How To Implement a Risk-Based Vulnerability Management Methodology

20 April 2023 - ID G00777685 - 22 min read

By Craig Lawson

Vulnerability management has long been viewed as a compliance function instead of a threat-prevention capability. Security and risk management leaders should implement Gartner's RBVM methodology to prevent threats, quantify operational risk and meet compliance mandates.

Overview

Key Findings

- For over a decade now, a statistically small number of vulnerabilities has represented a majority of operational cyber risk to organizations. The core risk lies in how vulnerabilities are exploited for a wide range of threats and operated by various threat actors. Therefore, it is critical that organizations identify and prioritize vulnerabilities. Also, organizations must have a range of compensatory threat-prevention measures in place — apart from just patching.
- A limited number of organizations have implemented operational risk quantification to improve resource allocation against the most pressing threats. Too many organizations rely on the well-intentioned, legacy framework approach. The issue is that these are neither evidence-based nor adjusted dynamically for your environment. In many cases, they are assisting threat-actor activities rather than hindering them. This is a key reason why the volume of breaches in recent years has continued unabated.
- Organizations are confronted with a large number of vulnerabilities being discovered by assessment functions. Concurrently, organizations often have little contextualized guidance on how to reduce the risk of breaches.
- Patching is more nuanced and complicated than the "just patch it" thinking frequently found in legacy vulnerability management (VM) frameworks. Organizations will continue to struggle to patch systems at the same time scale threat actors operate. This reality must be considered for any VM program to succeed. Therefore, security and risk management (SRM) leaders must have various compensating controls outside of just patching.

Recommendations

Security and risk management leaders responsible for vulnerability management (VM) should:

- Implement a risk-based vulnerability management (RBVM) program that includes assessment of a broad range of assets. Also, apply quantification principles to allow for prioritization and then have a range of compensating measures that includes more than just patching. Doing so will help reduce the organization's exposure to threats while concurrently helping quantify the organization's threat landscape.
- Adopt the RBVM methodology as it uses additional context, such as asset context, threat-actor activity and compensating controls. It also employs the base vulnerability assessment (VA) telemetry to evaluate and identify true risk. This evidence-based approach can significantly reduce the possibility of a breach.
- Look to augment your VA tool with dedicated vulnerability prioritization technology (VPT), breach and attack simulation (BAS), external attack surface management (EASM) and attack path assessment tools. Doing so will provide better vulnerability prioritization and more effective operational risk quantification. These emerging technologies reduce the onerous manual work required and are now present as features in most VA solutions — although efficacy varies.
- Use evidence- and risk-based approaches to improve functions like patching with compensating controls. Examples of controls include intrusion prevention system (IDPS), network detection and response (NDR), web applications firewalls (WAF/WAAP), multifactor authentication (MFA), application control and network segmentation (including zero-trust principles). These controls can help compensate for the risk of a breach when unable to patch vulnerabilities, reduce the attack surface and prevent vulnerabilities from being exploited.

Introduction

A vulnerability, when viewed solely in isolation using the traditional treatment method based on critical, high, medium and low ratings, is problematic for several reasons.

The **common vulnerabilities and exposures** (CVE), the **common vulnerability scoring system** (CVSS) and the **common weakness enumeration** (CWE) open standards are mature and widely adopted. These examples represent a laudable development for the security industry as a whole. However, another reality remains in that threat actors pay little to no attention to the scoring of a vulnerability. They prefer to use "what works," including regularly capitalizing on lower than critically ranked CVSS common weakness enumerations and vulnerabilities. Currently, it is also a reality that critically ranked vulnerabilities are not the most exploited in terms of aggregate volume (see Figure 1).

The large volume of vulnerabilities that organizations have to deal with makes it impractical to try to remediate all of them, despite the unrealistic mandates of many compliance frameworks still in place to this day. This has led to the situation where many VM strategies that Gartner reviews are still not anchored to evidence and rely on inflexible frameworks, with very few applied dynamic and risk-based principles.

Many security frameworks overlook the complexity of patching. For example, vulnerabilities often can't be patched for valid reasons — for example:

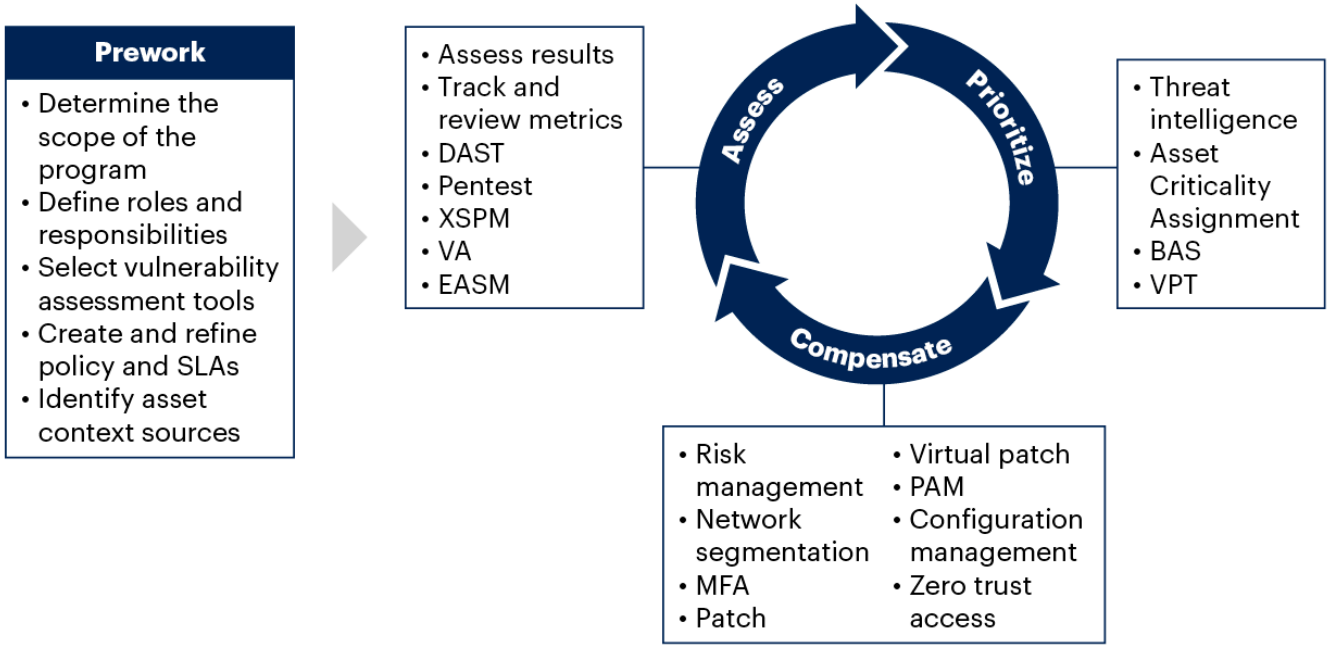
- Availability of patches. There are a number of vendors who simply do not issue patches in a timely manner.
- Compliance frameworks for critical infrastructure that can slow down patching by putting caveats on how this infrastructure must operate.
- Untested patches that can break overall functionality. This can be the result of the lack of regression testing that can happen if the emergency patching path is actioned.
- The prevalent and problematic issue of software cohabitation dependencies. Such dependencies will require testing or SRM leaders will need to wait for all related patches from other vendors to be available on systems before proceeding with the patch identified as the required redress.

The traditional method of vulnerability management has also caused significant friction between security and IT operations teams over the years, which continues to this day. The two teams often have competing deliverables, such as security versus uptime. These problems are compounded by the uncontrollable x-factor of threat actors. To support a more productive relationship between security and IT operations teams, SRM leaders should use the RBVM methodology, which has a more pragmatic and evidence-based approach to patching.

RBVM is different from traditional VM methodologies — namely, in its focus on applying risk quantification targeting to your specific threat landscape and advocating for a range of compensatory methods outside of just patching. Having a pragmatic recognition of reality is only partially effective. Accordingly, SRM leaders need to focus on methodologies, such as RBVM, that can provide the best results with the time and resources available.

Figure 1: Gartner's Risk-Based Vulnerability Management Methodology

Gartner's Risk-Based Vulnerability Management Methodology



BAS = breach and attack simulation; DAST = dynamic application security testing; EASM = external attack surface management; MFA = multifactor authentication; PAM = privileged access management; VA = vulnerability assessment; VPT = vulnerability prioritization technology; XSPM = extended security posture management.

Source: Gartner

777685_C

Gartner

Analysis

Using an evidence-based approach for vulnerability management helps the VM program in meeting compliance mandates but, more importantly, makes your organization far less prone to a breach. Overall, it assists SRM teams in better understanding cyber risks presented by a range of threats and threat actors. RBVM achieves this by more accurately quantifying operational cyber risk, allowing faster and better decisions to be made — and proactively improving your organization's security posture.

This approach will result in a deeper understanding of your organization's current threat landscape. Also, when actioned in a reduced attack surface, it can provide breathing room for additional patch installation. This could be done where sensible regression and cohabitation testing can be performed (see **Innovation Insight for Attack Surface Management**). While Gartner, at this time, does not have the quantitative data to validate this sentiment, it is well-understood in IT operations that a considerable amount of outages and downtime comes from trying to patch or update systems.

Patching represents credible availability risk to a business and, ironically, so too does not patching. Real progress lies somewhere in the nuanced middle path.

Gartner frequently receives inquiries from clients who are challenged with how to successfully treat all vulnerabilities identified during VA activities. There is often a large gap between the discovery of vulnerabilities and the resources available within IT operations to treat them within the time frame in which attackers operate.

Figure 2 shows, on average, how long a vulnerability takes to be exploited. If you can't patch or apply compensating controls measured in days, you are at credible risk of a serious breach. Threat actors prefer and overwhelmingly target known vulnerabilities, thus taking this situation to their advantage.

However, one important remaining point is that vulnerabilities that do get exploited in the wild, which are statistically small, have long been used by threat actors. The active vulnerability in Apache's Log4j software library illustrates a high-profile example that came to prominence in December 2021.[1] Log4j is still seeing a large number of attempted exploitations by a wide range of threat actors. This has been quite a frequent occurrence over the last 20 years.

Much of this reality has to do with how VA yields a large number of vulnerabilities. This describes various severity-risk weightings based on static parameters, like the CVSS. This is not a problem of VA per se, as these tools are generally accurate in their findings. However, the challenge lies in how large many organizations' IT assets and digital footprints are, so it's the volume that is an accuracy issue.

However, the CVSS base score is not a complete measurement of real-world risk (see Note 1). It does not take into account the "x-factor" of threat actors. Additionally, CVSS was never designed for exhaustive assessments or estimations of threat-actor activity, so its effectiveness is not at fault.

Some organizations follow a general philosophy of partial remediation driven by static compliance frameworks, often focused primarily on critical- and high-ranked vulnerabilities. This can include, for example, "remediate X% of critical severity vulnerabilities within four weeks of discovery" or "apply patches from vendors on a monthly basis." Both alternatives reduce VM to a pure metrics exercise where risk is expressed as a numerical value. Unfortunately, this approach does little to reduce risk in real terms, as attackers normally have the first-mover advantage and do not primarily focus on vulnerability severity levels.

Implement Risk-Based Vulnerability Management as a Program by Iteratively Following Three Key Steps

Figuring out what vulnerabilities and systems to remediate first remains a critical challenge. A large number of Gartner inquiries that have focused on VM in the past several years mention this challenge.

Gartner's position is that the ideal way to prioritize vulnerabilities for remediation and mitigation is based on real risk to your organization. Compliance mandates are inescapable; VM has been seen as a compliance process for too long. The reality is that an RBVM program is an evidence-based way to understand and be able to proactively reduce an organization's attack surface and account for the most substantial risks.

> **Just because an organization has performed vulnerability management the same way for a long time, that doesn't mean it was the right approach.**

While high-profile threats in the media continue to drive high interest, coverage is not often focused on the root cause. Many clients spend too much energy focusing on threats that are not relevant to their organization.

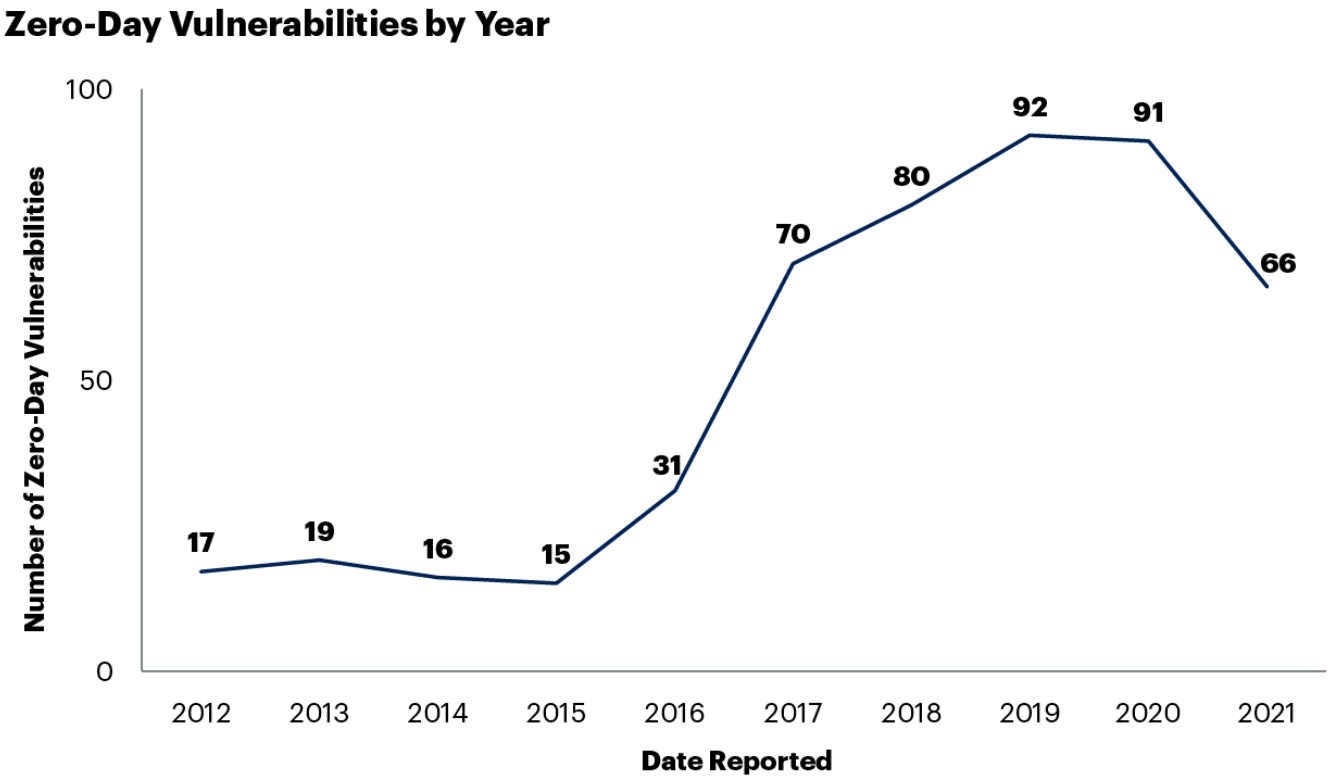
For a considerable amount of time, threats in cybersecurity (for example, malware of all sorts) have had a direct correlation with vulnerabilities. Vulnerabilities — and the exploitation of vulnerabilities — remain a key "root cause" that is driving cyber attacks to this day.

Achieving provable cyber-risk reduction with VM requires an understanding of how to improve this process on operational levels. In other words, a key outcome of RBVM is to reduce the largest amount of cyber risks that will impact your business using the resources you already have. It is not possible for an organization, at any security maturity level, to achieve zero vulnerabilities in its environment. Thus, it is imperative that SRM leaders focus their constrained resources on the vulnerabilities that matter the most to the organization, as this directly, effectively and efficiently reduces the attack surface.

> **The unprioritized and ignored vulnerabilities may seem less insignificant but can represent a material risk today and in the future.**

RBVM is an iterative process that is critical to achieving better outcomes for any VM program (see Figure 2). Overall, vulnerabilities and their exploitation by attackers are driving the threat landscape. In addition, most malicious activity is also coming from already-known vulnerabilities and not zero-day vulnerabilities.

Figure 2: Zero Day Vulnerabilities by Year



Source: Gartner (data drawn from the IBM X-Force vulnerability database)
777685_C

Gartner

The RBVM methodology is an iterative model that has three primary steps:

- Assess
- Prioritize
- Compensate

Assess

Base-level-vulnerability-assessment functions are a well-recognized and staple process, with clients of all sizes using technologies for a wide range of managed security service providers (MSSPs) and outsourcers.

Assessment in RBVM is a task that is performed iteratively with no real beginning or end, and VA and VM have been security processes for decades. The RBVM contains several functions:

- Reviewing previous assessment results to look for improvements and observations on the current state of the VM program in relation to various items:
  - Review and assess how VM metrics are tracking over time. For more information, see Tracking the Right Vulnerability Management Metrics and Outcome Driven Metrics.

    - Regular sessions with the other asset owners who are responsible for patching, configuration changes and system updates.
    - Account for any architectural and asset-class changes — for example, consuming more cloud services, covering remote workers and deploying the Internet of Things (IoT) or operational technology (OT).
    - Review assessment coverage to make sure the organization is covering enough of its assets and providing sufficient visibility.
- Assessing if previous actions and compensatory work are still effective or an ongoing piece of work to complete.
- Noting any new exceptions into the program that are handled outside or separately from the core VM process. Exception management remains an operational chore for many organizations.
- Performing new risk management and VAs to discover state changes of existing assets and services that need to be accounted for.
- Conducting new assessments to check the state of any new assets that have appeared or have not been previously assessed with net new assessment content.

Vulnerability assessment is a mature technology market. It can be performed in many ways, such as through:

- Active scanning — with credentialed scanning being preferred and sometimes mandated due to its improved efficacy.[2]
- Passive scanning to create VA telemetry without directly interrogating assets but from techniques like monitoring network traffic.
- Using agents deployed locally on hosts.
- Using APIs to assess the state of cloud services or where APIs are used for enumeration.
- Scanning assets from an external perspective to ensure complete coverage.

The goal is to assess the organizational assets to understand the state of the software, firmware and configuration of all assets — be they internal, external or even running in the cloud (see **Market Guide for Vulnerability Assessment**). For the assessment phase, there are a number of enabling technologies that must be considered as part of a comprehensive RBVM program. Examples include VA, vulnerability prioritization technology (VPT), threat intelligence, EASM and BAS. These technologies are all valid and should be considered as part of a comprehensive RBVM program for the assessment phase from a technology point of view. The VA is increasingly converging, and technologies like VPT and EASM are now evidenced in many VA solutions.

Assessment is also moving to be predominantly delivered from the cloud, although on-premises solutions will persist for some time. The assessment phase covers the usage of tools performing assessment functions and provides an overall view of your environment, further driving the other parts of the VM program. Accordingly, SRM leaders should consider other elements while performing the assessment phase:

- Review your VM program and how it is delivering on other related goals related to compliance, governance and how VM folds up into risk management. VM should not be treated in isolation as it must interlock into other security operations functions.
- Review and reassess how the organization is tracking against key metrics in your VM program. For more information, see **Tracking the Right Vulnerability Management Metrics**.
- Review how the discovered assets are also being classified in terms of their business criticality. This should be a key driver in how SRM leaders prioritize the VM program.
- In addition to the tools being used, ensure the VM function is staffed adequately. In case the organization is short of staff, the prioritization features in RBVM will help direct the time you do have to the most pressing issues.

Prioritize

Taking the telemetry from the assessment function, and just as critically, your knowledge of the business and its assets, is key to success for this phase. In terms of technology, this entails performing post-processing telemetry with analytics on the volume you get from tools generating vulnerability and asset telemetry. Currently, this represents one of the biggest improvements to any security operations program.

An evidence-based prioritization drawing on real-world threats allows SRM leaders to understand some key concepts in achieving better operational risk quantification. This evidence-based approach is one of the key reasons why RBVM looks the way it does today.

For over the last decade, it has been a statistical reality that only a few vulnerabilities have been exploited in the wild (see Figure 3). Therefore, it is a critical metric for organizations to know:

- How many vulnerabilities you have.
- How many of them are being exploited in the wild.

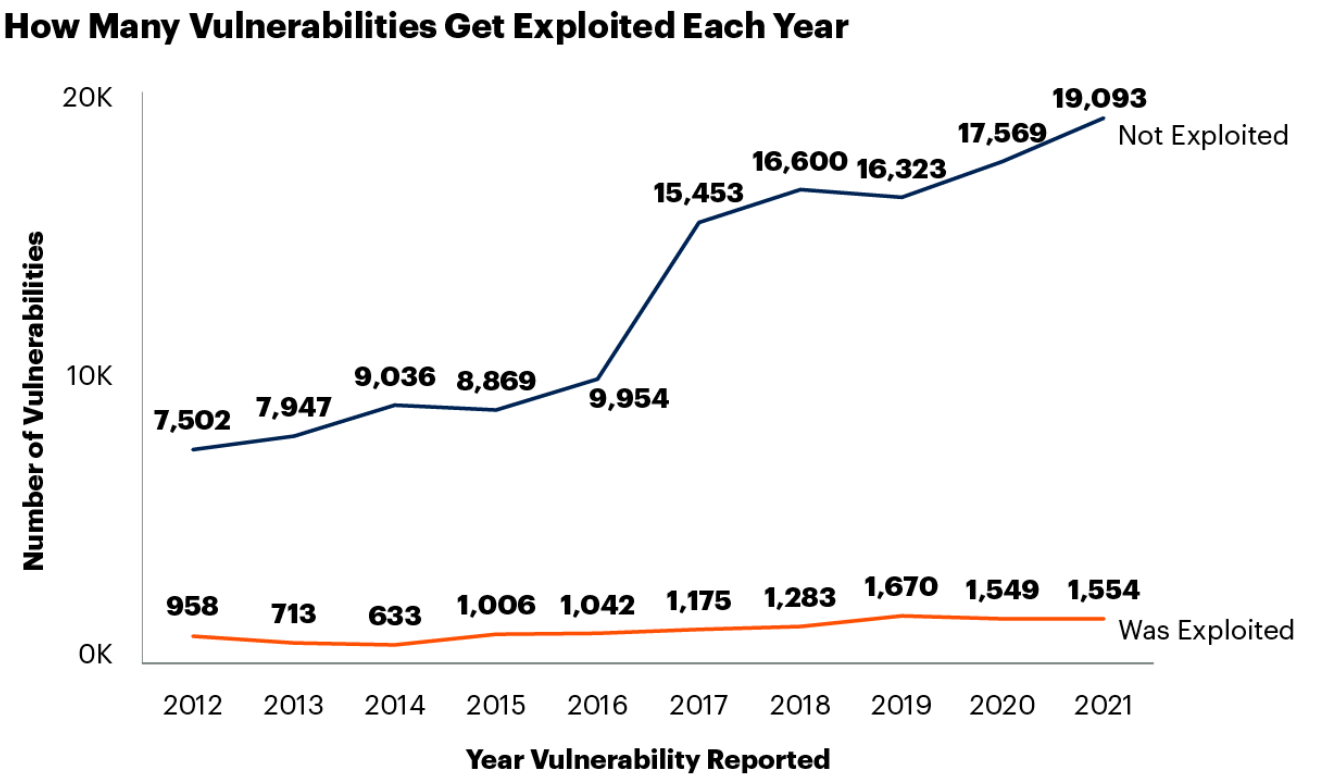
In terms of people and processes, SRM leaders need to input some key nuances, as no one knows the environment better than they do. This entails describing the prioritization to account for items such as:

- Compliance and regulated assets.
- Assets that support critical business processes.

- Assets that are related to critical infrastructure.
- Any exceptions that need to be noted, including other security and compensating controls.

This all adds crucial context necessary in the RBVM program, as it is required for moving to the next phase in the RBVM process. It will involve taking active steps in your environment that are aligned with your organization's threat landscape.

Figure 3: How Many Vulnerabilities Get Exploited Each Year



Source: Gartner (data drawn from the IBM X-Force vulnerability database)
777685_C

Gartner.

Example of technologies enabling prioritization:

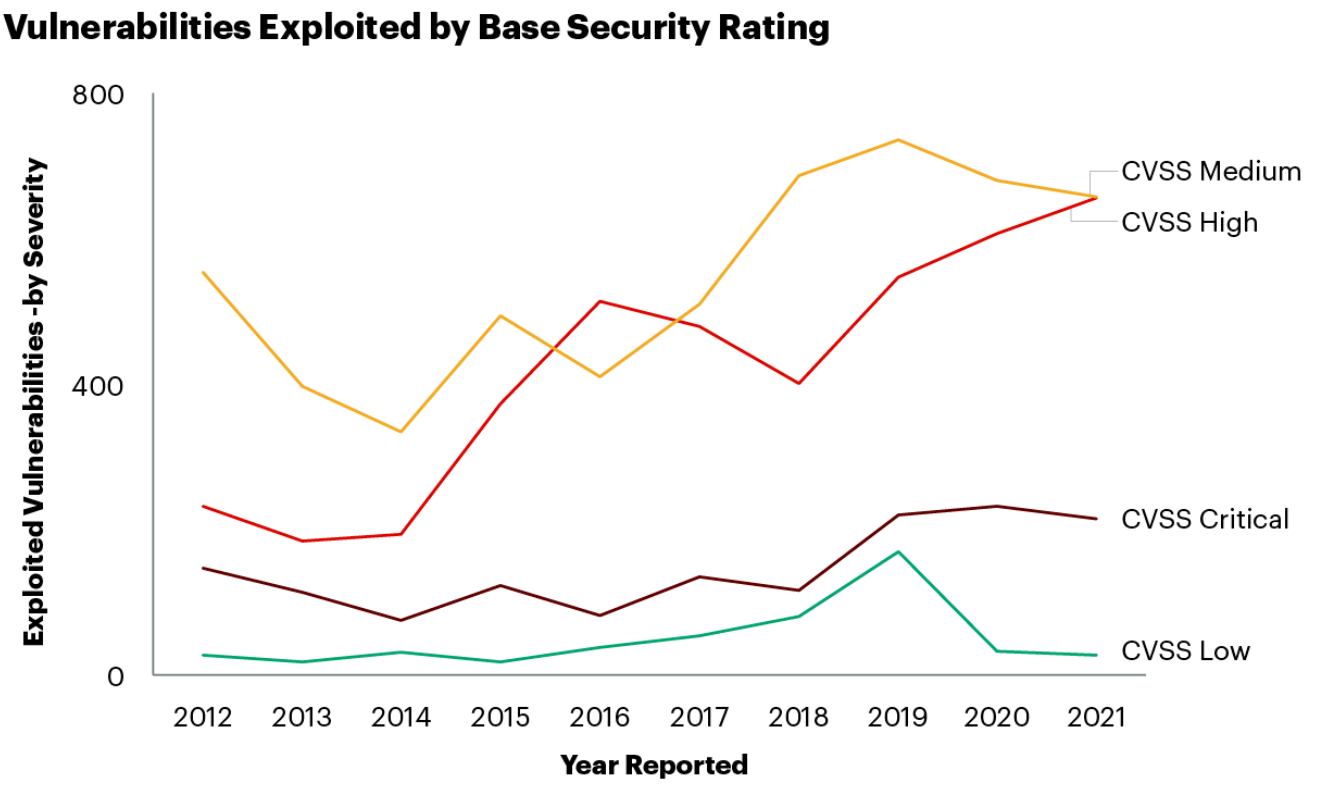
- Vulnerability prioritization technology (VPT). These tools are available in a majority of vulnerability assessment solutions today and from a group of smaller vendors. The principle here is to apply quantitative methods to drive the focus of your VM process so that the most pressing threats are addressed as the highest priority.
- Breach and attack simulation (BAS). While these tools are part of an overall small market, they have a demonstrable capability to proactively highlight how vulnerabilities — and the exploitation of vulnerabilities — will directly affect your environment. Credible risks, like ransomware and phishing, are staple use cases for BAS and security control validation.

- External attack surface management (EASM). These tools focus on the external portion of an organization's footprint to help increase the overall visibility of assets and identify the credible risks they may present.

Many mainstream VA solutions today include some or all of these technologies. In terms of efficiency, however, particularly for smaller organizations, having fewer tools is often a better approach. Therefore, you should prioritize metrics that provide pragmatic results and drive better operational outcomes that align with your digital business's risks (see **Outcome-Driven Metrics for Cybersecurity in the Digital Era**). Also, these metrics balance the need to protect and secure your business with the need to run it effectively.

For all vulnerabilities exploited, the counterintuitive fact is that critical vulnerabilities (ranked as 10 according to CVSS), in aggregate volume, are not the most exploited (see Figure 4). By aggregate, vulnerabilities rated as high and medium are exploited — again, in aggregate — at higher numbers than what critically ranked are. This means threat actors prefer to use "what works" in most cases.

Figure 4: Vulnerabilities Exploited by Base Security Rating



CVSS = common vulnerability scoring system
Source: Gartner (data drawn from the IBM X-Force vulnerability database)
777685_C

Gartner

Compensate

Ideally, patching would be the perfect method to prevent vulnerabilities from being exploited and remains a belief that patching is able to solve this issue. It is not. In reality, preventing vulnerabilities from being exploited is not always possible or even feasible with just patching for most end user organizations. Therefore, SRM leaders must shift the dogmatic belief that everything can be patched at a faster pace than threat actors can operate.

For example, there are entirely valid reasons patching isn't able to be mandated the way it is in traditional VM programs:

- Patching breaks things all the time. It is a regular occurrence to see system outages due to patching, even in mature environments with good IT operations and patching tooling. In essence, this is also a credible risk to an organization regarding meeting availability metrics. It should be no surprise that IT operations have a more circumspect view of the risks of patching without rigorous verification processes.
- Patches might not be available for all vulnerabilities (see Figure 5).
- Due to complexities arising from the cohabitation of often dozens of different pieces of software on systems, patches can't be applied without affecting other applications or critical business functions that hosts support.
- In highly-regulated systems, patches can sometimes have mandates, meaning they are unable to be applied as rapidly as threat actors are operating.

From a security perspective, patching is commonly treated as a monolithic process where all patching has a level of uniformity. While security teams are not — and likely never will be — the asset owners with the final say in patching and IT operations, SRM leaders should:

- Look for patches that can be applied with a high degree of reliability and security benefits. For example, software like web browsers and other end-user apps — such as office suites and business intelligence (BI) tooling — have a record of being attacked regularly and concurrently. Therefore, SRM leaders should make these pieces of software more fully automated.
- Search for patches that require testing and are patched on a regular cadence. Most vulnerabilities do not go to get exploited in the wild. Therefore, patches of a regular cadence can ensure that compensating controls are in place for IT operations (often measured in only 2-4 weeks).

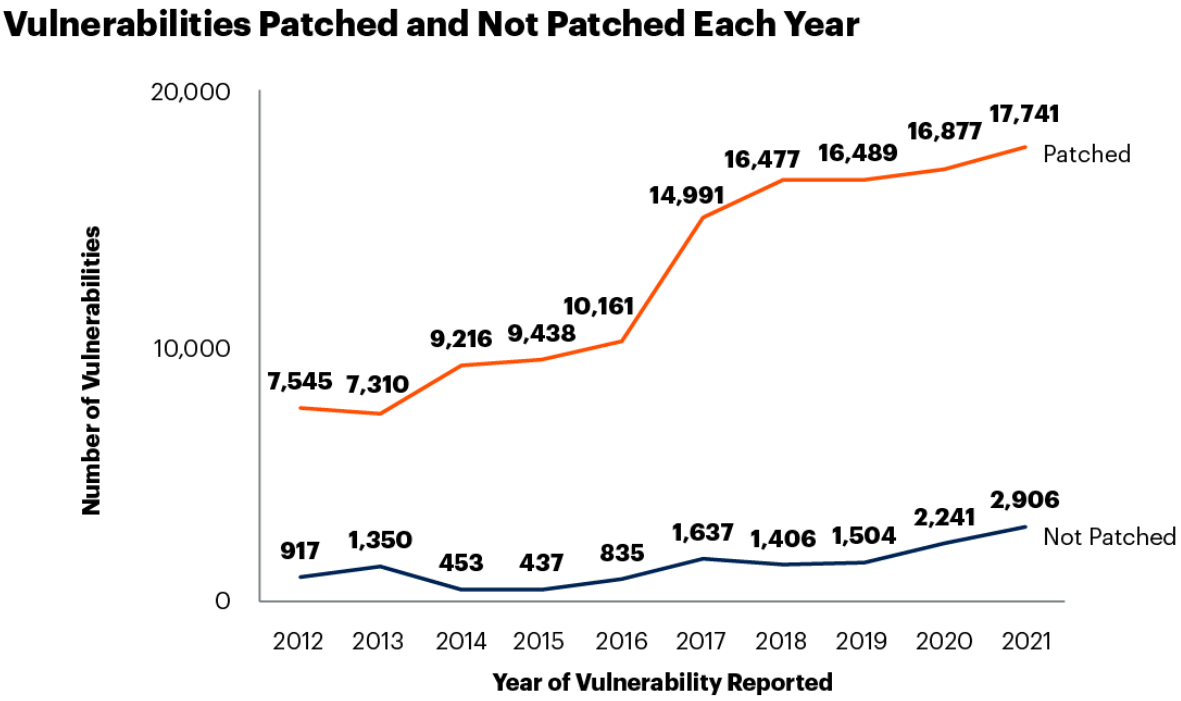
Thus, a range of options that don't rely just on patches being deployed must be considered. A "plan b" is required.

Technologies like intrusion prevention system (IPS), intrusion detection system (IDS), network detection and response (NDR), Web Application and API Protection (WAAP), RASP, application control, network segmentation and strong authentication are excellent and mature examples of compensating controls. They directly help deal with detecting and preventing the exploitation of

vulnerabilities in an environment. Other tools can help compensate for other realities to use along with patching. These include:

- Enhanced monitoring and analytics — including user and entity behavior analytics (UEBA) and identity threat detection and response (ITDR).
- Privileged access management (PAM). It helps compensate for other realities in your environment to use alongside patching. For more information, see **Guidance for Privileged Access Management** and **Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response**.

Figure 5: Vulnerabilities Patched and Not Patched Each Year



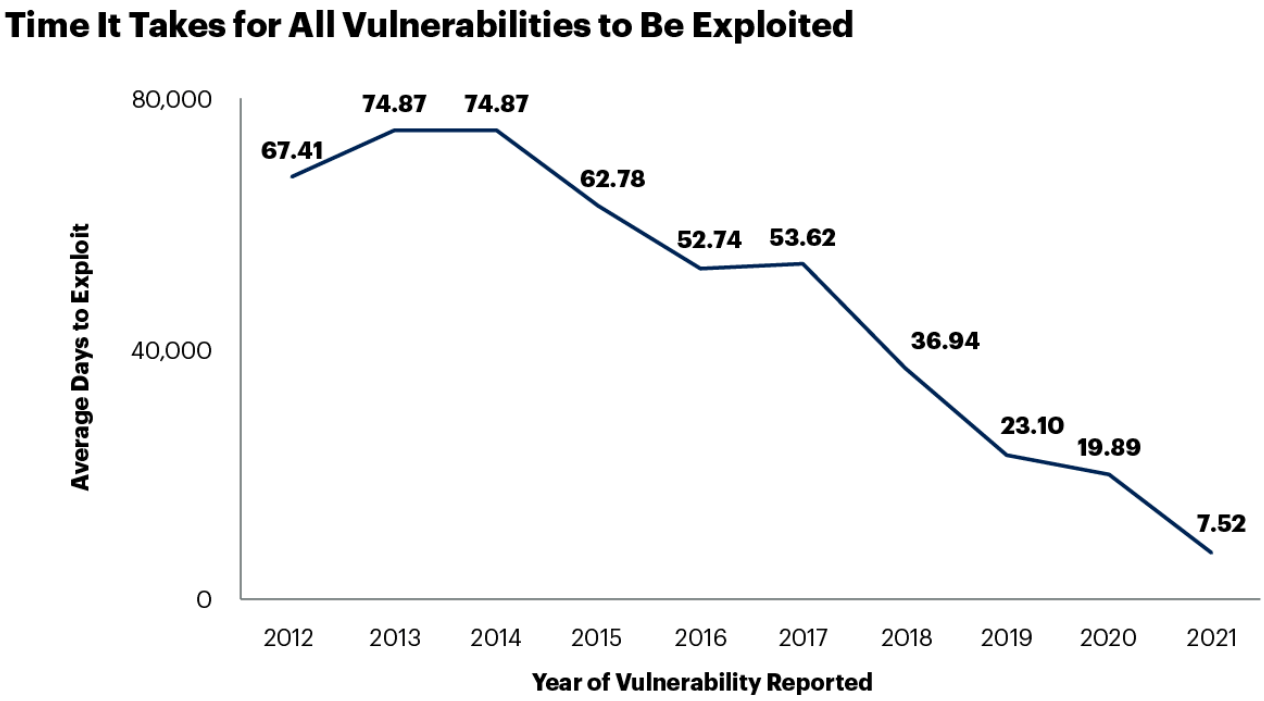
Source: Gartner (data drawn from the IBM X-Force vulnerability database)
777685_C

Gartner.

One key issue for building an RBVM program is understanding the exploitation time frames of threat actors. Figure 6 shows, on average, regardless of severity and including zero-day vulnerabilities, how long it takes for vulnerabilities to be exploited in the wild. In recent years, the time frame of an attack steadily dropped to be measured in days. This makes a compelling use case for SRM leaders to have a wide range of options to help mitigate the exploitation of vulnerabilities and not rely only on patching.

Also, the static, inflexible method of taking 14 to 30 days to deal with critical vulnerabilities (CVSS 9-10) and longer for other ratings is, in fact, systematically benefiting threat actors. With the average now at approximately seven days, many VM programs instituting hard-time limits fly in the face of the evidence.

Figure 6: Time It Takes for All Exploited Vulnerabilities to Be Exploited



Source: Gartner (data drawn from the IBM X-Force vulnerability database)
777685_C

Gartner

A significant part of the operational friction with vulnerability management lies in understanding how many subcomponent owners and roles of this process exist (see Figure 7). This is why the "compensate" phase of RBVM remains an operational difficulty to this day.

Figure 7: Sample RACI Chart for Vulnerability Management

Example Vulnerability Management Roles and Responsibilities

R Responsible A Accountable C Consulted I Informed

Activity	Vulnerability Management	Security Operations	IT Operations	Security/Risk Management	Business
Define VM policy and processes	R	I	C	A	I
Deploy and operate VA tool	A	R	C	I	N/A
Remediate vulnerabilities according to VM policies	C	I	R	I	I
Approve Exceptions when required	C	I	I	R	R A
Apply mitigation measures when required	C	I	A R	I	I
Oversee performance and results of VM program	R	I	C	A	I

May be the same organization initially based on organization size

Source: Gartner
773547_C

Gartner

For example, security teams generally own the scanning process and ideally perform prioritization. However, the long list of various asset owners who often have competing SLAs have the final say in how patching, configuration and hardening are applied to the organization's assets. Examples of asset owners include the server, desktop, network, cloud, OT and IoT teams.

In cybersecurity, there are various levels of governance, from chief information security officers (CISOs) and risk managers to operations staff. All have a role in vulnerability management. However, the security teams can underestimate the complexity and risk posed by performing patching.

One solution is to help by looking for where you automate some patches. This can be done by using the evidence in your IT service management (ITSM) tool. ITSM is a system that records patching activities and retrieves data to see if organizations have any software that is regularly attacked or has a high degree of reliability in being patched.

For instance, web browsers and office software tend to regularly see active exploitation and are currently reliably patched by many organizations. Hence, organizations should determine which software gets attacked relatively frequently and which has a good record of being able to be patched in your organization.[3]

In recent years, there has been some progress in recognizing that VM is not just a compliance function but also a credible threat-prevention capability when the evidence is taken into account.

Accordingly, VA vendors are now consuming many of the historically-separate technology elements due to consolidation and acquisitions, thus delivering VA across infrastructure, web, OT and IoT. Also, VA vendors are beginning to cover cloud services, vulnerability prioritization as well as consuming technology from more niche markets, like EASM.

Evidence

Chart data in this research was sourced from the IBM X-Force vulnerability database with special credit to Scott Moore and the XFDB team.

[1] **Apache Log4j Vulnerability Guidance**, Cybersecurity & Infrastructure Agency.

[2] **Binding Operational Directive 23-01**, Cybersecurity & Infrastructure Agency.

[3] **Software Updates Strategies: a Quantitative Evaluation against Advanced Persistent Threats,** arXiv.

Acronym Key and Glossary Terms

RBVM	risk-based vulnerability management
PAM	privileged access management
NDR	network detection and response
IPS	intrusion prevention system
DRPS	digital risk protection services
EASM	external attack surface management
WAF	web application firewall

Notes 1: Remediation Work & CVSS Scoring

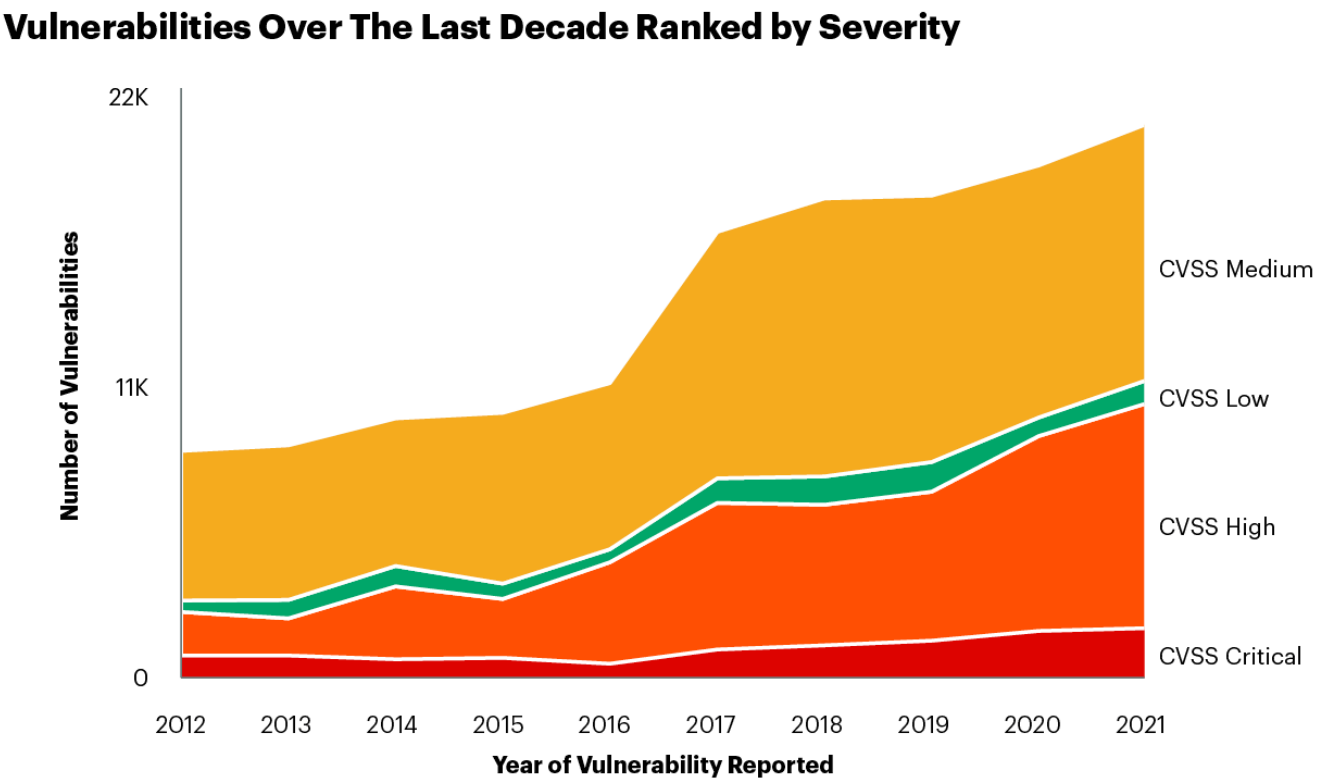
The Cybersecurity & Infrastructure Agency (CISA) published a binding operational directive in 2021 regarding reducing the risk of known exploited vulnerabilities (KEVs). For more information, see **Binding Operational Directive 22-01**. CISA's KEVs are publicly accessible threat intelligence that can help prioritize vulnerabilities. Accordingly, the directive is intended to help agencies prioritize their remediation work and emphasizes that KEVs should be the top priority for remediation.

The directive also guides which vulnerabilities are more important to remediate — critical and high or KEVs. The study reveals that organizations should focus on active threats instead of addressing thousands of vulnerabilities that may never occur in real-world attacks.

Ultimately, CISA recognizes CVSS scoring as part of an organization's vulnerability management efforts, especially with machine-to-machine (M2M) communication and large-scale automation. This directive serves as guidance and does not release organizations from compliance obligations, including resolving other vulnerabilities.

Figure 8 shows vulnerabilities ranked by severity over the last decade using the CVSS scoring.

Figure 8: Vulnerabilities Over The Last Decade Ranked By Severity



CVSS = common vulnerability scoring system
Source: Gartner (data drawn from the IBM X-Force vulnerability database)
777685_C