SEVCO SECURITY

MARCH 2023

State of the Cybersecurity Attack Surface

Executive Summary

Remote and hybrid work have become standard operating procedure for many enterprises. It has increased productivity and employee satisfaction, but it comes with tradeoffs: when corporate networks extend into employee homes, enterprise attack surfaces expand along with them.

Employees today routinely log in from home, but that is often from their personal devices. The flexibility is necessary to empower remote workers, but there are a lot of security pitfalls. It's critical for enterprises to establish a basic understanding of what and where those devices are. This is foundational knowledge for security programs.

In the summer of 2022, we issued the first State of the Cybersecurity Attack Surface report, which revealed some troubling truths about the lack of visibility most enterprises have into their IT assets—and the risk that lack of visibility introduces. We identified real security gaps in the form of IT assets missing endpoint protection or not covered by enterprise patch management systems.

In our latest State of the Cybersecurity Attack Surface report, we continue to see enterprises struggle with these issues. We also examine a new and more imminent threat: IT assets that are accessing corporate networks but are not accounted for in any enterprise source. These assets consist largely of employees' personal devices connecting from home as well as devices and servers used in Shadow IT projects conducted outside the scope and purview of IT and security teams. In either case, these devices are missing the security tools that will protect your IT environment if the device is exploited. The risk here is clear: you can't protect the assets you can't see.

Finally, the report looks at an increasingly relevant issue as we head toward what many believe is an inevitable recession. At a time where companies are looking for ways to cut costs, our data shows that companies are paying for a staggering number of endpoint protection and patch management licenses for IT assets that may not be active.

Whether it's leading to increased spend on unused software licenses or creating gaps in visibility to increase your risk exposure, the inability to create a comprehensive IT asset inventory that accurately reflects the dynamic attack surface is costing companies. 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

Non-enterprise IT assets have proliferated across enterprises, creating a modern shadow IT environment with enormous security gaps.

- Data aggregated from visibility into nearly 1 million IT assets shows that 17% of all IT assets accessing corporate networks do not appear in any enterprise source, such as endpoint protection, configuration/patch management systems, directory services or mobile device management (MDM).
- 14% of Windows clients accessing corporate assets are not enterprise devices, 6% of Windows servers are not in any enterprise software inventory and 5% of MacOS devices accessing corporate assets are not enterprise devices.

In a time of cost cutting, enterprises are paying for a staggering number of unused stale software licenses.

- Approximately 17% of endpoint protection software is licensed but not in use.
- Approximately 6% of patch and configuration management software is licensed but not in use.

Enterprises continue to struggle with visibility into IT assets, resulting in networks rife with vulnerabilities.

- More than 19% of all IT assets are missing endpoint protection, while nearly 27% of IT assets are uncovered by enterprise patch management solutions.
  - This includes 23% of Windows servers missing endpoint protection and 21% of Windows servers going uncovered by patch management.

State of the Cybersecurity Attack Surface

Non-enterprise IT assets have proliferated across enterprises, creating a modern Shadow IT environment with enormous security gaps.

Data aggregated from visibility into nearly 1 million IT assets shows that **17%** of all IT assets accessing corporate networks do not appear in any enterprise source, such as endpoint protection, configuration/patch management systems, directory services or MDM tools. These non-enterprise devices are accessing enterprise networks, yet security teams have no visibility into the security of the devices. The findings reveal that:

- 6% of Windows servers are not in any enterprise software inventory
- 14% of Windows clients accessing corporate assets are not enterprise devices
- 5% of MacOS devices accessing corporate assets are not enterprise devices.

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

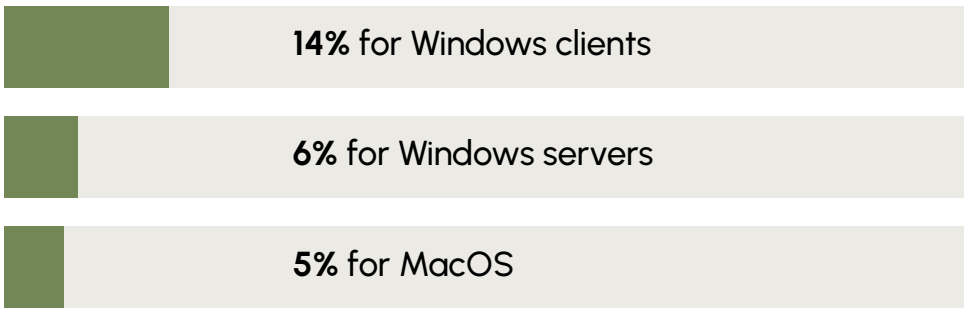
- **Windows clients**: Systems running a Microsoft Windows client or embedded operating systems;
- **Windows servers**: Systems running Microsoft Windows operating systems regardless of intended function; and
- **MacOS assets**: Only systems running Apple's MacOS operating system and do not include iOS devices.

Most concerning in these findings is the fact that 6% of Windows servers are not in any enterprise sources. The likelihood is that these are the result of Shadow IT: instances unsanctioned by IT or security teams that were spun up—likely without applying the company's security protocols—to accomplish some sort of specific task. Instead of decommissioning these servers, teams may have simply abandoned them. As a result these servers remain connected to the network as a potential attack surface access point. In other instances, the servers may be actively being used as part of an ongoing Shadow IT initiative.

The Windows clients evading detection are often systems or personal devices accessing a company's SaaS office automation assets but not in the company's MDM solution—or personal system connecting to the company's' IT infrastructure. While connecting to SaaS automation tools may be permissible, doing so at scale and without visibility into what assets are accessing the network introduces significant risk. The enterprise attack surface includes new devices and assets into which security teams have no visibility.

While personal devices will likely always access a company's IT environment—we have smartphones for this very purpose, after all—if they're not protected by mobile device management or other security tools, any exploit of the device could result in a breach of the company's IT environment. If a personal device is compromised, attackers will have access to everything the compromised device has access to. This is a problem for most employees, and it can be an existential threat if it is an IT or finance employee, or worse, someone with admin privileges.

Figure 1:



Percentage of different types of devices missing from any enterprise source.
These non-enterprise devices are unprotected and could be vulnerable to exploitation.

In a time of cost cutting, enterprises are paying for a staggering number of unused software licenses.

In this report we define stale licenses as devices that continue to appear in one instance of a company's inventory source (endpoint protection, for example) but is not identified in any other source—and the device agent hasn't reported in for more than 30 days. It's simple to see the issue here: these are devices with paid licenses that either no longer exist or devices that were incorrectly decommissioned. Either way, the company is paying for licenses that are not being used.

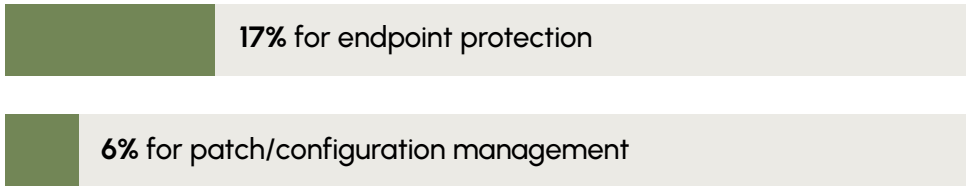
Our report finds that:

- Nearly 17% of endpoint protection software is licensed but not in use
- More than 6% of patch and configuration management software is licensed but not in use

"While connecting to SaaS automation tools may be permissible, doing so at scale and without visibility into what assets are accessing the network introduces significant risk."

In the face of economic headwinds, many companies find themselves in cost-cutting mode. At the very least, they must justify existing spend. Surveys have found CEOs are actively looking to contain costs and reduce discretionary spending. IT and security budgets are holding steady for most enterprises, but at a time when organizations are looking to tighten belts and cut costs, developing an accurate IT asset inventory can give teams an opportunity to right-size existing IT and cybersecurity spend, and to reallocate budget on more productive security tools and programs.

Figure 2:



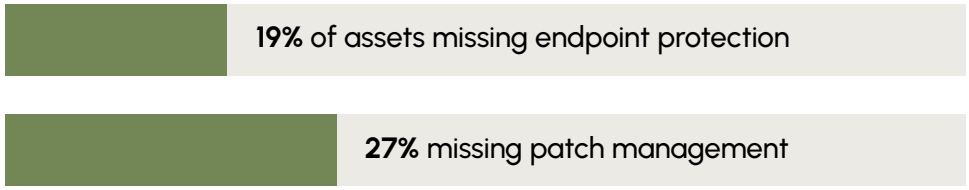
Percentage of stale licenses in different tools.
These are licenses for devices that no longer exist.

"At a time when organizations are looking to tighten belts and cut costs, developing an accurate IT asset inventory can give teams an opportunity to right-size existing IT and cybersecurity spend, and to reallocate budget on more productive security tools and programs. "

Enterprises are struggling with visibility into IT assets, resulting in networks rife with vulnerabilities.

The latest data shows that 19% of IT assets are missing endpoint protection while 27% of IT assets are missing from patch management.

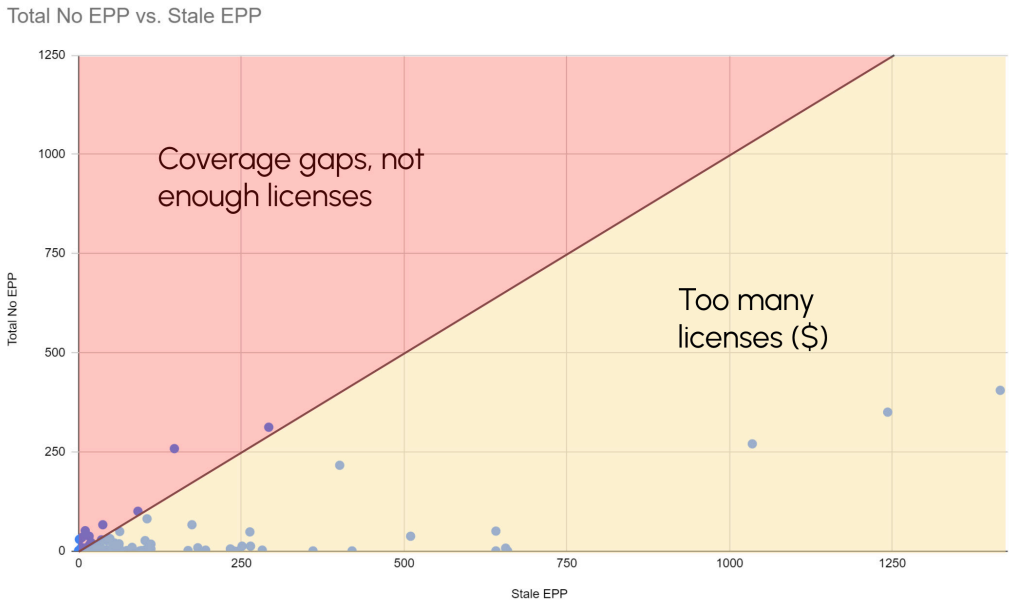
Figure 3:



Percentage of devices missing from endpoint protection or patch management.
These devices are active and visible in other tools.

Interestingly, the data showed very little overlap between organizations with stale licenses and organizations with security gaps, at least in the case of endpoint security. This demonstrates that these are discrete issues with their own sets of problems. Organizations with unknown security gaps may not have enough licenses and devices may be at risk, while organizations with stale licenses are overpaying for software – licenses for devices that no longer exist.

Figure 4:



With respect to endpoint security tools, there is very little overlap between organizations with stale licenses (who may be paying for too many licenses) and those organizations with security gaps (who have devices not protected by security tools).

Conclusion

Digital transformation has been a boon to the productivity of hybrid and remote workforces, but it has also expanded the enterprise attack surface exponentially. The diversity of devices, users, and applications being used by enterprises is more complex than ever before.

IT and security teams are challenged with keeping their environments operational and secure. But without knowing how many assets are in their environments, the difficulty of ensuring security is compounded. How do organizations secure what they can't see?

How do they protect assets from known vulnerabilities if they don't know about the assets themselves?

This underlines the importance of a comprehensive IT asset inventory, and why it's foundational to every compliance framework. Losing track of IT asset inventory is an enormous risk. Enterprises are littered with forgotten or abandoned deployments, any of which can be enough for malicious actors to gain a foothold.

What can enterprises do to secure the entirety of their attack surface?

- Complete an audit of security and IT tools to determine gaps in coverage—this requires correlating and deduplicating devices across sources to check coverage
- From this comprehensive inventory, determine if there are orphaned devices that might be vulnerable
- Consider implementing MDM to better secure personal devices

Last, once you have a comprehensive inventory, you can determine if you have stale devices in any of your tools—devices in a single tool which haven't checked in for, say, 30 days. IT and security teams should remove the devices from those tools and either reallocate the licenses to other devices, or deprecate the licenses to save costs or use the budget for more productive ends.

IT environments are constantly changing as new devices and new tools are introduced. Malicious actors have become very adept at leveraging those changes to take advantage of vulnerabilities. In order to maintain the upper hand against sophisticated adversaries, it is critical for IT and security teams to maintain an accurate and up to date asset inventory that reflects the reality of their dynamic IT environment.

Glossary of terms used in this report

IT asset: A device that is collected from an inventory source in the customer environment and correlated with devices collected from other sources to produce a unified devices inventory.

Source: An inventory source in the customer environment that can provide information about devices.

Orphaned IT assets: Assets that are either missing security controls or the agent on the devices is no longer communicating with them, creating additional vulnerabilities.

Stale licenses: Devices that continue to appear in one instance of a company's inventory source (endpoint protection, for example) but is not identified in any other source—and the device agent hasn't reported in for more than 30 days.

Windows clients: Systems running a Microsoft Windows client or embedded operating systems.

Windows servers: Systems running Microsoft Windows operating systems regardless of intended function.

MacOS assets: Only systems running Apple's MacOS operating system and do not include iOS devices.

Contact Us

sevcosecurity.com

@sevcosecurity

1401 Lavaca Street #857
Austin, TX 78701

About Sevco Security

Sevco is the cloud-native CAASM platform delivering the industry's most accurate, real-time IT asset inventory. Hundreds of companies rely on Sevco's 4D Asset Intelligence engine to bridge the gap between IT and security teams. By providing a continuously updated inventory of assets, Sevco autonomously identifies and closes previously unknown security gaps, while dramatically improving incident response. Sevco's patented asset telemetry uncovers significant security gaps and out-of-compliance assets in every deployment without fail. Founded in 2020 and based in Austin, Texas. For more information, visit https://sevcosecurity.com or follow us on LinkedIn.