The Complete Checklist for Vulnerability Scanning

Identify, Prioritize, Remediate and Report Every Vulnerability in Your Network

The failure to address known vulnerabilities invites significant risk and creates gaps in your network, allowing cybercriminals to exploit these weaknesses. The increased sophistication and frequency of cyberattacks makes it even more challenging and time-consuming to detect and address network risks, with an average of 60 new vulnerabilities reported every day.

To help you properly handle this threat, we've identified crucial must-dos that will help streamline your vulnerability management processes. This checklist will ensure that your IT team stays informed about all emerging IT security gaps, empowering them to discover, resolve and report on all known internal and external vulnerabilities in a timely manner.

Unidentified Vulnerabilities Put Your Business At Risk

(According to a Ponemon Institute survey)

60%
of breach victims attribute their incidents to unpatched known vulnerabilities

62%
were unaware of their vulnerability prior to experiencing a data breach

52%
of organizations believe manual processes put them at a disadvantage in responding to vulnerabilities

It's time to take a proactive approach with vulnerability management, a critical layer in a successful risk management strategy.

When to Follow This Checklist?

- If your organization relies on the IT network you manage to operate effectively
- If your network is threatened by vulnerabilities that hit without warning
- If your IT data is scattered across different applications with varying interfaces
- If you lack the tools to identify invisible vulnerabilities in a streamlined manner
- If you are subject to government and industry regulations and standards that mandate vulnerability scanning

Do These Circumstances Sound Familiar?

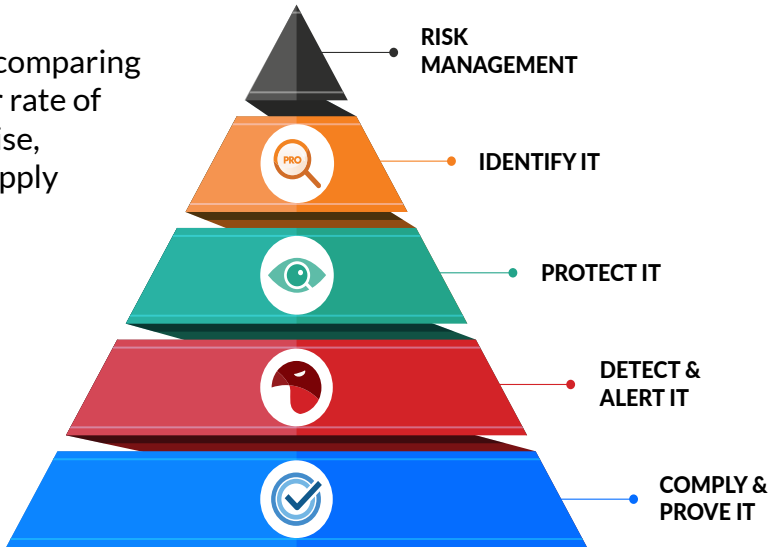
Identifying security gaps and vulnerabilities in your IT infrastructure can be simple. Follow the steps listed below to effectively identify, address and remediate the vulnerabilities lurking in your network.

Implement an Efficient Vulnerability Management Strategy

Vulnerability management is the process of identifying, classifying and prioritizing vulnerabilities in an organization's network that cybercriminals can exploit. The network scans provide an overview of the weaknesses, misconfigurations, open ports, malware and other security gaps using automated tools. Once the scan is complete, vulnerabilities should be reviewed, prioritized and remediated.

Without vulnerability scanning, it's impossible to achieve an effective security posture. Additionally, vulnerability scans are mandated by most data protection regulations worldwide, making it crucial for compliance purposes. Outlined below is a series of steps you should perform to implement an effective vulnerability management strategy.

- ☐ Set up and configure the scanner(s) on each managed network.
- ☐ Bind the scanner to a specific client site and schedule the scan.
- ☐ Scan for security vulnerabilities such as:
  - » Outdated and unpatched software
  - » Missing and poor data encryption
  - » Operating system and security misconfigurations
  - » Missing and broken authentication
  - » Poor cyber hygiene and human error
- ☐ Schedule regular scans on a frequent basis to identify new vulnerabilities and confirm the previous ones you addressed didn't reoccur.
- ☐ Review the results of the scans as soon as they are complete and immediately address any critical or high vulnerabilities.
- ☐ Set a regular maintenance schedule to take care of routine patches and lower the risk of vulnerabilities.
- ☐ Monitor your risk profile monthly by comparing the rate of new vulnerabilities to your rate of resolving them. If the delta is on the rise, increase the frequency of scans and apply more resources to your remediation efforts until you catch up.



Many IT security professionals focus on "offense" by deploying firewalls, anti-malware, EDR and other systems to prevent hackers from successfully intruding into the network. But none of these tools are 100% effective. This is why it's equally important to work on your "defense". An effective vulnerability management system will harden your network and provide an important additional layer of protection, giving you the power to manage and correct IT security flaws on an ongoing basis. Implementing IT risk management tools, like VulScan, is a vital practice to consistently ensure the health of an organization's IT systems and operations.

Identify IT Vulnerabilities Before the Hackers do

With a powerful vulnerability management tool like VulScan, you can avoid embarrassing and costly data breaches, schedule internal and external scans as and when you please, and take advantage of its flexibility and scalability to suit your organization. It is designed to help reduce cyber-risks through automated and ongoing network vulnerability discovery and management.

VulScan is the industry-leading vulnerability management tool used by thousands of IT professionals to eliminate all known internal and external threats across their IT environment.

Vulnerability Management for the Rest of Us!
Discover Its Power for Yourself.

VULSCAN

Stay focused on the most important risks and issues

SCHEDULE A DEMO

Get expert guidance whenever you need it

REQUEST A QUOTE

Show corporate leadership your value

WATCH ON-DEMAND DEMO