ARCTIC WOLF

BUYER'S GUIDE

Managed Vulnerability Assessment (MVA)

Buyer's Guide MVA

The percentage of organizations that needed more than 90 days to patch a cyber attack.

— Verizon's 2018 Data Breach Investigations Report

The growing attack surface compounds cyber risks for organizations. The implementation of new digital initiatives, the adoption of the Internet of Things (IoT), and the continued move to the cloud help drive innovation—but at the cost of an increased exposure to threats.

Several high-profile attacks in the last few years, from WannaCry to the Equifax breach, drove home the point that adversaries can wreak tremendous havoc by using an unpatched app or system as a starting point for their attacks. Yet Verizon's 2018 Data Breach Investigations Report[1] found that it takes 56% of organizations more than 90 days to patch. That leaves an alarmingly wide window for cybercriminals to exploit vulnerabilities.

TABLE OF CONTENTS

Buyer's Guide MVA

PRIORITIZING RISKS WITH VULNERABILITY ASSESSMENT AND MANAGEMENT

The reality for overwhelmed security teams is that even with the best technology and processes in place, it's impossible to address all vulnerabilities. Something somewhere will always need patching, and you never have complete visibility across your entire network.

When you protect a building from intruders, you prioritize physical security measures based on where the high-importance assets are located. In the same way, overcoming the visibility gap in your IT environment requires you to prioritize your risks.

Vulnerability assessments enhance security by enabling you to address high priorities using a risk-based approach. It's a proactive strategy that reduces your attack surface and improves your security posture.

MANAGED VULNERABILITY ASSESSMENTS HELP OFFLOAD THE BURDEN

Vulnerability scanning show you a point-in-time view of your ecosystem. It's only effective when performed continuously. The challenge is that security teams are constantly putting out fires, responding to thousands of alerts each day. Vulnerability assessments are yet another day-to-day task that stretch their resources.

Managed vulnerability assessments solve that challenge by taking the vulnerability assessment workflow off the in-house team's shoulders.

Combining the latest technology with a highly skilled team of outside experts, a managed vulnerability assessment vendor serves as an extension of your team to provide the best protection possible for your environment. The goal is to find the vulnerabilities before the attackers do, and quickly address the most critical ones.

Quick Reference

- **Antivirus:** A legacy technology that identifies viruses and malware based on known signatures.
- **Endpoint detection and response (EDR):** A second-generation endpoint security solution focused on advanced threats, including continuous monitoring and response.
- **Host-based scanning:** The process of using endpoint agents to monitor activity, applications, and configurations for policy violations, as well as creating an inventory of hardware and software on the hosts.
- **Managed detection and response (MDR):** A comprehensive service for continuous monitoring, threat detection, and incident response provided by a third-party vendor.
- **NOC (network operations center):** A centralized location for network management, monitoring, and control.
- **SIEM (security information and event management):** An integrated system that combines security information management and security event management to collect and correlate security events and alerts.
- **SOC (security operations center):** A centralized approach that combines security technology, people, and processes to manage threats — from prevention and detection to investigation and response.
- **Vulnerability assessment:** The process of identifying, classifying, and prioritizing vulnerabilities across your network, device, and user environment.
- **Vulnerability scanning:** The process of detecting and classifying weaknesses that threat actors can exploit to compromise your security.

Buyer's Guide MVA

ADVANTAGES OF MANAGED VULNERABILITY ASSESSMENTS

Vulnerability management provides many benefits:

- Identifies security vulnerabilities in your network, endpoints, and even users
- Prioritizes risks
- Provides actionable reports to mitigate risks

Note that vulnerability management is different from managed detection and response (MDR), which monitors and responds to threats in your environment—vulnerability assessments aim to reduce your exposure by enabling you to proactively eliminate risks. Unlike endpoint solutions that only give you visibility into your hosts, vulnerability management provides a complete view of your cloud and network infrastructure.

Managed solutions typically include the following components:

- **External scanning:** These vulnerability assessments cover external-facing surfaces such as firewalls, web servers, email servers, domain name servers, VPN servers, cloud infrastructure and cloud-based apps. Typically, the managed solution provider uses its cloud platform to conduct this scanning remotely.
- **Internal scanning:** Focused on your core IT infrastructure, internal scanning identifies vulnerabilities that result from vectors like misconfigurations and unpatched or outdated apps. Internal vulnerability assessments include endpoints, app servers, WiFi access points, email and web security gateways, and IoT devices.
- **Host-based scanning:** Using agents that run on devices, host-based scanning monitors active processes, applications, and configurations that violate set policies. It also enables you to take inventory of hardware and software running on the hosts, giving you an inside view of endpoints.
- **Security controls benchmarking:** For effective risk management, you need to know if your security posture is improving or declining over time. Benchmarking against other organizations in similar industries lets you understand where you stand and how to improve.

CLOSING THE WINDOW OF VULNERABILITY

Two years after the global havoc unleashed by WannaCry, hundreds of thousands of computers have still not been patched in the United States[2]. If that sounds like an exception rather than the norm, consider this: A 2018 report found that the average exposure window for critical web application vulnerabilities and for critical infrastructure vulnerabilities was, respectively, 69 and 65 days[3]. It also found that the oldest vulnerability dated back to 1999.

Whether you have vulnerabilities because a vendor hasn't offered a fix or because you can't keep up the pace with a patching schedule, the bottom line is that when you mitigate risks you often prevent security breaches.

WannaCry is a case in point. Microsoft issued a patch for the Eternal Blue vulnerability a month before the exploit became available on the dark web. Nonetheless, two months later the ransomware spread east-west like wildfire through unpatched servers across the world.

Attackers act quickly when they see an opening. Managed vulnerability assessments help you get ahead of their game by acting as a force multiplier for your IT team and helping you close those windows of opportunity.

> Two years after the global havoc unleashed by WannaCry, hundreds of thousands of computers have still not been patched in the United States.
>
> —"WannaCry? Hundreds of US schools still haven't patched servers," ArsTechnica

RISK ASSESSMENT IN THE NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework is a widely adopted set of best practices that help organizations improve their security postures. The framework uses risk-management processes to prioritize mitigation, and categorizes activities into five functions: identify, protect, detect, respond, and remediate.

Vulnerability scanning aligns with the first two steps of the framework. Step 1 (identify) includes an inventory of categories such as systems, assets, and people. NIST lists asset inventory and management among the potential outcomes for this step.

In step 2 (protect) the focus is on limiting and containing the impact of a security incident. Performing a risk assessment to identify and patch vulnerabilities based on prioritized risks is an important step towards incident containment.

Key Features and Capabilities

Managed solutions providers range widely in the type of capabilities they offer for vulnerability management. When you're evaluating potential partners, make sure they tailor their solution to your unique needs.

Look for the following key features:

Asset inventory

Your attack surface constantly changes as you add more users and hosts. To build and maintain a comprehensive inventory of assets, you need dynamic asset identification. Then you can profile and classify your IT assets automatically and continuously so that no new asset falls through the cracks.

Internal and external scanning

Threat actors explore endless entry points into your network, so it's not enough to assess your external-facing surfaces like web servers and firewalls. Endpoints, for example, are commonly targeted during attacks, yet visibility into all the endpoints across the environment is typically a challenge for organizations.

Comprehensive risk profiling

You need meaningful, actionable data that helps you not only understand your security posture but also helps prioritize your mitigation strategy. With comprehensive risk profiling, you can identify those issues that are of highest priority based on risks within the context of your business, both from internal and external networks.

Compliance assessment

Most compliance regulations require a risk-assessment program. However, the parameters are not the same for each regulatory requirement (e.g., HIPAA, NY DFS, FFIEC, PCI-DSS). Make sure your managed vulnerability assessments solution can meet the compliance standards that are specific to your industry.

Actionable reporting and prioritized risk mitigation

Organizations typically have different stakeholders whose objectives, as well as depth of technical understanding, will span the range. A C-level or board audience wants summarized, high-level risk assessments that are easy to digest. Meanwhile, your IT and security team needs a deeper, highly technical report. You need to satisfy both audiences.

Buyer's Guide MVA

TOP CRITERIA FOR EVALUATING MANAGED VULNERABILITY ASSESSMENT VENDORS

Continuous scanning and 24x7 eyes-on-glass monitoring

If you're scanning only periodically, you're leaving the window of opportunity wide open for cyberattackers. By the time you discover a threat, it's likely that the adversary has burrowed deeper into your environment.

To eliminate any gaps in monitoring, you need to scan assets continuously. Some vendors only offer continuous artificial intelligence-driven scanning, but relying completely on AI can leave blind spots.

Risk scoring for prioritizing actions

Security teams are constantly putting out fires, and by necessity have to focus on the highest priorities first. It's not enough for them to know where the vulnerabilities are, they need to know which ones have the highest risks.

Your managed security partner should facilitate this process by providing a risk-scoring mechanism that drives your mitigation priorities. Look for a vendor whose scoring system is easy to understand and enables you to operationalize risk management.

Compliance reporting and custom reports

Compliance is top of mind for all organizations because violations carry a heavy cost, both in financial terms and in less tangible consequences such as reputational damage. Managed vulnerability assessments keep you compliant with requirements for a risk-assessment program.

Before you choose a vendor, make sure the compliance reporting aligns with your industry and other applicable requirements. Additionally, the ability to generate custom reports is invaluable for meeting the needs of different stakeholders, based on the level of their technical knowledge.

Predictable pricing

It's estimated that there are around 3.5 network-connected devices per person, and experts expect that rate to grow to more than 7 devices per person as early as 2020[4]. More devices at your organization means more endpoints to manage, and subsequently more attack vectors. Some vendors price their vulnerability assessment offering on a per-device, or per-endpoint basis, meaning that as your organization grows, so does the cost of your vulnerability assessment solution.

Choosing a vendor that provides solution pricing based on the number of servers and users adds a level of pricing predictability that is manageable, understandable, and grows more linearly as your organization grows.

Consistent relationship with your vendor

Even with easy-to-understand and comprehensive reports and prioritized assessments, questions about mitigation will arise. You need a provider who can help you navigate best practices and offer insights based on deep expertise.

Look for a vendor who not only has experienced analysts available around the clock, but who offers a dedicated team for your account. This team will become familiar with your business, environment, and requirements, which will give them greater ability to provide the right recommendations in the right context.

Buyer's Guide MVA

IMPORTANT QUESTIONS TO ASK VENDORS

Process and capabilities

- What does the vendor scan?
- How often does the vendor scan?
- How are vulnerabilities prioritized?
- What kind of proactive tactics do they use?
- How do you get visibility into the threats? (e.g., is there an easy-to-understand cloud-based platform?)
- How are the risks quantified so you can take action?
- Does the solution monitor user-based risks?
- What kind of visibility do you get into endpoints?

Service offering

- How does the vendor measure success?
- How does the solution support your compliance needs?
- Will you receive a dedicated point of contact and support?
- How do the vendor's services scale and tailor to your needs?
- Does the solution offer configurable custom scheduling for scans?
- Does the vendor have additional capabilities, such as penetration testing tools?

FINAL THOUGHTS

With technology-driven growth and innovation, protecting your environment becomes exponentially more challenging. Proactive strategies are becoming more critical to securing your assets. Vulnerability assessments help you get in front of threats by closing the window of opportunity for attackers to exploit your security weaknesses.

The realities of resource constraints imposed on security teams limits their abilities to proactively close various security gaps. Yet a proactive approach not only reduces your exposure but also minimizes the number of incidents to which your team needs to respond.

A managed vulnerability assessment partner adds tremendous value by taking some of the day-to-day burden off your in-house team's shoulders. But more importantly, it brings deep expertise and best-in-class technology to help you better manage risks.

Your managed solution is a critical part of your success. Take the time to evaluate potential vendors to ensure you choose a highly experienced and responsive partner well-suited to your needs.

About Arctic Wolf: Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf™ Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. For more information about Arctic Wolf, visit arcticwolf.com.

1. Verizon 2018 Data Breach Investigations Report
2. "WannaCry? Hundreds of US schools still haven't patched servers," ArsTechnica
3. 2019 Vulnerability Statistics Report, edgescan
4. Number of network connected devices per person around the world from 2003 to 2020, Statista