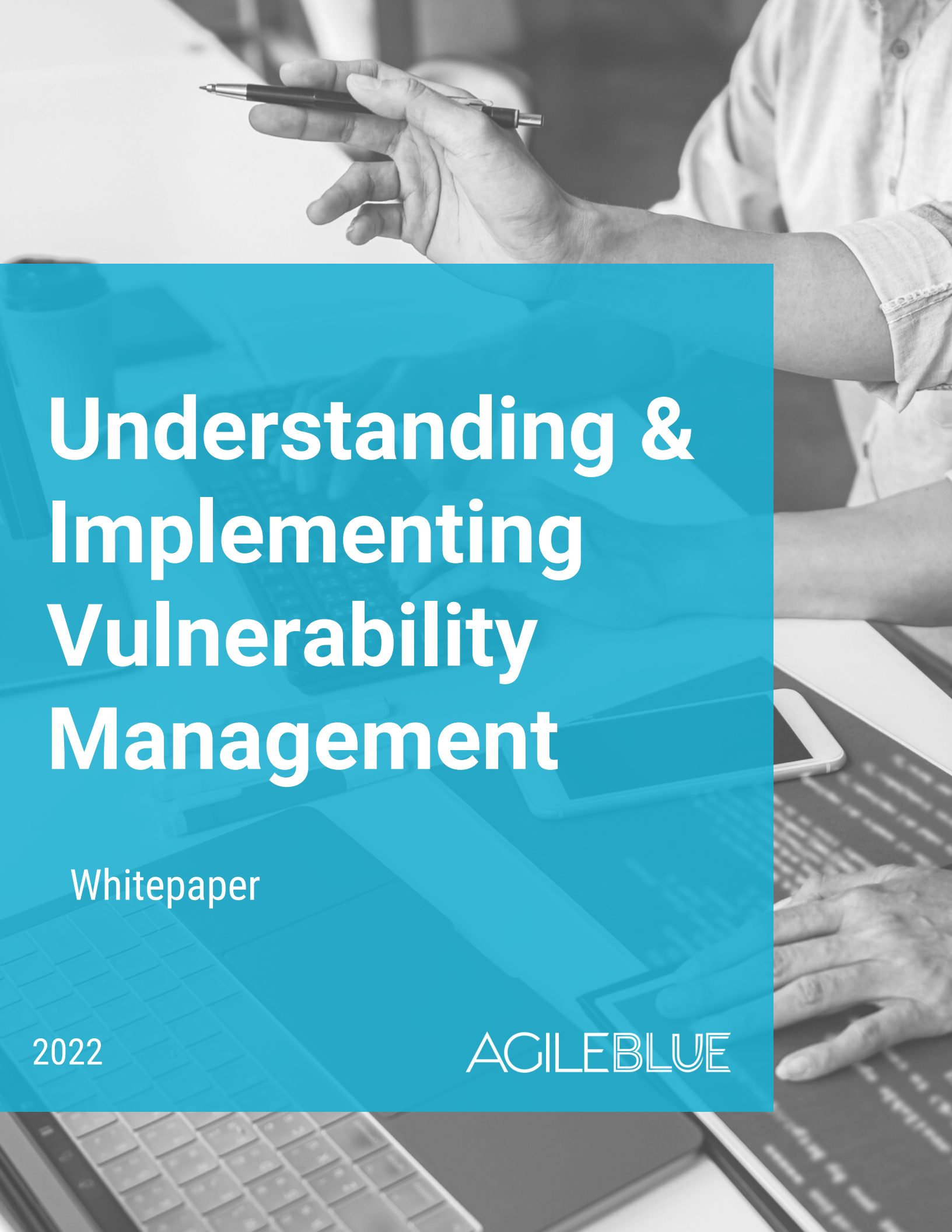


Understanding & Implementing Vulnerability Management

Whitepaper

2022

AGILEBLUE

OVERVIEW

Defined as the "cyclical practice of identifying, classifying, prioritizing, remediating and mitigating" software vulnerabilities," vulnerability management aims to identify vulnerabilities found across endpoints, systems, and workloads. It is a continual process that should be implemented into every organization's cybersecurity strategy to effectively mitigate the growing number of vulnerabilities. A proactive approach, vulnerability management seeks to close the security gaps before they are exploited by threat actors, making vulnerability management an integral step in avoiding cyber-attacks. It's important to note that vulnerability management isn't a set-it-and-forget-it approach. IT teams within organizations must be aware that new vulnerabilities may emerge daily within the organization, and the continued monitoring of possible security gaps is essential for continual threat mitigation.

The Evolution of Vulnerability Management

Vulnerability management has changed dramatically in its process and needs over the last couple of decades. In the early 2000s, IT teams only periodically ran manual scans for vulnerabilities because they didn't have anywhere near the number of current vulnerabilities. Conducting vulnerability scans every few weeks will no longer cut it in the current threat environment. According to an article by Security Ledger, roughly 1,000 CVEs were disclosed in 2000. Data reports indicate that somewhere between 18,000-30,000 vulnerabilities were reported in 2021. Because thousands of vulnerabilities are discovered year after year, organizations must take a serious approach to proactively address security gaps within their digital infrastructure daily to bolster their cybersecurity posture to the highest level possible.

Copyright © 2022 AgileBlue. All rights reserved.

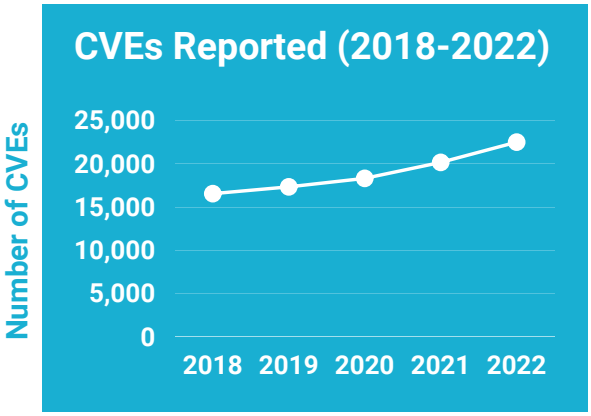
WHY YOU NEED VULNERABILITY MANAGEMENT

Growing Number of Vulnerabilities

Data collected by Statista shows that 2022 brought in the highest figure to date of common IT vulnerabilities and exposures (CVEs), with over 22.5 thousand. They've also collected data showing that Q3 of 2022 ended with approximately 15 million data records being exposed worldwide through data breaches, which is a 37% rise from Q2 of 2022. There is a large landscape with room for security gaps in your entire digital infrastructure, from your cloud to your endpoints and everything in between. All it takes is one vulnerability to give attackers the avenue they need to exploit your organization.

Rising Breach Costs

In the most recent Cost of a Data Breach Report conducted by IBM, they surveyed 550 organizations worldwide that experienced data breaches between March 2021 and March 2022. They found valuable insights into how costly data breaches and ransomware attacks had been throughout the year. They reported that the average cost of a data breach in 2022 was $4.35 million, reaching a new record high. This number indicated that breach costs have risen by 13% since 2020. Additionally, IBM reported that the average ransomware attack scored even higher, with an average price from start to finish of $4.54 million.



Source: Statista

22,500

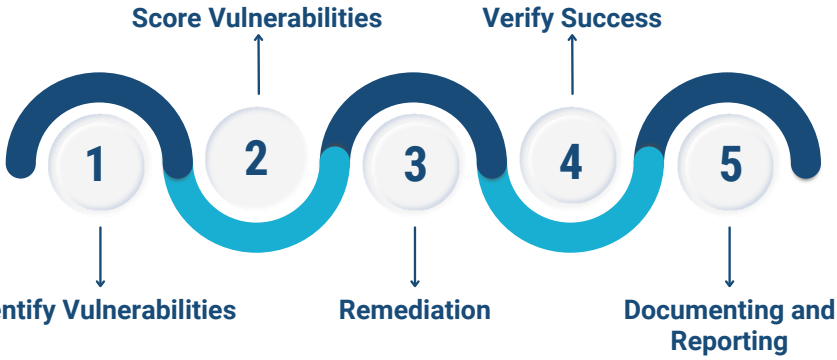
CVEs reported in 2022.

Making it the highest record to date.

Source: Statista

Copyright © 2022 AgileBlue. All rights reserved.

THE 5 STEPS OF VULNERABILITY MANAGMENT



1 Identify Vulnerabilities

The first step revolves around identifying the vulnerabilities. The identification of vulnerabilities is typically carried out through vulnerability scanning. The first step is crucial because it lets an organization know where they are at risk of attack. In this step, an automated vulnerability scanner searches and identifies vulnerabilities in the organization's digital infrastructure. The scanner creates an inventory of all IT assets, including servers, firewalls, operating systems (OS), routers, laptops, and desktops. The vulnerability scanner will also probe endpoints such as IoT devices, software, file systems, third-party applications, and system configurations. During this stage, the organization needs to identify which devices are protected and which components are not and learn how system endpoints can potentially be breached.

2 Score Vulnerabilities

After vulnerabilities are identified, vulnerabilities need to be categorized according to their risk level. This is typically done using the Common Vulnerability Scoring System (CVSS). CVSS allows organizations to prioritize which threats to focus on first. The scoring of vulnerabilities ranges from 0.0 to 10.0, with 10.0 being the highest risk level. Scoring is as follows;

Common Vulnerability Scoring System (CVSS)

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

Copyright © 2022 AgileBlue. All rights reserved.

3 Remediation

This next step focuses on treating vulnerabilities according to the risk levels identified in step two. The most common way vulnerabilities are treated is through patching. Patching often can effectively remediate most identified vulnerabilities. Given that nearly 85% of all security breaches are due to unpatched software, it is vital to use a patch management system that ensures that operations systems and third-party software are regularly updated.

4 Verify Success

Step four consists of verifying that vulnerabilities have been patched through follow-up audits. Specifically, through penetration testing, additional scans and other IT reporting. should be used to confirm that remediation measures for vulnerabilities are working. It is also essential to check that new vulnerabilities have not been created during this process.

5 Documenting and Reporting

An organization's C-suite and IT executives will need to understand the current risk state at all times. Therefore, regular documenting and reporting is necessary. Reports should be targeted, allowing you to easily compare and demonstrate the risks in the most current report with previous reports. Documenting vulnerabilities and security plans are also often needed to meet compliance requirements. Finally, recording vulnerabilities and remediations show overall accountability for an organization's security and will aid in improving security responses in the future.

Copyright © 2022 AgileBlue. All rights reserved.

CONCLUSION: ACT NOW

Countless organizations lose massive amounts of money every year due to cyber-attacks at the hands of unpatched vulnerabilities. To avoid this outcome, we highly encourage you to reassess the value you put on your vulnerability management processes, and ensure your organization is taking a proactive approach to mending security gaps.

If your organization doesn't currently have a vulnerability management process put into place, it is important that you understand that without vulnerability management, you are inherently at risk of attack. Do not wait for an unknown vulnerability to be exploited by cyber criminals to act. Act now and work through the process of implementing a vulnerability management program today to secure your organization's future.

Copyright © 2022 AgileBlue. All rights reserved.

AGILEBLUE

WE'VE GOT YOU COVERED

AgileBlue's integrated vulnerability scanning gives you complete visibility of your network assets and vulnerabilities. With built-in vulnerability risk ranking and dynamic network health scoring, you will get the full picture of your organization's vulnerabilities and their associated risk levels so that you can address them accordingly. Our vulnerability scanner allows you to customize the frequency of scans on a continual or scheduled basis to ensure scans are run regularly. Other added benefits include:

- Meeting compliance standards
- Scans via agent or network scanner
- Asset discovery and vulnerability scanning of all devices on your network, including any IoT and IP device
- Reduce cost and cyber vendor sprawl

For more information, visit us at AgileBlue.com.

Ready to start protecting your company?

REQUEST A DEMO