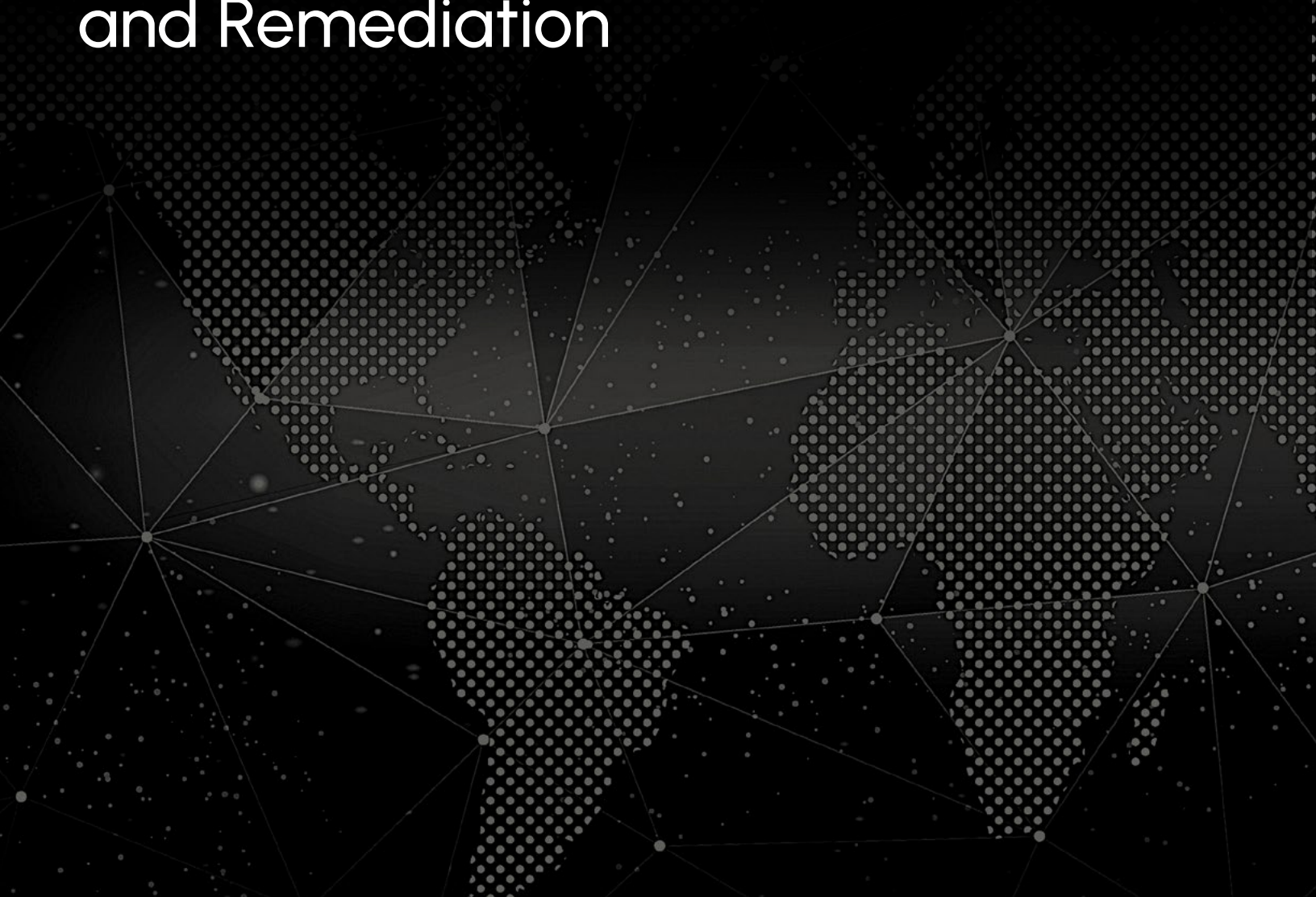
SEVCO SECURITY

WHITE PAPER

Modernize Your Vulnerability Management

Key Tactics for Prioritization and Remediation



Introduction

Security and vulnerability management teams are in a never-ending race against time to find and shut down vulnerabilities. Today's adversaries are faster and stealthier than ever, taking advantage of unpatched systems, misconfigurations, and gaps in security coverage.

But security teams, burdened with incomplete asset inventories, an overwhelming volume of vulnerabilities, and manual prioritization processes often find themselves outpaced by attackers. The result? A staggering 60% of breaches happen because of vulnerabilities that go unpatched—even when a fix is available.[1]

Security leaders know the stakes are high, but the scale of modern IT environments makes traditional approaches to comprehensive vulnerability management feel like a monumental task. With security risks to manage across a sprawling digital landscape, the challenge isn't just identifying vulnerabilities—it's about knowing which ones to prioritize. The complexity only grows when vulnerabilities extend beyond software to include environmental vulnerabilities like configuration errors, missing security controls, and even unmonitored devices.

This paper examines the root causes of the vulnerability management challenge and explores strategies that can help security teams to prioritize and manage risk at scale. The goal? To flip the script on vulnerability management, equipping security teams with the tools to confidently prioritize the most critical risks and thwart attackers before they strike.

A staggering 60% of breaches happen because of vulnerabilities that go unpatched—even when a fix is available.[1]

[1] Ponemon Institute. Cost and Consequences of Gaps in Vulnerability Response

Overwhelming volumes: The new norm

One of the most daunting challenges security teams face today is the sheer volume of vulnerabilities that they must continuously manage. With thousands of potential risks emerging daily, keeping up has become a near-impossible task. As the number of vulnerabilities grows, so does the complexity of managing and remediating them.

What's behind this surge? To effectively modernize vulnerability management, it's crucial to first identify the key factors driving the increasing volume and complexity.

Modern IT complexity

One of the biggest forces fueling the rise in vulnerabilities is the growing complexity of modern IT infrastructures. Organizations are increasingly adopting cloud technologies, operating hybrid infrastructures, and enabling remote workforces—expanding the digital footprint and, with it, the attack surface. Every endpoint, remote worker, third-party integration, and cloud asset represents a potential entry point for attackers.

The scale of the challenge is staggering. Just considering common vulnerabilities and exposures (CVEs)—which represent only a subset of vulnerabilities—the volume is expected to increase by 25% in 2024, amounting to roughly 2,900 new vulnerabilities each month.[2] For security teams already stretched thin, that's a relentless flood of risks to assess, prioritize, and remediate.

Likewise, as the attack surface grows larger and more complex, the more difficult it becomes to track and secure every asset. Unmanaged or hidden assets often slip through the cracks, and it's these overlooked environmental vulnerabilities and security gaps that frequently fly under the radar. Indeed, unmonitored assets contribute to over 50% of breaches today.[3]

Just considering common vulnerabilities and exposures (CVEs)—which represent only a subset of vulnerabilities—the volume is expected to increase by 25% in 2024, amounting to roughly 2,900 new vulnerabilities each month.

[2] Security Magazine. CVEs expected to increase 25% in 2024

[3] Spiceworks. External Exposure Management: Are Your Attack Surfaces Safe?

SEVCO SECURITY

Environmental vulnerabilities

While software flaws tend to dominate vulnerability management efforts, they are just one part of the equation. Environmental vulnerabilities pose an equally significant threat. These environmental issues, often overlooked, contribute heavily to the overwhelming volume of risks. Here are some of the most critical types of environmental vulnerabilities that security teams must manage:

Devices missing security controls

A major contributor to the growing vulnerability problem is the sheer number of devices operating without critical security controls. When endpoint detection and response (EDR), vulnerability scanning, or patch management are absent or misconfigured, these devices become easy targets for attackers.

And the scale of this issue is significant. Based on Sevco Security research, 28% of an organization's IT assets are missing at least one crucial control, such as endpoint protection or patch management.[4] Without proper controls in place, these assets pose a significant risk to the organization.

End-of-life systems

Another significant vulnerability threat is the prevalence of end-of-life (EOL) systems. These assets, which no longer receive security patches or updates from their vendors, remain connected to enterprise networks, creating a persistent risk of known-but-unpatched vulnerabilities.

Sevco Security research indicates that 6% of an organization's IT assets are in the EOL stage.[5] As these systems are no longer supported, they become prime targets for attackers who are aware of their inherent weaknesses. Adversaries often seek out these outdated systems knowing they offer easy access to critical systems and data.

Shadow IT

The rise of shadow IT—systems and devices that operate without IT's knowledge—presents a significant challenge for vulnerability management. A staggering 17% of an organization's IT assets are missing from inventory tracking, making them invisible to vulnerability scans and assessments.[6]

The foundation of every vulnerability management program relies on an accurate and real-time asset inventory. Without a complete asset inventory, security teams can't protect what they can't see. And this leads to a high volume of environmental vulnerabilities that pose significant risk.

Reality check for comprehensive vulnerability management

The uncomfortable truth is that most vulnerability management programs still focus almost entirely on software vulnerabilities, ignoring the broader scope of environmental risks. The overwhelming volume of vulnerabilities isn't just due to software flaws—it's compounded by the unmanaged, unprotected, and unmonitored assets lurking in every corner of the organization's digital estate.

When environmental vulnerabilities are left out of the equation, remediation efforts are incomplete. Security teams may be pushing patches, but if controls are misconfigured or assets are invisible to vulnerability scans, those patches aren't being applied where they're needed most. This not only compounds the overall vulnerability volume but also wastes time and resources as efforts to remediate are often misaligned with the real risks.

[4,5,6] Sevco Security. State of the Cybersecurity Attack Surface

Challenges with prioritization

A critical component of effective vulnerability management is the ability to prioritize threats based on their potential risk and impact. With the ever-increasing volume of vulnerabilities, security teams face a daunting task: determining which threats to address first.

The reality is that security teams will rarely, if ever, reduce the vulnerability count to zero, so focusing on where to invest time, resources, and energy is crucial. However, several key issues complicate this prioritization process.

Siloed vulnerability data sources

One of the biggest challenges organizations face is the fragmentation of vulnerability data across multiple systems. For example, it's not uncommon for teams to rely on different tools: one for network vulnerabilities, another like a vulnerability scanner for software flaws, and yet another for exposure management. However, these tools often operate in silos, and the data they produce isn't reconciled.

This scenario is all too common in vulnerability management. Security professionals must manually analyze and reconcile data from various sources, leading to a scattered, incomplete picture of the organization's risk landscape. This process is not only time-consuming but also prone to inaccuracies, as the full context of vulnerabilities may be lost or misinterpreted when data is fragmented.

Manual efforts

The challenge of manually consolidating and prioritizing vulnerabilities from various sources adds a significant layer of difficulty for security teams. With the sheer volume and complexity of data they must navigate, it's no wonder that 72% of security professionals cite difficulties with prioritizing vulnerabilities as a major cause of delays in their response efforts.[7]

In practice, security teams are inundated with thousands of new vulnerability alerts each day. The manual process required to sift through and assess these alerts is both labor-intensive and time-consuming. As a result, 77% of security teams report that they lack the necessary resources to manage the volume of patches required, further compounding the problem.[8]

Missing contextual insights

Another critical issue with prioritizing what's an active risk is the lack of contextual insights and exploit intelligence. Simply relying on metrics like Common Vulnerability Scoring System (CVSS) or Exploit Prediction Scoring System (EPSS) often fall short as they don't provide a complete picture of the risk. For example, a vulnerability may have a high CVSS score but is not being actively exploited in the industry or region, making it a lower priority. Conversely, a lower-severity vulnerability could pose a significant risk if it's being actively exploited or if it affects a critical business asset.

This is where risk-based vulnerability management (RBVM) comes into play. RBVM emphasizes prioritizing vulnerabilities not just based on severity scores, but by considering the actual risk to the organization. Effective prioritization requires a thorough understanding of business impact, using risk factors like asset importance, exploitability, and asset accessibility. Security teams need to evaluate whether an asset is critical to operations where the organization operates, whether it's exposed to external threats, and if there's evidence of active exploitation in their specific context.

Without these insights, teams may mistakenly deprioritize vulnerabilities on high-value assets or waste time addressing vulnerabilities that don't present an immediate threat. This misalignment leads to ineffective risk management and leaves organizations vulnerable to targeted attacks.

[7,8] Ponemon Institute. Cost and Consequences of Gaps in Vulnerability Response

Strategies to modernize vulnerability management

Vulnerability management is the backbone of any solid security strategy, but today's overloaded systems demand a fresh approach. Security teams need more than just band-aid solutions—they need a strategy that cuts through the noise and delivers real protection.

By adopting the right tools and modernizing their vulnerability management processes, organizations can shift from constantly playing catch-up to a more proactive, risk-based approach. This allows teams to focus on the vulnerabilities that matter most, close response gaps, and stay ahead of the evolving threats in today's complex IT landscape.

Strategy 1: Include environmental vulnerabilities

Vulnerability management today often centers on software flaws, but to build a truly resilient defense, security teams need to expand their focus to include the broader environment. A significant paradigm shift is needed—one that emphasizes environmental vulnerabilities just as much, if not more, than software vulnerabilities.

Why prioritize environmental vulnerabilities? Because without addressing the security gaps in the environment, software vulnerability management alone will always fall short. Consider this: assets missing vulnerability assessment or patch management are effectively invisible in your vulnerability management program. Teams could be diligently applying patches to known software flaws, but if entire systems or devices are unaccounted for, those efforts will always deliver incomplete protection.

Take it a step further—if security teams are relying on EDR as a safety net for those devices, the risk doesn't disappear. What happens when an asset is missing both EDR and vulnerability assessment controls? That's a massive blind spot, and attackers know it. By prioritizing environmental vulnerabilities, organizations will close these gaps and elevate their vulnerability management effectiveness.

This approach shifts vulnerability management from a reactive, patch-focused process to a proactive, holistic strategy. It challenges the traditional view and gives security teams a clearer, more comprehensive view of the risks that matter most.

Strategy 2: Automate vulnerability prioritization

Given the overwhelming volume of vulnerabilities, accelerating prioritization is essential. Manually sifting through countless vulnerabilities across siloed systems is slow, resource-intensive, and prone to error. To keep pace, security teams need to embrace automation to streamline this process.

Automation technology can intelligently consolidate data from disparate vulnerability sources, quickly rationalizing and prioritizing vulnerabilities based on pre-defined criteria, such as severity, exploitability, and asset importance. The speed automation brings is key—it enables teams to focus on high-priority threats first, leaving no room for guesswork or wasted effort. By shifting from manual triage to automated prioritization, security teams can overcome the flood of vulnerabilities and respond to the most critical threats faster than ever.

Strategy 3: Prioritize based on business context

Vulnerabilities differ in their potential impact, which is why context matters. It's not enough to prioritize threats based on technical severity alone. To make vulnerability management truly effective, teams must consider the business relevance of each vulnerability. This is where the latest technology, equipped with business context and exploit intelligence, plays a pivotal role.

The technology should automate the analysis of business context by gathering asset intelligence and evaluating attributes across the environment—such as who interacts with the assets, their location, and the software installed. Using predefined rulesets or custom queries, security teams can automate this analysis, ensuring vulnerabilities are prioritized based on their actual impact to the business.

This approach not only saves time but also ensures that both environmental and software vulnerabilities are addressed with the urgency they demand. This way, teams can efficiently protect critical assets and make informed decisions without being overwhelmed by the volume of potential threats.

Strategy 4: Validate remediation is complete

While IT and security teams share the same goal of protecting assets, they often operate in silos, making it hard to ensure that remediation efforts are fully completed. In fact, 32% of organizations say tracking remediation progress is one of the biggest challenges when it comes to managing security risk.[9]

To mature vulnerability management processes, it's essential to verify that remediation actions, such as installing patches or deploying missing EDR agents, have actually been completed. A closed IT ticket doesn't guarantee that a vulnerability was remediated. Rather than relying on ticket closures as proof of completion, organizations must validate—at the asset level—that the fix was implemented.

Security teams can use a unified platform that—in addition to supporting the previous strategies— validates remediation by confirming whether software updates, agent deployments, or upgrades to end-of-life operating systems have been successfully applied to each asset. As part of the remediation validation, the platform should also track key metrics—such as mean time to remediation (MTTR)—so teams can easily monitor their performance against service-level objectives (SLOs).

By validating remediation and tracking MTTR metrics, security teams can consistently surface any issues with the remediation process that need to be addressed, establish a more robust security posture, and enhance the overall effectiveness of their vulnerability management efforts.

[9] Hyperproof: 2024 IT Risk and Compliance Benchmark Report

Sevco's approach

Sevco simplifies vulnerability management by aggregating and correlating data from all existing IT and security tools to produce a comprehensive inventory of an organization's devices, identities, software, vulnerabilities, and the controls deployed to protect them along with the associated attributes for these assets reported by each system. Sevco's synthesis of these disparate perspectives generates the most comprehensive and accurate real-time view of asset and vulnerability information coupled with their business impact and enriched with exploit intelligence from VulnCheck.

Sevco provides a seamless approach to manage all vulnerabilities—software and environmental—addressing the full scope of potential risks in an organization's environment. By automating the process of identifying and prioritizing vulnerabilities, Sevco empowers security teams to cut through the noise. The Sevco platform brings business context into every prioritization decision, allowing teams to focus on the most immediate and relevant risks. Whether it's an emerging exploit or a critical asset in need of protection, the platform provides real-time insights so that teams can direct their resources where they matter most.

Sevco's approach empowers teams to overcome the inefficiencies of manual processes and siloed tools. With real-time, actionable insights, teams can confidently and proactively prioritize vulnerabilities to close gaps in vulnerability response and validate their effective remediation.

Conclusion

Today's fragmented and manual approaches to prioritizing vulnerabilities are pushing security teams to their limits. When so much time and effort is spent juggling disparate data sources, patching the same vulnerabilities over and over, and sifting through massive volumes of alerts and lists of potential risks, it's no wonder critical threats fall through the cracks. The result is a vulnerability management program that can't keep pace with the growing complexity of modern IT environments.

To modernize vulnerability management, teams need a shift in strategy—one that incorporates a holistic view of the attack surface, automates prioritization, and applies business context to every decision. By focusing not just on software flaws but also environmental vulnerabilities and leveraging automation to scale efforts on what to prioritize, security teams can direct their resources toward active risks that matter most to the organization.

Sevco's comprehensive, real-time approach to vulnerability management delivers the tools and insights organizations need to transform their vulnerability management programs. By providing a unified platform that integrates real-time asset intelligence and vulnerability insights with critical business context, Sevco empowers organizations to scale their efforts and effectively address their most pressing security risks.

Ready to elevate your vulnerability management strategy? Book your demo today.

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. Sevco was founded in 2020 and is based in Austin, Texas.

20241002