01

Attack surface expansion

Due to technological advancements and the evolution of Everywhere Work, organizations' attack surfaces are bigger and more complex than ever.

Problem today

Organizations are overseeing a fast-growing ecosystem of devices, tools and assets on their networks — all of which are proliferating rapidly. Yet they have limited visibility into this expanding digital universe.

More than half of IT professionals Ivanti surveyed say they are not very confident they can stop a damaging security incident in the next 12 months. **And more than 1 in 3 say they are less prepared to detect threats and respond to incidents compared to one year ago.**

ivanti

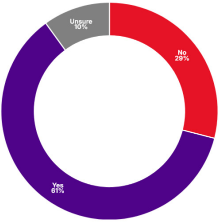
Attack Surface Management

Executive Summary and Key Findings

Download Executive Summary

Unmanaged BYOD is common across organizations

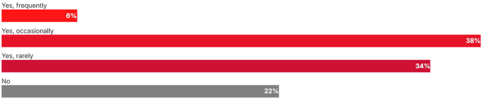
Q: Does your employer know you use a personal device for work?



2024 ASM Report | Ivanti
n = 4,998

BYOD still exists even when banned

Q: You mentioned that BYOD is not allowed. Despite this, does it still exist?



2024 ASM Report | Ivanti
n = 318

50%

of office workers say they use personal devices at work.

32%

of those, say their employers don't know.

Why it matters

The problem is not simply a matter of complexity (i.e., the proliferation of devices and assets leading to sprawl and inefficiency). **This growing ecosystem is driving an ever-expanding array of vulnerabilities and exposures, which can lead to data breaches, downtime, noncompliance, reputational risk and much more.**

ivanti

Expanded IT Visibility Horizon

See more on this topic ›

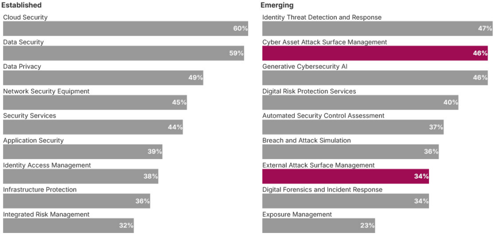
For these reasons and more, attack surface management (ASM) is now a mission-critical part of cybersecurity defense. (And Ivanti's research shows increasing investments in ASM.)

ASM strategy supports continuous discovery and visibility into emerging threats and active exploits, as well as a data-driven method to prioritize and manage vulnerabilities.

As attackers grow more sophisticated, organizations must face these threats by planning and strategizing from the perspective of their adversaries: Where would an attack begin? What systems would be breached first? How would the attack unfold?

Why ASM now?

Organizations are increasing investments in attack surface management



2024 ASM Report | Ivanti
Responses from IT and security professionals (n=706).

02

Siloed data

With so much structured and unstructured data generated every day across the digital ecosystem, critical signals about enterprise health and security are easy to miss.

Problem today

Large attack surfaces generate massive streams of data, but organizations are often not good custodians of that data — meaning it's siloed or inaccessible to the people who need it to protect the organization and drive business outcomes.

How do IT and security professionals say data silos impact them at work?

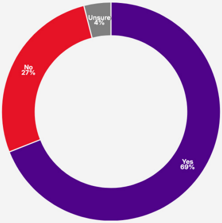
> I often need to access data stored in another system, but to get the information I am only able to speak to someone with access as opposed to getting the access required.

> I don't always have all the data I need to make good decisions and I lose valuable time gaining access to it.

> Incomplete information means that I have to guess.

More than half of organizations report significant silos

Q: Are security data and IT data siloed in your organization?



2024 ASM Report | Ivanti
Responses from IT and security professionals (n=706).

Why it matters

Cybersecurity professionals report that **data silos impact their ability to act quickly and decisively**.

82%
say their productivity suffers due to data silos.

40%
say data silos slow incident response times.

33%
say a lack of alignment with other functions within the organization means stakeholders can't agree on the right/best course of action.

In other words, **data silos are not only inefficient; they limit insights and drive up exposure**. But it doesn't have to be that way. Cyber asset attack surface management (CAASM) tools can solve organizations' data problems by integrating EASM and DRPS data, giving organizations unprecedented access to data, intelligence and visibility.

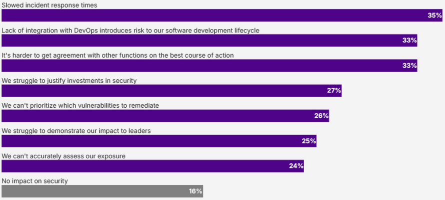
ASM tools: a primer ⌄

ivanti
Connected and Secured Asset Data in One Place

See more on this topic ›

Silos slow response times, among other challenges

Q: How does siloed data impact security?



2024 ASM Report | Ivanti
n = 917. Respondents could select multiple options.

03

Prioritization

Organizations struggle to assess risks, prioritize a response and act on threats in a coherent way.

Problem today

Organizations struggle fruitlessly to prioritize which vulnerabilities to mitigate due to a variety of confounding factors:

> **External factors:** a fast-evolving threat landscape; an unprecedented volume and pace of vulnerabilities and attacks
> **Internal factors:** poor visibility into their attack surface; an inability to assess the severity of existing vulnerabilities; challenges coordinating and communicating a response

Although 64% of organizations say they have a documented methodology for prioritizing security patching, when we look deeper, the findings are troubling.

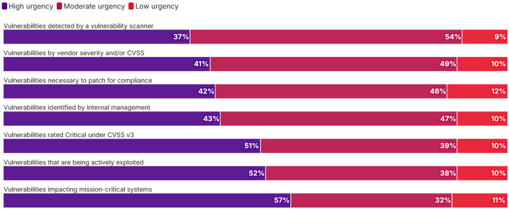
Security professionals rate nearly all types of vulnerabilities (e.g., active exploits, patches required for compliance, leadership directives) as at least “moderately urgent” if not “highly urgent.” **And when all vulnerabilities are a priority** ... **none are**.

ivanti
Shifting Security Left

See more on this topic ›

When everything is a priority, nothing is.

Q: How do you prioritize which vulnerabilities to patch?



2024 ASM Report | Ivanti
Responses from IT and security professionals (n=706).

Why it matters

Given the persistent shortage of qualified security professionals, **teams need to allocate resources effectively to keep their organizations secure** — which is why prioritizing the organization’s risk response is so important.

How is this done? ASM uses algorithms and methodologies to output risk scores, which prioritize exposures based on factors that include the likelihood of an attack, the severity of the risk, the potential negative impact and more.

This type of risk management and optimization is critical, given the amount of internal and external data that security professionals must oversee and analyze. The result? **Less downtime, fewer business interruptions and an improved cybersecurity posture overall**.

4.3 incidents

The average number of security incidents organizations have reported in the last 12 months

33.8 hours

The approximate time it took organizations to restore service following their most serious security incident

04

Supplier risk

An organization’s suppliers and vendors are an extension of its attack surface — but many don’t treat them as highly connected entry points for attackers.

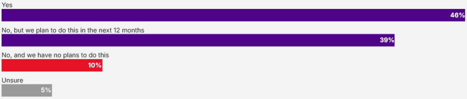
Problem today

A 2023 study by Capterra found that **61% of companies had been impacted by software supply chain attacks in the preceding 12 months**.

Even so, Ivanti's research finds that fewer than half of organizations (46%) have identified the vulnerable third-party systems/components in their software supply chain — though an additional 39% say they plan to do this in the coming year.

Fewer than half have identified supply chain vulnerabilities

Q: Has your team identified the third-party systems/components that are most vulnerable in your software supply chain and will cause the largest organizational impact if compromised?



2024 ASM Report | Ivanti
Responses from IT and security professionals (n=706).

Why it matters

Your vendors' and partners' attack surfaces are extensions of your organization's attack surface. A single breach in your software supply chain can have damaging impacts — on revenues and reputation, as well as on compliance risk and liability exposure. One example: Target's massive data breach a decade ago was due to attackers getting ahold of credentials stolen from a third-party vendor ... a refrigeration and HVAC systems manufacturer, hardly the entry point most would imagine for a damaging breach. The retailer later revealed it booked $162 million in expenses in 2013 and 2014 related to that event, equivalent to $213 million today.

To prevent such attacks, ASM can monitor internet-facing assets to help you better understand your organization's holistic risk profile, including risks introduced by your supply chain. And it can play a vital role in vetting new suppliers, vendors, partners and even acquisition targets.

Gartner® 2023 research finds that, "despite a dramatic rise in software supply chain attacks, security assessments are not performed as a part of vendor risk management or procurement activities. This leaves organizations vulnerable to attacks."*

05

Action steps

Experts weigh in on how organizations can understand the full dimensions of their attack surface vulnerabilities and take steps to manage that risk.

Set priorities, harmonize data and leverage automation

In today's digital landscape, we're redefining what constitutes an asset. It's no longer just about physical devices. A myriad of asset types are emerging — transforming closed networks into open systems running on IP protocols. This shift has significantly expanded the "blast radius" for organizations of all sizes, exposing them to increased risks due to misconfigurations and internet exposure.

I recommend following a principle called DEER: Discover, enumerate exposures, remediate.

The real challenge to the DEER principle is the sheer amount of data organizations must harness and leverage. On average, every organization has 60 to 70 different sources of data coming at it. There are five things an organization needs in order to effectively manage all this data:

1. The ability to ingest the data.
2. The ability to normalize the data.
3. The ability to label the data.
4. The ability to prioritize the data based on an attacker's intent.
5. An understanding of what the organization's priorities are.

Once you have a clear prioritization, you need to build up a very robust remediation strategy. And each step of this can be done as a shift-left (which is developer-centric) or shift-right (which is security-centric).

Next comes automation, where service management can come into play. Develop automated workflows for device management, as well as writing tickets to developers, ops and security teams. Then create automated workflows to ensure that remediation is happening with very little human intervention.

Dr. Srinivas Mukkamala
Chief Product Officer, Ivanti

Identify supply chain vulnerabilities and make them part of the calculus

Organizations need to pay more attention to supply chain and vendor security. To do it effectively, consider adopting these four directives:

1. Establish clear vendor security requirements that align with organizational policies and comply with industry regulations such as GDPR and HIPAA. These standards should be clearly communicated to all vendors and suppliers.
2. Conduct thorough risk assessments of your vendor ecosystem to understand how well each supplier meets security requirements today. Conduct regular audits and compliance checks to ensure ongoing adherence.
3. Make sure vendors are an integrated part of your incident response plan (IRP), especially if they have access to your organization's systems and data. This will ensure there's a predefined process for managing incidents involving vendors.
4. Ensure that security measures are incorporated into contractual agreements with vendors, to hold them accountable and ensure a mutual understanding of each party's role in maintaining security.

Above all, your approach with vendors should be collaborative, encouraging regular communication about potential threats and ways to improve security measures together.

Daren Goeson
Senior Vice President of Product Management, SUEM, Ivanti

Keep in mind: sophisticated attack surface management is dynamic above all else

Organizations need to understand emerging external risks — particularly those unique to their specific industries and markets — and how those risks interact with internal vulnerabilities.

You cannot evaluate risk without context. Your security team may find a vulnerability in a supplier's software that's a "5" (i.e., medium). Not so bad. But an attacker may discover it and think, "that's only a 5, but if I pair it with this other vulnerability, I now have RPE capabilities."

Attack surface management software and prioritization have to take into account the *dynamic* nature of each vulnerability and each finding that's out there. As vulnerabilities morph and trend, or if they get tied to ransomware or get exploited, an ASM solution will identify how to drive and change those prioritizations dynamically.

The state of our software changes daily, but some of those may not be implemented internally. Somebody else can influence and change our attack surface by exploiting a minor defect — and that suddenly becomes a top priority. So, good attack surface management is highly dynamic, plugged into trends and continuously reevaluating risk based on new data.

Rex McMillan
Vice President of Product Management, Ivanti

Methodology

This report is based in part on two surveys conducted by Ivanti in late 2023 and 2024: "2024 Everywhere Work Report: Empowering Flexible Work" and " 2024 State of Cybersecurity: Inflection Point". In total, these two studies surveyed 15,000 executive leaders, IT professionals and office workers. This report also cites research from third-party sources.

*Gartner, Mitigate Enterprise Software Supply Chain Security Risks, By Dale Gardner, 31 October 2023 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.