The ROI of Effective Vulnerability Management

3 Ways Risk-Based Vulnerability Management Saves Time, Money and Resources

KENNA Security

Introduction

The 'do more with less' challenge

As businesses grapple with disruption and uncertainty, most Security and IT leaders are being asked to stretch budgets as far as they will go. "Do more with less" is hitting home now more than ever.

For those of us in the vulnerability management (VM) space, ensuring money, resources, and time are strategically spent is difficult, but it's also imperative. Resources may be dwindling, but the vulnerability problem sure isn't. Between 2016 and 2019, the number of Common Vulnerabilities and Exploits (CVEs) published in the National Vulnerability Database (NVD) tripled compared to the preceding six years (see Figure 1).

Vulnerability management can be a notorious resource drain for many organizations who struggle to regularly patch thousands or

LEARN THE 3 KEYS TO MAXIMIZING ROI

1 Focus on risk

2 Align around risk

3 Investigate, remediate, report

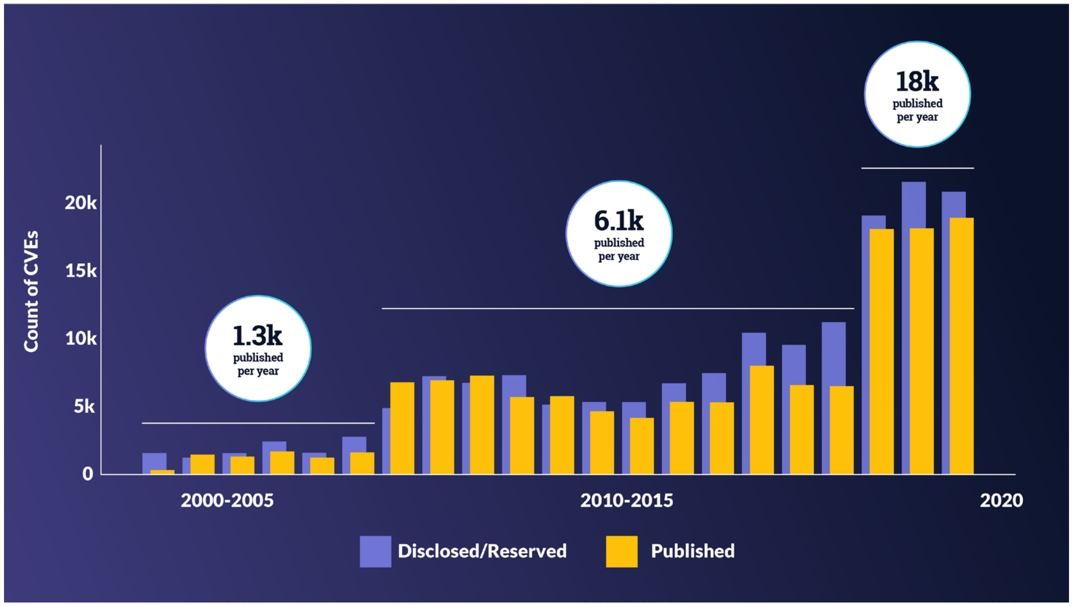


Figure 1: Number of CVEs added to NVE from 1999 to 2019

Before you know it, you’re stuck in a “spray and pray” routine that yields a critical problem: You’re actually doing little to reduce risk, while at the same time you’re expending a ton of resources.

even millions of vulnerabilities. Even in the best of circumstances, a mandate to “patch everything” is likely to produce a poor return on your investment in time and technology. But solving the vulnerability management challenge doesn’t have to break your budget or require more staff.

As with most daunting to-do lists, efficient and cost-effective VM is all about prioritization.

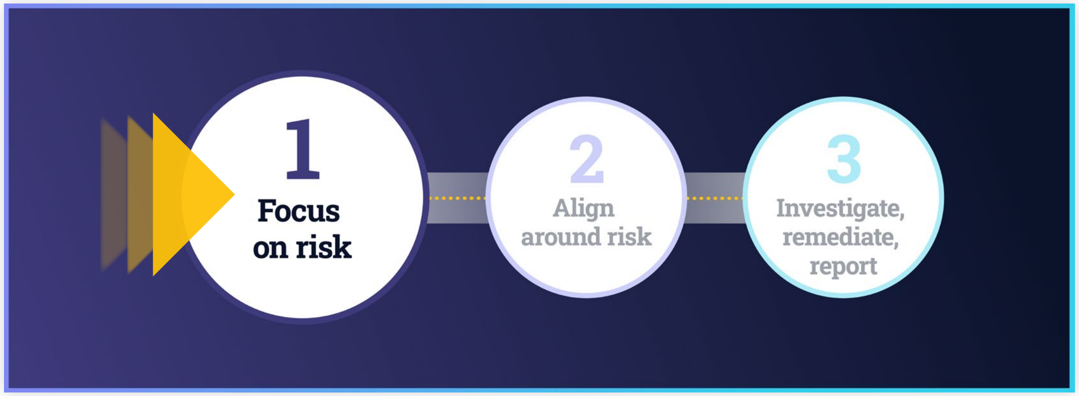
Not everything is a risk

It’s easy to point to your infrastructure and application vulnerabilities and say, “Everything is at risk.” But if everything is at risk, then everything needs to be patched. Suddenly you’re running in circles trying to figure out how to patch an endless list of vulnerabilities. And before you know it, you’re stuck in a “spray and pray” routine that yields a critical problem: You’re actually doing little to reduce risk, while at the same time you’re expending a ton of resources.

There’s a better way. Read on to learn more about the significant downsides of the “everything is at risk” mentality. And discover the measurable cost benefits that can come from embracing a modern, risk-based vulnerability management approach grounded in real-world threat intelligence and data science.

Three Ways to Realize ROI

1. Save resources by focusing on risk



Only around 2% of vulnerabilities are actively exploited in the wild.

Source: Kenna Security, Prioritization to Prediction, Vol. 1

Focus on the vulnerabilities that matter most

The truth is that it simply doesn't make sense to treat every vulnerability equally. Some vulnerabilities are more critical and need immediate attention; some are less likely to cause an issue and can be deprioritized. In fact, only around 2% of vulnerabilities are actively exploited in the wild, according to the flagship installment of the Prioritization to Prediction research series spearheaded by the Cyentia Institute and Kenna Security. So if the other 98% of vulnerabilities pose little to no threat to your business, then the traditional, "everything is at risk" approach to VM is clearly inefficient and unnecessarily costly.

With a risk-based approach to vulnerability management, you can focus resources on patching a smaller number of vulnerabilities that pose a real risk to your organization.

Data-driven prioritization is a must

But it's not just prioritizing vulnerabilities that will make a difference—you have to be confident that you're identifying that real risk accurately. It's not a place for guesswork. This is where threat intelligence driven by data science plays a critical role. Too many organizations rely on very basic vulnerability information—often just the Common Vulnerability Scoring System (CVSS), or a vendor that essentially repurposes CVSS data without adding much additional intelligence. Compared to remediating based on CVSS 7+, a modern vulnerability management model delivers twice the efficiency, with half the effort, according to Prioritization to Prediction, Vol. 1.

Real savings from modern vulnerability management

It's worth noting, too, that some organizations understand that CVSS is not a sufficient solution. So they mount a DIY project in the hope that they can

FOR ONE U.S. FINANCIAL SERVICES FIRM,

2.8 million vulnerabilities

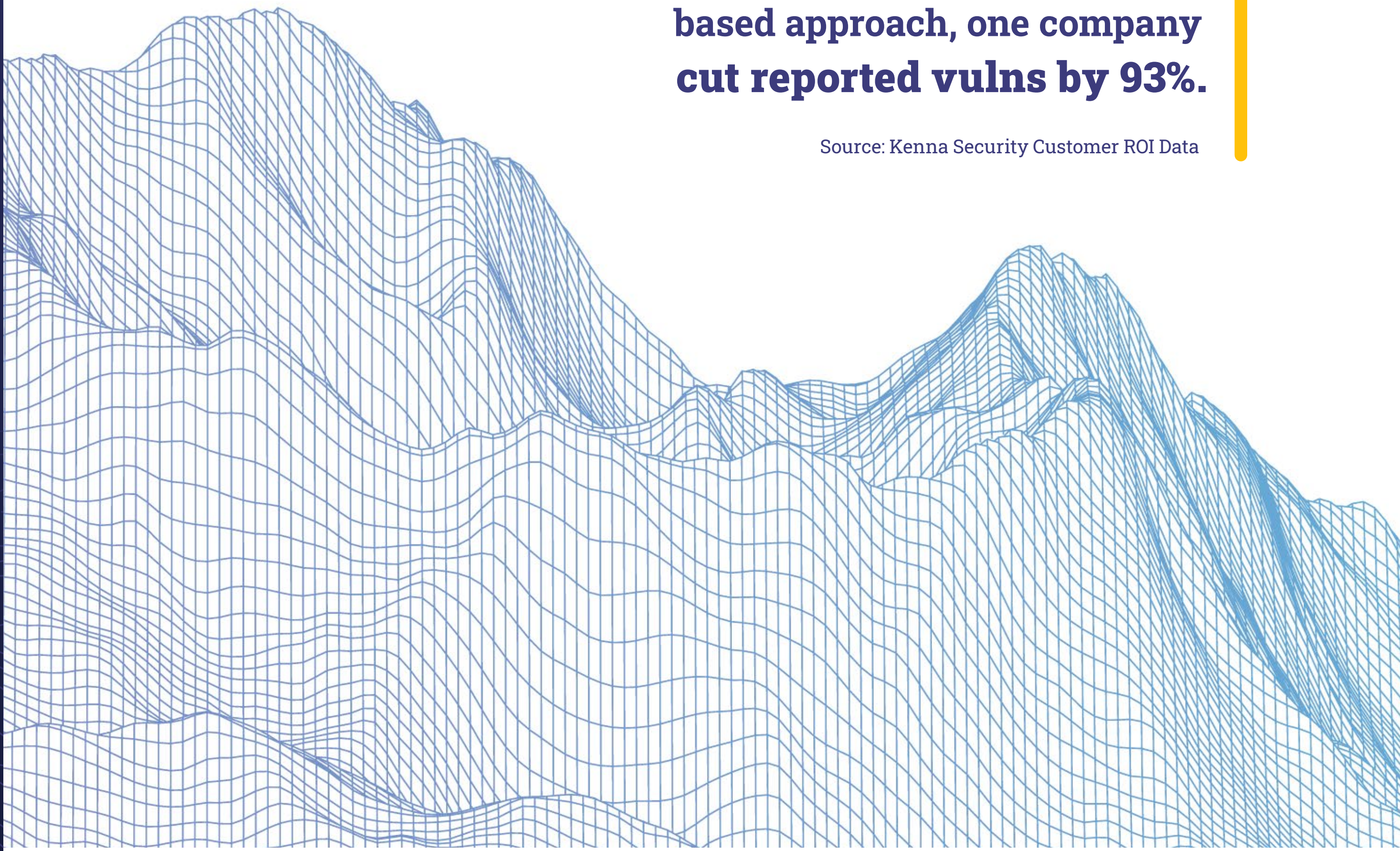
SHRUNK TO LESS THAN 200,000 — ALL IN UNDER 60 DAYS.

forgo having to drop dollars on another investment. But in fact, home-grown vulnerability management systems can cost millions a year—it's far from a cost saver.

By remediating the right vulnerabilities, using a data-driven approach that incorporates contextual awareness around every vulnerability, you can dramatically reduce the number of vulnerabilities that need to be patched. One recent convert, a U.S. financial services firm, started with a staggering 2.8 million vulnerabilities reported using the company's former risk remediation strategy. Once they made the transition to a modern vulnerability management approach, that number shrunk to less than 200,000—and all in under 60 days, to boot.

Yes, the number of vulnerabilities to be patched dropped substantially. But crucially, the company in question also saw a dramatic reduction in the time, money and resources required to remediate those vulnerabilities, further underlining the fact that aligning the entire company behind a risk-based approach to vulnerability management can be transformative for time- and budget-strapped IT teams.

> **After transitioning to a risk-based approach, one company cut reported vulns by 93%.**
>
> Source: Kenna Security Customer ROI Data



2. Align your teams around your risk

1
Focus on risk
2
Align around risk
3
Investigate, remediate, report

Let's take a closer look at how those cost and resource savings play out. It's helpful to focus the conversation on one particular area in which resources seem to quickly spiral out of control: the inefficient "battle" between Security and IT.

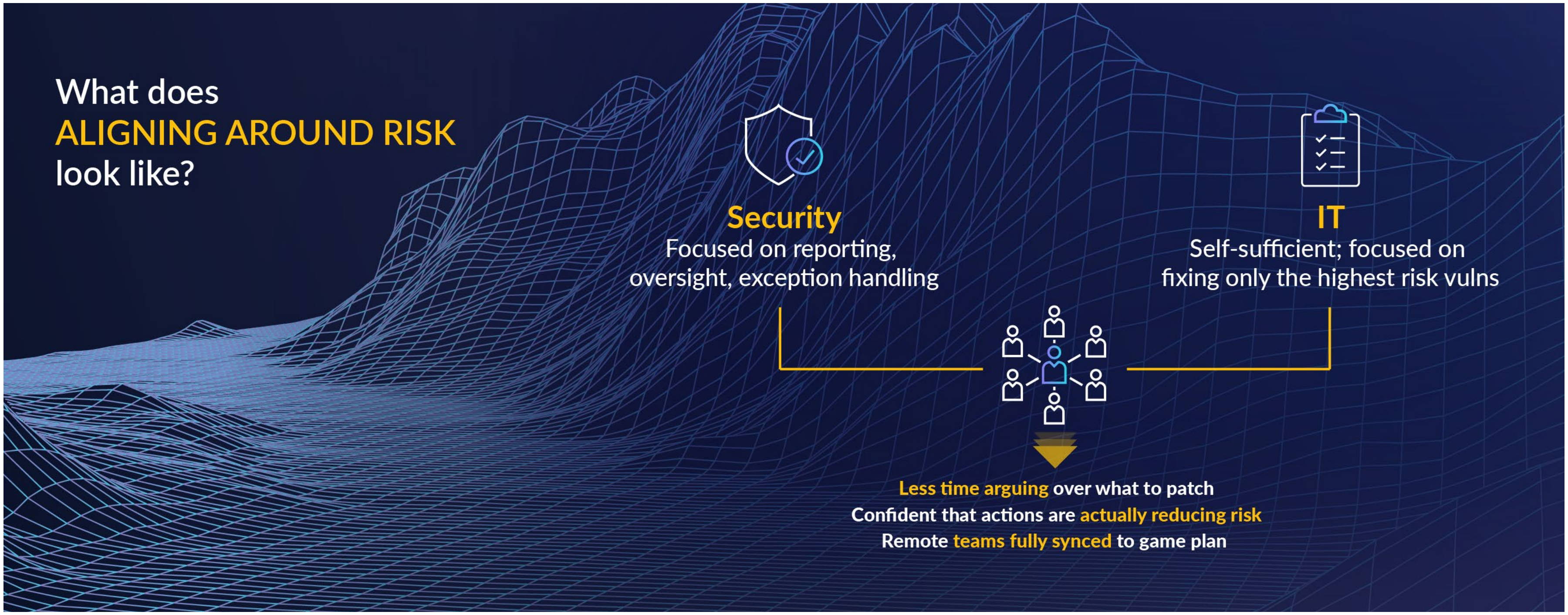
Turning passionate people into partners

There are millions of vulnerabilities in your organization, and your Security team is chomping at the bit to reduce risk, but they're struggling to identify where to begin. At the same time, your IT team is consistently flooded with demands to implement patches (among their many other tasks), and most of the time they don't even understand why they are patching what they're being asked to patch. Each team is measuring "success" by different metrics, both teams are left stretched thin, and there is rising friction between the groups. All the while, your organization's risk posture becomes increasingly precarious.

What happens if we can reduce the friction between IT and Security? "When the friction between IT and Security is reduced or eliminated," notes security product veteran Jason Rolleston, "it turns passionate people into partners, and allows them to work toward common goals, not against each other."

Battles always come at a cost. And the battle between Security and IT is an especially expensive fight without much to show in return. It serves to reason, then, that aligning Security and IT will yield far more productive results.

> When the friction between IT and Security is reduced or eliminated, it turns passionate people into partners, and allows them to **work toward common goals,** not against each other.
>
> *Jason Rolleston, security product veteran*



What does
ALIGNING AROUND RISK
look like?

Security
Focused on reporting, oversight, exception handling

IT
Self-sufficient; focused on fixing only the highest risk vulns

Less time arguing over what to patch
Confident that actions are **actually reducing risk**
Remote **teams fully synced** to game plan

Visualization exercise:

What does aligning around risk look like?

Picture this: There are still millions of vulnerabilities within your infrastructure and applications. But now, your Security and IT teams have agreed upon a risk-based approach to remediation, which means you put time and resources toward prioritizing and patching only the vulnerabilities that need to be patched.

In this environment, efficiency reigns.

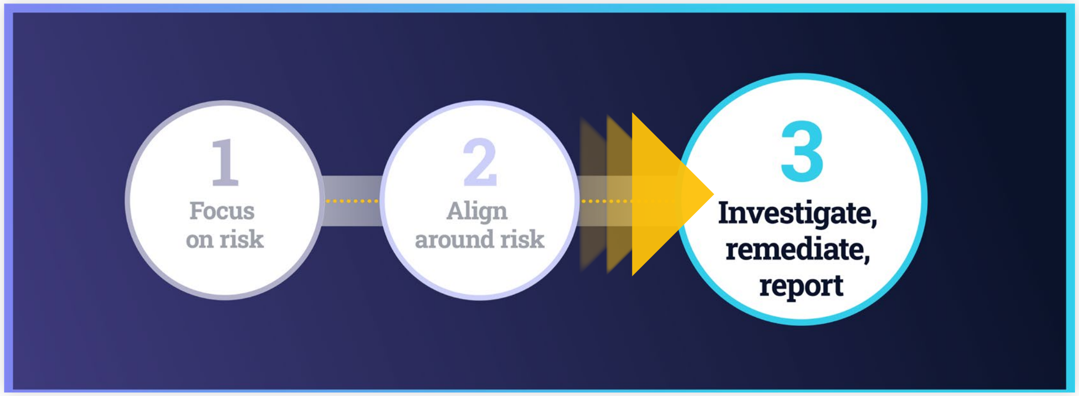
- **Your Security team is now focused on reporting, oversight, and exception handling, and IT is operating self-sufficiently.**
- **There's no need for Security to tell IT what to do; IT can see the assets they have and make decisions based on a shared alignment on a risk score, knowing that every patch they deploy is one that meaningfully reduces risk.**
- **There are far fewer disagreements about what to patch, how to patch it, and how to measure success.**
- **Security and IT spend less time arguing, and "weekly patch meetings" are a thing of the past.**
- **Remote employees are more confident they're working from the same game plan as their team members.**

Every company has finite resources. To be confident in your team's ability to remediate vulnerabilities in a timely, efficient manner, you need to make the most of those finite resources.

With a risk-based approach, the CISO can trust that risk is being managed effectively, and the CIO can repurpose limited IT resources to other priorities.

> **Align around risk, and weekly patch meetings are a thing of the past.**

3. Show me the data: investigate, remediate, report



So far, we've looked at ways a vulnerability management approach based on data-driven prioritization and threat intelligence can save time and, subsequently, free up valuable resources to stretch your budget a bit further.

But don't take our word for it. Let's look at the data: results from actual practitioners of a risk-based, modern vulnerability management strategy.

Vulnerability investigation

First and foremost, the job at hand is about taming your vulnerabilities. The task of investigating vulnerabilities in a traditional approach is often manual and lacks the context necessary to identify which vulnerabilities pose a real risk to the organization. But when you can easily understand the vulnerabilities within your environment and quickly determine which pose a real risk and thus are a higher priority, you are bound to see a reduction in time spent.

Vulnerability remediation

Remediation is much simpler when you're not trying to patch things randomly or take on too many fixes at once. With risk-based vulnerability management, you're moving away from spreadsheets, and IT and Security alike understand precisely what needs patching, why it needs to be patched, and what impact those patches have on your organization's overall risk posture. There's no more arguing, no more guessing—just action.

Since adopting a data science-driven, risk-based approach:

74%

OF COMPANIES REDUCED TIME SPENT ON VULNERABILITY INVESTIGATION BY OVER 25%

55%

OF COMPANIES REDUCED TIME SPENT ON VULNERABILITY INVESTIGATION BY OVER 50%

Source: TechValidate

With a risk-based remediation approach:

68%

OF ORGANIZATIONS REDUCED TIME SPENT ON REMEDIATION BY OVER 25%

44%

OF ORGANIZATIONS REDUCED TIME SPENT ON REMEDIATION BY OVER 50%

Source: TechValidate

Since adopting a modern vulnerability management approach:

78%

OF COMPANIES HAVE BEEN ABLE TO REDUCE TIME SPENT ON REPORTING BY MORE THAN 25%

53%

HAVE REDUCED THAT TIME BY MORE THAN 50%

Source: TechValidate

Reporting on risk

Every organization struggles to some degree with reporting risk. Even if you're experienced at generating remediation reports, chances are it's still challenging to communicate the status and progress of your company's risk in a way that's meaningful to people who don't speak IT or Security.

And you've no doubt mulled over questions like:

- **Our executive leadership needs to understand our risk posture over time, but how do I demonstrably visualize this?**
- **How do I prove my team's work is yielding results?**

An intuitive and easy-to-digest report is key to aligning leadership with the right level of risk for your organization's circumstances. Offering easily interpreted risk scores and other metrics, modern, cloud-based vulnerability management platforms can help significantly lessen the time it takes to gather, interpret, and communicate large data sets in a clear and helpful way.

From investigation to remediation to reporting, saving time and freeing resources to focus on other priorities is essential. And in today's world, we know all too well that priorities are not in short supply, although resources surely are.

What does it take to improve your vulnerability management ROI?

Leading industry analysts have put their official stamp of approval on risk-based vulnerability management, verifying what many companies already know: vulnerability management needs meaningful, data-based prioritization to be impactful and lower your risk.

Transforming your remediation program to focus on the vulnerabilities that pose the biggest risk to your organization—the 2% of vulnerabilities in your environment that are likely to be exploited—doesn't just lower your risk posture. It also drives down costs, helps you make smarter use of resources, and produces a self-service environment where Security and IT efficiently work toward the same goal by acting on specific, data-driven guidance.

Your risk-based vulnerability management checklist

It's difficult to imagine achieving all these benefits with a vulnerability management environment built around spreadsheets and CVSS scores. Yet even investing in a third-party vulnerability management solution is no guarantee you'll achieve the ROI you're looking for.

That's why it's important to look for a vulnerability management platform that doesn't take a "good enough" approach when it comes to managing the right level of risk for your business. Vulnerability management solutions that are simply bolted on to existing vulnerability scanning tools tend to cut important corners, such as lacking the depth and breadth of real-world threat intelligence needed to assess the risk a vulnerability poses to your particular environment.

When evaluating solutions, therefore, it's vital to look for solutions that are recognized for their ability to prioritize vulnerabilities based on risk. But because "risk-based" has become a popular marketing mantra for vulnerability management solution vendors, a few other characteristics will differentiate "me-too" offerings from truly modern vulnerability management solutions.

For the most effective risk reduction environment, insist that your next vulnerability management solution incorporates the following:

✓ **Real-time data from your entire IT environment.** When assessing risk, context is everything. Understanding your inventory of assets, from systems and devices to applications, gives you a more comprehensive picture of your attack surface.

✓ **Real-world threat intelligence.** When you gain the ability to understand what's happening in the wild, you can make more informed and proactive decisions about your own environment. This includes things like identifying likely targets of opportunity for attackers, knowing which vulnerabilities have been weaponized, and getting detailed information about malware activity.

✓ **Prioritization capabilities powered by advanced data science.** It's not enough to know a vulnerability exists. A modern risk management program requires that you know exactly which vulnerabilities are the biggest threat to your unique organization, and then establishes a remediation priority, with specific guidance on actions to take, so you and your team are always aligned and ready to get to work.

✓ **Natural language processing.** This advanced technology investigates social media sites, the dark web, and other places where vulnerabilities are discussed, then extracts language associated with vulnerabilities for more complete risk assessments.

✓ **Predictive modeling.** This capability calculates the risk of a vulnerability as soon as it is revealed—even before an exploit can be built for it.

✓ **A risk metric anyone can understand.** Prioritization alone doesn't define a truly modern vulnerability management solution. For Security, IT, DevOps and executive teams to align around risk, you'll need a metric that takes into account how prevalent the vulnerability is in your environment, the potential severity an exploit would represent, and external threat intel that could indicate the likeliness of an exploit. The best solutions combine all this into a metric—or score—that is simple, understandable, and repeatable.

✓ **The ability to set risk-based SLAs.** The most advanced vulnerability management solutions allow you to gain even greater efficiency and IT/Security alignment by setting service-level agreements (SLAs) based on your organization's risk tolerance, rather than on purely arbitrary timelines.

Status check: What’s your risk efficiency?

Discover what kind of productivity and efficiency gains you and your team stand to make when you transition from your current CVSS-based or scanner-based vulnerability management strategy to a modern, data-driven approach to vulnerability management.

Answer two quick questions about your current remediation program, and we’ll show you how many vulnerabilities pose a significant risk to your IT environment. We’ll also compare that result with what your existing strategy deems worthy of your time, money and resources.

What’s your risk efficiency? Calculate it now.

Learn more.

The Future of Vulnerability Management is Risk-Based, featuring research from Gartner.

Prioritization to Prediction: Analyzing Vulnerability Remediation Strategies, featuring research from the Cyentia Institute.

Distinguishing Common Practices from Best Practices in Vulnerability Management, on-demand webinar featuring research from the Cyentia Institute.

How to Implement Risk-Based Vulnerability Management Now, an implementation guide from Kenna Security.

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

www.kennasecurity.com

KENNA Security