eBook

The State of Vulnerability Management

Chapter One:
The Escalating Problem in Vulnerability Management

Nucleus

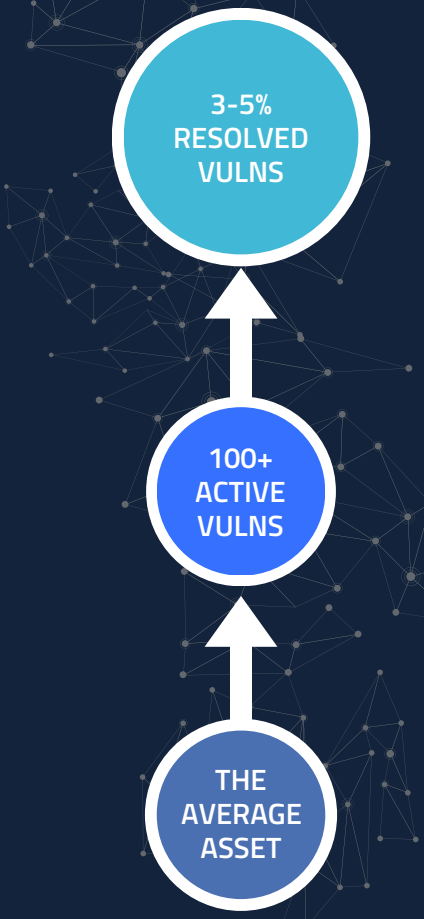
Chapter One:
The Escalating Problem in Vulnerability Management

Six years ago, vulnerability exploitation was barely on people's radar as a factor in prioritization. Today, 37% of incidents start with vulnerability exploitation, according to a 2022 Mandiant M-Trends report, making it the leading attack vector for initial access into organizations and a top cybersecurity risk, even bypassing phishing emails.[1]

A separate report by Kaspersky revealed that there were more initial intrusions from exploitation of vulnerabilities in Internet-facing applications in the last few years than there were breaches involving malicious emails and compromised accounts *combined*.[2] — And unfortunately, this surge in exploitation isn't ending anytime soon.

Even when you look past initial attack vector, vulnerability exploitation is still involved in over half of breaches [3], making it a huge risk to organizations. And the problem only continues to balloon year over year...both in the speed at which attackers are capitalizing on exploited vulnerabilities, and in the way that technology and assets outgrow most organization's current vulnerability management programs.

In this series, we're going to be breaking down how vulnerability management has grown and evolved over time, plus how to modernize your program using things like risk-based vulnerability management to actually get ahead of the problem and focus on the vulnerabilities that matter.



Source: Nucleus

In the modern vulnerability management space, it is widely accepted that too many vulnerabilities are discovered and known within an organization to possibly resolve and fix all of them.

So, how did we get here in the first place? Over the last decade, organizations have significantly expanded the way that they use technology to do business, moving from solely focusing on network devices to steadily growing in their use of applications and cloud infrastructure. No surprise here, especially when you look at how many organizations made the rapid move to a digital workplace over the last few years.

They've also increased the size of the teams that they have spinning up new systems and the number of assets being created, leading to the necessity of an aggregated approach simply to oversee it all.

However, as businesses themselves have accelerated, the corresponding maturity of their vulnerability management systems have been left in the dust. This is largely because, up until now, vulnerability management had primarily been a hands-on task left to vulnerability management teams and system administrators to painstakingly work through, finding and patching issues one at a time.

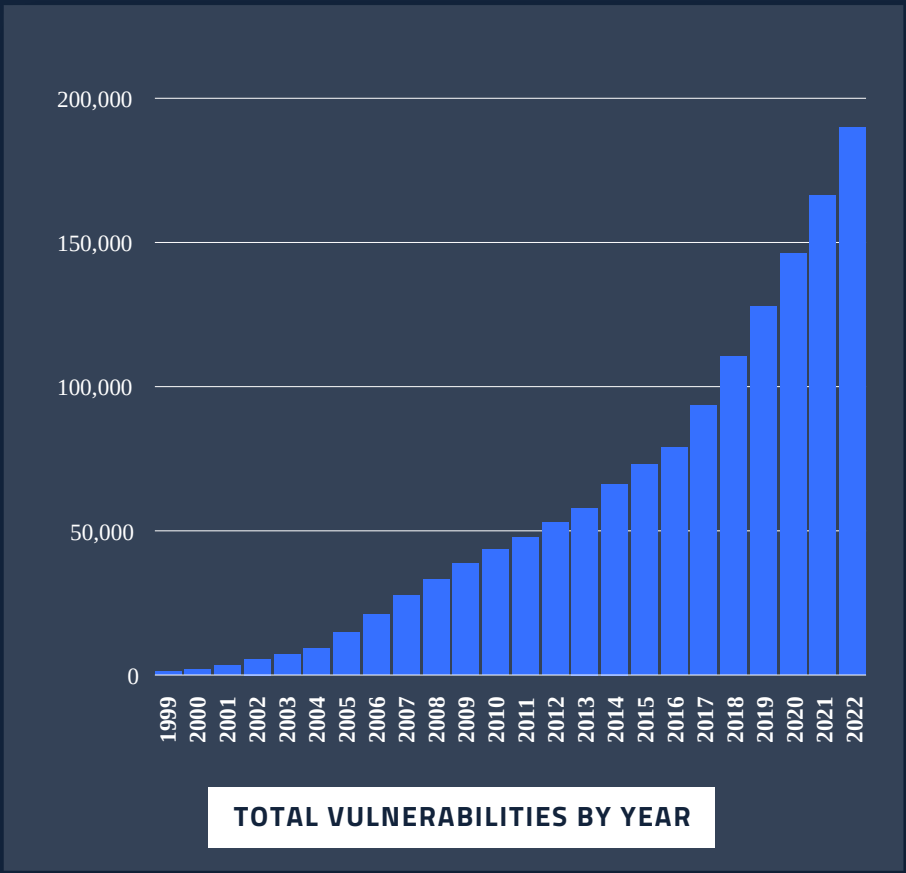
For many small and medium-sized businesses, this is probably still the case. But for larger organizations with tens of thousands of employees (and just as many devices or assets), it's physically not possible to hire enough people to triage and patch that many vulnerabilities quickly.

You can no longer use a hands-on approach to tackle vulnerabilities

In 2022, there were more than 24,000+ new vulnerabilities discovered globally.[4] At this rate, the sheer number of new vulnerabilities coming into your system each day will always be greater than the number you are able to fix with a hands-on approach. We see this in the fact that an average of 72% of vulnerabilities remain unpatched within 30 days, according to the Security Navigator 2023 report by Orange Cyberdefense.[5]

Plus, this problem only gets greater as your business grows, as companies with 10,000+ employees see the largest portion of medium and critical-risk vulnerabilities, while medium-sized organizations with 101–1,000 employees see the largest portion of high-risk vulnerabilities.[6]

So, whether you're facing a queue of 150,000 or 1,500,000 vulnerabilities, it doesn't matter how many your team fixes each day, month, or quarter, because the truth of it is, you're never going to manually be able to fix your current vulnerabilities faster than the number of new ones coming in. That's the actual problem we're facing in vulnerability management today.



Source: NIST National Vulnerability Database

You can't fix what you don't know

In addition to the escalation of new vulnerabilities easily overwhelming the strapped teams who are put in charge of overseeing and managing their assets, the scale of the data brought in by their related tools and vendors can also be overwhelming within the systems they use. This can be due to a lack of normalization among assets and systems, or a larger lack of visibility in general when it comes to finding, tracking, and patching vulnerabilities quickly.

However, having clear oversight of your vulnerabilities is essential when it comes to vulnerability management because, without it, businesses cannot have full understanding over their risks, assets, connections, and requirements. It also puts pressure on already stretched teams and can lead to serious gaps in management and execution over their vulnerability program.

BETWEEN 5%-20%

The number of known vulnerabilities firms are able to fix per month

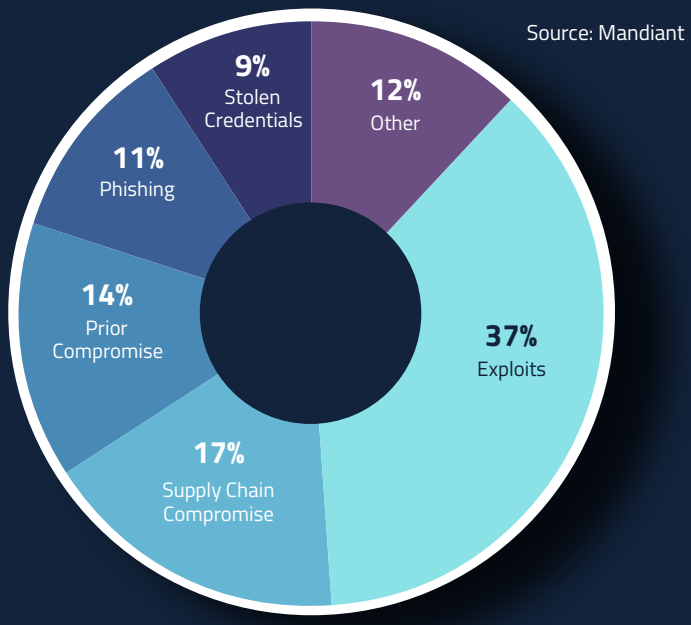
Source: First.org

Attackers are weaponizing vulnerabilities quicker

The sheer number of vulnerabilities that we are seeing each year is not the only thing leading to the escalation of vulnerability management problems. The time between the discovery and initial exploitation of a vulnerability is also becoming shorter, and the number of mass exploitations is increasing.

78% of identified attack paths use known vulnerabilities (CVEs) as an initial attack vector.[7] Palo Alto researchers found threat actors typically scan for systems with a just-disclosed flaw minutes after the CVE is announced.[2]

For example, they observed an authentication bypass flaw in an F5 network appliance (CVE-2022-1388) being targeted 2,552 times in the first 10 hours alone after vulnerability disclosure.[2] In addition to searching for vulnerabilities quickly, attackers have also gotten faster at exploiting the vulnerabilities they find.



Source: Mandiant

A study by Rapid7 showed that the mean time to known exploitation for vulnerabilities in 2021 was just 12 days — a 71% decrease from 42 days in 2020 — which they attribute to a sharp rise in zero-day exploit activity.[8]

Time is money... so are unresolved vulnerabilities

As we stated earlier, vulnerability exploitation is involved in over half of all breaches, making it not just an overwhelming problem for your vulnerability team, but an expensive one for your entire company. The average cost of a data breach in the United States in 2022 was $9.44m, with the US holding the record for the highest cost of data breaches for the 12th year in a row.[9]

$9.44M

Average cost of a data breach in the United States

Source: IBM

83%

Number of organizations with more than one data breach

Source: IBM

However, while the amount of time that it takes to identify and contain a breach is an average of 277 days (or about 9 months), it's been confirmed that shortening that amount of time to 200 days or less can actually minimize the full cost of breaches for your organization.[9] Companies who were able to contain data breaches in under 200 days saw an average savings of $1.12m, with organizations who had deployed AI and automation programs saving nearly $3.05m in breach costs, as they were able to identify and contain a breach 28 days faster than those who didn't.[9]

Conclusion

The Escalating Problem in Vulnerability Management

All of this just shows that traditional approaches to vulnerability management no longer provide sufficient defense against modern threats. The probability of a breach or compromise occurring due to vulnerability exploitation is higher than any other cyber attack vector, and the speed of vulnerability remediation is critical. However, with the increasing volume of new vulnerabilities discovered each day, the speed required to stay ahead of attackers is only achievable with a risk-based approach to vulnerability management.

In the next chapter of our series, we'll be tackling tackling how you can get better outcomes through precise and targeted vulnerability management, including how to use vulnerability intelligence and vulnerability decision trees for a more risk-based approach.

SOURCES:
1: M-TRENDS 2022 Report, Mandiant
2: Vulnerability Exploits, Not Phishing, Are the Top Cyberattack Vector for Initial Compromise, Dark Reading
3: Intelligence-led Vulnerability Management, Nucleus Shortcuts
4: NIST National Vulnerability Database
5: Security Navigator 2023 Report, Orange Cyberdefense
6: 2021 Vulnerability Statistics Report, Edgescan
7: 2022 State of Public Cloud Security Report, Orca Security
8: Annual Vulnerability Intelligence Report: 2021 Edition, Rapid7
9: Cost of a Data Breach 2022 Report, IBM