The 4 Stages of Modern Vulnerability Management

KENNA Security

The 4 Stages of Modern Vulnerability Management

When it comes to vulnerability management, there's a line being drawn in the sand. On one side are organizations still relying on educated guesswork and "good enough" tools to determine their top threats; on the other, those that have embraced data-driven risk prioritization. Security and IT professionals already well know what the first scenario entails.

But the second is new to many. And for them, we've prepared this exploration into how an enterprise can mature its vulnerability management efforts to drive down costs, optimize use of their finite resources, and efficiently align Security, IT, and DevOps teams around the one thing everyone cares about: risk.

Traditional vs. modern

Traditional vulnerability management (VM) is a stagnant state. Traditional VM is characterized by prioritization based on the Common Vulnerability Scoring System (CVSS), spreadsheets, and tension between Security and IT teams. Because you achieve little to no movement toward real risk reduction, it can often feel like you're on a hamster wheel that spins and spins, making it nearly impossible to dismount. Frequently, decisions are made out of context to your own company's risk profile, industry, and applications. And truth be told, you're most assuredly spending time and money patching vulnerabilities you don't need to. That's because just 4 percent of vulnerabilities actually pose a threat to any given organization.

Because **just 4% of vulnerabilities** actually pose a threat to any given organization, you're most assuredly spending time and money patching vulnerabilities you don't need to.

Prioritization to Prediction, Volume 3

Mature modern vulnerability management requires shifting your performance indicators, aligning incentives, and restructuring the relationship between Security and IT operations.

On the opposite end of the spectrum sits modern vulnerability management. Almost the exact inverse of traditional approaches, modern vulnerability management is a journey that gains momentum as you progress, powered by data and frictionless teamwork that results in meaningful risk reduction. How? The foundation of modern vulnerability management is a focus on the highest-risk vulnerabilities by taking into account a wide spectrum of internal and external threat and vulnerability data. This data is fed into predictive models, allowing you insight into not only what has been exploited but also the likelihood of future vulnerability exploitations—and how that likelihood might increase the risk to your infrastructure, networks, or applications. Modern vulnerability management is designed to give you the control and visibility required to to gain ground in your efforts to lower your risk profile.

Where are you on this journey?

We've discovered that the hallmarks of a fully mature vulnerability management program are somewhat different from what we imagined. When we started, we thought that big companies would just use our data and our tools, lower their risk, and live happily ever after. In other words, what we thought was the end of the story was really the training montage. Over the years, however, we saw something different—something more meaningful—happen inside our customers' organizations. And that meant we had to work with them to shift performance indicators, align incentives, and help restructure the relationship between Security and IT operations.

But it doesn't happen overnight,

and anyone who tries to convince you that their out-of-the-box solution is instantly transformative needs to be given some serious side-eye. Like we said, it's a journey.

Four stages of progress

We at Kenna Security have defined four stages of the modern vulnerability management journey, outlining the key differentiators of each and the necessary catalysts that help organizations progress to the next stage.

To determine where you're going, you have to understand where you are. Take a look at these four stages, and identify which one you're in to help define your path forward to lower your true risk and become a well-oiled, threat-remediating machine.

STAGE 1: CHAOS

1. Stage 1 of Modern Vulnerability Management: Table Stakes (aka Chaos)

The key characteristics

Chaos. The first stage of vulnerability management is, for the most part, toddler time. It's chaos. The organization faces millions of vulnerabilities, and there's a widespread (though erroneous) belief that any one of them could be the entry point for a group of hackers that can cause massive damage. Despite the overwhelming size of the problem, most organizations have, on average, the capacity to patch just one out of every 10 vulnerabilities. At this stage, vulnerability prioritization is driven by table stakes tools and scores assigned via the Common Vulnerability Scoring System (CVSS), in addition to scanner platforms. When your scanners detect a vulnerability, it gets added to a spreadsheet. To estimate the risk that the vulnerability poses, you look to CVSS. This amounts to table stakes for vulnerability management today.

Internal friction. What follows isn't pretty. IT operations–usually tasked with patching vulnerabilities–and Security–whose job it is to assess the severity of vulnerabilities–spend a lot of time fighting over which vulnerabilities to patch and how much time IT should spend on these issues. In some organizations, there's an additional layer of conflict as varying stakeholders—those in finance, sales, or operations—begin to argue that their systems require more protection than others. Regulatory issues and compliance with industry standards drive decision-making as well, and not for the better. Too often, companies end up patching vulnerabilities that aren't dangerous at all.

> **Most organizations have the capacity to fix just one out of every 10 vulnerabilities.**
>
> Source: Prioritization to Prediction, Volume 3

Pushing a boulder up a hill. Companies in this stage often believe vulnerability management to be a task similar to that of Sisyphus from Greek mythology; a difficult, stressful, and painful exercise that is doomed to failure. Just as Sysphus would never complete his task of rolling the boulder up the mountain, organizations cannot eliminate all vulnerabilities and those chartered with doing so end up suffering away with no hope of victory or respite. Pretty brutal, right?

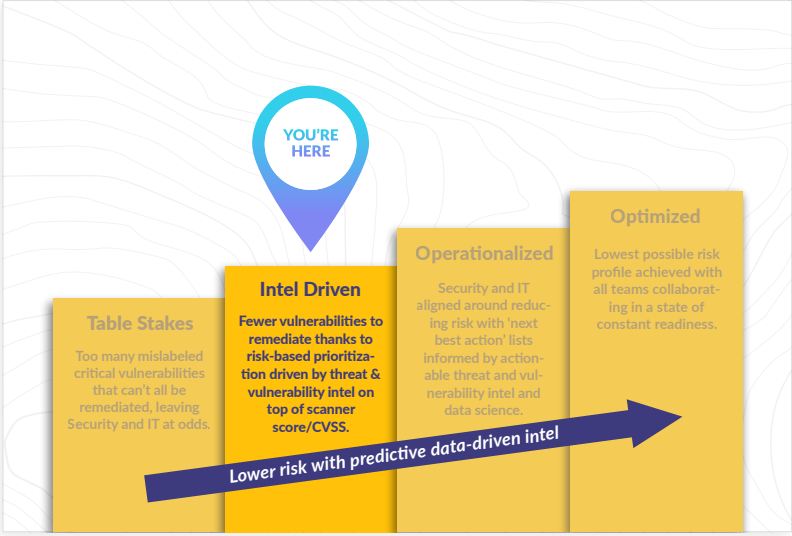
> **33% of all organizations are falling behind in their efforts to knock out high-risk vulnerabilities.**
>
> Source: Prioritization to Prediction, Volume 3

Catalysts to Progress

Take a look at your data. It's safe to say that most modern enterprises live and breathe data. But not all data is created equal. Growing out of this stage means turning to a different set of data. Remember that while most organizations only have capacity to fix just one out of every 10 vulnerabilities, even fewer—just four in 100—pose a viable threat to that specific organization.

In other words, most organizations have more than enough capacity. What they don't have is data that tells them which vulnerabilities are actually dangerous (in other words, they lack the intel and the insight to know where to apply their capacity). And so begins the next stage of the modern vulnerability management journey.

STAGE 2: PUTTING THE PIECES IN PLACE



2. Stage 2 of Modern Vulnerability Management: Intel-Driven, or Putting the Pieces in Place

The key characteristics

CVSS is still a source of truth—just not the only source. As we mentioned above, CVSS is a popular source for understanding which vulnerabilities should be addressed first. For years CVSS was as good as it got. But it's just not good enough anymore. What CVSS approximates is the ease and impact of exploit. It does not measure the risk that a vulnerability will be exploited. In fact, many vulnerabilities with high CVSS scores pose little to no risk of exploitation or weaponization, compounding the challenge of wasted cycles and resources. You need more information, and a big part of this second stage of maturity involves incorporating that information.

Many vulnerabilities with high CVSS scores pose little to no risk of exploitation or weaponization.

Inefficiency. Ideally, you're spending the right amount of resources on the threats posing the highest risk to your business. Anything less than that equates to lost time, money, and cycles that could have been spent elsewhere. It also creates a breeding ground or frustration amongst team members who are knowingly dedicating their efforts towards remediation that will have little to no effect on the organization's risk. And for those efforts that are impactful, a lack of clear, cohesive reporting keeps teams from celebrating their wins.

Lack of context. CVSS isn't the only method that lacks context. Many vulnerability prioritization platforms tout the ability to adequately sift out the highest risks, yet their data sources are lacking in crucial context, including the specifics of an organization, its applications, and its risk tolerance. So recommendations they serve up are incomplete or, worse, incorrect.

Catalysts to Progress

Pull in the right data. The quality of a vulnerability management program is directly related to its ability to accurately quantify whether a vulnerability has been weaponized in the past, or is exploitable in the future. When a hacker deploys an attack, or when a vulnerability is exploited by Security researchers interested in creating a proof of concept, it creates a record.

Rather than relying on the theoretical risk of a vulnerability, data scientists can examine how hackers have operated in the past to detect well-worn behavioral patterns. Kenna Security intakes data from a sprawling list of sources, including scanners, penetration testing results, bug bounty programs, databases of vulnerabilities and exploit intelligence, and multiple threat intelligence feeds processed and analyzed to deliver actionable insight.

Evaluate and score vulnerabilities. We've learned that certain vulnerabilities are more likely to be exploited than others. Certain variables, like which vendor made the application a vulnerability affects, or whether a proof-of-concept exploit has been published, tend to be more indicative of future weaponization than other variables. Conversely, a vulnerability that can lead to memory corruption in an asset is less likely to be weaponized.

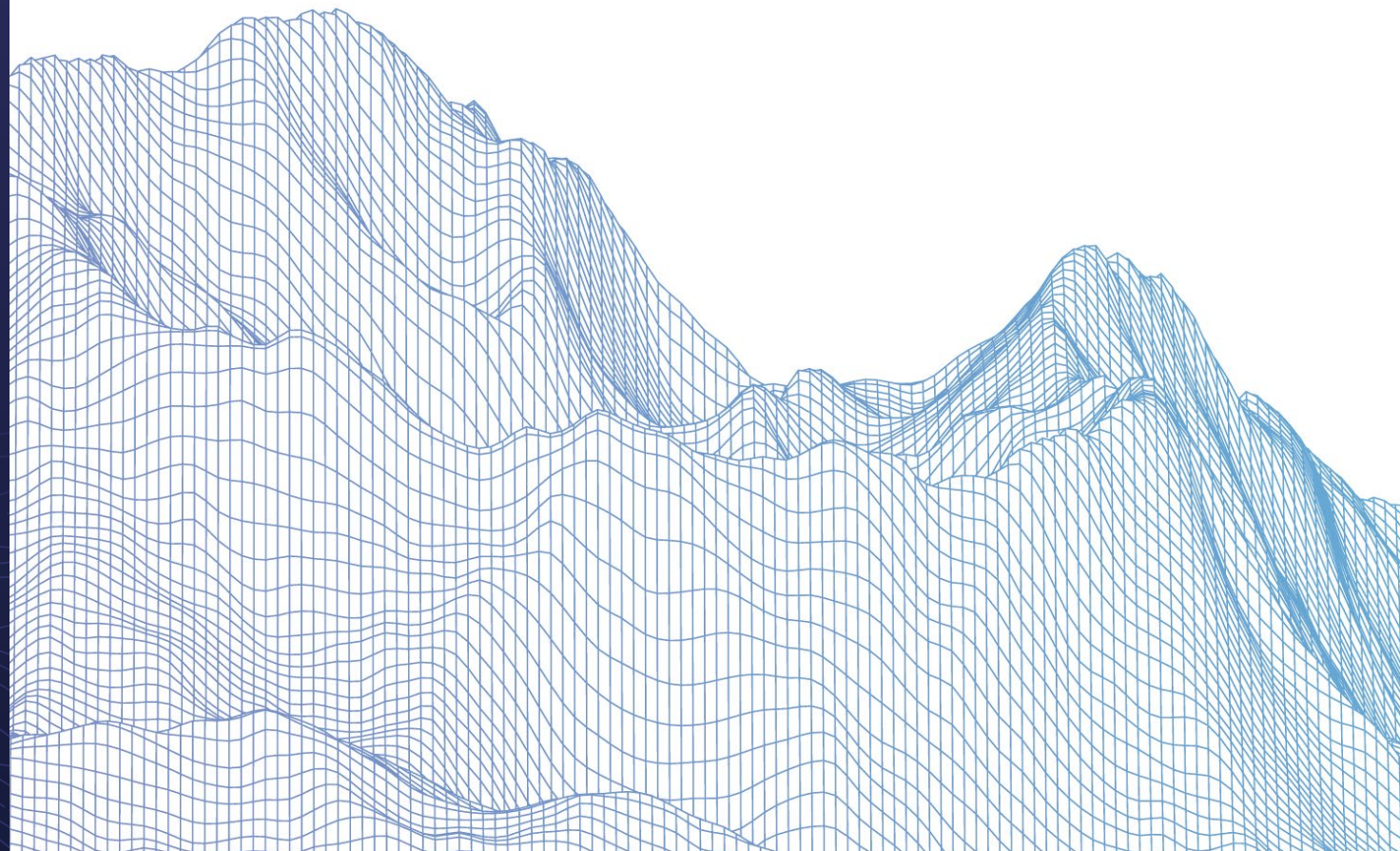
Gartner has called out the critical need to assess assets, for configuration issues and vulnerabilities, and to be able to prioritize what you do with that assessment, based on the risk to your organization.

Gartner, Inc: Market Guide for Vulnerability Assessment, Craig Lawson, Mitchell Schneider, Prateek Bhajanka, Dale Gardner, Nov. 20, 2019

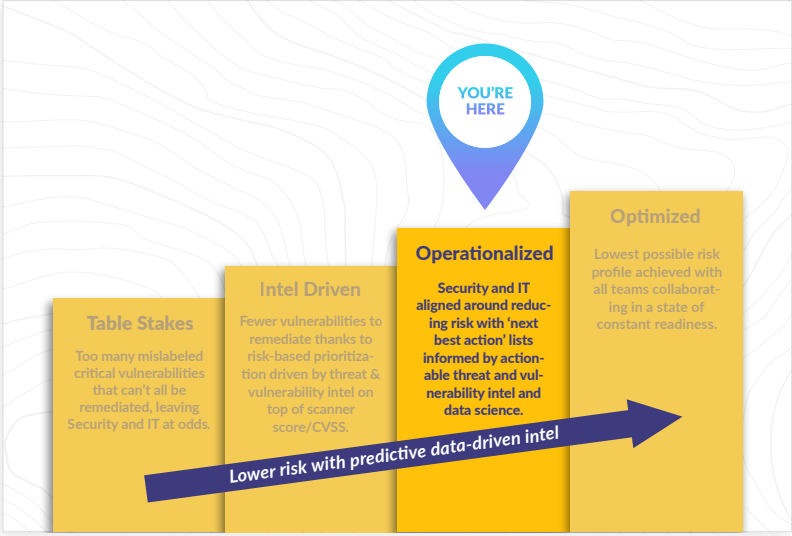
All of these factors can be harnessed to quantify the risk any individual vulnerability poses to an organization. In aggregate, these risks can be used to create an overall risk score for an entire enterprise or for segments of it. And the name of the game is lowering that risk score. This is made even more doable because Security and IT teams are working from the same source of data-backed truth, with justification and context baked in.

Embrace risk-based vulnerability management. The process of evaluating a risk based on this granular set of internal and external data combined with predictive modeling is known as risk-based vulnerability management, or RBVM. Our research shows that with the right data, RBVM can drive down risk more thoroughly than other rubrics. For example, some enterprises have protocols under which vulnerabilities with CVSS scores above 7 are patched. Data science suggests, however, that many vulnerabilities above that threshold pose little risk of exploitation. Meanwhile, some vulnerabilities that fall below that threshold pose even greater risk to the organization.

RBVM is the insight that enables truly modern vulnerability management. But to get the benefits of RBVM, organizations need a tool that can operationalize these insights.



STAGE 3: ALIGNMENT AND AUTO-PILOT



3. Stage 3 of Modern Vulnerability Management: Operationalizing Alignment and Engaging Auto-Pilot

The key characteristics

Risk prioritization is in full swing. Gone are the days of CVSS-driven spreadsheets and murky justifications for vulnerability patching. Teams operating in this stage have kicked their RBVM into high gear and have their remediation game plan already mapped out for them thanks to threat and vulnerability intelligence and predictive data science. And Security and IT are operating on the shared goal of continuously driving down that risk score.

Forging a common language of risk. One of the odd things about risk is that it doesn't mean the same thing to all people. In enterprise cybersecurity, what some people view as risky, others see as harmless. When there is no way to talk rationally about risk, just about everything seems risky–and thus, there are demands to patch far more than the organization has capacity for. Companies in this stage are often attempting to forge a common definition and language around risk to align teams and stakeholders and determine priorities. If you have agreed-upon language and a tool that identifies and quantifies risk, you can identify your riskiest vulnerabilities, prioritize them, and create communal buy-in to the game plan.

Modern vulnerability management goes even further, because it realigns the organization's overall approach to risk by evaluating and measuring risk across the full IT stack. Modern vulnerability management accounts for every vulnerability, on every asset, across every segment of the network, and uses data science to distill that information through a single, easy-to-understand lens.

To reconcile IT risk (ensuring high availability of applications and services, while reliably meeting SLAs) and Security risk (working to mitigate the chance of breaches), it helps to focus on the same thing.

How Can You Reconcile the Different Definitions of Risk?

+ **IT**
  No downtime, Meet SLAs

+ **SECURITY**
  Zero breaches

→ Focus on **high-risk** vulnerabilities first

Reducing conflict. When an organization starts using the lingua franca of risk-based vulnerability management, the number of vulnerabilities that IT needs to patch declines dramatically (remember, only 4% of vulnerabilities pose an actual threat).

And that reduces conflict. How? There's very little to argue about if data science is clear and transparent. With a holistic view of risk, everyone knows what the next best action is. IT operations teams, for example, know which vulnerabilities they need to prioritize and why they should be the priority — they are looking at the same data the Security team is looking at. Many Kenna Security customers adopt a self-service approach for IT, with Security teams providing oversight and helping to handle exceptions.

Catalysts to Progress

Make time for higher value initiatives. Modern vulnerability management isn't just about making life easier for the Security team. It's also about reducing the amount of time that IT spends patching–and that means more time to devote to other, higher value initiatives. These are features of modern vulnerability management, but they aren't the overarching theme.

By aligning the stakeholders around a common ground truth, it is possible to know exactly what the organization's risk posture is, and it's easier to communicate that with board members, non-technical executives, compliance officers and even regulators.

The head of cybersecurity of a major financial institution recently told me he hadn't logged into Kenna.VM in months. At first, I was a little worried, but then he said their IT teams were logging in and proactively patching their own systems on a day-to-day basis. He wasn't logging in because he just didn't need to.

Jason Rolleston, Kenna Security Chief Product Officer

STAGE 4: REMEDIATION VELOCITY

4. Stage 4 of Modern Vulnerability Management: Optimizing Remediation

Let's look at the journey so far.

STAGE 1: Table stakes (aka chaos). We've discussed a state of chaos that all organizations face at the beginning of the vulnerability management journey. Most organizations are trying to tackle an impossible number of vulnerabilities without the tools or the data to meaningfully reduce risk. They use CVSS as a proxy for danger, when that score wasn't built for that. And there are widespread arguments between IT operations and Security over which issues to patch first, and how much time to devote to patching.

STAGE 2: Intel-driven, or putting the pieces in place. Organizations in this stage of maturity are experiencing the telltale signs of inefficiency and uninformed decision making, thanks to shortcomings of the data at their disposal. They will begin to recognize they need not just data, but the right data in place, and they'll begin to lay the groundwork for establishing a risk-based vulnerability management program.

STAGE 3: Operationalizing alignment and engaging auto-pilot. In the third state of vulnerability management maturity, organizations have begun using a solution that harnesses machine learning and big data analytics to identify the vulnerabilities that pose the most significant risk to their organization. At this point, these teams are not only prioritizing the riskiest vulnerabilities, but identifying those that are likely to become dangerous in the future. Even more, IT and Security are getting along, because there's no real argument over which mitigation measures they need to take. Alignment is operationalized and the workflow goes on auto-pilot.

The Key Characteristics

Remediation velocity. In the fourth and final stage, managers begin to re-align their thinking away from risk scores and toward optimizing their VM operation via a new idea: remediation velocity.

Picture this: new vulnerabilities pop up every day. Most are harmless. Occasionally, something really dangerous is released into the wild. It doesn't happen often, but we do see it. Many recent examples stem from the release of vulnerabilities that are easily exploitable or already have exploits available.

The best cybersecurity teams in the world are still only playing defense. They can't control what malicious actors do. And so, every once in a while, the scores jump. That's the natural ebb and flow of a highly mature vulnerability management program. And when they do, these teams rely on their optimized and streamlined systems to help them take action in a targeted and timely fashion.

Self-service teams. This fourth stage of a mature vulnerability management program is also marked by a key characteristic: in most cases, IT operations can serve themselves. Security teams focus on reporting, oversight of mitigation efforts, and handling exceptions. Incentives also shift to include meeting SLAs and lowering overall risk scores.

Alignment across AppDev and AppSec. Tools and critical threat information is made readily available and accessible for both application security and

application development teams. In this stage, teams can continuously, effectively and proactively triage and remediate the application findings and vulnerabilities that pose the most risk.

Risk-based SLAs. Speaking of SLAs, you can't control what threat actors do, but you can control how your organization reacts to these situations. Mature cybersecurity teams know this. And that's why they integrate risk-based thinking into the creation of their SLAs. Risk-based SLAs enable organizations to use data and their own appetite for risk to establish an appropriate speed of response to new, high-risk vulnerabilities.

These appetites for risk are divided into three categories:

- **Companies that are content to be as fast as their peers.**
- **Companies that want to be leaders in their sector.**
- **Companies that want their remediation strategies to exceed the speed of threat actors' ability to weaponize vulnerabilities.**

Our research backs up the idea that SLAs are an important contributor to maturity and effectiveness. Programs that set firm remediation deadlines for high-risk vulnerabilities tend to patch them faster.

2.8 million vulnerabilities

SHRUNK TO LESS THAN 200,000 — ALL IN UNDER 60 DAYS FOR ONE U.S. FINANCIAL SERVICES FIRM.

In Your Future: Success–and Sanity

Mature vulnerability management programs are stable and enduring. Because of this, the methods and metrics for evaluating the programs shift. But whatever stage your program is in, success–and sanity–are possible.

It may seem as though highly mature vulnerability management programs are reserved for companies with endless resources and robust Security and IT teams with a collaborative and supportive culture. This just isn't true. Everyone begins somewhere and with the right mindset and key pieces in place, even the scrappiest of teams can begin to excel at lowering their risk profile.

What's undeniable is that every day, the need to improve, operationalize and optimize your VM program is becoming less of a choice and more of a business imperative. And "good enough" solutions, with their lack of data science-driven prioritization and risk assessment, are no longer anything close to good enough. Time is of the essence, and the stakes are high.

Take the first steps toward mature vulnerability management.

Let's move you forward.

6 steps to going risk-based.
How to Implement a Risk-Based Vulnerability Management Approach

What the next level of VM looks like.
Unlock The Next Level of VM: Modern Vulnerability Management

Find out what your risk remediation efficiency is—and what it could be.
Risk Efficiency Calculator

For even more information on modern vulnerability management solutions, or to see modern vulnerability management in action, visit

www.kennasecurity.com

KENNA Security