SEVCO

September 2022

# State of the Cybersecurity Attack Surface

## Executive Summary

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people, one of the largest and most impactful data breaches in recent history. After years of investigation, the U.S. Senate issued a scathing report assigning blame, in large part, to the company's inability to maintain an accurate IT asset inventory.

The report stated that "Equifax lacked a comprehensive IT asset inventory, meaning it lacked a complete understanding of the assets it owned. This made it difficult, if not impossible, for Equifax to know if vulnerabilities existed on its networks. **If a vulnerability cannot be found, it cannot be patched.**"

The Equifax case is one example of an existential and underreported cybersecurity issue: the vast majority of organizations do not have comprehensive visibility of every asset they need to secure. As a result, attackers often understand the networks they're targeting better than the security teams tasked with securing them. The uncertainty around cyber asset attack surfaces upends the foundation of every major security framework and presents a challenge to security teams: they can't protect what they can't see.

Lack of visibility is the single biggest challenge facing security teams today. In our first **State of the Cybersecurity Attack Surface** report, we look at this issue, with data from visibility into more than 500,000 IT assets. The research identifies a significant gap in the IT assets that are not only missing endpoint protection or not covered by enterprise patch management solutions. It also uncovers the more insidious threat of "stale" IT assets that act as ticking timebombs for enterprises.

Given the success that attackers have exploiting hidden IT assets, it is highly likely that malicious actors will continue to target them until organizations do a better job of developing comprehensive IT asset inventories that accurately reflect their dynamic attack surface. Sevco Security will continue to track trends related to the cybersecurity attack surface.

Sincerely,

**J.J. Guy**
**CEO and Co-Founder, Sevco Security**

**Key Takeaways**

**Increasingly complex enterprise environments have created chaos and enterprises are not adequately protecting their IT assets**

- Data aggregated from visibility into more than 500,000 IT assets shows that 12% of all IT assets are missing endpoint protection
- The same data set shows that 5% of IT assets aren't covered by enterprise patch management solutions.

**Enterprises are over-indexing on Windows client protection and not paying enough attention to Windows servers**

- Windows servers are the most vulnerable target, with 19% of all Windows servers missing endpoint protection, compared to 11% of Windows clients and 12% of MacOS assets

**MacOS assets are 2-3X more likely to be missing patch management than Windows clients and servers**

- 14% of MacOS are missing patch management vs. 5% of Windows servers and 4% of Windows clients

**Stale IT assets are an emerging, insidious threat**

- Stale IT assets are assets that appear in the security control console as being installed on the device but haven't checked into that control for a considerable period
- 3% of all IT assets are "stale" in terms of endpoint protection, while 1% of all IT assets have stale patch management coverage

## State of the Cybersecurity Attack Surface

**Increasingly complex enterprise environments have created chaos and enterprises are not adequately protecting their IT assets.**

Data aggregated from visibility into more than 500,000 IT assets indicates that lack of visibility into IT assets has created enterprises rife with vulnerabilities, with:

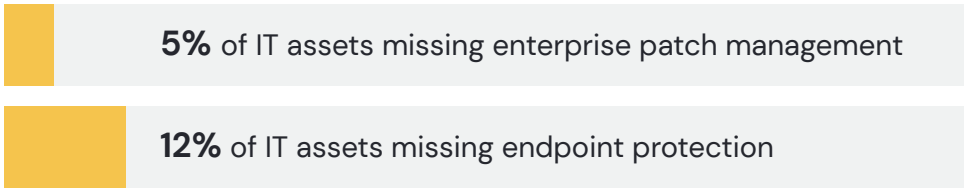
- 12% of IT assets are missing endpoint protection
- 5% of IT assets are uncovered by enterprise patch management solutions

Devices, servers, and other IT assets that are not running endpoint security are a critical and direct threat to organizations, serving as unguarded points of access to enterprise networks that can be exploited by malicious actors. Our data shows that 12% – nearly 1 of every 8 IT assets across a corporate network – lack endpoint protection.

An increasing number of modern attacks involve targeting unpatched servers and devices. Most enterprises have robust patch management tools that are effective at what they're designed to do: applying patches to **known** IT assets. Companies are not getting breached because their patch management tools are ineffective. They're getting breached because it's impossible to patch an **unknown** asset, as is the case with 5% of IT assets covered in this data set.

Without an accurate IT asset inventory count, security teams have no way of knowing if their operational risk mitigation controls such as endpoint security and patch management are deployed in the proper places. Too often, they are not.

**Figure 1:**




Assets not covered by endpoint protection or enterprise patch management

## Enterprises are over-indexing on Windows client protection and not paying enough attention to Windows servers

IT assets covered in this report were sorted into three primary categories:

- **Windows clients** – Systems running a Microsoft Windows XP through Windows 11 client or embedded operating systems
- **Windows servers** – Systems running Microsoft Windows Server 2003 through Windows Server 2022 regardless of intended function
- **MacOS assets** – Only systems running Apple's MacOS operating system and do not include iOS devices

Surprisingly, 19% of Windows servers – nearly 1 in 5 – lacked endpoint protection, far outpacing Windows clients (11%) and MacOS assets (12%). While common knowledge dictates that security teams would focus first and foremost on securing servers, which hold the enterprise crown jewels, our data indicates that this is not the case. There are several potential reasons for this lack of server protection.

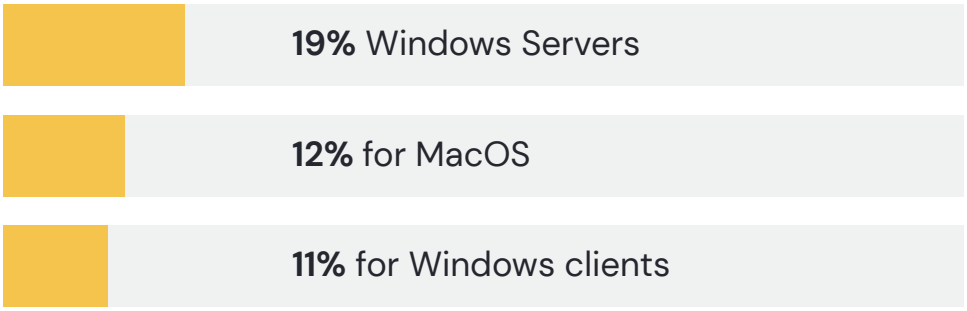
> "While common knowledge dictates that security teams would focus first and foremost on securing servers, which hold the enterprise crown jewels, our data indicates that this is not the case."

First, teams are loath to install anything on servers with the potential to impede functionality out of fear of interrupting revenue-generating activities. The business need for continuous uptime and seamless performance can trump security concerns for some organizations.

Additionally, unlike endpoint devices exposed to the outside world, servers sit behind a network that is already perceived as secure. This could lead to security teams viewing endpoint protection on servers as redundant or unnecessary, particularly in light of the aforementioned need for uptime and performance.

Deprioritizing server security can have significant consequences. In 2021, the HAFNIUM group targeted Microsoft Exchange Servers, allowing them to gain access to the servers and deploy web shells. The attackers were then able to gather credentials and exfiltrate information for further privilege escalation and lateral movement within impacted organizations.

**Figure 2.**




Percentages of different types of devices missing endpoint protection

## MacOS assets are 2-3X more likely to be missing patch management than Windows clients and servers

Roughly one in every seven (14%) Mac devices connected to corporate networks are operating outside of enterprise patch management programs, introducing significant security risks to organizations. At 2X-3X the rate of Microsoft devices (4%) and Microsoft servers (5%), this number stands out.

> "Mac devices have always enjoyed a better reputation for security than their Windows counterparts. Ironically, it may be this reputation that has given employees and security teams a false sense of security."

This may be in part because Mac devices have always enjoyed a better reputation for security than their Windows counterparts. Ironically, it may be this reputation that has given employees and security teams a false sense of security, leading them to deprioritize Mac security. Employees using Mac devices often do little to secure those devices beyond automatic updates, leaving them open to exploits in vulnerabilities to third-party apps.

**Figure 3.**


Percentages of different types of devices missing enterprise patch management

## Stale IT assets are an emerging, insidious threat

The risks associated with IT assets that are missing endpoint protection and patch management are relatively straightforward, but data points to the emergence of "stale" IT assets, which pose an even more insidious risk.

Stale IT assets are ones that appear in the security control console as being installed on the device but actually haven't checked in for a considerable period of time. For the sake of this report, we have defined stale assets as devices that had activity from any source in the past 14 days but no recorded activity from either patch management or endpoint protection during that same period.

"Stale IT assets are ones that appear in the security control console as being installed on the device but actually haven't checked in for a considerable period of time."

According to our data, 3% of all IT assets are "stale" in terms of endpoint protection, while 1% of all IT assets are stale from the perspective of patch management coverage. While there are several reasons why endpoint protection or patch management tools can fall off assets – an auto-upgrade might fail, or there could be an issue on the security tool's side – the end result is the same: an asset with stale security controls can be exploited by attackers.

While the volume of stale devices is not overwhelming, the risks they pose are more difficult to account for because they are essentially ticking timebombs posing as compliant assets. This is because the organization believes these assets have an agent installed on them and are therefore covered. However, security coverage isn't a true/false game. In the case of a stale device, the agent is installed but it's not checking in. That results in missing updates and probable malfunctioning agents. This is particularly insidious because someone might think the agent is installed and working – and therefore the asset is protected – but it isn't.

## Conclusion

The uncertainty of enterprise inventory – the elements that make up an organization's cybersecurity attack surface – upends the foundation of every major security framework and presents a challenge to security teams: it's impossible to protect what you can't see.

Today's hackers have a sophisticated understanding of where vulnerabilities exist across most enterprises, and they rely on unprotected, out-of-date IT assets as the easiest path to enterprise data. Securing your organization against the risks of vulnerable IT assets is a complex and multi-layered process. But until security teams can create a comprehensive, accurate IT asset inventory to mitigate against the threat of invisible or stale assets, attackers will continue to have the upper hand.

**Contact Us**

sevcosecurity.com

@SevcoSec

1401 Lavaca Street
#857 Austin, TX 78701

**About Sevco Security**

Sevco exists to fix a decades-old problem: attackers know the networks they target better than the companies that own them. Sevco is a cloud-native asset intelligence platform that delivers converged asset inventory and generates real-time asset telemetry, then publishes both for use by other IT systems. Sevco makes sense of the data our customers already have, making their existing products and procedures more effective. Founded in 2020, Sevco is based in Austin, Texas. For more information, visit https://sevcosecurity.com or follow us on LinkedIn and Twitter @SevcoSec.