

A decorative graphic on the right side of the page consists of a grid of blue squares. A white diagonal line runs from the top-left corner towards the bottom-right corner, separating the white background from the blue grid. Some squares in the grid contain smaller, lighter blue squares.

WHITEPAPER

Vulnerability management then and now - a history

VULCAN.[™]

Table of contents

- The State of Vulnerability Management
- Vulnerability Management Platform:
The First Generation
- The Limitations of the Old Approach
 - CVSS Scores Aren't Live or Wild
 - The Challenges That Come With Patching
 - Costs: Financial and Otherwise
 - Divided Teams
- Vulnerability Management Platform: The Field Today
 - Complete Visibility is Essential
 - Automation is Required
 - The Value of Risk-Based Vulnerability Prioritization
- Going Beyond Prioritization, the Vulcan Cyber Advantage



The state of vulnerability management

Today's IT environment is notably different to that of the 1990s, with both infrastructure and applications changing substantially. While it has enabled us to reach new highs, it has also created new challenges.



Nowadays, enterprises are locating much of their data resources on the cloud, with self-contained, siloed data centers and networks no longer being the norm. Additionally, creating applications has changed remarkably. Rather than going through long deployment cycles, companies that work with CI/CD practices and have implemented DevOps practices are able to deploy almost continuously. This enables businesses to update their products with less downtime, which has become the new norm for their customers. In order to manage these processes, teams must now use more tools than ever before, adding to the complexity of managing and controlling networks.

These changes and others have affected the threat landscape. IT teams must protect a greater number of assets than ever before: not only on-prem, but also cloud-based assets as well, which increasingly incorporates third-party software.

In recent years, we've seen the number of vulnerabilities disclosed skyrocketing, with over 30,000 new vulnerabilities disclosed in 2017-18 alone. By the same token, the time it takes threat actors to exploit vulnerabilities has dropped substantially, demanding a much quicker response.

The situation has become challenging for security practitioners. It stems from both a methodological problem and a logistical one. In terms of methodology, for too long security teams have focused on the vulnerabilities with the highest CVSS scores or focused on mitigating "zero day" vulnerabilities rather than concentrating on the items that pose the greatest actual threat to their specific enterprise. This methodological issue is compounded by a logistical one: there is a serious shortage of qualified personnel. Studies show that in the US alone, there will be a shortfall of 3.5 million cybersecurity personnel by 2021. The combination of these challenges and the lack of human resources to deal with them make it vital for companies to reevaluate their approach vulnerability management.

We've broken down the old approach to vulnerability remediation and examine its limitations and weaknesses. We also outline current vulnerability management platforms, highlighting what is needed in order to keep up with 2020's threat landscape.




Vulnerability management platforms: the first generation

Back in the late 1990s and early 2000s, when only 1,000 vulnerabilities might be detected in an entire year, vulnerability management was a manual process, even for large enterprises. The software was manually scanned, problems were detected, IT decided what needed to be fixed, and the problem was solved. There was no need for automation, and a quick rescanning of the system was all that was needed afterwards. With under 100 vulnerabilities a month to be handled, everything could be taken care of as part of regular IT duties, like configuring new users and

other tasks. It might have been hectic, but the problems were solved.

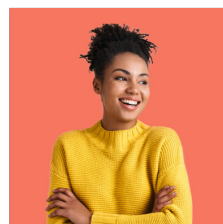
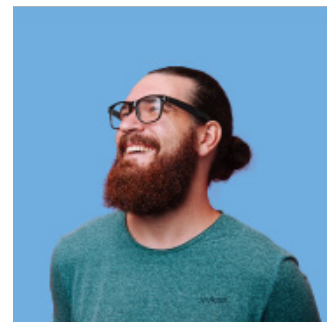
Ten years later, the internet has enabled companies to operate via remote locations. This, in turn, introduced new risks in the form of unwanted access. In addition, networks now include more software to support the industry-wide shift to the cloud and changes in development practices as previously mentioned, combined with software not being tested thoroughly, has led to the [explosion of vulnerabilities](#) over the last [decade](#).



**Start
prioritizing
for free**

TRY VULCAN FREE

VULCAN.



Limitations of the old approach

Security and IT teams soon found out that the old approaches were ineffective. The shift in IT environments changed the odds of being affected by vulnerabilities. It became more likely that they would use software containing vulnerabilities. The old methods of manually analyzing, prioritizing, and remediating stopped being practical. Given the large number of vulnerabilities, it was clear that not all could be addressed, and a new, scalable prioritization strategy or method was needed. Unfortunately, the tools developed over a decade ago cannot meet these needs; they have ceased to be practical or useful by themselves.

CVSS SCORES AREN'T LIVE OR WILD

A significant methodological shift that needs to be made is to change our approach to prioritizing vulnerabilities. Until recently, many people have used objective scores like the CVSS as the sole reference for assessing vulnerability criticality. However, this methodology is mistaken. To begin with, [CVSS scores were never designed to be a measure of risk](#). One reason for this is that they are based on isolated conditions, focusing on technical severity alone: they do not factor in the significance that the vulnerable assets have on the business. In reality, the same vulnerability could impact different networks in a different manner, as the assets and the business-functions that are at risk may vary. As so, it is essential to prioritize vulnerabilities according to the business-risk they pose.

Moreover, CVSS scores don't indicate which threats are actively being exploited in the wild. A vulnerability ranked as "medium" that sits on

an asset in the production environment, that is part of an active campaign should raise more of a concern than a "high" one that has no known exploit, sitting on a testing environment. However, if all you relied on to prioritize your vulnerabilities were CVSS scores, you wouldn't know which vulnerabilities should be addressed first. Make no mistake about it, hackers will use [the easiest, surest way](#) into a network in order to get data, meaning that focusing on CVSS scores could result in devastating outcomes for businesses.

The greatest threats that require your attention are the ones that can do the greatest damage to your assets right now. Given a company's limited resources, it is essential that risk analysis forms the basis of prioritizing your remediation efforts. It is essential that you focus on the vulnerabilities that are the most likely to threaten your network and its data.



THE CHALLENGES THAT COME WITH PATCHING

The traditional [“find it, fix it” approach](#) to remediation had security teams aiming to patch all vulnerabilities and doing so manually. While these measures may have been appropriate 10-20 years ago, they no longer make sense, no matter how big a company’s security team is.

In addition to the practical improbability of remediating everything, [patching itself is risky](#) for several reasons:

- **Risk of downtime:** While playing an integral role in keeping your network safe, patches are also likely to result in downtime. In the past, it was common practice for web-based services to be offline for several hours a week due to maintenance (i.e., patching and other activities). Nowadays, that’s unacceptable. This has to be taken into consideration when deciding the best way to remediate the vulnerability.
- **Risk of interference with other assets:** There’s a risk that a patch applied to remediate a vulnerability on one asset will interfere with another asset in your network. This stems from the fact that patches offered by vendors cannot take into account all elements of each network. The odds of this kind of problem increase substantially for cloud-native enterprises.
- **Risk of faulty patches:** Patches may contain flaws that were not be exposed during testing and will eventually impact production. The risk of this is increased by the current demand for quick deployment.

All in all, with these challenges, it is clear that there is great need for alternatives to patching, such as [compensating controls and workarounds](#). Sometimes, applying these measures will have the same effect as a patch in terms of strengthening security within the network, without causing the challenges raised above. This is why enterprises need a vulnerability management and remediation program that considers a wide set of approaches, rather than a patch-first mindset.



COSTS: FINANCIAL AND OTHERWISE

It is worth taking a moment to consider the cost of vulnerability management and remediation. In the 1990s, a reasonably-sized IT department could handle most of the tasks involved as part of their regular work. Tasks were given to various teams without much disruption. However, by 2020, the effort that enterprises are putting into managing vulnerabilities and misconfigurations, and eventually remediating them grew significantly. It was estimated that the [average enterprise currently invests around 413 weekly hours](#)—equivalent to almost ten and a half full-time employees—on vulnerability detection, remediation and reporting!

Not only were the old methods ineffective, but they also became expensive. Manual remediation is not only time-consuming, it is repetitive and often quite challenging. It tends to be unpredictable and downtime has become a serious issue for many teams. It requires prioritizing the vulnerabilities within the system, correlating them to the importance of the assets on which they are found, and the impact they may have on the business. Then, security professionals need to find the right solution, implement it and test it in production. Even with the largest and best trained staff, for most organizations, this process poses a major challenge that can cause anything from mere frustration, errors, to major financial damage.

Needless to say, these costs are trivial compared to the cost of an actual breach -- [in 2019, the average breach cost \\$3.92 million.](#)

DIVIDED TEAMS

The final problem with the old methods is that they perpetuated and even deepened [existing gaps between security and IT/DevOps teams](#) - vulnerability management came to be seen by IT/DevOps teams as a burden put upon them by security teams. This was particularly true because the processes involved were manual, time-consuming, and for the most part, involved implementing “outside” solutions with no consideration about how they would affect the enterprise’s specific network. Additionally, security and IT/DevOps teams often use different terminology as they come from different frameworks.

As a result, the teams involved often neither worked together nor communicated well. The knowledge that could have been gained about the software involved or how changes in architecture or components might improve the enterprise security was simply lost. These processes deepen the gap between the different teams, making the remediation process all-the-more challenging.

Vulnerability management platforms: the field today

Today's best vulnerability management platforms have been designed with the following principles in order to overcome the difficulties described above: visibility, automation of remediation, and improved prioritization of vulnerabilities.

COMPLETE VISIBILITY IS ESSENTIAL

First, modern vulnerability management platforms must provide complete visibility of a network's assets and how they interact. At the end of the day, you can't defend what you don't know you have. Without a complete mapping of all the different components in your network, your remediation efforts will be incomplete, and inevitably fall short. All aspects of the network need to be scanned- a misconfiguration in your scanner can cause blindspots, leaving the network exposed. Moreover, you must know how these are connected and interact with one another so you can be sure your remediation efforts won't lead to "surprise" side effects, including unintended downtime.

Visibility is also crucial when it comes to remediation tracking: knowing which steps were taken on which tools, when, and by who. Obtaining this 360 degree view into the remediation process can be challenging, because often tools and teams are spread across different platforms, making it difficult to view them all from one place.

AUTOMATION IS REQUIRED

Next, modern vulnerability remediation platforms need to fully support and implement automation as much as possible, from [threat detection to remediating vulnerabilities in scale](#). Automation quite simply saves time and money. It can ensure that appropriate measures are applied in a timely manner, freeing your teams to accomplish more than they would if they were working manually.

But besides its economic value, automation can ensure that the same steps are always applied to multiple instances of a recurring problem. If it is necessary to take certain measures in a certain order, incorporating automated playbooks or workflows will ensure that everything is done consistently and correctly. This could prevent human-derived errors that will inevitably cause downtime.

Automation is fast becoming the only viable method of meeting today's challenges because it is the only way that security teams can ensure that the same remediation solution is accurately driven throughout the entire network, promoting consistency and minimizing the margin of error.



THE VALUE OF RISK-BASED VULNERABILITY PRIORITIZATION

As discussed above, [risk-based prioritization](#) is essential for modern vulnerability remediation.

This approach ensures that your remediation resources are focused on the most urgent issues, reducing the likelihood of costly breaches. Moreover by focusing on how vulnerabilities affect your unique system, this approach encourages IT, security, and other stakeholders to work together in order to

effectively remediate vulnerabilities. Security teams need to take into account that every organization is affected by numerous factors in its environment. This also applies to organizational and business objectives; some assets are business critical and some are not and this must be evaluated when making the decision which patch to deploy or which systems to upgrade.



**It's time to own
your risk.**

REQUEST A DEMO

VULCAN.



Going beyond: the Vulcan Cyber advantage

The Vulcan Cyber remediation platform enables enterprises to overcome these challenges, providing complete automation and orchestration of the remediation process. It enables security teams, for the first time, to actually remediate the vulnerabilities and misconfigurations within their digital environments, rather than adhere to prioritization.

The platform begins by ingesting vulnerability assessments within Vulcan for contextual riskbased prioritization of all vulnerabilities and misconfigurations discovered. It pinpoints the most

business-critical threats, according to the risk they pose to the environment and focuses the remediation efforts. Through Vulcan's proprietary remediation intelligence database, containing millions remediation actions, the platform is able to recommend the most appropriate fix for any vulnerability - from configuration changes, through compensating controls to patches, if needed, based on a network's specific characteristics. Then, through its automation engine, the platform enables teams to implement solutions automatically, scaling the remediation process and effectively reducing risk.