SEVCO SECURITY

JUNE 2024

State of the Cybersecurity Attack Surface

Executive Summary

As an industry, we have become quite proficient at identifying and quickly remediating CVEs. Security teams ingest, process, and act on information related to these critical vulnerabilities with astonishing velocity. But within the enterprise environments that CVEs threaten, there exists a quieter, more nefarious threat. There are lurking dangers that continue to go unnoticed, and more importantly unpatched—environmental vulnerabilities.

These environmental vulnerabilities—vulnerabilities in the configuration or state of your IT environment, be they missing controls, unknown assets (shadow IT), or system software that is out of date and end-of-life—are hiding in plain sight throughout enterprise environments, creating a landscape of threats that security teams can't see, but are still accountable for. They may not drive headlines the way that high-profile CVEs like Log4Shell or Spring4Shell have, but the threat they introduce to enterprise environments is just as dire.

Over the past several years, Sevco Security has issued its semi-annual State of the Cybersecurity Attack Surface report, which examines the ways in which enterprises are struggling to get visibility into their IT assets. In this latest version, we look at data from Sevco prospects and customers showing the extent to which enterprises are susceptible to these insidious environmental vulnerabilities. Throughout enterprise environments, IT assets are missing critical controls such as endpoint protection and patch management, creating environmental vulnerabilities that leave paths to data exposed, and companies susceptible to malicious actors. Our report found that **28% of all IT assets are missing at least one critical control**—either endpoint protection or patch management.

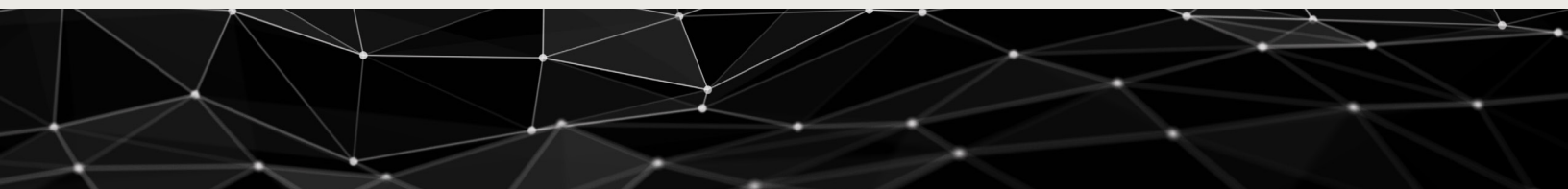
The report also highlights some ticking timebombs that are threatening IT environments. IT assets connecting to enterprise networks have software classified as "end of life" (EOL), meaning that they no longer receive support or software updates from the vendor that created them. These EOL assets create instances of known-but-unpatched environmental vulnerabilities across enterprise networks, and our data shows that **6% of all IT assets have reached the EOL stage.**

And finally, for the first time this report will look beyond the data and examine how the issues represented by the data manifest themselves in customer environments.

Sincerely,

J.J. Guy

CEO and Co-Founder, Sevco Security



Key Takeaways

Environmental vulnerabilities are rampant, resulting in massive security gaps across enterprise networks

- Data aggregated from visibility into 1.2 million assets shows that 28% of all IT assets are missing at least one critical control—either endpoint protection or patch management
- The same data set shows that 22% of IT assets aren't covered by enterprise patch management solutions, while 10% of all IT assets are missing endpoint protection.

End-of-life (EOL) assets are common in enterprise networks, allowing malicious actors to exploit known-but-unpatched vulnerabilities

- Across the data set, more than 6% of all IT assets have reached the end-of-life stage, creating instances of known-but-unpatched vulnerabilities.
- 23% of IT assets are not covered by enterprise vulnerability management systems.

State of the Cybersecurity Attack Surface

Environmental vulnerabilities are rampant, resulting in massive security gaps across enterprise networks

For the sake of this report, we are narrowing our focus to one type of environmental vulnerability: IT assets that are missing at least one critical control—either they are missing endpoint protection, or they are assets that are not covered by enterprise patch management solutions.

Data aggregated from visibility into **1.2 million** IT assets, including servers and devices, shows that a surprising number of these assets accessing corporate networks services are missing critical safeguards, including endpoint detection and patch management. Our data shows that:

- 28% of IT assets are missing at least one critical security control, creating enterprise networks rife with environmental vulnerabilities.
- 22% of IT assets are not covered by patch management solutions.
- 10% of IT assets are missing endpoint protection.

Environmental vulnerabilities are an underreported cause of security gaps. Security leaders often say that vulnerability management is their primary technology investment area but IT attack surfaces are still filled with environmental vulnerabilities, with more **than one in four IT assets missing at least one critical security control.**

High-impact CVEs are the threats that drive headlines and get attention, but it's these environmental vulnerabilities that present a more persistent and nefarious threat to organizations. The root cause for these environmental vulnerabilities is more organizational than technological: it stems from the simple fact that most organizations have separated responsibility for maintaining assets (IT) and those accountable for securing those assets (Security). The root of the environmental vulnerability problem is not a failure of technology nor a failure of security and IT teams; it's a failure of the organizational structures we've built to address these issues.

These structural issues have led to IT environments that are putting companies at risk. When IT assets are missing endpoint security, malicious actors have a direct path to their networks. Devices and servers that are uncovered by vulnerability management solutions create a more dire threat because they aren't being scanned for CVEs. And devices and servers missing from patch management tools may have CVEs on them, but they aren't getting patched, leaving them open to exploitation by bad actors. Most enterprises are highly proficient at patching known IT assets, but it's the hidden or unknown assets that go unpatched that introduce the highest level of risk.

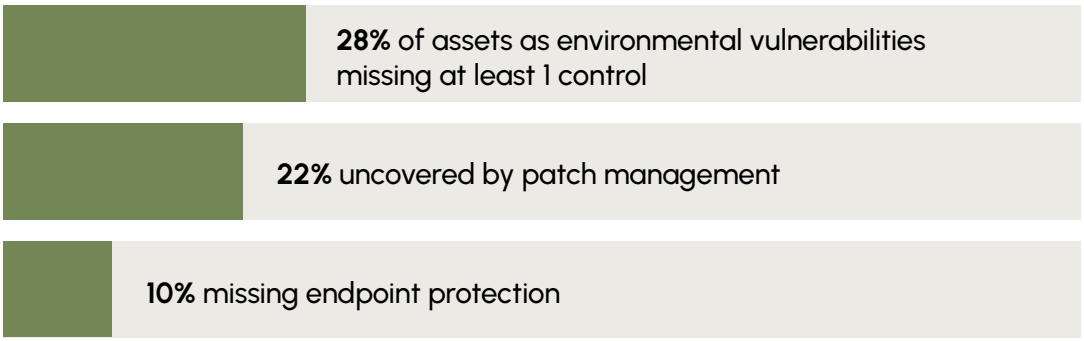


Figure 1: Environmental vulnerabilities like missing controls are rampant in IT environments

End-of-life (EOL) assets are common in enterprise networks, enabling malicious actors to exploit known-but-unpatched vulnerabilities

Trusted systems that have been in use for a long time are fertile ground for environmental vulnerabilities. Hardware, software and IoT devices that have been deployed for years will frequently reach the end-of-life stage, when a provider has ended mainstream support but still offers limited extended support. Our data shows that:

- Across the data set, more than 6% of all IT assets have reached the end-of-life stage, creating instances of known-but-unpatched vulnerabilities
- 23% of IT assets are not covered by enterprise vulnerability management systems.

These EOL IT assets, once vulnerable, will remain easy targets for malicious actors until removed from the network. Rife with well-known, actively exploited vulnerabilities but without the ability to patch, assets nearing or reaching their EOL stage abound in many organizations, often below the radar of IT teams.

Unlike novel attacks that require resources and creativity, known but unpatched vulnerabilities are low hanging fruit: easy to exploit using existing, proven techniques. The low effort/high yield combination makes known-but-unpatched vulnerabilities among the most popular targets for malicious actors. They pose a severe risk to cybersecurity and IT operations if not addressed.

Additionally, the data shows that nearly one in four enterprise endpoints (23%) are not covered by a vulnerability management system, resulting in a large number of IT assets not receiving scans on a regular interval. Vulnerability scanning allows organizations to identify changes to their IT environment that may signal increased risk. When assets are not included in regular vulnerability scans, it leaves the IT environment more vulnerable to attacks—both through exploited CVEs and environmental vulnerabilities.

There are times when EOL systems are inevitable. For example, you may have a service that only works with Windows XP. But it's important for security teams to be aware of those scenarios so that they can provide extra protection with mitigating controls for these devices and ensure they're scanned regularly for vulnerabilities.

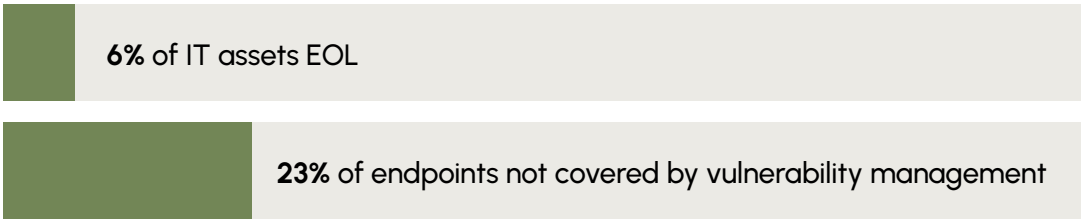


Figure 2: Issues leading to known-but-unpatched vulnerabilities

Beyond the Data: Environmental Vulnerabilities in Enterprise Environments

Data points that indicate the prevalence of environmental vulnerabilities are useful because they can illustrate the extent of the issue. But when enterprises are trying to safeguard their environments, data points don't help them. For the first time, this report will detail real-world examples from Sevco customers and prospects that demonstrate how these environmental vulnerabilities can manifest themselves throughout the enterprise.

Old servers and operating systems, leading to incomplete migrations

As IT and security teams dig into their IT asset inventories, many companies find operating systems and servers they didn't believe were in the environment. As shared in this report, across the average enterprise environment, more than 6% of all IT assets have reached the end-of-life stage, creating instances of known-but-unpatched vulnerabilities.

When one organization turned to Sevco to better understand its IT asset inventory, our team identified that more than 14% of IT assets had reached the EOL stage, including multiple instances of server operating systems as old as Windows Server 2003, and desktop operating systems back to Windows 7. These EOL operating systems in critical areas of enterprises are environmental vulnerabilities that could be open to exploitation.

Limited visibility into migrations

Unfortunately, identifying the vulnerable assets and migrating them to a newer OS is not as simple as it may seem. When this company underwent a large migration to upgrade from EOL systems, the security team mandated that business units roll out the upgrade. While business units confirmed that the migration had taken place, there was no process in place to verify. A subsequent scan by Sevco revealed a 41% improvement in devices that had reached EOL stage, but surprisingly 8% of assets remained EOL despite the business units confirming they'd completed the migration.

Without the scan from Sevco, there was no way to verify that the migration had taken place. Mandating a migration and relying on business units to confirm can create a false sense of security that the environment is running on the latest, updated software—when the fact remains that environmental vulnerabilities, including EOL assets, continue to be pervasive.

Inaccurate sources of truth for endpoints

When the same company attempted to verify that its IT assets were all covered by endpoint security, environmental vulnerabilities made it impossible for them to do so accurately. This company's configuration management tool reported that all endpoints were in the system. However, a subsequent scan from Sevco revealed that, while the configuration management system was reporting full coverage, 2 percent of enterprise endpoints were absent from the system—a validation failure that put the organization at risk.

In this case, the customer was using its configuration management tool as the single source of truth for the security team, which had been given a false sense of security about the extent of its endpoint protection.

Conclusion

Security teams have become adept at identifying, prioritizing, and remediating CVEs but are still far too susceptible to environmental vulnerabilities. These environmental vulnerabilities threaten the security of organizations and jeopardize the intellectual property of organizations and personal information of consumers, but organizations are failing to address them despite investing in tools designed to enable them to do so. This growing vulnerability backlog—and the inability to effectively address it—presents grave risks to organizations.

The findings in this report demonstrate that organizations have limited visibility into cyber asset attack surfaces, which upends the foundation of every major security framework and presents a challenge to security teams: they can't protect what they can't see. Maintaining accuracy in a dynamic environment is a challenge, and enterprises are struggling to track changes over time. To truly understand your attack surface, you must be able to centralize known and surface previously unknown vulnerabilities in one place, prioritize the most critical issues across the environment, automate the remediation to fix priority issues, and validate that remediation efforts are actually completed.

When organizations fail to achieve these things and environmental vulnerabilities continue to lurk across enterprise networks, the easy, knee-jerk reaction is to treat it as a failure of security teams to adapt. But the reality is that these are failures of the organizational structures we've built to address the issues, leading to a misalignment between IT and security teams.

The way forward is to address the organizational issues that enable these vulnerabilities to exist and prevent those responsible and accountable for addressing them from doing so effectively and efficiently. Additionally, security teams should incorporate tools that provide visibility to enable cross-department accountability. Until that happens, we will continue to see enterprise networks filled with environmental vulnerabilities.

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.

Environmental vulnerability: For the sake of this report, we are classifying an IT asset that is missing at least one critical control—either they are missing endpoint protection, or they are assets that are not covered by enterprise patch management solutions—as environmental vulnerabilities. The broader definition includes any vulnerabilities in the configuration or state of your IT environment, be they missing controls, unknown assets (shadow IT), or system software that is out of date and end-of-life.

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 asset intelligence company that delivers enterprise-wide visibility and prioritization across all classes of vulnerabilities. Built upon the industry's most accurate, real-time inventory of an organization's devices, users, software, and controls, Sevco enables CISOs and security teams to fully understand the risk and business impact of unaddressed vulnerabilities for more informed prioritization. Sevco automates and validates remediation, tracking metrics to close the loop between issue identification and remediation to drive more proactive security. Founded in 2020 and based in Austin, Texas. For more information, visit https://sevcosecurity.com or follow us on LinkedIn.