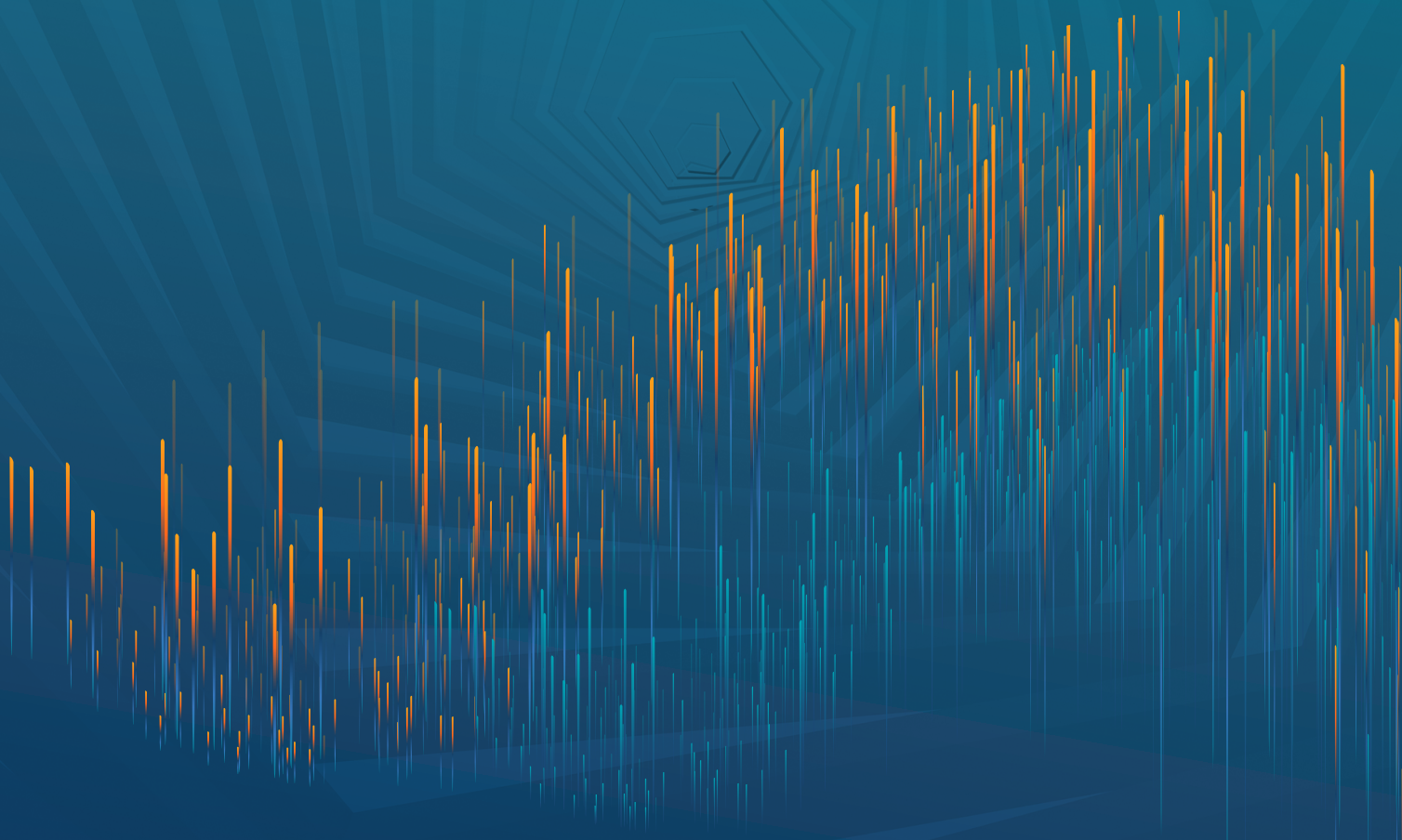
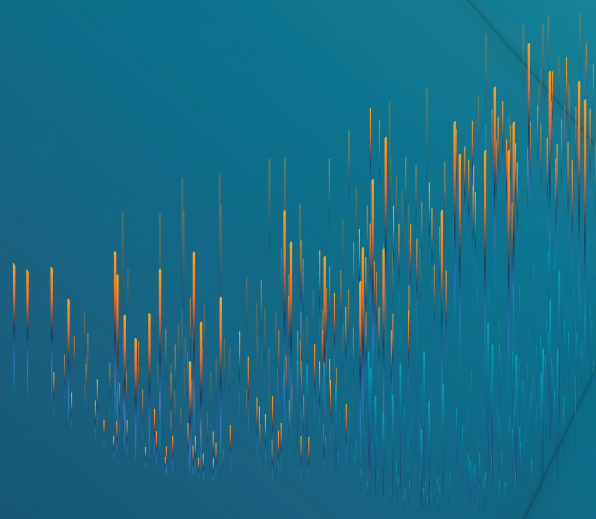
tenable

FOCUS ON THE VULNERABILITIES THAT POSE THE GREATEST RISK



Gartner says:

"By 2022, organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches."[1]



Legacy vulnerability management is no match for today's digital world

No matter how long you've been in cybersecurity, you know vulnerability management is essential to identifying and reducing cyber risk. Why? Because behind every major cyberattack is a vulnerability that was left unaddressed.

But, there's one big problem: Over the last 20 years, the attack surface evolved, and vulnerability management failed to keep up with it.

Today's IT environment is ever-changing. Propelled by digital transformation, our world is now written in code, buzzing with new technologies, platforms and devices. Think cloud, IoT, mobile, web apps – even industrial equipment connects into this chaotic landscape.

Different types of assets constantly enter and exit the enterprise. On top of that, some are ephemeral – lasting mere seconds or minutes.

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

More assets, more vulnerabilities. It's that simple.

Given the ballooning attack surface, it's no surprise the number of vulnerabilities is rising. In fact, the tally is downright daunting. From 2016 to 2018, new published vulnerabilities surged from 9,837[2] to 16,500 per year.[3] On average, this means enterprises find 870 vulnerabilities per day across 960 IT assets.[4]

Adding to the challenge, vulnerability severity appears to be increasing. Due to changes made in the industry-standard Common Vulnerability Scoring System (CVSS), the majority of vulnerabilities are now categorized as high or critical. According to CVSSv3 ratings, 60% of vulnerabilities are considered high or critical compared to 31% in CVSSv2 (see Figure 1).[5]

[2] *Vulnerability Intelligence Report*, Tenable Research, 2018

[3] U.S. National Vulnerability Database (NVD)

[4] Tenable Research

[5] *Vulnerability Intelligence Report*, Tenable Research, 2018

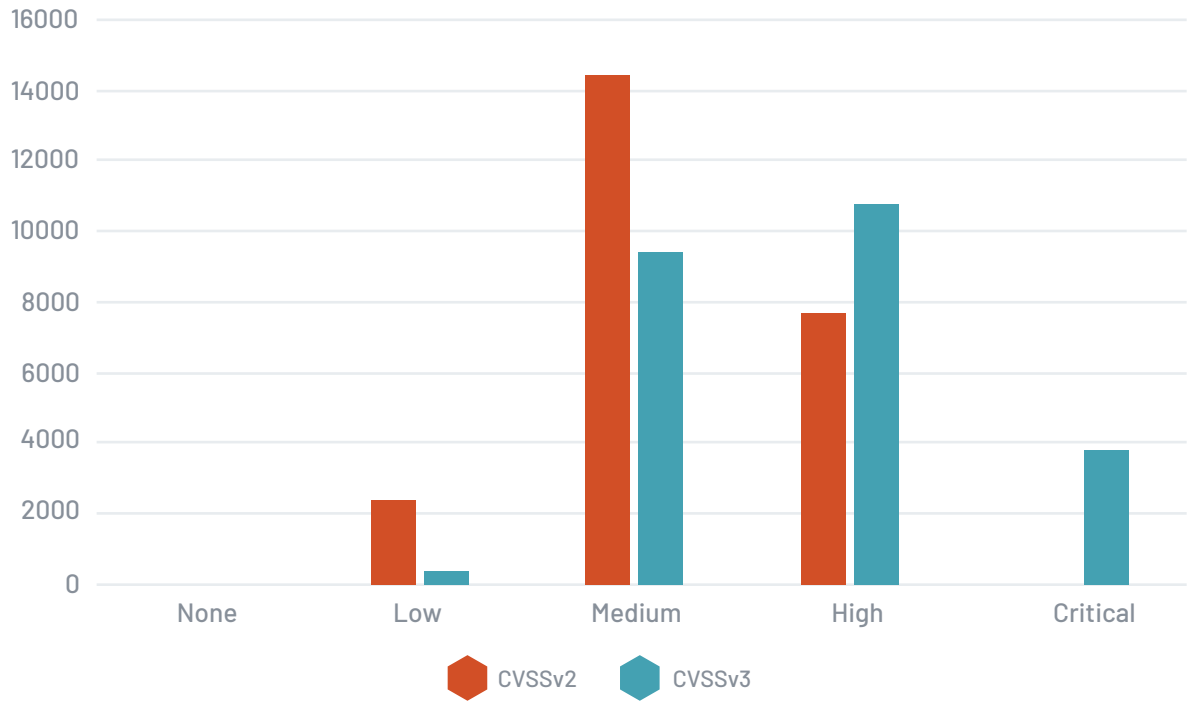


Figure 1. CVSSv2 vs CVSSv3 Classification

As a result, security teams are dealing with more vulnerabilities than they can possibly handle. Spreading these limited – and valuable – resources too thin can quickly lead to inefficiency and job burnout. And with CVSS essentially being risk-unaware, the last thing you need is to waste precious time remediating vulnerabilities that pose little to no risk.

The race against attackers continues – and they're in the lead

Upon analyzing the 50 most prevalent critical and high-severity vulnerabilities from approximately 200,000 vulnerability assessment scans over a three-month period, Tenable Research found attackers have a seven-day head start on defenders.[6] Threat actors are sprinting ahead, exploiting vulnerabilities before security teams know they're at risk.

On average, attackers have a 7-day head start on defenders.

[6] *Quantifying the Attacker's First-Mover Advantage*, Tenable Research, 2018

Without continuous visibility into the vulnerabilities plaguing the organization, it's impossible to know where you're weak. Legacy vulnerability management is mainly compliance-driven, geared at demonstrating regulatory adherence and checking all the right boxes. This means vulnerability scanning and remediation schedules are often intermittent, punctuated by audit cycles, leaving security painfully unaware of significant vulnerabilities. Fortunately, there's a way to get ahead of these dangers – and essentially flip the attacker's advantage.

Seize the opportunity with risk-based vulnerability management

Everyone in security knows there are no guarantees against breaches. But a proactive defensible approach is the next best thing. The easiest way to do that? Risk-based vulnerability management.

With risk-based vulnerability management, you can confidently answer these three key questions:

1. Where is the business exposed?

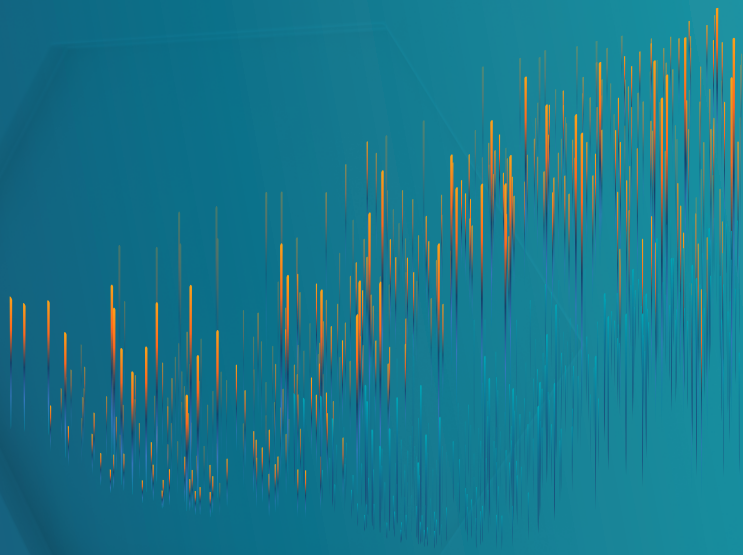
2. Where should we prioritize based on likelihood of exploitation?

3. What is the impact to the business if a vulnerability is exploited?

Risk-based vulnerability management helps you cut through the immense volume of vulnerabilities, giving you the precise focus you need to act swiftly and effectively.

"Start monitoring this as a key metric: How many vulnerabilities, do you have, that are being exploited in the wild"

– Gartner [7]



First, solve the fundamental visibility problem

You can't protect what you can't see, and you can't fix issues you don't know about. Yet, gaining comprehensive visibility across the whole of your evolving attack surface is no easy feat.

Both the attack surface and threat environment are constantly in flux, so siloed, point-in-time assessments leave a lot of room for misinformed decision-making. Risk-based vulnerability management goes far beyond the static, fragmented visibility provided by legacy vulnerability management and delivers the total, dynamic view – adding cloud, containers, web apps, IoT, operational technology and just about any asset on any computing platform (see Figure 2).

[7] *"Gartner's Strategic Vision for Vulnerability Management,"* Craig Lawson; Gartner Security & Risk Management Summit Presentation, August 2019, Sydney, Australia

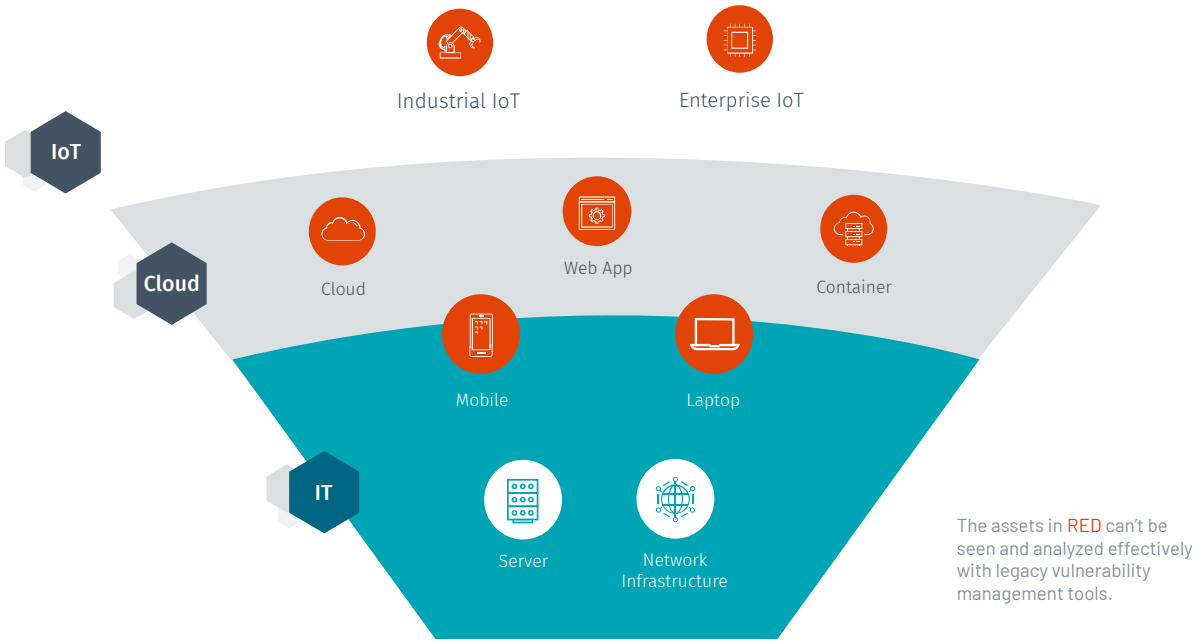


Figure 2. Eliminate all blind spots with risk-based vulnerability management

With risk-based vulnerability management, you'll have an accurate view of all potential risks to the organization.

Then, answer the prioritization question

Risk-based vulnerability management also answers the question: "What should we fix first?" Prioritizing using CVSS alone isn't sufficient because it is limited to a theoretical view of the risk a vulnerability could potentially introduce and therefore categorizes the majority of vulnerabilities as high or critical. CVSS doesn't take into account whether the vulnerability is being exploited in the wild. Nor does it understand if the vulnerability is on a business-critical service or system.

For example, CVSSv2 and CVSSv3 prioritize remotely exploitable vulnerabilities, requiring no user interaction. But, attackers prefer to use proven tactics that consistently yield success. They typically leverage client-side vulnerabilities, executed through phishing attacks, drive-by malware, malvertising, etc. If you prioritize based on CVSS alone (e.g., patch all 9 and above), you end up wasting time and energy patching vulnerabilities that will never be exploited – and missing those favored by attackers. To effectively prioritize, you need a risk-driven approach that prioritizes critical assets and vulnerabilities known to be targeted by attackers.

With risk-based vulnerability management, you can shrink the scope of critical vulnerabilities – and distill real risks from the theoretical (see Figure 3). It uses machine learning to automatically analyze and correlate vulnerability severity, threat actor activity and asset criticality, giving you clear guidance on where to focus remediation efforts based on risk.

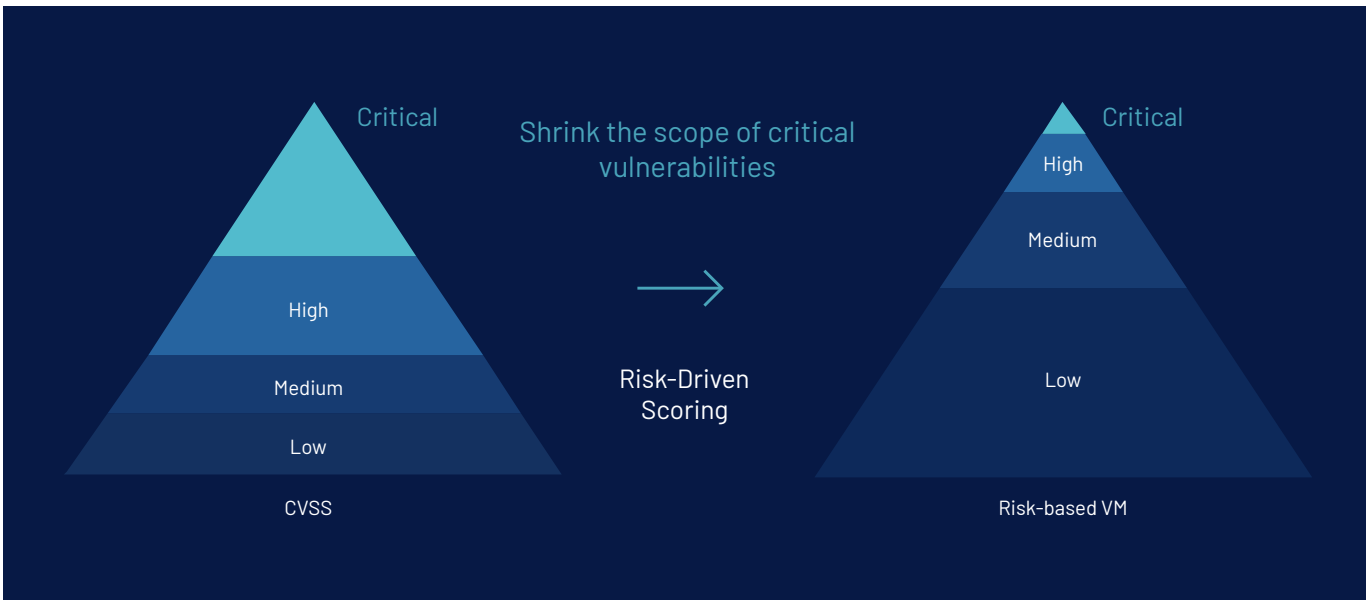
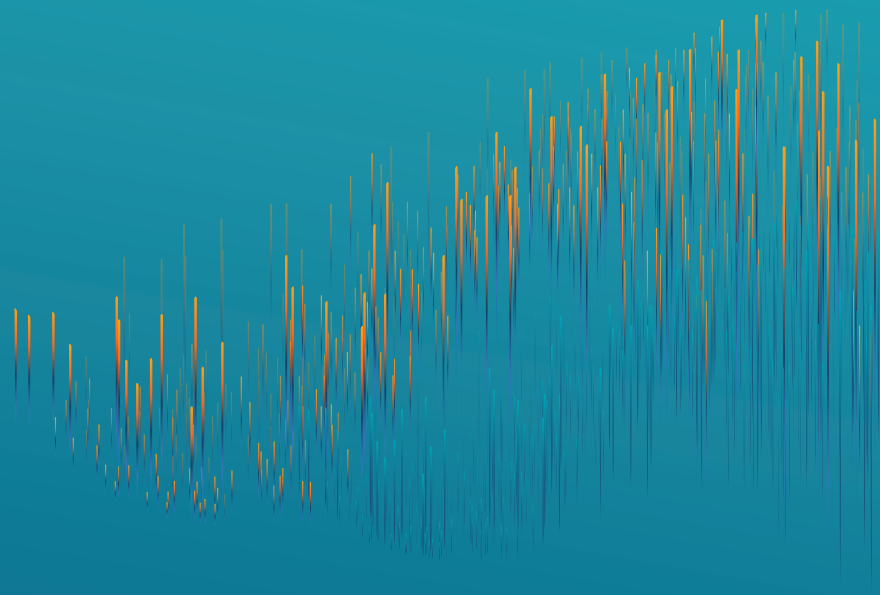


Figure 3. Prioritization using CVSS vs risk-based VM

Given the mountains of data generated across today's attack surface, it's impossible for resource-crunched teams to process it all manually. Let machine learning do the analysis and correlation, so you can work with IT on fixing the vulnerabilities that matter.



"As our organization grows organically and moves from legacy systems to cloud environments such as GCP, AWS and Microsoft Azure, our attack surface is rapidly expanding. We had a significant number of vulnerabilities. Around 250,000 vulnerabilities were detected initially, several of which were classified as being critical and exploitable due to some of the legacy applications. It is essential that my team efficiently prioritize our vulnerabilities to reduce our cyber risk, and stay one step ahead of the threats."

– Mike Koss, Head of IT Security and Risk, NBrown Group

Risk-based vs legacy vulnerability management

Why Legacy Vulnerability Management Falls Short	How Risk-Based Vulnerability Management Elevates You
Assesses Only Traditional IT Infrastructure	**Sees the Entire Attack Surface**
• Only assesses traditional, on-premises assets (e.g., desktops, laptops, servers, network devices). • Puts business services at risk by ignoring large parts of the attack surface.	• Discovers and assesses the entire attack surface, including traditional assets, mobile, web apps, cloud, container, IoT and OT assets. • Maps traditional and modern assets to business systems to measure overall business system risk.
Classifies Vulnerabilities by Severity Data	**Prioritizes Vulnerabilities Using Machine Learning–Powered Insights**
• Classifies too many vulnerabilities as high and critical – failing to effectively triage. • Categorizes vulnerabilities by severity alone – with no awareness of risk, asset criticality or any other context. • Technical metrics don't map to business outcomes, causing confusion and potentially a false sense of security.	• Pinpoints the subset of vulnerabilities posing the greatest risk to the organization – so they can be quickly addressed. • Prioritizes vulnerability remediation based on business context, including vulnerability data, threat intelligence (e.g., near-term likelihood of exploitability) and asset criticality. • Risk-based metrics for assets and business systems guide strategic decisions.
Checks Minimum Compliance Boxes	**Drives Risk-Based Decisions**
• Only meets minimum requirements to pass an audit. • Focuses exclusively on in-scope assets; often ignores other business-critical assets.	• Uses best practices to protect the business from cyber risk. • Accounts for all assets, including the many important business systems that do not have compliance requirements.
Provides Static, Point-in-Time Snapshots	**Delivers Dynamic, Continuous Visibility**
• Only assesses assets and performs remediation monthly (or less frequently). • Analytics are based on old data – leading to late and incomplete corrective action.	• Discovers and assesses new assets immediately; assesses known assets continuously. • Analytics are updated daily to reflect changes in risk based on the shifting threat landscape and/or business importance of the asset.
Reactive	**Proactive**
• Keeps you in firefighting mode since risk assessment is a guessing game. (High-profile and zero-day vulnerabilities are often perceived as bigger threats than the risk they actually represent.)	• Provides utmost focus – optimized, automated processes identify and address the few high-risk vulnerabilities.

Turn the impossible into the achievable (and eliminate friction with IT)

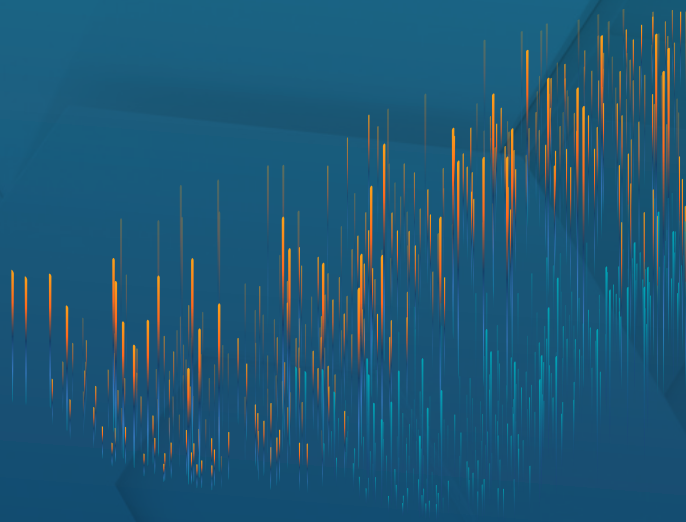
A recent Ponemon Institute survey found that 51% of security teams spend more time navigating manual processes than responding to vulnerabilities, leading to insurmountable response backlogs.[8] Pair that with a serious industrywide skills shortage and it's easy to see why team efficiency is essential.

Risk-based vulnerability management gives you the laser focus you need to guide your team while showing the business you're actively minimizing cyber risk. You'll know you're taking the right actions to manage risk because you're concentrating on the few vulnerabilities likely to be exploited and that cause most harm. And you'll also routinely track these two KPIs:

- Time to assess: How long does it take between vulnerability publication and your team's assessment of the vulnerability?
- Time to remediate: How long does it take your team to respond to – and work with IT to remediate – the critical vulnerabilities, which are actively exploited in the wild and/or pose the greatest risk?

"We can't dump [a] list of 10,000 [vulnerabilities] on the IT team and expect them to engage with us. If I give them a list of a couple hundred? They'll engage."

– Dan Bowden, CISO, Sentara Healthcare



[8] *Measuring & Managing the Cyber Risks to Business Operations*, Ponemon Institute, 2018

By monitoring these metrics, you'll have an honest read on what's working – and what's not. This newfound clarity will better equip you for your conversations with IT. Instead of tossing them a spreadsheet with hundreds or thousands of vulnerabilities to address, you'll partner with them on fixing the small percentage that actually need attention. Having data you can rely on makes a world of difference when it comes to identifying gaps in process and demonstrating progress toward common goals.

Measure and manage risk to business systems

With risk-based vulnerability management, you'll have the insights you need to protect business systems. If a business system's cyber risk is unacceptable, you can quickly determine where to focus additional security controls to mitigate risk.

You'll also be able to easily communicate your attack surface's cyber risk to business leaders. The data you rely on to effectively measure and manage your risk-based vulnerability management program is automatically encapsulated into a risk-based metric business owners will understand.

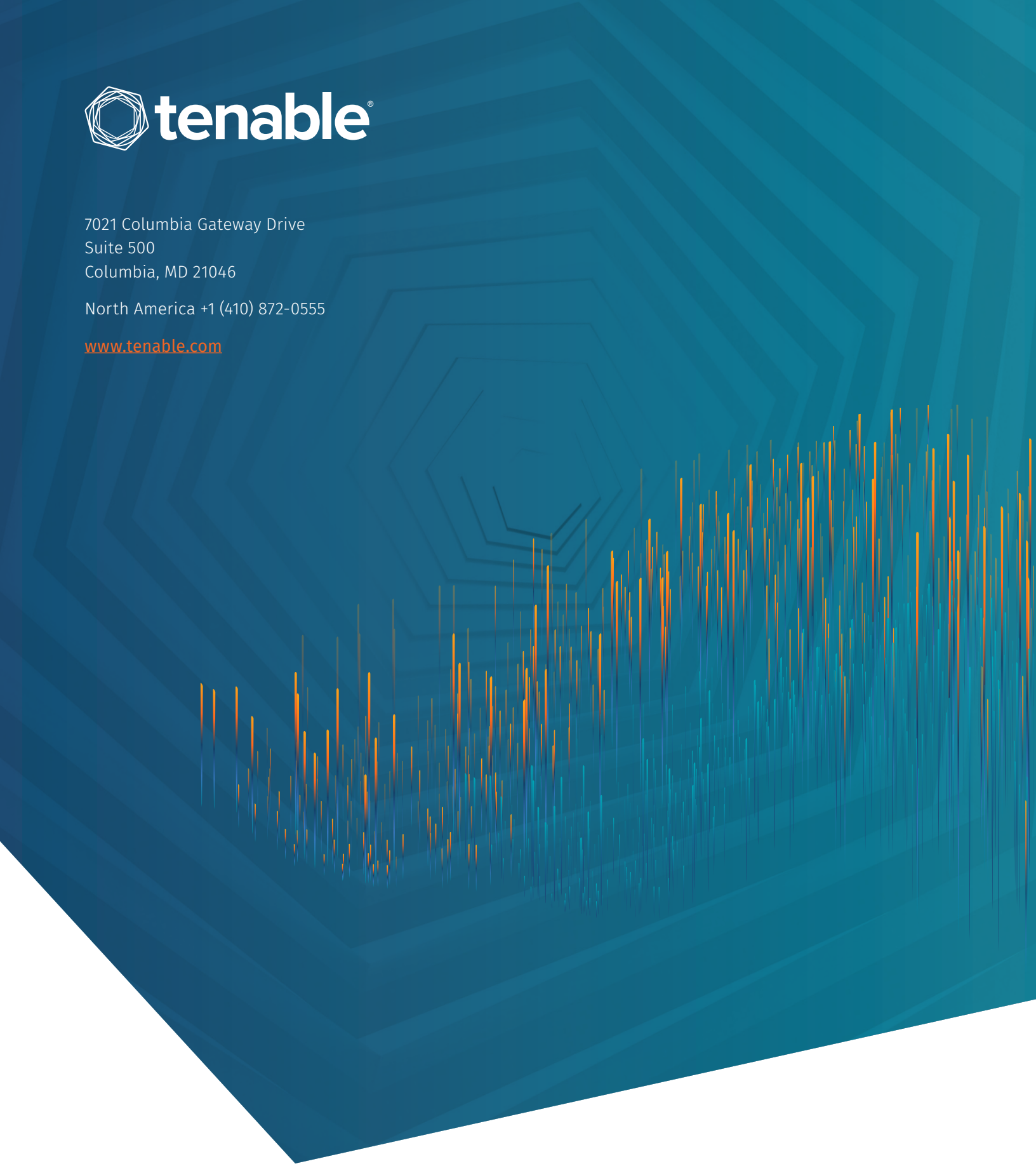
Want to reduce your immediate workload by 97%?
Try Predictive Prioritization.
Predictive Prioritization combines research insights, threat intelligence and vulnerability rating to reduce the number of vulnerabilities requiring immediate remediation by 97%. See how it works – check out the interactive demo.

Get your priorities straight – try risk-based vulnerability management today

Most security teams say they have X many people working on Y number of cases or their company has Z number of critical vulnerabilities open. How do those numbers translate to a lesser likelihood that the company will be breached? They don't.

Reducing numbers alone does not lower your risk. Eliminating the vulnerabilities that pose immediate danger is what makes the difference.

Want to see how risk-based vulnerability management can provide utmost focus for your security team? **Get started today**.



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

01/17/20 V01