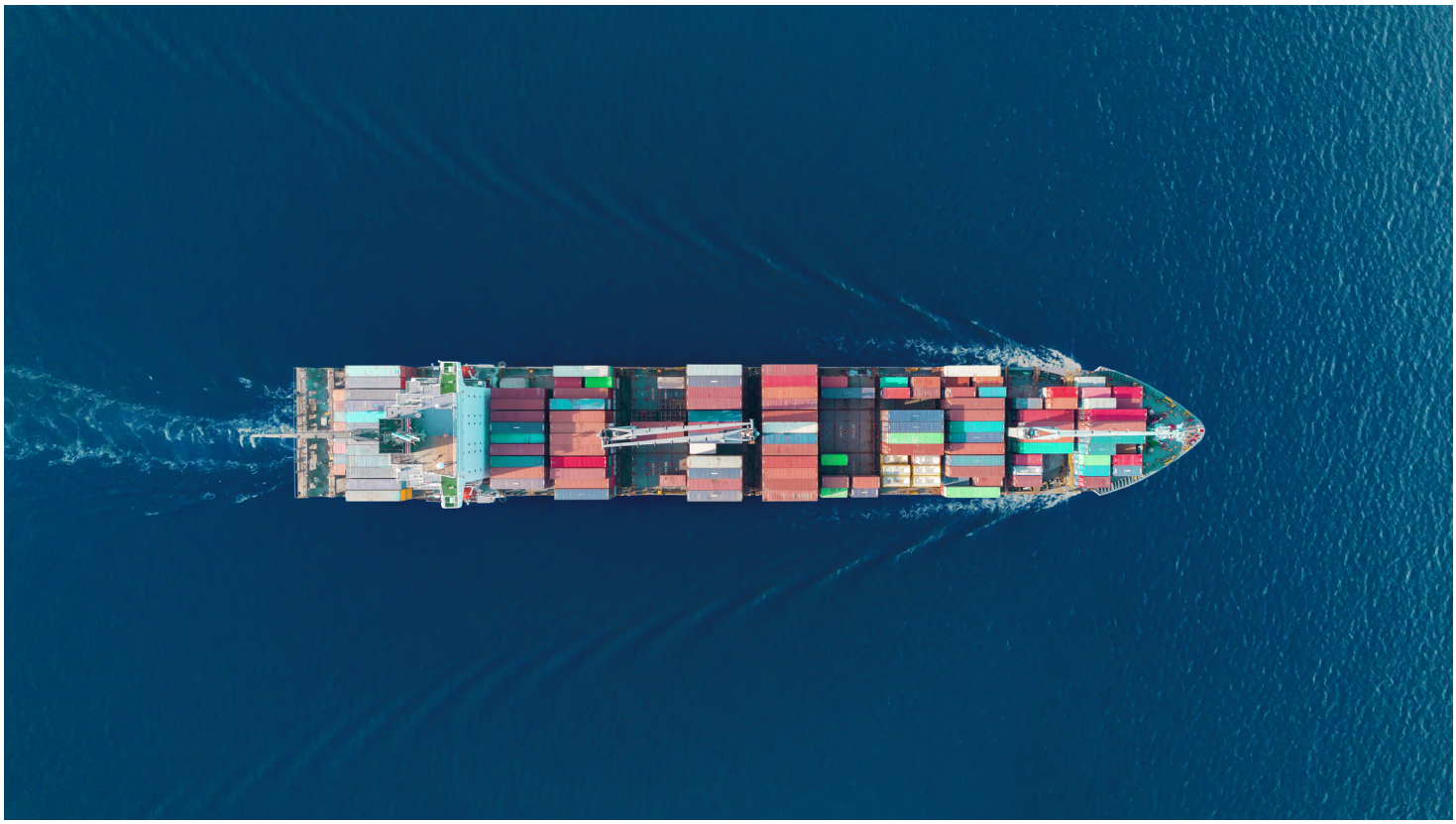
have unknown misconfigurations and vulnerable systems[1]

> "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**

While certainly valuable, asset management systems only cover assets that your IT and security team already know about, and cyberthreat 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 ASM solution provides automated monitoring and continuous discovery that heightens visibility into your attack surface. Only 34% of organizations surveyed 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 that have experienced a cyberattack because of unmanaged or unknown assets.[1]

Visibility into the attack surface must increase for enterprises to, at the very least, quantify their cyberattack risk. The data shows 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.



Case study

Armellini Logistics experiences shadow IT's impact

In December of 2019, Armellini Logistics was the target of a sophisticated ransomware attack. The company quickly recovered, but its IT team adopted a more proactive approach to cybersecurity following that incident. It 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 the company with a daily prioritized list of risks from which it 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

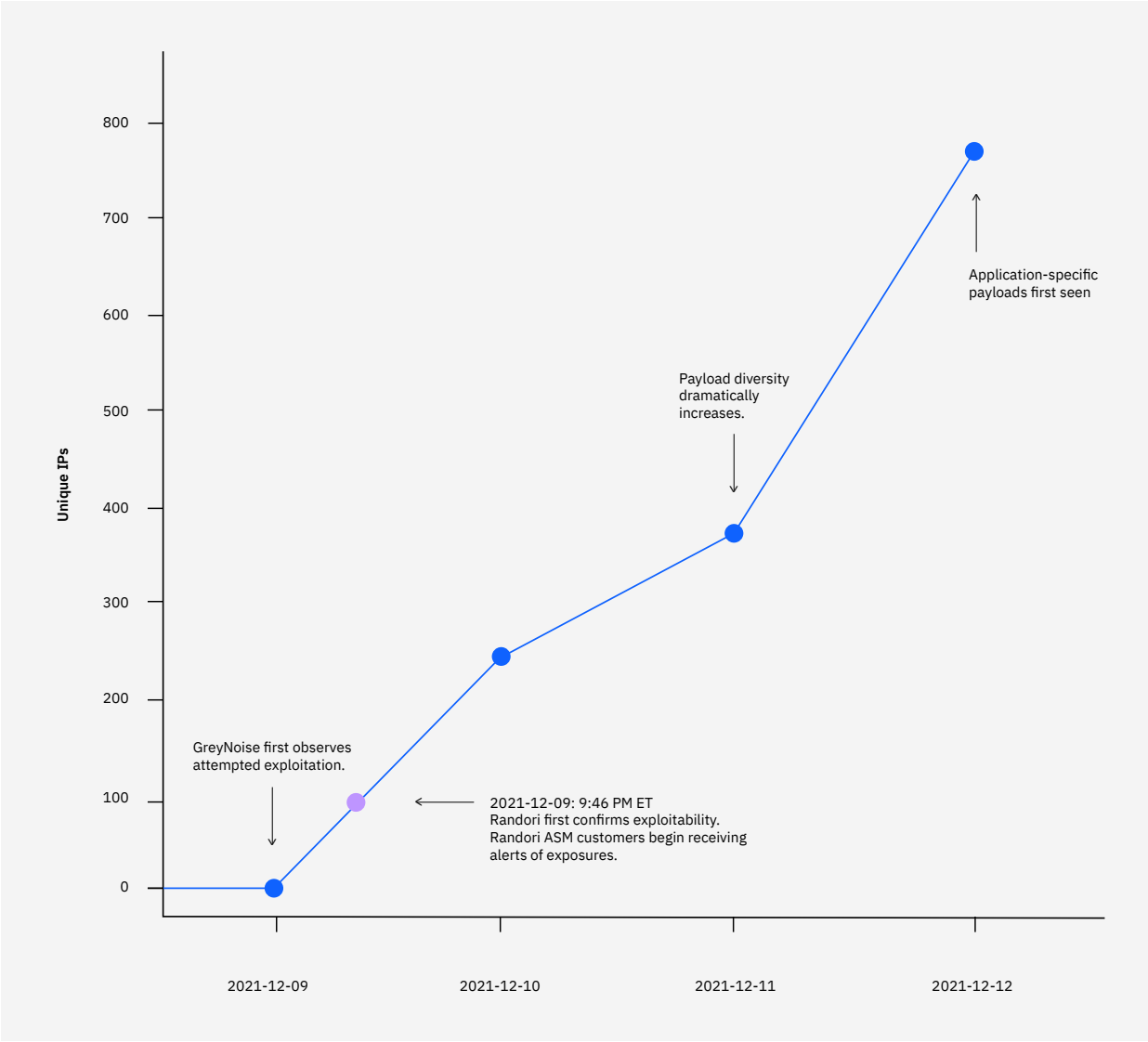
Tomorrow’s threats, yesterday’s technology

Three in four organizations still rely on spreadsheets for ASM.

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. It didn’t take malicious attackers much longer than that to start widespread exploitation of Log4j.

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.

> “What started off as homogenous spray and prey has quickly become active targeting of specific app applications.”
>
> **Remy**
> GreyNoise Intelligence



As attackers 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 its attack surface, compared to 48 hours for attackers to develop a working exploit.[1]

In the case of Log4j, that means the average organization was exposed and potentially under active attack for five days before it even knew if it was exposed. From this perspective, it's 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 ASM their number one investment priority for 2022.[1]



Time for attack surface discovery:
80+ hours[1]

Top things that would improve ASM

31%

Increasing the frequency of vulnerability scanning dedicated to discovering and assessing the posture of external-facing assets[1]

29%

Improving our ability to analyze and assign risk scores to assets in our external attack surface based on threat intelligence about their exploitability[1]

25%

Providing more ASM training to security and IT staff[1]

External ASM 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 in to 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

Just 1 in 20

vulnerabilities are ever exploited in the wild[1]

EASM is the top priority for 2022

Thirty-one percent of enterprises say EASM is their #1 investment priority for 2022.[1]

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 (EASM) solution.[1]

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

Top things that would improve ASM

1. Ability to use latest intelligence to assign risk scores and prioritize by exploitability
2. Increased frequency of discovery and scanning
3. Increased awareness and training around ASM

In 2022, organizations plan to get serious about maturing their ASM programs and are taking real steps to achieve them. The most common actions organizations are taking include increasing investments in EASM solutions, establishing formal KPIs and metrics around their ASM programs, and beginning to use EASM solutions to derive greater value from their penetration testing and red teaming efforts.

Top investments as organizations seek to improve their ASM programs

1. Prioritizing investments in EASM
2. Establishing formal KPIs and metrics for ASM
3. Using EASM to improve their penetration testing and red team effectiveness[1]

Why are enterprises starting with EASM?

There are a few reasons why enterprises have decided to start with EASM 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 reevaluate 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.

Last, 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 ASM has a long way to go. As organizations continue to recognize the importance of a robust and effective ASM program, we expect to continue to see high demand for solutions and expertise that help organizations take a more proactive approach to ASM for years to come.

Organizations need to resolve their challenge by gaining visibility into their growing attack surface while fixing 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.

Why IBM?

IBM Security Randori Recon offers an ASM solution that uses a continuous and accurate discovery process designed to uncover shadow IT and get you on target quickly with correlated and contextualized findings. Learn more about Randori Recon and how it can help your organization stay one step ahead of attackers.

To learn more, contact your IBM Business Partner:
Specialist Computer Centres plc
07976 014124 | sarah.hilton@scc.com
scc.com

Note

1. Security Hygiene and Posture Management, Enterprise Strategy Group, October 2021.

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
October 2022

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.