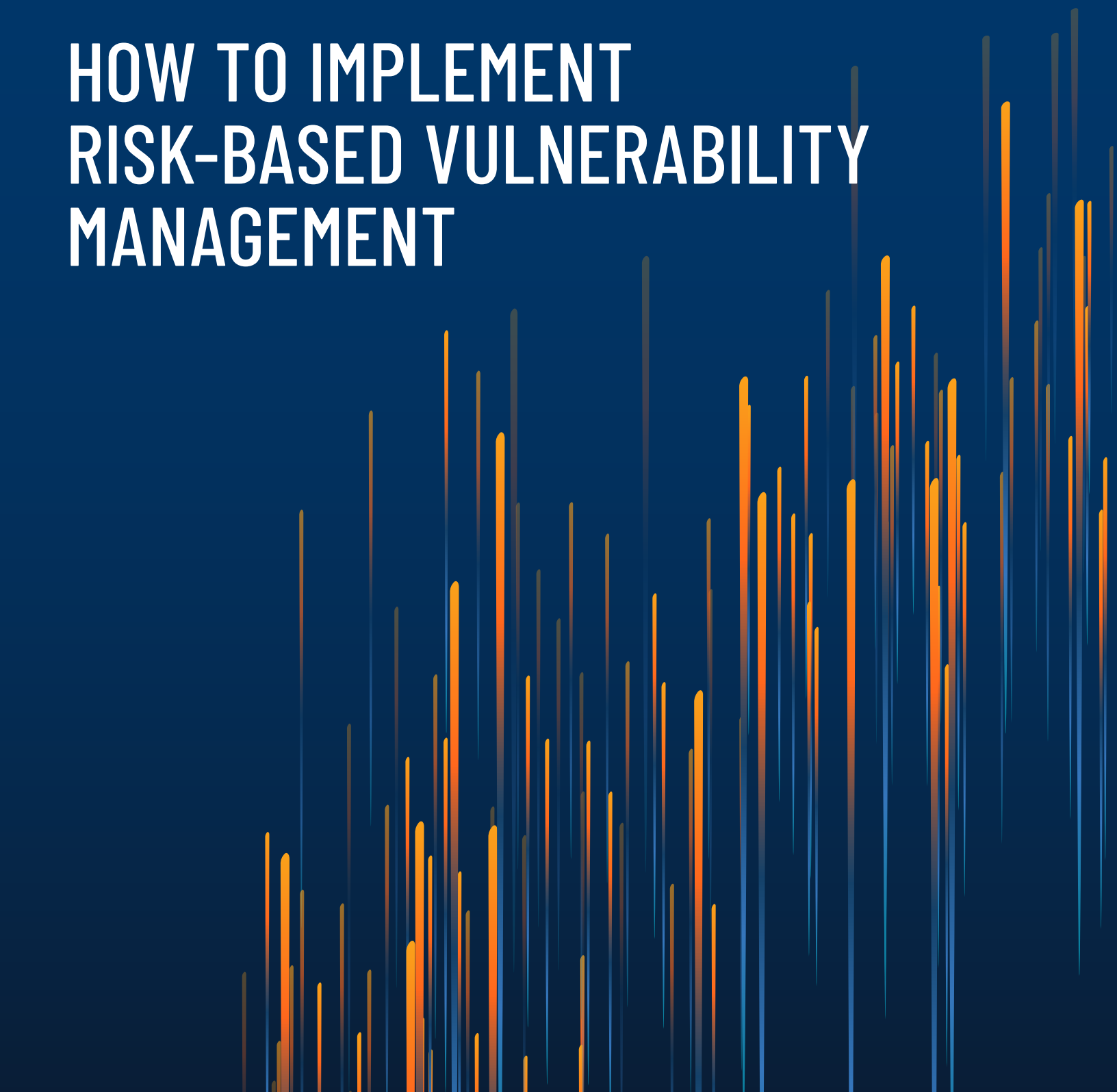
tenable

HOW TO IMPLEMENT RISK-BASED VULNERABILITY MANAGEMENT



In 2019, the U.S. National Vulnerability Database recorded **17,313 new vulnerabilities,** compared to 6,447 in 2016.[1]

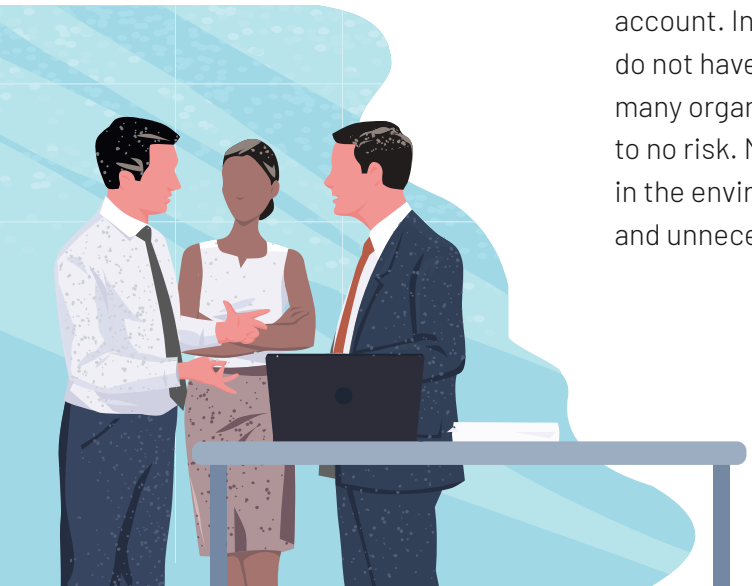
More vulnerabilities, more risk

No matter the size of your organization, the number of vulnerabilities it's exposed to every day is growing exponentially. In fact, in the last three years, the number of vulnerabilities published each year has almost tripled.

The explanation is simple: With digital transformation driving ever-increasing numbers and types of devices, technologies, and assets such as cloud, OT, and containers, the cyberattack surface keeps growing. More surface, more vulnerabilities. At the same time, the severity of vulnerabilities is increasing and cybercriminals keep getting smarter.

76% of vulnerabilities with a CVSS score 7 and above have no exploit code written against them.[1]

Security teams struggling to stay ahead of vulnerabilities are being stretched thinner and thinner. Legacy approaches focused on the Common Vulnerability Scoring System (CVSS) don't take risk into account. In fact, 76% of vulnerabilities with a CVSS score of 7 or above do not have exploit code written against them. By depending on CVSS, many organizations are wasting time on vulnerabilities that pose little to no risk. Meanwhile, nearly half of dangerous vulnerabilities are left in the environment. The result? Wasted time, missed opportunities, and unnecessary business risk.



[1]Source: Tenable Research

The power of putting threats into context

But, there's good news. Risk-based vulnerability management offers a smarter approach to protecting the business based on machine learning–generated risk models. This approach assesses vulnerabilities in the context of business risk. As a result, security teams can move from being reactive to being proactive, and focus on the vulnerabilities that pose the greatest immediate risk to your organization.

While legacy methods emphasize just two steps, identifying and assessing vulnerabilities, a risk-based approach takes it further, giving you a comprehensive, efficient way to reduce business risk.

To reap the benefits of risk-based vulnerability management, you'll need modern solutions capable of providing complete visibility, continuous assessments, and a more proactive, strategic approach. In addition, traditional processes must be extended to also include three additional capabilities: prioritization, remediation and measurement.

Step 1: **Discover everything**

Identify and map every asset.

Vulnerability management always starts with scanning your entire attack surface to identify points of exposure.

You can't assess what you can't see

Legacy solutions can only scan traditional IT, which consists of on-premises assets including desktops, network infrastructure and servers. This only provides partial visibility. Today's IT landscape is complex and constantly changing. With organizations embracing virtual and cloud assets, custom apps, IoT and connected operational technology (OT), it's critical to gain visibility into these dynamic aspects of the attack surface, as well.

Discovery also has to be continuous. Many companies follow a periodic scanning schedule, often determined by compliance audits. But siloed, point-in-time scanning delivers a limited view of assets and potential issues. The enterprise network is always changing, which means infrequently scanning for vulnerabilities won't cut it anymore. It's the equivalent of having a security camera that takes a photo once a day instead of a video camera running around the clock.

In practice, to gain full visibility, you need to replace your legacy scanner with one that can identify and map every asset across the attack spectrum. You need a solution that's dynamic and holistic, scanning everything from network infrastructure to containers, and providing continuous visibility into the entire ecosystem. Live discovery is vital to vulnerability management.

Step 2: **Assess in context**

Understand the state of every asset.

For your assessment to have impact, you need a solution that can evaluate vulnerabilities in the context of your business as well as the broader threat landscape.

Beyond one-dimensional scoring

While CVSS has been the primary tool for assessing vulnerability threats for over a decade, it's widely known to be flawed. One reason is because CVSS base scores are static. Each new vulnerability is given a severity rating once, typically within two weeks of a vulnerability being discovered. And, the overwhelming majority are never updated. With today's changing threat landscape, that score quickly becomes outdated.

In addition, organizations that exclusively rely on CVSS scores to decide which vulnerabilities to focus on don't put the vulnerability in any degree of context, such as threat and exploit information, current attacker activity and the importance of the affected asset to the business.

A common method is to prioritize any vulnerability that scores 7 or higher. But, with 56% of all vulnerabilities falling into this bucket, teams are quickly overwhelmed by sheer volume. A large enterprise might have tens of millions of vulnerabilities – there's simply no human way to keep up.

And, without putting threats into context, your team may be wasting time on vulnerabilities that don't matter – while leaving others open that should be remediated immediately. You need a solution that is constantly assessing the full context of each vulnerability and updating its risk score accordingly.

First, assess exploit potential

All vulnerabilities are not created equal. In fact, the majority of them are never exploited and therefore don't pose a risk to your organization. Only 20% of all vulnerabilities have an exploit available, meaning a proof of concept has been written and published. But, many of these are written by white hat researchers, as required by their employers, and the percentage of vulnerabilities actually used in cyberattacks is small. Only 24% of CVSS 7+ vulnerabilities have an exploit available – with a fraction of those actually being exploited in the wild[2].

[2] Source: Tenable Research

Determine the likelihood an exploit will occur

Analyzing attacker activity in the broader threat landscape provides valuable insights into which of your vulnerabilities are more likely to be exploited in the near future. A risk-based approach puts vulnerabilities in context by taking into account those with a greater propensity for exploit. If attackers aren't currently targeting specific vulnerabilities, you can focus your resources on what's a larger risk at that moment.

Then consider the business impact

Every IT asset plays a unique role in your business. The relative importance of the asset to your operations impacts how critical a vulnerability on that asset would be. The more vital an asset is to an organization, the greater the risk if it's compromised – even if the vulnerability itself doesn't score high. Business-critical services and systems, which vary by organization and industry, will have a greater impact on a business if attacked.

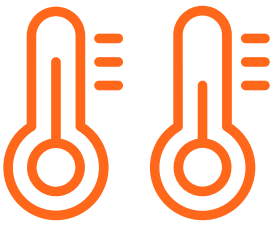
Even a lower-rated vulnerability on a business-critical asset may pose a high risk. For example, a vulnerability that scores 5 and is on a company's financial database may be deemed more critical than one that scores 10 but is on a less important asset, such as a web server. Only when you are armed with the full contextual data can you make an informed decision.

"Vulnerabilities can be discovered and assessed, while the exploitation of vulnerabilities can be anticipated and predicted with risk-prioritized, preemptive actions taken to change the organization's security and risk posture."

– Gartner[3]

[3] *How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation*, Gartner, January 2020

> "Implement multifaceted, risk-based vulnerability prioritization, including factors such as vulnerability severity, current exploitation activity, business criticality and exposure of the affected system."
>
> – Gartner[4]



Step 3: **Prioritize**

Leverage threat intelligence and business context.

This is where all the contextual data comes together to facilitate informed decision-making. With valuable security resources already stretched thin, time spent manually parsing through CSV files and spreadsheets is a waste. There is simply no physical way your teams can conduct the necessary research at scale. Automation is required to facilitate this process.

To stay ahead of attackers, risk-based vulnerability management employs machine learning algorithms that identify and recognize patterns of activity to predict which vulnerabilities are most likely to be exploited. It then combines this data with the vulnerability score and asset criticality score and prioritizes the riskiest vulnerabilities to fix first, continuously updating priorities as the threat landscape changes. And, it does it all faster than any human team possibly could.

Automation makes it possible to enable continuous, comprehensive vulnerability data analysis at scale. It allows you to focus first on what matters most, so you can stop wasting time and resources on the vulnerabilities that pose little to no risk. The right solution will help your team become far more effective, reducing the greatest amount of risk with the least amount of effort. At the same time, it will free you from manual tedium, so you can focus on more strategic security initiatives.

[4] *How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation*, Gartner, January 2020

Step 4: **Remediate**

Drive measurable results toward a common goal.

Once your team determines which vulnerabilities to prioritize, it's time to partner with IT to address them. Effective collaboration between security and IT is crucial for remediation and can help ensure that all of your efforts to discover, assess and prioritize deliver maximum benefit.

The short list

> "Improve remediation windows and efficiency by using technologies that can automate vulnerability analysis." – Gartner[5]

Sending IT a list of thousands of vulnerabilities to fix with no clear direction isn't going to yield results. With risk-based vulnerability management, you can give IT an actionable, short list of vulnerabilities to fix, which can forge a stronger, more effective partnership between your teams. In addition to ensuring the highest-risk vulnerabilities are fixed first, this also helps security teams show why those at the top of the list take priority, enhancing their credibility throughout the organization.

Integration with IT systems

By integrating vulnerability management with your IT systems, you can create a closed-feedback loop that ensures the most important work is done first. When security teams prioritize critical vulnerabilities for remediation, they should add remediation intelligence into IT workflows. This explains why a vulnerability is high priority and how to fix it. When the vulnerability has been fixed, the IT platform needs to send that information back to security, closing the loop and ensuring remediation of critical vulnerabilities. It's the most efficient way to make sure vital fixes get made right away and nothing important slips through the cracks.

[5] *How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation, Gartner*, January 2020

Facilitate security and IT collaboration

Take advantage of the Tenable and ServiceNow integration to improve operational efficiency across security and IT teams:

- Respond quickly and reduce errors through automation and orchestration
- Scale processes via parallel, repeatable and measurable workflows
- Achieve closed-loop remediation via targeted re-scans

Step 5: **Measure**

Identify gaps and areas for improvement.

As with any strategy, calculating key metrics shines a light on what's working and can help pinpoint areas in need of improvement. In this case, you want to look at security and maturity metrics such as time to assess, time to remediate, and cyber exposure rating over time to see how your organization's performance compares to industry standards. If what you're doing doesn't measure up against best practices, adjust accordingly. You can't improve what you don't measure.

Use metrics to enable mind-shift

Briefing stakeholders and executives on the number of vulnerabilities the team has fixed doesn't provide an accurate picture of security. You need to show them you're fixing the right things.

Using metrics to demonstrate the reduction in business risk can help bridge this gap and make the case for your security team's effectiveness. Internally, measuring success is good for morale and helps keep teams engaged and active. And communicating business outcomes to the C-suite and other key decision-makers will prove the value of the investment in new tools and solutions.

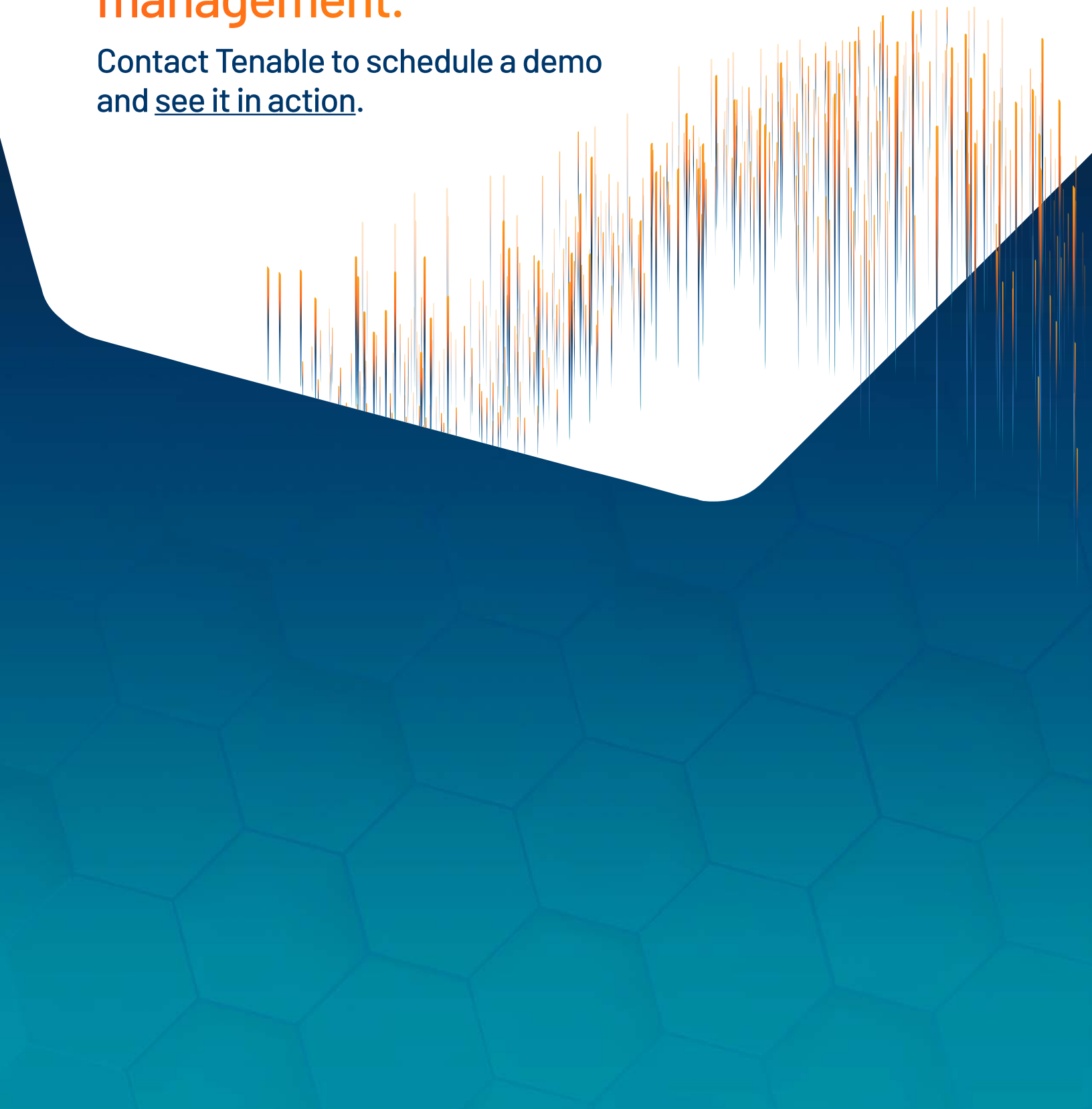
"By 2022, organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches."

– Gartner[6]

[6] *A Guide to Choosing a Vulnerability Assessment Solution*, Gartner, April 2019

Re-think your security strategy with risk-based vulnerability management.

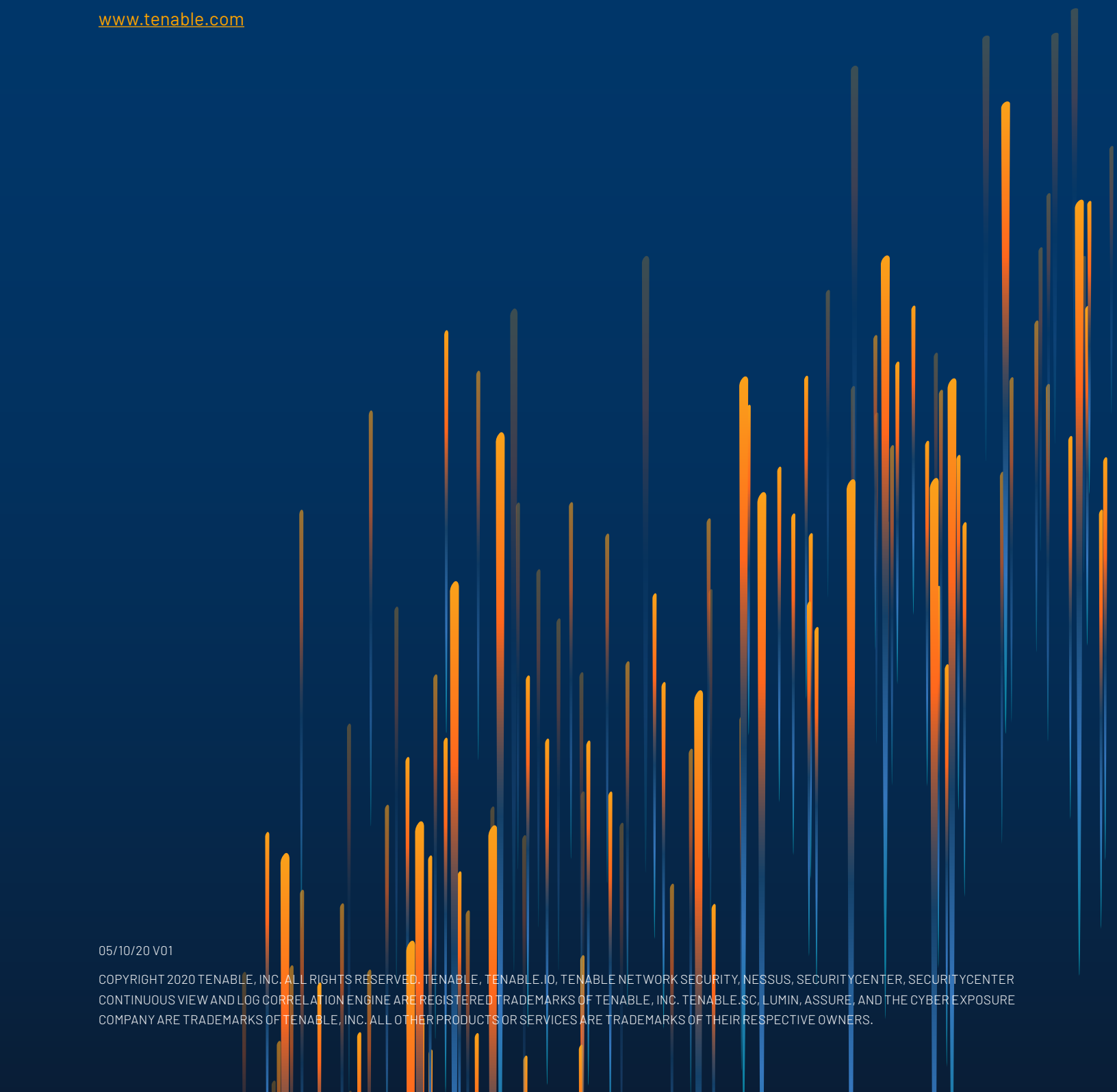
Contact Tenable to schedule a demo and see it in action.



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com



05/10/20 V01