SEVCO SECURITY

OCTOBER 2023

State of the Cybersecurity Attack Surface

Executive Summary

Modern enterprise attack surfaces are larger, more sprawling, and more complex than ever before—and it's a trend that is not going to reverse itself any time soon. While some companies are calling employees back to the office, the fact remains that remote work locations have become—and will remain—an extension of corporate networks.

At the same time, additional external forces have impacted the size and complexity of enterprise attack surfaces. Whether it's corporate layoffs leaving orphaned devices and other assets; new SEC rules that underscore the need—and demand accountability for—comprehensive, evidence-based intelligence on the assets, configurations, and security controls; or upcoming regulations like PCI DSS v4.0, the dynamics around the enterprise attack surface are continually changing.

One year ago, we issued the first State of the Cybersecurity Attack Surface report. That report exposed the fact that enterprises are struggling to get visibility into their IT assets. And more troublingly, that lack of visibility introduces security gaps and vulnerabilities. While enterprise attack surfaces and the dynamics surrounding them are in a perpetual state of flux, our data shows that there is one constant: the inability to really understand your attack surface is dangerous.

In our third State of the Cybersecurity Attack Surface report, we continue to see enterprises struggle with many of the same issues they've been grappling with—they are blind to IT assets missing endpoint protection, patch management, and, as we now include in this report, vulnerability management. "Stale" IT assets continue to proliferate across corporate networks. Organizations are unnecessarily paying for unused licenses while facing budget cuts and economic challenges.

We also examine how small businesses are faring in their efforts to safeguard their attack surface. Faced with the choice of defending their IT environment themselves or partnering with a managed security service provider (MSSP), it's evident that those MSSPs are there for a reason—they are very good at what they do.

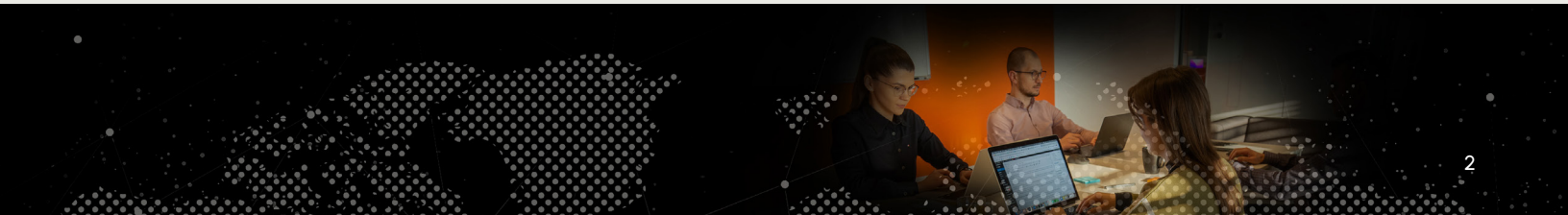
Finally, the report identifies some ticking timebombs that introduce tremendous levels of unnecessary risk: devices banned by the United States government and end-of-life devices that no longer receive critical security updates from their vendors of origin. While neither are found on networks at an overwhelming volume, there are thousands of such devices lurking—creating an easy entry point for malicious actors.

Please read on for our findings, and as the threat landscape continues to evolve, Sevco Security is committed to tracking the trends related to the cybersecurity attack surface.

Sincerely,

J.J. Guy

CEO and Co-Founder, Sevco Security



Key Takeaways

Stale IT licenses are rampant in most enterprises with costly impacts.

- Approximately 22% of endpoint protection software is licensed but not in use, up from 16% last year.
- Approximately 7% of patch and configuration management software is licensed but not in use, up from 6% last year.
- Approximately 24% of endpoint detection software is licensed but not in use, up from 17% last year.

Companies are still struggling to gain visibility into assets accessing their network—creating gaps in security.

- Data aggregated from visibility into nearly half a million IT assets shows that 11% of all IT assets are missing endpoint protection.
- The same data set shows that 15% of IT assets aren't covered by enterprise patch management solutions.
- A whopping 31% of IT assets are not covered by enterprise vulnerability management systems.

SMBs managing their own environments are among the most vulnerable.

- SMBs trying to secure their attack surfaces on their own are missing patch management on 27% of their devices, while SMBs working with a managed security service provider (MSSP) are missing patch management on just 3% of devices.
- SMBs trying to secure their attack surfaces on their own are missing endpoint protection on 21% of their devices, while SMBs working with an MSSP are missing endpoint protection on 4% of devices.

A surprising number of banned or seriously compromised assets are accessing enterprise networks.

- Nearly one-half of one percent of IT assets across enterprises have been banned by the US government.
- Approximately 1% of IT assets across enterprise environments are end-of-life, and half of those do not have endpoint protection.

State of the Cybersecurity Attack Surface

Stale IT licenses are rampant in most enterprises with costly impacts.

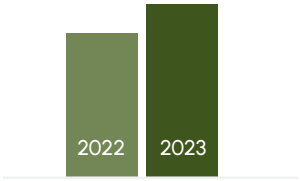
In this report, we define "stale" licenses as devices that still appear in a company's inventory source such as endpoint protection or patch management but are not visible in any other source—and the device agent hasn't reported into these tools for more than 30 days. These devices present a clear problem: 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:

- Approximately 22% of endpoint protection software is licensed but not in use, up from 16% last year.
- Approximately 7% of patch and configuration management software is licensed but not in use, up from 6% last year.
- Approximately 24% of endpoint detection software is licensed but not in use, up from 17% last year.

Over the past year, companies have been under increased pressure to cut costs, reduce new spending, and justify existing expenses. As a part of this industry-wide belt-tightening, employee layoffs have become commonplace. This data shows that not all companies are performing the necessary due diligence of decommissioning licenses for departing employees, resulting in an uptick in stale assets. The licenses for these stale assets represent potential additional cost savings.

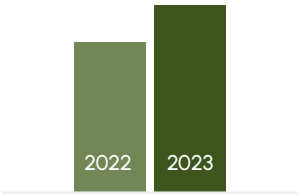
When cost savings are the driving force behind a reduction in the workforce, it is critical for companies to understand which licenses are associated with impacted workers. Developing an accurate IT asset inventory can give teams an opportunity not only to right-size existing IT and cybersecurity spend, but to ensure the appropriate licenses are decommissioned.

Figure 1: Stale licenses compared to last year



22% of endpoint protection software is licensed but not in use, up from **16%** last year

7% of patch and configuration management software is licensed but not in use, up from **6%** last year



24% of endpoint detection software is licensed but not in use, up from **17%** last year

Companies are still struggling to gain visibility into assets accessing their network, creating gaps in security.

Data aggregated from visibility into nearly half a million IT assets shows that a surprising number of IT assets accessing corporate networks services are missing critical safeguards, including endpoint detection, patch management, and vulnerability management. Our data shows that:

- 11% of all IT assets are missing endpoint protection.
- 15% of IT assets aren't covered by enterprise patch management solutions.
- 31% of IT assets are not covered by enterprise vulnerability management systems.

IT assets (including servers and devices) that are missing endpoint security represent a vulnerability and direct path for malicious actors to access enterprise networks. Our data shows that one out of every nine IT assets across a network is missing endpoint protection.

Additionally, threat actors are increasingly targeting unpatched servers and devices. While the majority of enterprises have patch management solutions in place, they can only patch known assets. It's the hidden or unknown assets going unpatched that introduce the highest level of risk. This problem is especially acute for macOS devices: 33% of macOS devices in enterprise environments without an asset intelligence solution are missing patch management, an especially acute problem given the recent BLASTPASS vulnerability that was discovered in September.

In addition to exacerbating security risks, these unknown IT assets also introduce risks around regulatory compliance. If IT and security teams do not know what devices are in their IT environment, it's unlikely that they'll be capable of fulfilling the requirements of most security compliance frameworks—especially in industries subject to strict regulations like PCI or HIPAA.

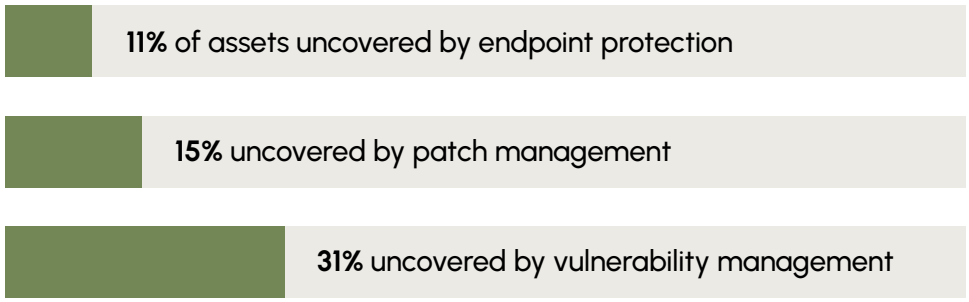
Fortunately, the data shows that organizations utilizing an asset intelligence solution are faring far better than companies that are not. When comparing subsets within our data, organizations utilizing an IT asset intelligence solution had nearly half the gaps in coverage of their patch management tool compared organizations without such a solution.

"If IT and security teams do not know what devices are in their IT environment, it's unlikely that they'll be capable of fulfilling the requirements of most security compliance frameworks—especially in industries subject to strict regulations like PCI or HIPAA."

The data shows that a significant portion of enterprise endpoints (31%) are not covered by a vulnerability management system, resulting in a large number of IT assets not receiving scans on a regular interval. As workforces have become more dynamic and dispersed post-COVID, this data points to failures in the traditional scanner-based systems used by many organizations, which have become ineffective for a more mobile workforce.

With so many enterprise endpoints going unscanned and introducing added risk, it is clear that organizations should be utilizing vulnerability management systems that have an agent component.

Figure 2:



SMBs managing their own environments are among the most vulnerable.

We examined data by company size and found that SMBs, which we define as organizations with fewer than 3,500 employees, working on their own to secure their attack surface are by far the most vulnerable organizations. However, SMBs working with a managed security service provider (MSSP) to protect their attack surface are among the most secure organizations. Our data shows that:

- **21%** of IT assets are missing endpoint protection for SMBs that do not use an MSSP, compared to **4%** for organization partnering with MSSPs.
- **27%** of IT assets are missing patch management for SMBs that do not use an MSSP, compared to **3%** for organization partnering with MSSPs.

Small businesses have IT and security budgets that are stretched thin. With that comes smaller security teams and fewer resources to defend their dynamic attack surface. Defending IT assets against malicious actors is a challenge for large enterprises with seemingly limitless budgets—but it's nearly impossible for SMBs to accomplish internally. Our data underscores the critically important role that MSSPs play in helping small businesses secure their environments, enabling them to focus on executing their core business.

A surprising number of banned or seriously compromised assets are accessing enterprise networks

Perhaps the most surprising data point unearthed by researchers: nearly 0.5% of IT assets across enterprise networks are devices that have been banned by the United States government.

These devices, which include IOT devices manufactured by Huawei, ZTE and Hikvision, are explicitly banned from being on government networks or networks supporting government entities. They are banned because they are known vectors for embedded malware and other types of illicit activity, representing direct and actively exploited threats to the enterprises whose networks they are attached to.

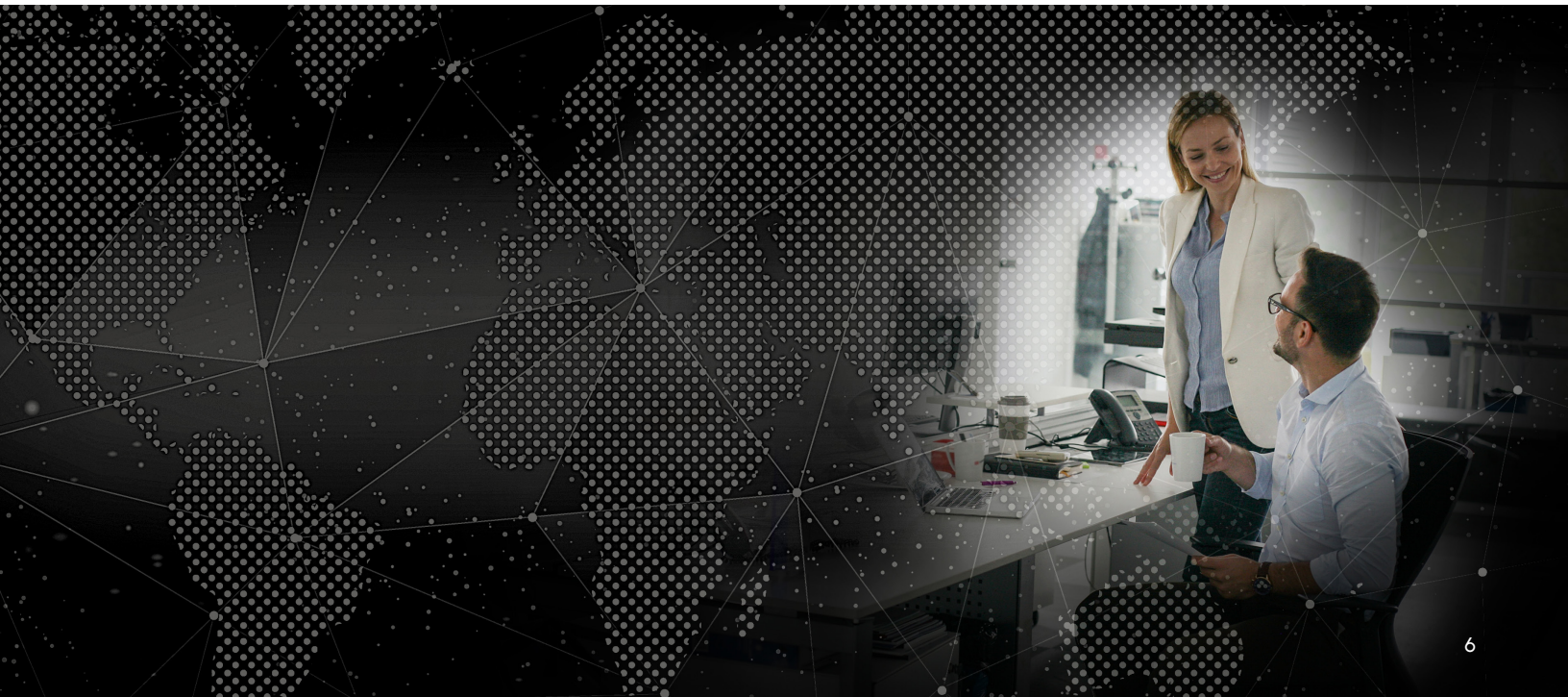
Interestingly, the vast majority of organizations comprising the data set have zero banned devices on their network.

For those that do have these devices, they tend to have quite a few. One organization had banned devices comprising 7.5% of their IT asset inventory.

Additionally, approximately 1% of devices connecting to enterprise networks have software classified as "end of life," meaning that they are no longer receiving support or software updates from the vendor that created them. When new vulnerabilities are discovered in end-of-life devices, there is no mechanism for fixing them.

These devices, which are frequently exploited by malicious actors on the hunt for easy targets, exist as persistent threats to their networks. They also introduce regulatory compliance concerns associated with operating unsupported operating systems. For example, Windows 7, went end of extended support in January 2023. Many people did not notice the date. However, there are still a large number of systems, including those covered by PCI DSS, that are utilizing Windows 7 in production environments. This poses a significant risk.

Organizations with end-of-life devices on their networks must be able to identify those devices and remove them or replace them with newer, supported software, but often lack the visibility to do so without an accurate IT asset inventory.



Conclusion

Enterprise IT environments are synonymous with the cybersecurity attack surface. Fueled by increasing IT complexity and a broad set of external forces, including a shifting regulatory compliance landscape and workforce trends, those environments are in a constant state of flux.

Unfortunately, security teams are up against a natural imbalance of power. Attackers only need to find one unprotected or exposed asset, but security teams have the arduous task of finding and protecting every IT asset. Enterprises are filled with forgotten or abandoned devices and servers, and malicious actors have become very adept at exploiting those openings to get a foothold into corporate networks.

The findings in this report underscore the need for enterprises to take a more proactive approach to identifying vulnerabilities and go on the offensive with technology that identifies and drives remediation for vulnerable conditions. This means changing the mindset from vulnerability management to vulnerability hunting: finding and eliminating these weak points before attackers can exploit them.

Protecting dynamic enterprise environments is a challenge for security teams, and it is exacerbated by the simple fact that most organizations do not have an accurate inventory of the IT assets connected to their ever-changing, dynamic network. This lack of visibility is a foundational issue that limits attack surface visibility, puts organizations at significant risk of regulatory non-compliance, and leads to unnecessary spending on IT licenses that are not being used.

To effectively protect expanding and changing cybersecurity attack surfaces, security and IT teams must work together to develop a comprehensive understanding of their IT assets—where they are, how many there are, and which ones are putting them at risk. It's only with that visibility that security teams will be able to proactively prioritize response efforts and uncover security risk vulnerabilities faster.

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.

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

End-of-life devices: Devices that are no longer receiving software updates from the vendor that created them.

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.