

Vulnerability Management and Scanning

Monitor networks to keep vulnerabilities in check

At a Glance:

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. **Security vulnerabilities**, in turn, refer to technological weaknesses that allow attackers to compromise a product and the information it holds. This process needs to be performed continuously in order to keep up with new systems being added to networks, changes that are made to systems, and the discovery of new vulnerabilities over time.

IN THIS SECTION

Vulnerabilities, Exploits, and Threats

Vulnerabilities, Exploits, and Threats

Vulnerability Management and Scanning

Penetration Testing

Penetration Testing Tools

Incident Response

Incident Response Plan

Threat Detection

Vulnerability management software can help automate this process. They'll use a **vulnerability scanner** and sometimes endpoint agents to inventory a variety of systems on a network and find vulnerabilities on them. Once vulnerabilities are identified, the risk they pose needs to be evaluated in different contexts so decisions can be made about how to best treat them. For example, vulnerability validation can be an effective way to contextualize the real severity of a vulnerability.

The vulnerability management process can be broken down into the following four steps:

Step 1: Identifying Vulnerabilities

At the heart of a typical **vulnerability management solution** is a vulnerability scanner. The scan consists of four stages:

- Scan network-accessible systems by pinging them or sending them TCP/UDP packets
- Identify open ports and services running on scanned systems
- If possible, remotely log in to systems to gather detailed system information
- Correlate system information with known vulnerabilities

Vulnerability scanners are able to identify a variety of systems running on a network, such as laptops and desktops, virtual and physical servers, databases, firewalls, switches, printers, etc. Identified systems are probed for different attributes: operating system, open ports, installed software, user accounts, file system structure, system configurations, and more. This information is then used to associate known vulnerabilities to scanned systems. In order to perform this association, vulnerability scanners will use a vulnerability database that contains a list of publicly known vulnerabilities.

Properly configuring vulnerability scans is an essential component of a vulnerability management solution. Vulnerability scanners can sometimes disrupt the networks and systems that they scan. If available network bandwidth becomes very limited during an organization's peak hours, then vulnerability scans should be scheduled to run during off hours.

If some systems on a network become unstable or behave erratically when scanned, they might need to be excluded from vulnerability scans, or the scans may need to be fine-tuned to be less disruptive. [Adaptive scanning](#) is a new approach to further automating and streamlining vulnerability scans based on changes in a network. For example, when a new system connects to a network for the first time, a vulnerability scanner will scan just that system as soon as possible instead of waiting for a weekly or monthly scan to start scanning that entire network.

Vulnerability scanners aren't the only way to gather system vulnerability data anymore, though. Endpoint agents allow vulnerability management solutions to continuously gather vulnerability data from systems without performing network scans. This helps organizations maintain up-to-date system vulnerability data whether or not, for example, employees' laptops are connected to the organization's network or an employee's home network.

Regardless of how a vulnerability management solution gathers this data, it can be used to create reports, metrics, and dashboards for a variety of audiences.

Step 2: Evaluating Vulnerabilities

After vulnerabilities are identified, they need to be evaluated so the risks posed by them are dealt with appropriately and in accordance with an organization's risk management strategy. Vulnerability management solutions will provide different risk ratings and scores for vulnerabilities, such as Common Vulnerability Scoring System (CVSS) scores. These scores are helpful in telling organizations which vulnerabilities they should focus on first, but the true risk posed by any given vulnerability depends on some other factors beyond these out-of-the-box risk ratings and scores.

Here are some examples of additional factors to consider when evaluating vulnerabilities:

- Is this vulnerability a true or false positive?
- Could someone directly exploit this vulnerability from the Internet?
- How difficult is it to exploit this vulnerability?
- Is there known, published exploit code for this vulnerability?
- What would be the impact to the business if this vulnerability were exploited?
- Are there any other security controls in place that reduce the likelihood and/or impact of this vulnerability being exploited?
- How old is the vulnerability/how long has it been on the network?

Like any security tool, vulnerability scanners aren't perfect. Their vulnerability detection false-positive rates, while low, are still greater than zero. Performing vulnerability validation with [penetration testing tools](#) and techniques helps weed out false-positives so organizations can focus their attention on dealing with real vulnerabilities. The results of vulnerability validation exercises or full-blown penetration tests can often be an eye-opening experience for organizations that thought they were secure enough or that the vulnerability wasn't *that* risky.

Step 3: Treating Vulnerabilities

Once a vulnerability has been validated and deemed a risk, the next step is prioritizing how to treat that vulnerability with original stakeholders to the business or network. There are different ways to treat vulnerabilities, including:

- **Remediation:** Fully fixing or patching a vulnerability so it can't be exploited. This is the ideal treatment option that organizations strive for.
- **Mitigation:** Lessening the likelihood and/or impact of a vulnerability being exploited. This is sometimes necessary when a proper fix or patch isn't yet available for an identified vulnerability. This option should ideally be used to buy time for an organization to eventually remediate a vulnerability.
- **Acceptance:** Taking no action to fix or otherwise lessen the likelihood/impact of a vulnerability being exploited. This is typically justified when a vulnerability is deemed a low risk, and the cost of fixing the vulnerability is substantially greater than the cost incurred by an organization if the vulnerability were to be exploited.

Vulnerability management solutions provide recommended remediation techniques for vulnerabilities. Occasionally a remediation recommendation isn't the optimal way to remediate a vulnerability; in those cases, the right remediation approach needs to be determined by an organization's security team, system owners, and system administrators. Remediation can be as simple as applying a readily-available software patch or as complex as replacing a fleet of physical servers across an organization's network.

When remediation activities are completed, it's best to run another vulnerability scan to confirm that the vulnerability has been fully resolved.

However, not all vulnerabilities need to be fixed. For example, if an organization's vulnerability scanner has identified vulnerabilities in Adobe Flash Player on their computers, but they completely disabled Adobe Flash Player from being used in web browsers and other client applications, then those vulnerabilities could be considered sufficiently mitigated by a compensating control.

Step 4: Reporting vulnerabilities

Performing regular and continuous [vulnerability assessments](#) enables organizations to understand the speed and efficiency of their vulnerability management program over time. Vulnerability management solutions typically have different options for exporting and visualizing vulnerability scan data with a variety of customizable reports and dashboards. Not only does this help IT teams easily understand which remediation techniques will help them fix the most vulnerabilities with the least amount of effort, or help security teams monitor vulnerability trends over time in different parts of their network, but it also helps support organizations' [compliance and regulatory requirements](#).

Staying Ahead of Attackers through Vulnerability Management

Threats and attackers are constantly changing, just as organizations are constantly adding new mobile devices, cloud services, networks, and applications to their environments. With every change comes the risk that a new hole has been opened in your network, allowing attackers to slip in and walk out with your crown jewels.

Every time you get a new affiliate partner, employee, client or customer, you open up your organization to new opportunities, but you're also exposing it to new threats. Protecting your organization from these threats requires a vulnerability management solution that can keep up with and adapt to all of these changes. Without that, attackers will always be one step ahead.

Find, prioritize, and reduce risk in your environment with InsightVM

[Start a Free Trial](#)



Stay in touch:



Legal

[Legal Terms](#)
[Privacy Policy](#)
[Export Notice](#)
[Trust](#)

Resources & Help

[Product Support](#)
[Resources](#)
[Security & IT Fundamentals](#)
[Vulnerability & Exploit Database](#)

Connect With Us

[Contact Us](#)
[Blog](#)
[Support Login](#)
[Careers](#)