Secureworks
a SOPHOS company

Vulnerability Management Buyer's Guide

The Current State of Vulnerabilities

Regular and timely vulnerability patching remains as important as ever in preventing threat actors from compromising networks. Cybercriminals make wide use of scan-and-exploit attacks where they scan networks, systems, and applications to identify vulnerabilities to exploit and then commence their attacks. In fact, vulnerabilities and stolen credentials are the largest initial access vectors used by threat actors, accounting for 72 percent of ransomware attacks.[1]

Vulnerability management presents an array of challenges for organizations. Given the sheer volume of vulnerabilities, it's nearly impossible for security teams to patch them all, and effectively prioritizing has long been a challenge. Organizations need to reduce the window of opportunity for threat actors, but legacy vulnerability tools are difficult to use, require significant human intervention, and demand a high level of expertise and sustained effort to operate and realize the full value. Plus, threat detection and response and vulnerability management functions have historically operated in silos, creating security blind spots.

Security teams have historically tried to combat vulnerabilities by investing in point solutions. However, these solutions often fall short in providing comprehensive coverage, especially as critical data increasingly resides outside the network. These systems also fail to consider the unique context of an organization's environment when prioritizing vulnerabilities. This problem is compounded by the fact that many organizations struggle to hire, train, and retain security staff, and the combination of gaps in visibility and missing context only increases the burden on limited security resources.

Why the Old Way of Doing Vulnerability Management Does Not Solve the Problem

The traditional approach to vulnerability management focuses on generating an all-encompassing list of discovered vulnerabilities in an organization's environment. Given the increasing volume of new vulnerabilities, just producing a list with no additional context or guidance on which vulnerabilities present the highest risk for a particular organization does very little to effectively mitigate risk. Additionally, security operations and vulnerability management functions tend to work in silos, creating a disjointed and inefficient response to vulnerabilities. Without real-time threat context from an organization's environment, the efforts of the vulnerability management team can be akin to shooting in the dark.

A New Approach to Vulnerability Management

Organizations must adopt more effective strategies for managing vulnerabilities. Risk-based prioritization helps security teams identify and patch the most critical vulnerabilities first. This prevents the overwhelming scenario where teams are inundated with a high volume of vulnerabilities without a clear understanding of which ones pose the greatest risk to their operations. Additionally, by tightly integrating threat detection and response with vulnerability management, organizations can identify which vulnerabilities are being targeted in their environment and prioritize them for remediation. With this approach, security teams advance their response beyond relying solely on hypothetical risk and move to incorporating known risk based on actual threats present in their environment.

Vulnerability management solutions that integrate with third-party vulnerability scanners provide flexibility and can help organizations detect a wider range of vulnerabilities across various systems and applications. Vulnerability scanners should automatically discover endpoints, network equipment and devices, web applications, and forgotten assets to scan for vulnerabilities. By integrating your current vulnerability scanner, you can avoid ripping and replacing your existing investment and gain more effective and efficient identification, prioritization, and remediation of vulnerabilities, strengthening your organization's overall defense.

Today's vulnerability management should also leverage artificial intelligence and machine learning to enhance the effectiveness of the solution and security resources. Automating manual tasks that security personnel would typically perform manually frees up those security resources to focus on other, more important work. Given that security teams cannot feasibly remediate every single detected vulnerability, it is essential to have automated systems in place that can accurately prioritize vulnerabilities based on risk using context from an organization's environment. This prioritization is key to establishing a robust and secure vulnerability management process. Put these elements together, and the result is a vulnerability management solution that includes the essential aspects of a complete program.

Questions to Ask a Vendor When Evaluating a Vulnerability Management Solution

- Does your solution incorporate known risk based on actual threats present in the environment when prioritizing vulnerabilities?
- How does your solution integrate with our existing security tools and infrastructure? Can it integrate third-party vulnerability scanner data?
- What is the process for determining which vulnerabilities could have the most impact on our organization? How long does that process take?
- What is your remediation planning process?
- What is the process for discovering vulnerabilities?
- What happens when a vulnerability is discovered?
- How does your organization handle the publication of vulnerabilities?
- Does your staff possess experience around set up and maintenance of vulnerability tools?
- Is your vulnerability technology easy to learn/use?
- How would you describe your organization's ability to react to a new vulnerability?
- Is your vulnerability technology able to learn based on scanning, patching, and reporting activities?
- Can your vulnerability management technology discover vulnerabilities throughout our environment (endpoint, network, and cloud)?
- Do your vulnerability management tools include threat intelligence feeds? If so, are they from the same vendor, and are they known in the industry for threat research and frontline security operations experience?
- What is the licensing model for asset discovery, vulnerability scanning, threat intelligence, and risk-based prioritization?
- How many and what types of factors are used in prioritization, and do they include the local context?

REQUIRED CAPABILITIES NEEDED TO SOLVE THE PROBLEM

What comprises the right vulnerability management solution?

Here are 5 must haves:

Uses risk-based prioritization that provides meaningful guidance on what to remediate first

Integrates threat detection and response with vulnerability management to inform response and remediation

Ingests data from third-party vulnerability scanners to optimize flexibility and existing investments

Leverages machine learning and automation to enhance the effectiveness of the solution and security resources

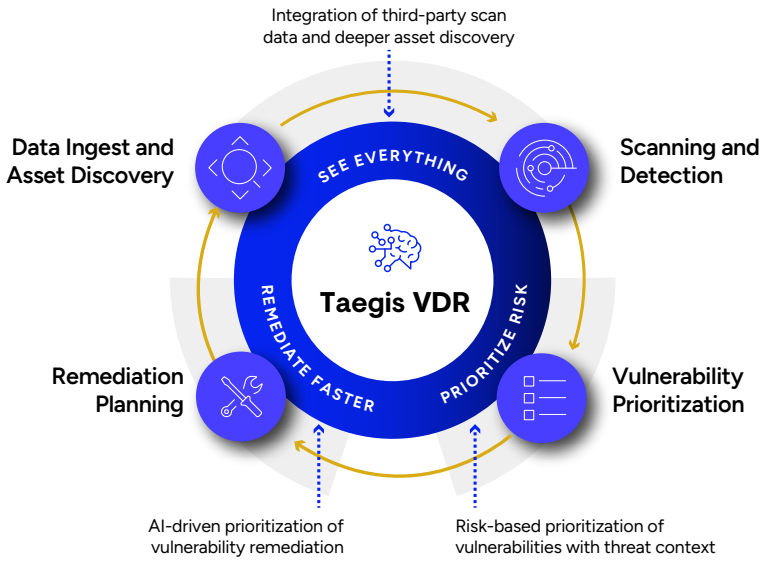
Automatically integrates threat intelligence for better context and prioritization

Why Secureworks?

Secureworks® Taegis™ VDR provides a risk-based approach to vulnerability management, prioritizing the most critical vulnerabilities informed by context from the environment and continuously updated threat intelligence from the Secureworks Counter Threat Unit™. Customers can achieve a 352% return on their investment with Taegis VDR via cost savings, risk reduction and productivity gains. Customers report, on average, a reduction in people costs of nearly $70K and avoidance of breaches valued at $250K over three years[2].

Taegis VDR leverages automation and intelligent machine learning algorithms to prioritize vulnerabilities using over 40 internal and external risk factors. The solution provides a prioritized list of assets to patch and remediate that includes the reasoning behind the ratings with remediation planning and tracking. This improves the speed and consistency of vulnerability management by automating manual tasks, improving prioritization, and accelerating remediation.

Customers can integrate their current vulnerability scanner to improve visibility and enhance the richness of available vulnerability context or leverage the Taegis Vulnerability Scanner with Taegis VDR. The Taegis Vulnerability Scanner is a lightweight, network-based scanner that automatically discovers assets throughout the environment. Additionally, vulnerability data from Taegis VDR is automatically added to threat detection and response workflows in the Secureworks extended detection and response platform, Taegis XDR. By combining these solutions, organizations can uncover vulnerabilities associated with security investigations to pinpoint the systems that are being targeted and prioritize them for remediation. This approach also offers insights into attackers' entry points and methods, helps with root cause analysis, and enhances security teams' responses.



352%

return on investment with Taegis VDR

$70k

reduction in people costs

$250k

value of breaches avoided

Integrates with:

Qualys.

tenable

Microsoft Defender

Secureworks® a SOPHOS company

Next Steps

Want to see how VDR works?

Request a demo to see how VDR delivers impact throughout the vulnerability management process.

LEARN MORE ABOUT VDR

1. 2024 State of the Threat Report: A Year in Review, October 2024
2. Forrester Total Economic Impact™ of Secureworks Taegis VDR, April 2023

Secureworks®
a SOPHOS company

Secureworks is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com