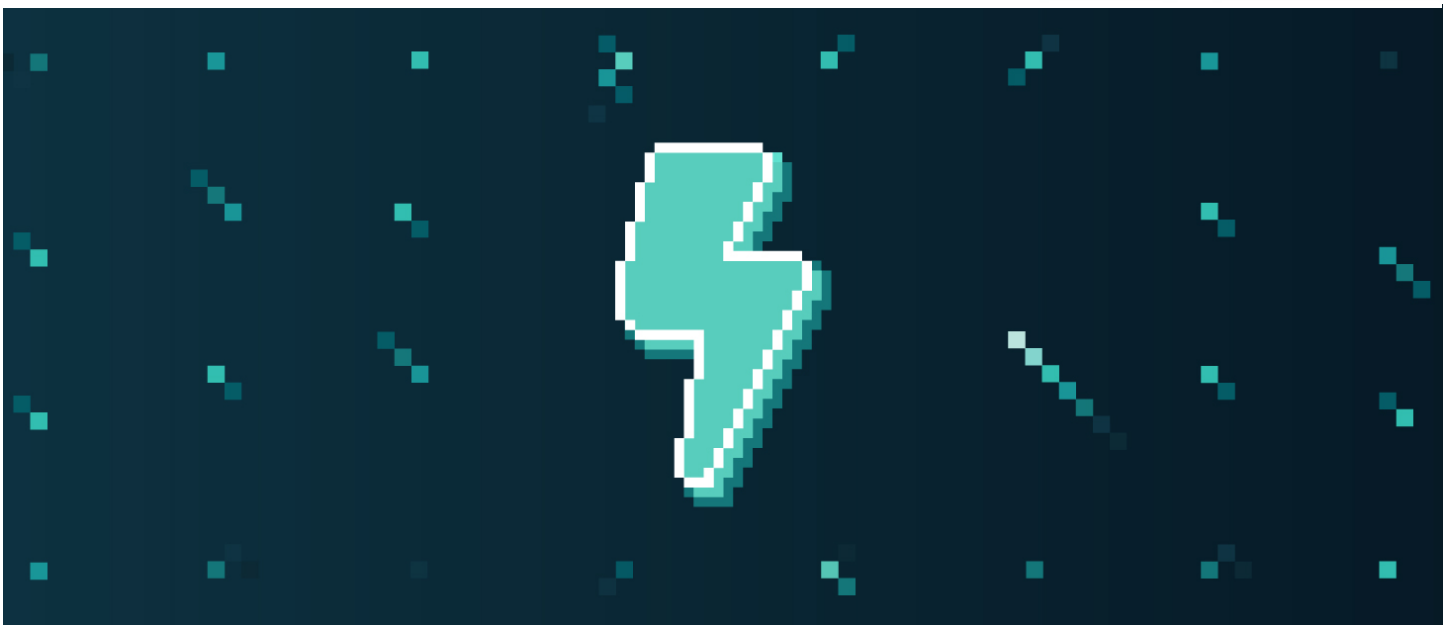


BACK TO BLOG

What is vulnerability management?

James Harrison

October 9, 2023

When it comes to protecting your IT environment, what you don't know can certainly hurt you. Finding where you're vulnerable is critical for every business today because cyberattacks can affect anyone – approximately 15M data records were exposed through data breaches in 2022 and Gartner has predicted that 45% of organizations will have experienced attacks on their software supply chains by 2025.

> 45% of organizations will have experienced attacks on their software supply chains by 2025

What we do How we do it Pricing Resources Company LOGIN TRY FOR FREE

doesn't include the frustration, lost productivity and impact on your reputation. Vulnerability scanning and vulnerability management are tried and trusted ways to protect yourself against these threats - they're often used interchangeably but they're not the same.

What is vulnerability management?

Vulnerability management is the continuous process of identifying, prioritizing, and managing cybersecurity vulnerabilities. With new vulnerabilities appearing every day, quarterly scanning and remediation is no longer enough - continuous vulnerability management has become business critical.

What's the difference between vulnerability management and scanning?

Vulnerability scanning is, at the simplest level, the use of software tools to identify and report on security flaws (known as vulnerabilities) in your IT systems. Scanners run many thousands of tests by probing and gathering information about your systems. These are designed to identify holes which could be used to steal sensitive information, gain unauthorized access to your digital systems, or disrupt your business.

Here are some of the common types of vulnerability which a scanner will check for:

- **Vulnerable software** – such as a weak version of a Nginx web server, a vulnerable FTP service, or weaknesses in a Cisco router or VPN.
- **Web Application vulnerabilities** – such as SQL injection, cross-site scripting (XSS) or directory traversal weaknesses.
- **Misconfigurations** – including software which has been incorrectly configured, commonly made mistakes, and security best practices which aren't being followed such as exposed SVN/git repositories, open email relays, and or a web server configured to reveal sensitive information

- **Encryption weaknesses** – such as use of weak encryption ciphers, weak encryption protocols, SSL certificate misconfigurations, and use of unencrypted services such as FTP.
- **Attack surface reduction** – exposed databases, administrative interfaces, and sensitive services such as SMB.
- **Information leakage** – these checks report on areas where your systems are reporting information to end-users which should remain private.

Not all vulnerability scanners check for all of the above, and the number and quality of checks vary too – for a deeper dive into vulnerability scanning, check out our ultimate guide. Ideally, a scanner will also prioritize any discovered risks by severity, so you know which ones to fix first.

Armed with this knowledge, you can look to protect yourself and take action to fix the vulnerabilities that are discovered. This overall ongoing process of identifying and fixing your weaknesses is known as vulnerability management.

Whilst a vulnerability scan is a software process with a definite start and end time, vulnerability management is the overarching process that continuously identifies, prioritizes and manages cybersecurity vulnerabilities. Vulnerability scanning is therefore just one crucial part of a vulnerability management program.

Where scanning identifies flaws and classifies risks, vulnerability management includes decisions on whether to fix, mitigate, or accept the risks alongside continuous monitoring, and on which vulnerabilities to fix first.

Try Intruder for free

Do all vulnerabilities pose the same risk?

Not all vulnerabilities are the same or pose the same risk to your business. The Common Vulnerability Scoring System (CVSS) is a free and open industry standard that many cyber security vendors use to assess and prioritize the severity of vulnerabilities.

The CVSS Base Score ranges from 0.0 to 10.0, and The National Vulnerability Database (NVD) adds a severity rating for CVSS scores. NVD also provides a library of common vulnerabilities and exposures (CVEs) from the not-for-profit MITRE Corporation. Below is one way to interpret CVSS scores:

CVSS Score	Severity Rating
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

A CVSS score isn't the be-all-and-end-all of vulnerabilities though. It gives a good indication of the risk to your business, but there are many other factors that can affect the seriousness of a weakness, such as:

- The sensitivity of the data on the system affected
- Whether a public exploit has been distributed or not
- Intelligence on whether attackers are actively exploiting the weakness

What is the vulnerability management process?

While there are different ways to define each stage in the vulnerability management process, the cycle is generally the same, even if the terminology varies. A good place to start is Gartner's Vulnerability Management Guidance Framework which includes several "pre-work" steps to help define the

1. Which assets will you measure for vulnerabilities?
2. Which assets or hosts are most critical to protect?
3. Who will be managing this program?
4. How long will you have to fix any vulnerabilities?
5. What tools will you need to scan and monitor?
6. What assets do you plan to cover?

Armed with this info, you're ready to build a robust and effective vulnerability management program...

What are the 4 steps of a vulnerability management program?

It's important to remember that the ultimate point of your vulnerability management program is to fix any flaws, so one of your KPIs should be how many critical vulnerabilities are fixed or mitigated as quickly as possible to minimize the window of opportunity for hackers. When you know what you need to monitor – asset discovery and inventory of your IT infrastructure should precede any vulnerability management program – you should follow these four steps:

- Find: find any vulnerabilities through scanning and testing
- Prioritize: understand which pose the most significant risk
- Fix: patch, block, remove or snooze vulnerabilities
- Monitor: keep on scanning for new or returning vulnerabilities

If you're just starting out on your vulnerability management program journey or want to build a more rigorous program,

Do I need a vulnerability management program?

Vulnerability management should be a core foundation of your overall security strategy. You simply can't afford to ignore the risks in your IT infrastructure. As networks grow more complex and dispersed, IT teams struggle to maintain visibility across their ever-expanding attack surface. Hackers know this and risks and attacks often go unnoticed until they've caused damage at considerable cost.

But vulnerability management has benefits beyond security. Regularly checking your network, systems, devices and applications can help you identify legacy technology and unpatched devices. This will not only keep improve your security but also optimize your systems performance.

Vulnerability management can also help you meet compliance. Regular scans, continuous monitoring and quicker remediation can help you stay ahead of compliance requirements and demonstrate your cyber hygiene to stakeholders, regulators and customers.

What's the difference between vulnerability management (VM) and attack surface management (ASM)?

Attack surface management is the process of discovering your assets and services, scanning them for vulnerabilities, fixing any flaws, and then reducing or minimizing their exposure to prevent hackers exploiting them.

Exposure in the context of ASM usually means reducing total surface that can easily be attacked. For example, a Remote Desktop service exposed to the internet is naturally easier to attack than one which is layered behind a VPN. In the latter scenario, an attacker first has to compromise or authenticate to the VPN, before attacking the Remote Desktop service.

Take the example of an admin interface like cPanel or a firewall administration page – these may be secure against all known current attacks today, but a vulnerability could be discovered in the software tomorrow – when it immediately

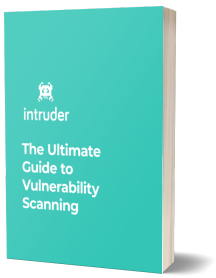
By reducing the exposure of your assets, and limiting which hosts can access them, this risk is reduced. This is because when a new vulnerability in the product is released, they cannot be remotely attacked by attackers over the internet.

So, a significant part of ASM is reducing exposure to possible future vulnerabilities by removing unnecessary services and assets from the internet. This what led to the Deloitte breach and what distinguishes it from traditional vulnerability management. Read more about attack surface management vs vulnerability management.

What to look for in a vulnerability management solution

Less can be more. You no longer need a complicated set of security tools and solutions that require people with specialized skills to manage vulnerabilities. Instead, you can now rely on a powerful, automated platform like Intruder to continuously monitor your internal and external attack surface including your web applications and APIs.

Whether you're just getting started on your vulnerability management journey or looking to optimize your cyber security to meet compliance in an increasingly complex threat landscape, Intruder has the vulnerability management solutions to get you there faster. ***Why not try it for free for 14-days and kickstart your own vulnerability management program today?***



Get Our Free "Ultimate Guide to Vulnerability Scanning"

Learn everything you need to get started with vulnerability scanning and how to get the most out of your chosen product with our free PDF guide.

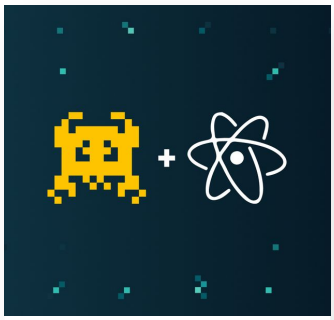
DOWNLOAD OUR FREE PDF GUIDE

Written by James Harrison

Recommended articles

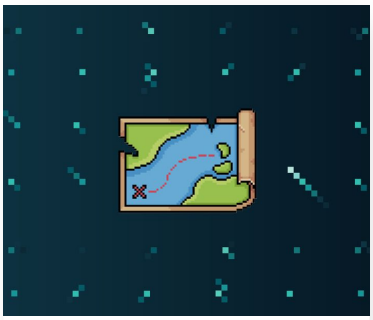
9 best DevSecOps tools for 2024

DevSecOps tools help identify security vulnerabilities early in your development process. Explore our



Introducing Nuclei: the scanner that packs a punch

Say hello to Intruder's new scanning engine



Cybersecurity compliance: The Essential Guide for 2024

Robust cybersecurity is more than best practice, it's often a regulatory requirement. Here's

list of the best tools for 2024.

Christian Gonzalez — November 29, 2023

Daniel Andrew — December 14, 2023

compliance requirements.

James Harrison — January 8, 2024

Ready to get started with your 14-day trial?

TRY FOR FREE

intruder

SOLUTIONS

Developers

Start-ups and scale-ups

Enterprise

COMPARISONS

Intruder vs Acunetix

Intruder vs Qualys

Intruder vs Rapid7

Intruder vs

USE CASES

Automated Penetration Testing

Cloud Vulnerability Scanner

Network Vulnerability Scanner

External Vulnerability Scanner

Internal

RESOURCES

Developer Hub

Help Centre

Blog

Guides

Glossary

Success Stories

Research

Webinars

COMPANY

About Us

Contact

Become a Partner

Careers (We're hiring!)

Protected by intruder

What we do How we do it Pricing Resources Company LOGIN TRY FOR FREE

Intruder vs Detectify
Intruder vs Pentest-Tools.com
Website Security Scanner

COMPLIANCE
SOC 2
ISO 27001
PCI DSS

Contact us