EBOOK

# 7 ESSENTIALS- VULNERABILITY MANAGEMENT

ManageEngine

# Table Of Content


**Does agent-based vulnerability management give you an edge? What about in remote work conditions?**

Eliminating blind spots is the key to an efficient ***vulnerability management program***, and endpoint agents do a great job of this. The scope of visibility, accuracy, and efficiency offered by agent-based scanning simply can't be achieved with agentless scanning.

Agentless scanning is network intrusive and is likely to result in traffic congestion every time a network-based scan is performed to discover and retrieve the vulnerability status of network assets. Additionally, it requires host credentials to access and run a detailed scan against an asset to inspect the file system, registry, and configurations. This brings up further issues with staying up to date with changing credentials and investing in secure storage options to prevent credential compromise.

On the other hand, agents are lightweight, multipurpose tools that reside within the endpoints. Since the agent resides on the client machine, it can bypass credentials and constantly keep tabs on new vulnerabilities, misconfigurations, and other security loopholes as they emerge without any restrictions on the scan window or disruptions to your network bandwidth.

Tracking assets over time in networks using dynamic IPs for network endpoints is no longer a problem since modern agents retain the vulnerability management server IP and are designed to reach out and report to the server in case of changes or disruptions. Besides, agents can replicate patch binaries directly from the server to the client directly from the server to the client machines, thereby eliminating the need for every client machine to download patches, drastically reducing overall bandwidth consumption.

Ever since the rapid paradigm shift to remote work in response to pandemic, many organizations have been relying on VPN gateways as the means to conduct vulnerability scans and patching procedures. This often results in bottlenecks that Ever since the rapid paradigm shift to remote work in response to pandemic, many organizations have been relying on VPN gateways as the means to conduct vulnerability scans and patching procedures. This often results in bottlenecks that slow down the update process. Plus, not all devices will stay connected to the network via VPN.

Endpoints may plug in and out of the network, and agentless scans can miss these devices if they're not connected to the network at the time of the scan. You can't afford to let your endpoints accumulate a heap of vulnerabilities while a sizeable proportion of them are beyond the bounds of perimeter security and exposed to insecure internet connections.

According to the International Data Corp-oration (IDC), **“70 percent of successful breaches begin at the endpoint.”**

Irrespective of the perimeter security or the lack thereof, knowing where assets are and securing each asset is essential, whether on the move, working from a different location, or connecting from a partner site. Endpoint agents are pivotal in maintaining uninterrupted visibility and control over your remote endpoints across your entire global hybrid IT.

With agents installed on your remote endpoints, you can have the agents download the essential patches from trusted vendors directly onto the remote machines without having to wait for the remote user to log on to your network via VPN, which can help avoid bottlenecks in VPN gateways. Forget location constraints; from scanning threats and vulnerabilities to deploying remediation, everything can be carried out seamlessly with the help of endpoint agents


02

**Do monthly or quarterly assessments based on compliance requirements suffice?**

A Microsoft study reveals tha*t 68% of the ransomware victims* did not have an effective vulnerability and patch management process in place.

Despite the reported number of breaches and the costs incurred globally due to unpatched and unsecured systems, many organizations never wake up to the fact that their network is on the verge of exploitation any minute.

Targeted attacks are rare. An overwhelming majority of attacks leverage known vulnerabilities that are prevalent across millions of endpoints across the globe.

Yet, many organizations still consider vulnerability assessment to be just another audit requirement and schedule their scans once a month or quarter or, even worse, once a year. These point-in-time snapshots of your network security posture don't lead to anywhere.

First of all, infrequent scans result in a deluge of scan data, producing hundreds of pages of reports, which



Yet, many organizations still consider vulnerability assessment to be just another audit requirement and schedule their scans once a month or quarter or, even worse, once a year. These point-in-time snapshots of your network security posture don't lead to anywhere.

can take anywhere from weeks to months to sift through. One major reason this is ineffective is because new vulnerabilities are identified every 90 minutes and patches are made available to them regularly. By the time you've finished pouring over the results of your scan, there may be new vulnerabilities taking root in your network.

Tracking assets over time in networks using dynamic IPs for network endpoints is no longer a problem since modern agents retain the vulnerability management server IP and are designed to reach out and report to the server in case of changes or disruptions. Besides, agents can replicate patch binaries directly from the server to the client machines, thereby eliminating the need for every client machine to download patches, drastically reducing overall bandwidth consumption.

out and report to the server in case of changes or disruptions. Besides, agents can replicate patch binaries directly from the server to the client machines, thereby eliminating the need for every client machine to download patches, drastically reducing overall bandwidth consumption.

The gap between vulnerability disclosure and active exploitation has shrunk in recent years, emphasizing the urgency of frequent vulnerability scans.

All it takes for an attacker is a single high-profile vulnerability to topple your business. Audit-based assessments should be a complement to continuous vulnerability assessments, not a replacement.

***The Center for Internet Security (CIS) emphasizes continuous vulnerability management in its top 10 security controls.***

Also, there's always the chance that you might fail to take timely action when you perform manual scans. Every time a new device or software instance enters your network, your organization is exposed to new vulnerabilities. Modern enterprises are tightly integrated with partners and customers. Every new opportunity opens up new avenues for risk.

On top of this, systems are changing all the time. You should run scans regularly as your IT ecosystem changes. A developer might write flexible firewall rules and create network shares for convenience while building software and leave them unchanged. Sometimes, administrators allow configuration changes for testing or troubleshooting purposes and forget to revert to the original state.

Basically, any undocumented changes could lead to misconfigurations that compromise security. That being the case, it's not only desirable, but also obligatory to employ automated vulnerability management tools to continuously monitor network assets, and track and resolve new vulnerabilities and misconfigurations as they emerge. Remember, you can't secure what you can't see.


03

## Are my vulnerability management efforts in vain without risk-based assessment?

About 29,603 new security vulnerabilities were disclosed in 2023!

With attackers developing exploits off public disclosures pretty soon, organizations need to be swift in their remediation efforts. But it can sometimes feel like there are too many vulnerabilities and too little time to address them all.

With limited resources and not enough time on hand, manually administering patches to all the vulnerabilities in your network is practically impossible. Even if you can afford to considerably bump up your sys admin/system ratio, it's unrealistic to have all Windows machines up to date with the latest patches the day after Patch Tuesday, since patching in itself will take a great deal of time depending on the number of systems, number of applications, type of resources to be patched, load handling capacity of the patching tool, organization's patching window, and testing process associated with patching. Additionally, patching window for servers are too narrow and extreme care must be taken when patching servers. One mistake can cause extended downtime and disruption to on-going business activities.

Though automation helps in shrinking the patching window to a significant extent, mindlessly automating patches to all machines without significant thought about remediation priority is utterly pointless. If the attacker manages to slip in and steal data by exploiting an imminent high profile vulnerability while your patching efforts are directed at low-risk vulnerabilities, your attempt to speed up patching using automations will be rendered futile.

Not all vulnerabilities pose an equal risk. Attackers know what works and what doesn't. Your ability to distinguish which vulnerabilities present an imminent risk to your enterprise security and which are less likely to be exploited makes all the difference between staying secure and falling victim to a cyber incident.

For instance, assume your vulnerability scan identifies 1,000 vulnerabilities in your network at one time. Patching them all at once is impossible, and patching them all in random order could leave highly critical flaws at the end of the queue while non-critical vulnerabilities are being patched first. But if you can cherry-pick those 100 high-profile vulnerabilities and patch them promptly, you'll stand a much better chance against cyberattacks.

To clarify, we're not advocating against patching all vulnerabilities. Given the rate at which new vulnerabilities surface, it's safe to consider vulnerabilities a constant threat to your network. That being said, the most reasonable approach is to eliminate vulnerabilities that present the highest risk at any given time first and automate rest of the patches after thorough testing.

This is why performing a risk-based vulnerability assessment to predict what is likely to be exploited and what the consequences will be is essential in effectively securing your network. This helps direct the IT security team's attention to the low hanging fruits instead of wasting time and resources on less

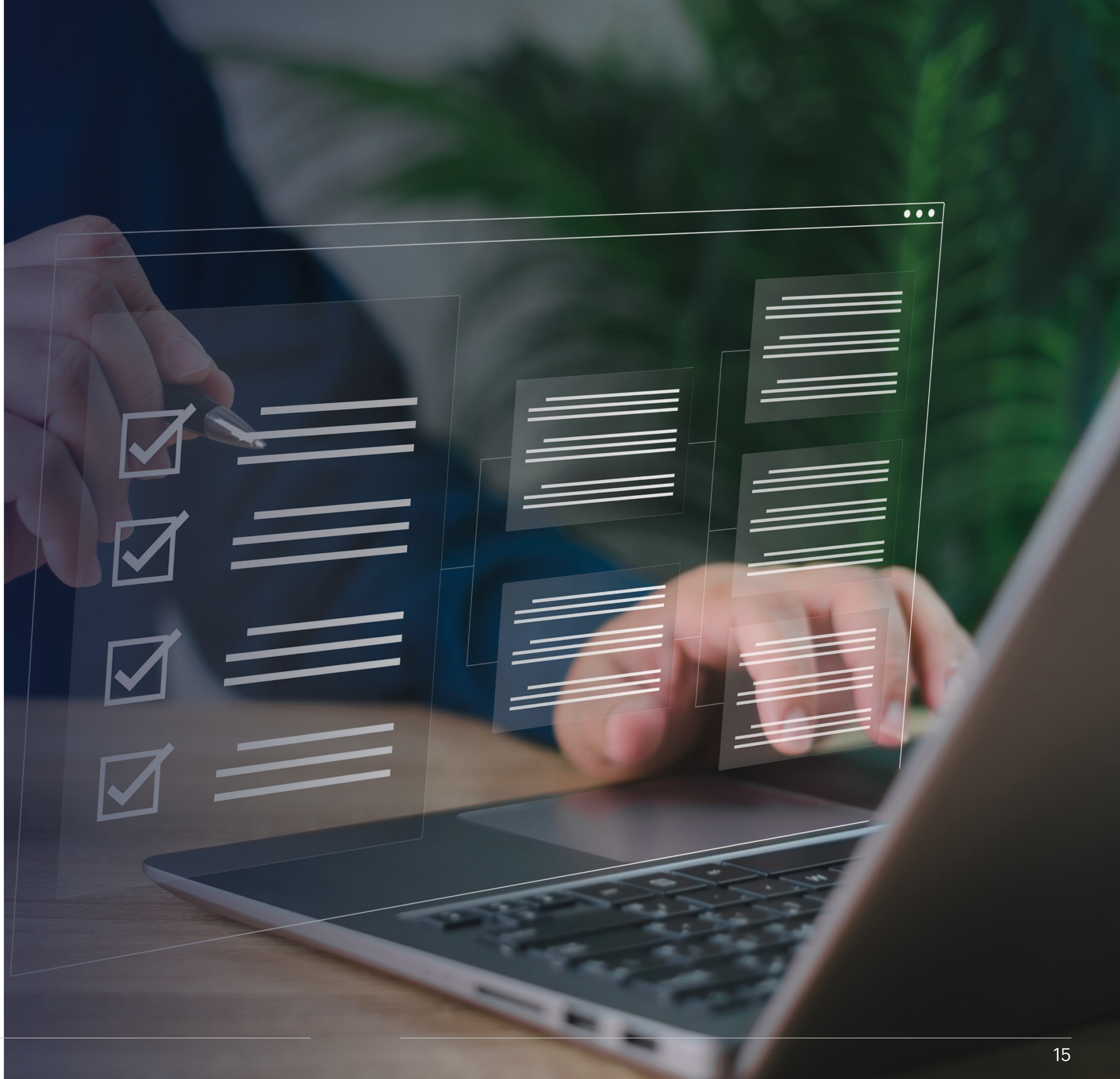
critical issues, the cost of fixing which can sometimes outweigh the risks.

### Here's more on the benefits you'll reap from risk-based vulnerability assessment:

- Identifying imminently exploitable and impactful vulnerabilities early on since most of them are wormable, meaning an exploit leveraging the vulnerability could worm through the network without requiring any interaction from admins or users.

- Giving context to vulnerabilities, which can be leveraged to determine their priority, urgency, and potential impact.

- Patching often can disrupt the normal operations of the business, as it consumes a good deal of network bandwidth and is typically accompanied by a subsequent reboot, which results in inevitable downtime. Prioritizing what truly needs to be patched immediately would help you strike a balance between risk mitigation and concomitant downtime




## What metrics do I need to track beyond CVSS scores to prioritize risks?

Common Vulnerability Scoring System (CVSS) scores have been viewed as the de facto measure to prioritize vulnerabilities. Vulnerabilities are assigned CVSS scores ranging from one to 10, with 10 being the most severe. However, they were never intended as a means of risk prioritization. If you've relied on CVSS scores alone to safeguard your organization, here's why you're probably using them incorrectly.

Because of its reputation as an industry standard, and the rate vulnerabilities are burgeoning, organizations leaned on CVSS scores for a framework for prioritization. But CVSS scores come with a slew of pitfalls. For instance, it's a general practice among organizations to consider anything above a severity score of seven as a High Risk. A large portion of the total vulnerabilities discovered every year fall into this bracket.

This is because an exploit of a vulnerability is based on the benefit that an attacker can leverage by exploiting it. Or, in other words, the impact that the attacker can unleash on an organization. Factors such as the technical feasibility of an exploit and public availability of proof-of-concept also influence the hacker's decision for which vulnerability to exploit.

CVSS scores are established for vulnerabilities within two weeks of their discovery, and are never revised. Sometimes, vulnerabilities with lower severity levels are exploited in the wild after the disclosure, and are never reflected in the CVSS scores.

Organizations prioritizing vulnerabilities based only on CVSS and severity ratings are left dealing with a substantial number of vulnerabilities classified as Severe but which pose little to no risk, defeating the whole purpose of vulnerability prioritization.

As a result, plenty of remediation efforts are dispersed on less exploitable vulnerabilities, while the important ones that require immediate attention remain exposed. This can be a slippery slope that gives you a false sense of security.

As a result, plenty of remediation efforts are dispersed on less exploitable vulnerabilities, while the important ones that require immediate attention remain exposed. This can be a slippery slope that gives you a false sense of

For vulnerability management efforts to pay off, organizations should augment their CVSS scores based assessment by adopting a multi-faceted, risk-based prioritization process based on factors such as vulnerability age, exploit availability, current exploitation activity, number of assets affected, affected asset criticality, impact type, and patch availability.

Now that we've established the variables essential to rigorously assessing your risk, let's discuss how they help you direct your attention to the most alarming areas, and adopt the best possible course of action.

## Understand the exploit availability and the exploit activity :

Knowing whether an exploit is

publicly available for a vulnerability is pivotal to vulnerability prioritization. These are the vulnerabilities that need immediate attention to break into your network and steal sensitive data.

Security teams should stay up to date on attacker activities by actively leveraging newly disclosed vulnerabilities and focusing their attention and efforts on ridding their endpoints of high-profile issues.

### Include the affected asset count and criticality to vulnerability prioritization:

Some assets are more important than others. Since web servers are at the perimeter of your network and are exposed to the internet, they're easy targets for hackers. Database servers—which record a wealth of information like your customers' personal information and payment details—should alsobe prioritized over other assets when defining the scope of your assessment, since even a lower-rated vulnerability on a business-critical asset like this may pose a high risk. Also, if a moderate to critical-level vulnerability is found to be impacting a larger proportion of IT assets, then it only makes sense to patch them immediately to lower the overall risk. In cases like these, vulnerability management solutions that wipe out a group of vulnerabilities across multiple endpoints using a single patch deployment task could come in handy.

### Identify how long a vulnerability has been lurking in your endpoint:

Once information on a vulnerability is out, the clock starts ticking, and the game is on between your security teams and threat actors. It's essential to keep track of how long high-profile vulnerabilities have been lurking within your endpoints. Letting a vulnerability reside in your network for a long time is an indication of weak security.

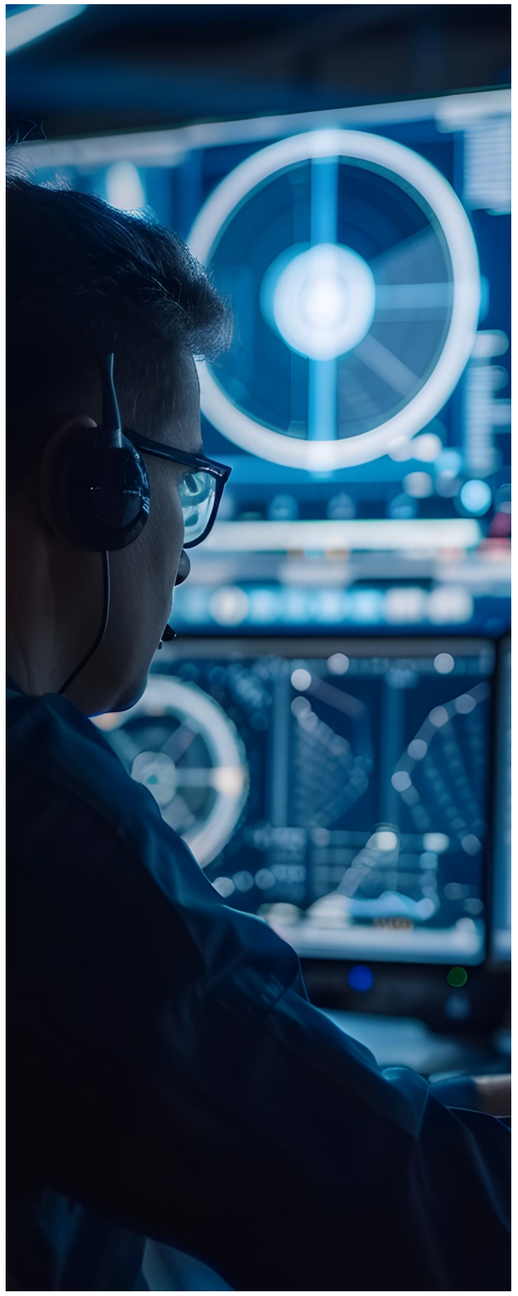
A vulnerability that seems less critical at first, might prove to be fatal over time, since attackers eventually develop programs that can take advantage of these flaws. A best practice is to immediately resolve vulnerabilities that have a known exploit or are actively exploited in the wild, followed by vulnerabilities that are labeled as Critical. Vulnerabilities categorized as Important are generally more difficult to exploit, but, as a rule of thumb, they should be remediated within 30 days.

### Triage vulnerabilities based on impact type :

Though ease of exploitation plays a significant role in risk assessment, exploitable vulnerabilities don't necessarily warrant an attack. In fact, attackers don't pick on vulnerabilities just because they've got a readily available exploit or require their least effort to exploit them, but because the vulnerability furthers their goals. Only then is the availability and ease of an exploit factored in.

Impact of vulnerabilities might include but not limited to, denial-of-service, remote code execution, memory corruption, privilege elevation, cross-site scripting, and sensitive data disclosure. More daunting ones are the wormable vulnerabilities, which allow any future malware exploiting them to propagate from vulnerable computer to vulnerable computer without user instigation.

Employing solutions that categorize and profile vulnerabilities based on the risk factors discussed above helps you triage vulnerabilities better and adopt an appropriate security response for your organization.




**Why juggling multiple tools for vulnerability assessment and patch management results in a siloed and inefficient workflow?**

*37% of the victims of cyberattacks* said they never scan their networks and systems to see what they need to patch.

Organizations tend to integrate a dedicated patching tool to their vulnerability assessment software to carry out remediation of vulnerabilities. There could be a couple of reasons why. Some organizations just want top-tier solutions for both patching and vulnerability management, thinking that would deliver the best possible result. Others might simply have no other choice if their vulnerability assessment tool doesn't come with built-in patching.

Vulnerability management should be approached as a unitary process, not an amalgamation of different products. Juggling multiple tools for vulnerability assessment and patch management results in a siloed and inefficient workflow. These tools are frequently handled by individuals from different teams, making it difficult to streamline processes like vulnerability scanning and assessment, ticketing, and patching.

When security teams identify and prioritize vulnerabilities, they need to send tickets to the IT teams detailing why the vulnerability is a high priority along with required action items to fix the vulnerabilities. When the vulnerabilities are fixed, the remediation/IT operations team needs to revert the status back to the security team, requiring the latter to perform additional validation to close the vulnerability management loop.

Two different teams leveraging two separate products not only causes delays in fixing the vulnerabilities, but also introduces the likelihood of potential disparity in data between integrated solutions and can affect the accuracy of tracking the entire cycle of vulnerabilities—from detection to closure—from a central location, thereby undermining the efficiency of the vulnerability management program.

Adding to this challenge, installing more than one agent from multiple vendors impacts system resource utilization and productivity. In dynamic environments characterized by the frequent coming and going of assets, an instance of one of the agents not being installed in any of the new assets could introduce further complications in the workflow.

Again, there's a cost factor associated with implementing separate solutions for vulnerability assessment and patching.

To do away with all these woes, your best bet is to invest in a vulnerability management solution that offers built-in patching functions that help you automatically correlate patches for detected vulnerabilities as well as regulate and monitor remediation of vulnerabilities from the same console.


## How do I defend my organization against zero day vulnerabilities, public disclosures, and other unpatchable situations?

Though deploying patches and putting an end to vulnerabilities once and for all sounds ideal, there are cases when vulnerability information is out but no fix has been rolled out by the vendor. This puts you behind the eight ball since attackers will be developing an exploit while your network is vulnerable, waiting for a patch. Let's look at a few different scenarios in which this could happen and possible methods to stay resilient.

## Zero-day vulnerabilities

When proof of concept (PoC) code of a vulnerability is exposed before the security hole is patched by the vendor, a zero-day exploit can occur. These vulnerabilities remain undisclosed and unpatched while being exploited in the wild, even before the vendor knows about them.

The very term "zero day" implies that the software developer or the vendor has zero days to patch the flaw since it often is unaware that the vulnerability exists before attackers begin to exploit it.

According to the Ponemon Institute's ***State of Endpoint Security Risk report***, an average of 80 percent of successful breaches were new or unknown "zero-day attacks". Generally, both security researchers and attackers alike are constantly probing operating systems and applications in search of weaknesses. They use an array of automated testing tools and reverse engineering techniques to find any holes that may exist in these infrastructures. If the good guys (i.e, security researchers, internet security firms, etc.) find the vulnerability first, they'll inform the vendor about the issue and withhold all details on the vulnerability until the vendor is able to release a patch to fix it. Cybercriminals, on the other hand, will use it to their own advantage if they're the first to discover a vulnerability.

There's no silver bullet solution that renders your network impenetrable to zero-day exploits. But following simple cyber hygiene can help organizations reinforce their cyber resilience and avoid joining the densely populated club of cyber casualties.

## Stay up to date with the latest patches

Although keeping all systems up to date with the latest patches can't guarantee complete safety against zero-day exploits, it will make it more difficult for attackers to succeed. With increased security in modern-day operating systems, it can take two or more known vulnerabilities to successfully launch a zero-day attack. So staying current with the latest updates for all your OS and applications could save your day.

## Enforce the principle of least privilege (POLP):

By limiting users' access rights to the bare minimum permissions required to perform their work, organizations can diminish the effects of successful attacks exploiting zero-day vulnerabilities.

### Block vulnerable ports and disable legacy protocols:

***The Wannacry ransomware attack that wreaked havoc on thousands of organizations before Microsoft came up with a fix could've easily been prevented if SMB V1 had been disabled and the firewall rule was set to block port 445.***

Ensure connections are blocked in the firewall to the NetBIOS trio, and check that insecure protocols such as Telnet, Server Message Block (SMB), Simple Network Management Protocol (SNMP), and Trivial File Transfer Protocol (TFTP) are disabled.

In scenarios like this, your best bet is to harden the security of your IT ecosystem (discussed in detail in the following section), isolate the systems affected, and blacklist the applications affected until a patch or workaround is available. Learn the best practices you can implement now to harden your environment against zero-day vulnerabilities.

### Public disclosures

In some rare cases, a software user might stumble upon a flaw and mention it online somewhere. Another instance may include a disgruntled security researcher disgruntled security researcher whose warning of a vulnerability in a product was left unheeded by the vendor, posting the vulnerability details in a public forum. There are also cases where the vendor unwittingly reveals the details of a flaw in a security bulletin before a patch is in place.

Usually, vendors quickly develop a workaround to mitigate the exploitation of the flaw. A tool that quickly and efficiently applies this workaround across all your endpoints to secure your environment against new threats is vital until a patch arrives to fix the flaw permanently.

### Forever-day vulnerabilities

Forget zero-day attacks on the latest software; legacy software that has reached the end of life will no longer receive security updates from the vendor and will remain forever vulnerable to any discovered vulnerabilities. The consequences of running an end-of-life software outweigh its benefits. Legacy OSs often can't run the latest applications, meaning they're stuck with legacy applications, which will eventually reach end of life, widening your attack surface.

Businesses in regulated industries may also face significant fines for running out-of-date systems.

This is why it's essential to keep track of which applications and OSs are approaching or have already reached end of life. Once they reach end of life, it's recommended that you migrate to the latest version of the end-of-life software.


## Should my security architecture be solely reliant on patching vulnerabilities?

Vulnerabilities are just an entryway into the network; there are several other security loopholes that attackers leverage to move through your network laterally. Therefore, care must be taken to extend visibility beyond just vulnerabilities in unpatched software and implement further controls to harden the security of your endpoints. Below, we discuss some practices you can implement that are effective in hampering attackers' attempts to break into your network.

A vulnerability scanning tool is only as good as its database of known faults and signatures. This database must be kept up to date since it serves as the baseline to scan continuously and rid your endpoints of security loopholes. Sweep your network for endpoints with disabled or out-of-date antivirus solutions, and make sure they're running enterprise-grade antivirus software with the latest definitions or signature files.



## Fine-tune User Account Control

One of the best ways to maintain access control and prevent unauthorized changes to your computer is through User Account Control (UAC). To squeeze all the benefits out of it, ensure User Account Control is set to:

- Switch to the secure desktop when prompting for elevation
- Prompt administrators for consent on the secure desktop
- Run all administrators in Admin Approval Mode
- Enable Admin Approval Mode for the built-in administrator account
- Prompt standard users for administrative credentials on the secure desktop
- Detect application installations and prompt for elevation
- Virtualize file and registry write failures to per-user locations
- Adhere to strong password and account lockout policies

Using easy-to-remember names or dictionary words as passwords is an indication of weak security. Often, hackers purchase credentials used in previous breaches and dictionary words to launch password-based brute-force attacks.

The average person reuses each password as many as ***14 times.***

Aside from enforcing long passwords, you should ensure users adhere to a mix of predefined password policies such as password complexity, minimum password age, maximum password age, and how many unique passwords that must be used before old passwords can be reused.

Complement strong passwords with account lockout policies to determine how many failed logon attempts are allowed before the account is locked out and how long it will be locked out. The account lockout policy is composed of three settings:

The account lockout threshold allows you to set the number of failed logon attempts accounts are allowed before the user account is locked out. Set the account lockout threshold value to 20.

Account lockout duration allows you to set the number of minutes the account will be locked. Set the account lockout duration value to 1,440 minutes.

The Reset account lockout counter after option allows you to set the amount of time that must elapse from the first failed login attempt for the failed logon attempt counter to reset to 0. Set the reset account lockout counter value to 30 minutes.

## Establish a secure foundation with security configuration management

Time to time, high-profile vulnerabilities and zero-days will rear their ugly heads, so poise yourself with a secure foundation so that your organization doesn't fall apart from a single vulnerability. If malware seeps into your network, it will leverage misconfigurations to worm its way toward its intended targets. Default settings, poorly documented configuration changes, or even technical issues can lead to misconfigurations in endpoints.

Deploying secure configurations is essential to address these configuration drifts and bring them back under compliance. Though the list of security configurations to be addressed in endpoints is long, let's take a quick look at the significant ones that we're most concerned with:

- Disable insecure TLS/SSL protocols that use cryptographically weak encryption algorithms, and enable the latest and more secure TLSv1.2. Also restrict the TLS communications from using default, NULL, or other insecure cipher suites and algorithms.
- Disable legacy protocols, such as Telnet, Server Message Block (SMB), Simple Network Management Protocol (SNMP), Trivial File Transfer Protocol (TFTP).
- Harden browsers by enabling safe browsing, restricting unsecure plugins, and deploying browser updates.
- Enable built-in memory protection components in the OS such as Structured Exception Handling Overwrite Protection



- Enable built-in memory protection components in the OS such as Structured Exception Handling Overwrite Protection (SEHOP), Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR).
- Disable anonymous logins, shares, and guest logins.
- Harden browsers by enabling safe browsing, restricting unsecure plugins, and deploying browser updates.
- Ensure BitLocker encryption is enabled to encrypt entire disk volumes.

## Audit active ports in use

Applications and services running on your system use ports to make themselves available over the network. Having continuous visibility over the ports that are active in your system is essential to discover what's listening on each port. By monitoring the ports in use and processes running in them, you can easily identify ports that may be activated by malware instances.

## Adopt secure remote desktop sharing practices

IT employees often use remote desktop sharing software to facilitate remote access and management of remote servers, virtual desktops, terminal servers, and applications over the internet for the ease of operation. Remote desktop sharing software improves productivity, but it also increases the attack surface, leaving the opportunity for an attacker to gain control over business-critical assets once they find a way to exploit the computer being used to access them remotely

If remote desktop sharing sessions are not encrypted, it might increase the possibility of a man-in-the-middle (MITM) attack. If at all possible, avoid remote desktop sharing tools. If you're left with no other option, at least secure your remote desktop connections with a strong password and prevent remote desktop servers from listening on default ports, thereby hampering attempts to establish an unauthorized remote connection.

Heaving a sigh already? Though you have a better understanding of

vulnerability management now, implementing all the best practices discussed throughout the e-book is likely to be a long haul. But what if we told you there is a single solution that could take care of it all for you?

# 08

**The one-stop solution to all your vulnerability management woes : ManageEngine**

ManageEngine offers prioritization-focused threat and vulnerability management software for enterprises offering built-in patch management. It's a strategic solution for your security teams, delivering comprehensive visibility, assessment, and remediation of threats and vulnerabilities across your network from a central console.

Aside from vulnerability manage-ment, it packs a powerful array of security features such as security configuration manage-ment, zero-day vulnerability mitigation, high-risk software auditing, antivirus auditing, port auditing, web-server hardening, firewall auditing, password policy management, BitLocker encryption, and automated patching to help you establish a secure foundation for your endpoints, so that you can rest assured that your network is in a solid security state.

## Endpoint Central

A complete UEM solution (cloud and on-premises) that offers Browser Security as well as Patch Management, Ransomware Protection, Software Deployment, IT Asset Management, Mobile Device Management, Remote Control, and much more.

**COMPLETE UEM & SECURITY SOLUTION**

## Vulnerability Manager Plus

A standalone risk-based vulnerability management solution that prevents threats in Windows and Linux.

**STANDALONE THREAT MANAGEMENT SOLUTION**

Follow us on:

sales@manageengine.com | +1-925-924-95

ManageEngine
a division of **Zoho** Corp.