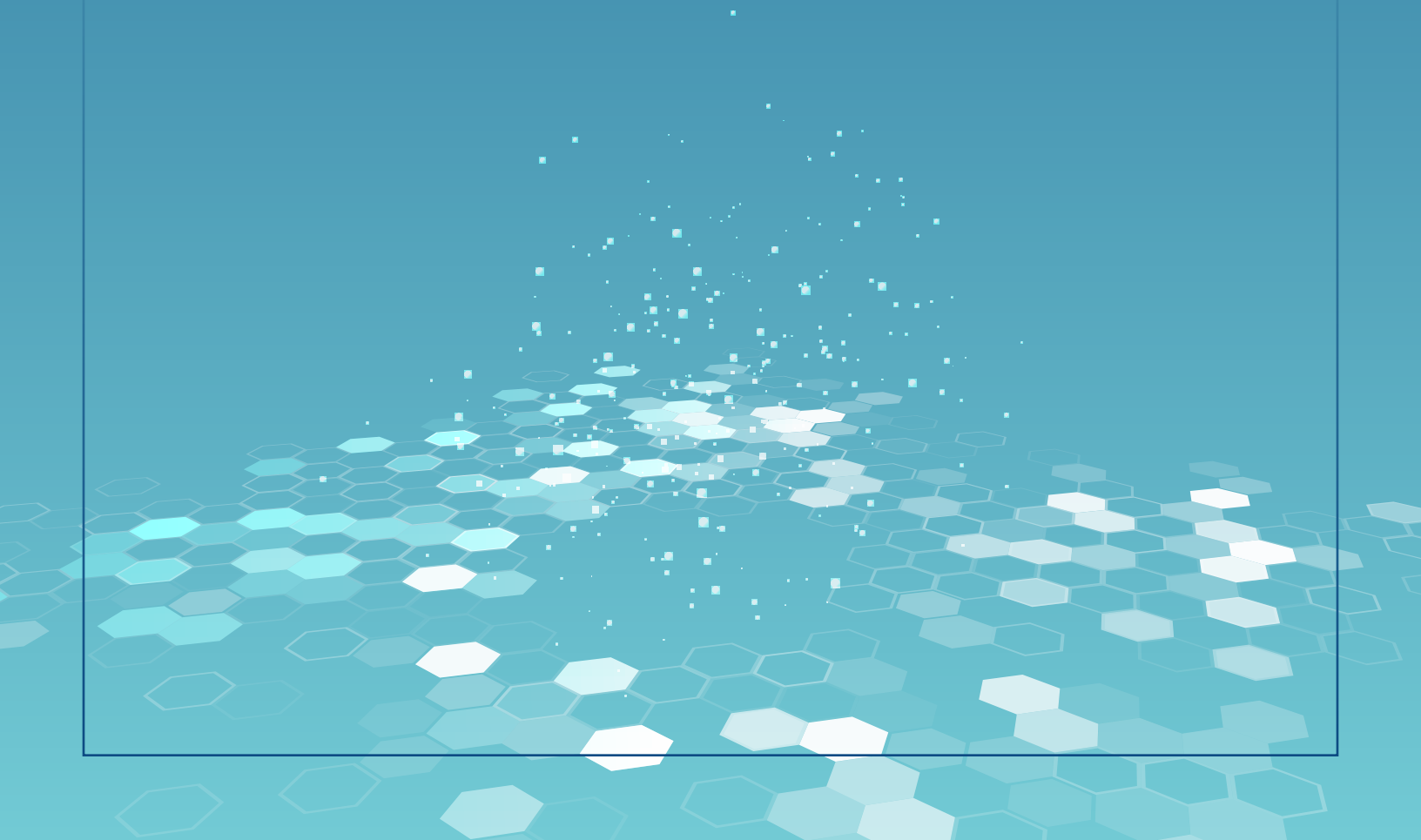
RAPIDFIRE TOOLS
A Kaseya COMPANY

# A Buyer's Guide to Vulnerability Management Tools



# INTRODUCTION

## Identify Vulnerabilities Before Hackers Do

In today's IT landscape, networks are constantly threatened by cyberattacks, with an average of 60 vulnerabilities discovered daily. Despite IT teams implementing robust antivirus and malware protection, the increasing frequency of attacks makes detecting and patching vulnerabilities more challenging and time-consuming.

Vulnerability management is crucial for any organization's risk assessment strategy and cybersecurity posture. While initially hidden, once a vulnerability is exposed and made public, it poses a "race against time" threat scenario. Protecting systems from cybercriminals is critical since they employ advanced tools to automatically scan networks for a single vulnerability that can give them access. By taking a holistic, ongoing approach to proactively identifying, managing and addressing network vulnerabilities, you can help your business avoid data breaches, costly regulatory fines and reputational damage.

In this buyer's guide, we'll explore the definition of vulnerability in cybersecurity, the concept of vulnerability management and its key aspects, the benefits of vulnerability management tools and more.

# VULNERABILITY IN CYBERSECURITY

A vulnerability is a weakness in a system or network that cybercriminals can exploit to gain unauthorized access and wreak havoc. What happens next is anybody's guess — the installation of malware, the theft of sensitive data, damaged, deleted or locked data caused by a malicious code and more. That's why it is extremely important for organizations to monitor and manage cybersecurity vulnerabilities since these gaps in a network can result in a full-scale systems breach.

Now let's look at how a vulnerability compares to a threat or risk (two other common buzzwords in cybersecurity).

### Vulnerability vs. threat

While vulnerabilities are gaps or weaknesses that undermine an organization's IT security efforts, threats are what an organization is up against — from malware attacks that plant dangerous executables to ransomware attacks that lock an organization's systems and data. No two threats are the same; some are more likely to exploit a vulnerability than others.

### Vulnerability vs. risk

Risk refers to the likelihood and impact of those vulnerabilities being exploited. While vulnerabilities are specific weaknesses, a risk accounts for the probability of cybercriminals exploiting a vulnerability and the incident's potential business impact on the organization.

## VULNERABILITY MANAGEMENT IN CYBERSECURITY

Vulnerability management is the continuous process of identifying, assessing, documenting, managing and remediating security vulnerabilities across endpoints, workloads and systems in a network. In short, vulnerability management is a systematic approach to closing security gaps that exist in a network before they can be taken advantage of by hackers.

## WHY ORGANIZATIONS NEED VULNERABILITY MANAGEMENT

Vulnerability management is a best practice that's recommended to protect sensitive corporate data. As such, implementing a robust vulnerability management process represents the starting point of an effective program that can help boost an organization's cybersecurity posture. With IT teams stretched thin trying to manage daily operations, vulnerability management helps decrease their workload and saves valuable time by automating the process of identifying potential weaknesses and entry points for cybercriminals in their network. It is a solution that helps organizations prioritize security concerns without the need for manual-intensive assessments or external consultants.

If you're running an organization, the goal of vulnerability management is to help you answer questions like:

- How can the vulnerability be exploited?
- How difficult or easy would it be to exploit the vulnerability?
- What would be the potential impact on the organization if the vulnerability is exploited?
- Do any security controls already exist to protect the vulnerability from being exploited?
- For how long has the vulnerability existed on the network?

## THE DIFFERENCE BETWEEN VULNERABILITY MANAGEMENT AND VULNERABILITY SCANNING

Vulnerability scanning and vulnerability management are two distinct processes within the realm of cybersecurity, each serving a specific purpose. As its name suggests, vulnerability scanning is the process of identifying, classifying and prioritizing vulnerabilities in an organization's network that cybercriminals can exploit. It provides an overview of the weaknesses, misconfigurations, open ports, malware and other security issues using automated tools. Once the scan is complete, the results are analyzed to assess which areas of the system need to be addressed and strengthen its overall security posture.

Sounds familiar? But not quite; vulnerability management is a broader term. It is an ongoing, comprehensive process that continuously manages cybersecurity vulnerabilities in a network. Vulnerability scans are a part of the vulnerability management process, where controls and steps are created to help an organization establish a cycle of measures that ensures vulnerabilities are quickly detected, assessed and remediated. Once complete, the cycle repeats.

## THE MOST COMMON TYPES OF VULNERABILITIES

Vulnerabilities come in all shapes and forms. Some of the most common types are:

- **Outdated and unpatched software:** This is the number one vulnerability identified by the U.S. Department of Homeland Security. Unpatched systems and software are probably the easiest targets for hackers. While every patch is aimed at eradicating a vulnerability, if a system or software is left unpatched, it's an open invitation to malicious activity.

- **Missing or poor data encryption:** It's easy for hackers to intercept data shared among systems in a network. On top of that, if the data is unencrypted or poorly encrypted, it's even easier for attackers to extract critical information.

- **Operating system and security misconfigurations:** System misconfigurations result from improper security controls or settings on a network asset. One of the first things cybercriminals do is scan a network for endpoints with system misconfigurations.

- **Missing or broken authentication:** Another common tactic attackers use is cracking or guessing employee credentials. Missing or broken authentication makes the credentials even more vulnerable.

- **Poor cyber awareness and human error:** An organization's employees are its first line of defense against cybercrime. However, employees with poor cyber awareness, or ones who unintentionally jeopardize an organization's security, are a huge vulnerability that is often overlooked.

- **Malicious insider threats:** Employees with access to vital systems may abuse their privileges and authority to share data, enabling hackers to infiltrate the network. Detecting and mitigating these threats requires a combination of network access control tools, monitoring and creating a strong security culture.

- **Zero-day Vulnerabilities:** Zero-day vulnerabilities are specific software flaws that the attackers are aware of but that a company or user has not yet identified. Since the vulnerability has not yet been identified or reported by the system manufacturer, exercising caution and checking systems for vulnerabilities is crucial to reducing the risk of zero-day attacks.

# THE ESSENTIAL STEPS IN THE VULNERABILITY MANAGEMENT LIFECYCLE

The vulnerability management lifecycle is a defined and accepted framework that constitutes six main interconnected steps that organizations must follow to systematically manage their vulnerabilities and enhance their overall cybersecurity posture. It is important to remember that each of these steps is part of an ongoing process.

**The vulnerability management lifecycle typically includes the following steps:**

STEP 01

## DISCOVERY

Building an inventory of all assets across the network and host details, including operating systems and open services. Additionally, IT teams need to develop a network baseline and identify security vulnerabilities on a regular, automated schedule.

STEP 02

## PRIORITIZATION

Categorizing assets into groups or business units and assigning a business value to asset groups based on how critical they are to business operations.

STEP 03

## ASSESSMENT

Determining a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat and asset classification.

STEP 04

## REPORTING

Measuring the level of business risk associated with assets according to security policies. Based on these insights, IT teams need to develop and document a security plan, monitor suspicious activity and define known vulnerabilities.

STEP 05

## REMEDIATION

Prioritizing and fixing vulnerabilities in an order determined by business risk. During this step, it's crucial to establish controls and demonstrate progress.

STEP 06

## VERIFICATION

The final step, before the cycle repeats, is conducting follow-up audits to verify if threats have been eliminated.

## THE BENEFITS OF USING VULNERABILITY MANAGEMENT TOOLS

A vulnerability management tool helps organizations effectively manage security vulnerabilities in their networks, systems and applications that cybercriminals could potentially exploit. Based on different configurations and scripts, vulnerability management tools run tests on assets and provide valuable insights about the vulnerabilities in an IT environment, degrees of risk from each and ways to mitigate them.

Overall, vulnerability management tools help strengthen cybersecurity in a proactive and informed manner. By running regular vulnerability scans, organizations can:

### ENHANCE SECURITY

Identify and address potential issues to safeguard your data from breaches and ransomware attacks.

### MEET REGULATORY COMPLIANCE

Generate reports highlighting and recommending mitigation of non-compliant systems or processes. This helps comply with industry-specific security regulations and avoid hefty fines.

### OPTIMIZE EFFICIENCY

Resolve performance bottlenecks, such as slow processing, unnecessary memory consumption and unstable internet connections, to improve the efficiency of your business applications.

### MAINTAIN CUSTOMER TRUST

Regular vulnerability scans as part of a comprehensive vulnerability management strategy enhances your credibility in the eyes of stakeholders while protecting their information.

## KEY FEATURES OF A VULNERABILITY MANAGEMENT TOOL

The ideal vulnerability management tool should have the following features:

- **Internal vulnerability scans:** Automate internal vulnerability scans inside an organization's network, receive alerts and generate detailed reports that help manage risks and enable recurring services.
- **External vulnerability scans:** External vulnerability scans help target external IP addresses, identify vulnerabilities and all the ports that can be accessed from the internet.
- **Scheduled network vulnerability scanning:** Configure scanners with customized schedules, saving time and targeting specific IP addresses or excluding systems to optimize IT operations efficiency.
- **Unlimited scanner appliances:** Deploy multiple scanners for network-wide vulnerability scanning, centralized management and a faster scanning process.
- **Automatic service ticket creation:** Automatically generate service tickets for efficient tracking and remediation of identified vulnerabilities.
- **False positive management:** Reduce "noise" and receive timely emails that help keep you updated with a prioritized list of anomalies, changes and threats.
- **Auto email alerting:** Automatically receive targeted email notifications of scan results, saving time and providing easy access to the latest information. These results can be filtered by IP range or severity.
- **Multitenant dashboard:** Effortlessly manage multiple networks and individual sites from a single, streamlined dashboard interface.
- **Custom scan profiles:** Configure scanning processes with specific port targeting that enables users to perform low-impact scans and optimize scan durations.
- **Authenticated scans/credentialed scans:** Conduct thorough internal vulnerability scans with authenticated credentials, detecting a wider range of security issues.
- **Common vulnerabilities and exposures (CVE) support:** Utilize CVE IDs to effectively search for and address specific vulnerability issues in scan results.
- **Customizable report generator:** Generate detailed reports that provide actionable insights on discovered vulnerabilities and the effectiveness of vulnerability management strategies.

## FACTORS TO CONSIDER WHEN SELECTING A VULNERABILITY MANAGEMENT TOOL

The following pointers cover what you should look for when purchasing a vulnerability scanning tool:

### Budget

Due to the wide range of prices for vulnerability scanners, you should choose one wisely, depending on your organization's budget.

### Scalability

The vulnerability scanner should be able to scale with the organization's growth and changing IT requirements.

### Compatibility

The vulnerability scanner tool should be compatible with the organization's existing IT infrastructure, including hardware, software and network devices.

### Vendor support

The vulnerability scanner tool should have a reliable vendor support system that can provide assistance in case of any issues or questions.

### Security

The vulnerability scanner tool should have robust security features to protect the organization's network data and prevent any unauthorized access.

### Ease of deployment

The vulnerability scanner tool should be easy to deploy and should not require extensive IT resources for installation and maintenance.

## VULNERABILITY MANAGEMENT TOOLS AVAILABLE TODAY

Today's vulnerability management tool market presents a wide range of products that promises to deliver enterprise-class results. However, users can select the vulnerability management tool that best fits their requirements, allowing them to find a solution that offers a suitable price point and user-friendly interface. For instance:


VulScan is a full-featured internal and external vulnerability management platform priced to be affordable for both MSPs and IT departments of any size. It includes a wide range of internal scanning tools, including lightweight discovery agents which run inside individual computers, as well as local and network scanners that can run as virtual machines. VulScan also includes a unique feature that allows internal scans to be performed from a computer external to the network. For organizations that don't have their own external data center, VulScan also offers an option of hosted external scanning service.

With VulScan, you can schedule scanners to run at any frequency at any time, and multiple scanners can run simultaneously on larger networks to speed up scanning. Scan results from each site are automatically consolidated and available to view through a web-based portal, with drill-in details that include issue specifics and remediation advice. VulScan also includes advanced features such as credentialed scans, trend reports, false positive management and direct integration with common ticketing systems in the market.

While VulScan may lack some of the extra bells and whistles found in the expensive enterprise solutions, it checks all the boxes that most IT technicians need and the RapidFire Tools developers add new features on a monthly cadence. In terms of value, VulScan tops the charts for Vulnerability Management Solutions.


Built from the ground up with a deep understanding of how IT security technicians work, Tenable's Nessus is designed to make vulnerability assessment simple, easy and intuitive. As a result, IT technicians spend less time and effort assessing, prioritizing, and remediating issues. Its feature-rich vulnerability management capabilities extend beyond traditional vulnerability scanning functions, offering authenticated scans, compliance audits and seamless integration with other security tools and platforms.

While it offers strong features, Nessus provides limited reporting output options to track remediation needs. This forces IT technicians to manually consolidate the information from multiple reports to form a comprehensive view for their clients. Organizations considering Nessus should assess these factors carefully to determine if it aligns with their specific needs.

NeXpose is a vulnerability management tool designed for on-premise use. This tool was one of the first headlining products that put its vendor, Rapid7, on the map. The NeXpose conducts a system-wide scan to monitor and identify threats by updating its processes and rescans whenever a new exploit is documented to enable real-time response.

However, when running ad-hoc scans, Nexpose has limitations since it requires IT technicians to manually assign assets to specific sites or groups before initiating the scanning process. Moreover, its extensive resource requirements, lack of integration options and high cost can hinder its effectiveness and limit its suitability for some organizations.

Qualys.

A popular provider of cloud-based and compliance solutions, Qualys claims its vulnerability management tool can, within a degree of accuracy exceeding 99%, identify the host operating system, services running and opened ports. Qualys provides extensive reporting and analytics, aiding in evaluating security posture and compliance status. Its robust vulnerability management capabilities enable organizations to identify and prioritize vulnerabilities efficiently, facilitating prompt remediation.

On the downside, some users have found Qualys resource-intensive, requiring significant computing power and storage capacity. Furthermore, Qualys is complex, clunky and cumbersome and requires additional development for IT technicians to set up and deploy rapidly. The complexity of the platform can be overwhelming for novice users, necessitating a learning curve and potentially additional training.

HostedScan

Founded in Seattle, Washington, in 2019, Hosted Scan is a company dedicated to making continuous vulnerability scanning and risk management accessible to more businesses. Hosted Scan Security states that they have built a solution that can import targets from various providers, keep track of an updated list of servers all in one place to generate aggregated reports and provide real-time email alerts for new vulnerabilities.

But it is worth noting that Hosted Scan Security lacks the capability to scan for internal vulnerabilities, limiting its effectiveness in identifying risks within the network. The platform also doesn't offer any comprehensive false positive management options, providing only basic vulnerability status choices without features like exclusion notes or IP/hostname tracking.

## SUMMARY

Vulnerability management is essential for a robust cybersecurity strategy and enables cybersecurity professionals to proactively identify, assess and mitigate vulnerabilities in systems, networks and applications that malicious actors could exploit. The goal of vulnerability management is to provide valuable insights into an organization's security posture, highlighting areas of concern that require immediate attention and establishing a cycle of processes that effectively mitigate them. Overall, leveraging vulnerability management empowers organizations to stay ahead of emerging threats, bolster their cybersecurity resilience and safeguard their valuable data assets.

When comparing vulnerability scanning options available on the market, there are many free scanners available for the do-it-yourselfers who want to build their own solutions. But these home-grown solutions usually require ongoing internal maintenance and troubleshooting and can barely keep up with the increasing threats. On the flip side, the market is dominated by enterprise-class solutions that are very expensive and complicated to set up and use on a regular basis.

With its impressive range of features, flexibility and scalability, VulScan has emerged as the ***#1 rated tool*** for use by MSPs and IT departments within small to medium-sized businesses worldwide. VulScan provides a complete package of all the essential features that helps you to identify and effectively manage vulnerabilities from anywhere.

To discover the power of VulScan and schedule a demo, visit:
https://www.rapidfiretools.com/network-vulnerability-management-demo/