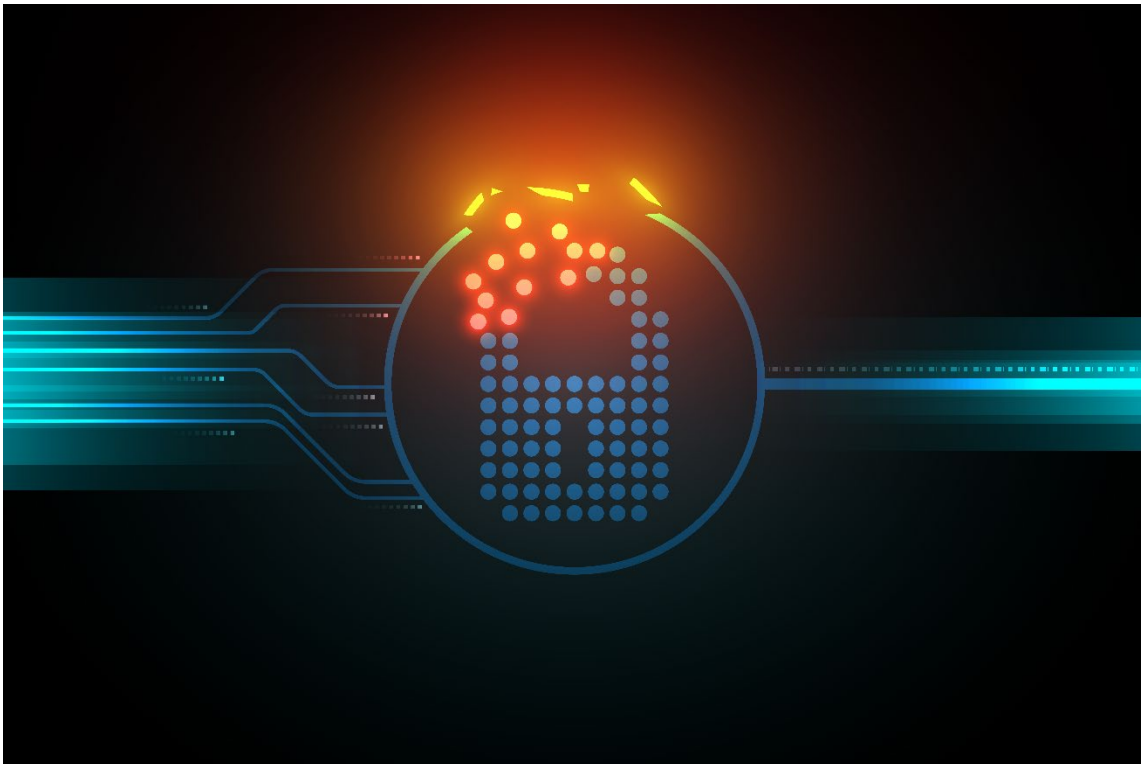
Buyer's Guide



Vulnerability Management: The Process, Lifecycle, and Tools for Success

VULSCAN
byRapidFireTools®

No cybersecurity discussion is complete without talking about internal and external vulnerabilities, and ideally, no cybersecurity strategy is complete without a plan for vulnerability management. Despite being so crucial, organizations often don't pay enough attention to both.

Until now, vulnerability management tools have been expensive and hard to use. And, while you can't control threats, you can control vulnerabilities.

In 2021, over 50 new vulnerabilities were identified EVERY DAY. Vulnerabilities may start out hidden, but as soon as they are identified and publicized, it becomes a race against time to protect systems from cybercriminals. Hackers use sophisticated tools to automatically scan thousands of businesses, looking for one vulnerability that will give them access.

Statistics show that most data breaches and ransomware attacks are caused by known vulnerabilities that just haven't been addressed. Lately, cyber insurance policies, business contracts, and new regulations are including strict requirements that demand vulnerability management.

The good news? You don't need to be a high-level security engineer to deliver this service. The right tool will help you automate the scans to run on a scheduled basis, send reports with discovered vulnerabilities and render suggestions on how to remediate them.

Weak vulnerability management can be attributed to the lack of clarity on what vulnerabilities truly are and how they can be managed before they are exploited by cybercriminals. Let's dive right in by first understanding what a vulnerability means.

WHAT IS A VULNERABILITY IN CYBERSECURITY?

In principle, a vulnerability is a weakness in a system or network that can be exploited by cybercriminals to gain unauthorized access to wreak havoc. What happens next is anybody's guess — installation of malware, the theft of sensitive data, damaged, lost or locked data caused by a malicious code and more.

Here are other definitions of a vulnerability:

- **National Institute of Standards and Technology (NIST):** Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.
- **ISO 27005:** A weakness of an asset or group of assets that can be exploited by one or more cyberthreats, where an asset is anything that has value to the organization, its business operations, and their continuity, including information resources that support the organization's mission.
- **IETF RFC 4949:** A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Now let's look at how a vulnerability compares to a threat and 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 and some are more likely to exploit a vulnerability than others.

Vulnerability vs. Risk

Risk refers to a thorough assessment of potential threats to an organization's security and vulnerabilities in its network. It doesn't just consider the probability of a vulnerability being exploited, but also includes the incident's potential business impact on the organization.

What are the most prevalent 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 and/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 and broken authentication:** Another common tactic used by attackers is cracking or guessing employee credentials. Missing and broken authentication make 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 the ones who unintentionally jeopardize an organization's security, are a huge vulnerability that is often overlooked.

Detecting vulnerabilities is just the first step of vulnerability management — a proven method of enhancing an organization's cybersecurity. Let's take a closer look.

WHAT IS VULNERABILITY MANAGEMENT?

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

Remember, vulnerability management is a race against hackers.

What is the difference between vulnerability management and a vulnerability assessment?

A vulnerability assessment is a project with a specific start and end date aimed at uncovering any vulnerabilities that cybercriminals could potentially exploit. Once the assessment report is prepared, the project is complete.

Vulnerability management, on the other hand, is an ongoing, comprehensive process that continuously manages cybersecurity vulnerabilities in a network. Vulnerability assessments are a part of the vulnerability management process, not the other way around.

What is the purpose of vulnerability management?

A vulnerability management strategy establishes controls and processes that help an organization identify vulnerabilities in its technology infrastructure. It creates a cycle of steps that ensure vulnerabilities are quickly detected, assessed, and remediated. Once complete, the cycle repeats.

Why is vulnerability management important?

The pandemic has accelerated the rise of cybercrime at an unprecedented pace. Without vulnerability management, an organization leaves all its door wide open to cybercriminals.

Every day you wait means another 50 unmanaged vulnerabilities.

WHAT IS A VULNERABILITY MANAGEMENT PROCESS?

Not that we know the objective behind vulnerability management, it's time to understand the various elements an organization must be pay attention to.

What are the main elements of a vulnerability management process?

While every organization takes a different approach to its vulnerability management process, it largely revolves around three main elements or phases.

Skipping any of them renders the entire process incomplete and ineffective.

1. **Identifying vulnerabilities:** This step usually involves a vulnerability scanner that identifies a variety of systems on a network and probes them for different attributes — operating system, open ports, installed software, file system structure, and more. Once obtained, this information is used to associate known vulnerabilities to the scanned systems to identify the systems with vulnerabilities. The results are delivered in the form of reports, metrics, and/or dashboards.
2. **Evaluating vulnerabilities:** After identifying the vulnerabilities, the next step is to evaluate them to assign different risk ratings and scores to determine the priority of each vulnerability. A few questions that can be considered while evaluating each vulnerability are:
    a. Is the vulnerability a true or false positive?
    b. Could the vulnerability be directly exploited from the internet?
    c. How difficult or easy would it be to exploit the vulnerability?
    d. What would be the potential impact on the organization if the vulnerability is exploited?
    e. Do any security controls already exist to protect the vulnerability from being exploited?
    f. For how long has the vulnerability existed on the network?
3. **Treating Vulnerabilities:** Once a vulnerability has been evaluated and validated, an organization must decide how it should treat it by involving the relevant stakeholders. The ways to treat vulnerabilities include:
    a. **Remediation:** Deemed as the ideal treatment of a vulnerability, remediation involves fully fixing or patching the vulnerability so that it can't be exploited.

b. **Mitigation:** Organizations can opt for mitigation when a proper fix or patch isn't yet available for the vulnerability. This method will reduce the likelihood and/or impact of a vulnerability being exploited, buying an organization time to eventually remediate the vulnerability.
c. **Acceptance:** Organizations can also decide neither to fix the vulnerability nor reduce its likelihood/impact. This is justified when the vulnerability is considered low risk and the cost of fixing it is greater than the potential cost the organization would incur if exploited. You must know the requirements in cyber insurance policies, contracts, and regulations before deciding to leave a vulnerability unfixed.

WHAT IS THE VULNERABILITY MANAGEMENT LIFECYCLE?

Right at the outset, we mentioned how vulnerability management is an ongoing process. It is a defined and accepted framework that constitutes six main steps. This helps identify and address vulnerabilities efficiently and in a continuous manner.

What are the steps in the vulnerability management lifecycle?

Before you understand each of the steps, let's remember that they are steps in a never-ending process (or rather, a process that must not end).

1. **Discovery:** Building an inventory of all assets across the network and host details, including operating systems and open services. You must also develop a network baseline and identify security vulnerabilities on a regular, automated schedule.
2. **Prioritization:** Categorizing assets into groups or business units and assigning a business value to asset groups based on how critical they are to business operation.
3. **Assessment:** Determining a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification.
4. **Reporting:** Measuring the level of business risk associated with assets according to security policies. You also need to develop and document a security plan, monitor suspicious activity, and define known vulnerabilities.
5. **Remediation:** Prioritizing and fixing vulnerabilities in an order determined by business risk. It's crucial to establish controls and demonstrate progress during this step.
6. **Verification:** Conducting follow-up audits to verify threats have been eliminated.

WHAT ARE VULNERABILITY MANAGEMENT TOOLS?

Vulnerability management tools simplify and automate the process of vulnerability management. While some focus solely on vulnerability scanning, others go beyond that to aid the entire vulnerability management process. Most products provide detailed analysis reports and charts built from scan results. Some also include an exploit software used as a penetration test tool, which allows an administrator to see how a hacker would exploit the vulnerability without disrupting network operations.

Vulnerability management tools help strengthen cybersecurity in a proactive and informed manner. A key aspect in deciding the impact of a vulnerability management tool is the type of vulnerability scanning it deploys.

A vulnerability scanner helps businesses secure their networks by identifying and addressing vulnerabilities in public-facing and internal assets that could be exploited by a hacker. It brings to light information about:

- Vulnerabilities in an IT environment
- Degrees of risk from each vulnerability
- How to mitigate a vulnerability

Vulnerability scanners can be largely divided into three types:

- **External vulnerability scanners:** External scanners check all the public-facing assets, including network firewalls, routers, and other "perimeter" devices, targeting areas of IT infrastructure that are exposed to the internet or aren't restricted to internal users and systems.
- **Internal vulnerability scanners:** These can be stand-alone servers or deployed as virtual machines on any computer attached to the network with sufficient capacity. The internal scanners can check any (or all) ports on any device within a network with an IP address, identifying known vulnerabilities a hacker or malware can exploit once inside.
- **Portable vulnerability scanners:** While it's best practice to have scanners permanently installed on the network for regular internal scanning, portable vulnerability scanners are also available that can be transferred from one network to another for ad hoc assessments and diagnostics.

THE VULNERABILITY MANAGEMENT PLATFORM YOU NEED

VulScan is a vulnerability management platform, purpose-built and priced to deliver Vulnerability Management services for every organization. It includes all the key features and functions you need, without the unnecessary bells and whistles that add complexity and cost.

VulScan delivers:

- Internal, external, and portable vulnerability scanning
- Unlimited number of assets per network
- Unlimited scanning frequency
- Portable vulnerability scanning option
- Native reports
- Web-based management portal
- Post-scan vulnerability reports
- Drill-down vulnerability management dashboard
- Built-in false-positive/exclusion management
- Support for multiple scanners running on the same network for increased speed
- Three pre-configured levels of scan intensity, including brute-force login attempts
- Security service ticket integration with most PSA tools
- Direct integration with Network Detective Pro for enhanced reporting
- Credentialed scans

Get a demo of VulScan and see how it puts you in the ideal position to deliver Vulnerability Management and reduce your risks.