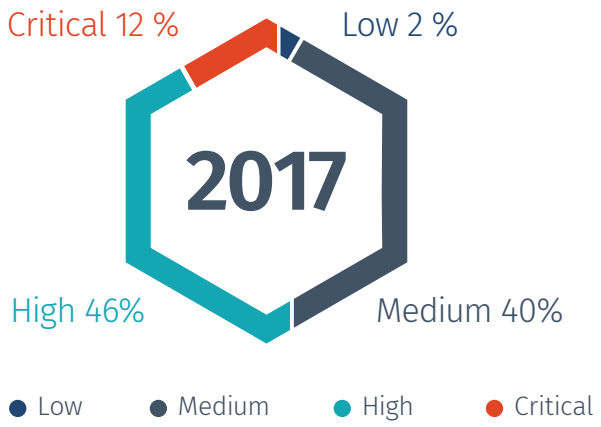
tenable

3 THINGS YOU NEED TO KNOW ABOUT PRIORITIZING VULNERABILITIES

The Current Landscape of Vulnerability Management

If you work in cybersecurity, you already know that vulnerability management is getting more and more complex.

The number of vulnerabilities is on the rise, and their severity is increasing. The Tenable Research Vulnerability Intelligence Report sheds light on the 15,038 vulnerabilities discovered in 2017, the majority of which were categorized as high or critical in severity based on the industry-standard Common Vulnerability Scoring System (CVSS).



15,038
CVEs 2017

53%
Growth 2017 vs 2016

16,500
CVEs 2018

> **And 2018's trends are even more sobering: According to the National Vulnerability Database (NVD), 16,500 new vulnerabilities were disclosed.**

As an organization's attack surface grows, so too do the volume and severity of vulnerabilities. Given the burgeoning complexity of IT infrastructure – with DevOps practices, cloud, containers and microservices becoming more mainstream, and IoT devices on the rise – vulnerability management can feel akin to working inside a pressure cooker.

According to a 2018 survey conducted by the Ponemon Institute, only 29% of organizations report having sufficient visibility into their attack surface.

Plus, organizations are facing shortages in resources and talent. 58% say shortages in skilled staff affect their ability to scan vulnerabilities in a timely manner, and 51% are bogged down by manual processes and insurmountable backlogs.

With an insufficient picture of your organization's vulnerability landscape and a scarcity of resources, how can you adequately scan for vulnerabilities and assess cyber risk, let alone satisfy C-suite and board members who need to understand cyber risk in relatable business terms? (It's enough to make anyone's head explode.)

Given this landscape, prioritization has become the key challenge for security professionals – it's what sets apart mature IT organizations, and gives you the competitive edge you need to effectively mitigate risk in today's era of digital transformation.

Guesswork, intuition, and relying on manual, outdated practices just won't cut it.

58% SAY
shortages in skilled staff affect timely scanning

ONLY 29%
of organizations report sufficient visibility into attack surface

Digging into the Importance of Prioritization

Most organizations recognize that a prioritization plan is necessary. Without a plan, you'll face a dizzying amount of work, essentially making near-random judgments on what to fix first.

But an inability to effectively prioritize vulnerabilities means more than miscalculating how to spend your time, of course.

The Ponemon report reveals that 91% of organizations have experienced at least one damaging cyberattack over the last two years, resulting in significant downtime for the business, forfeiture of sensitive customer or employee information, theft of business-critical information, or fines and/or lawsuits due to non-compliance.

91%
of organizations experienced one cyberattack in the last two years

> **Still, recognizing the need for a plan and adequately devising one isn't the same thing.**

It's common for organizations to prioritize based on the lowest-hanging fruit. These workflows aren't inherently bad, but tend to overlook the true risks to your business.
For example:

- Remediating every vulnerability with a CVSS score of 7.0 or higher means you'll address some of the most critical vulnerabilities, but you'll soon be overwhelmed by the sheer volume of risks. If everything is a five-alarm fire, nothing is.
- Fixing what's easiest to patch drives real (and sometimes imagined) productivity, but misses the point: Easiest doesn't mean likeliest.
- Tackling the newest threat first can seem advantageous, particularly when CISOs and CIOs are under pressure from customers, investors or the media. But, getting caught up in reactionary work means stripping time and resources from other, often more important, work. And the newest threat usually doesn't equal the likeliest.

It's not all doom and gloom, though. You can build an effective prioritization plan – one that takes an informed, risk-centric view, and protects your organization from cyberattack.

A 3-Step Approach to Vulnerability Management

A successful prioritization plan will help you answer: Where should we prioritize based on risk? Which vulnerabilities are likeliest to be exploited? What should we fix first?

We've pulled together this three-step approach to help drive better decision-making, reduce complexity, and ultimately mitigate cyber risks.

1. **Start with vulnerabilities that are being actively exploited.** All vulnerabilities represent weaknesses, but exploitable vulnerabilities reflect real risk. Use a vulnerability management tool that incorporates threat intelligence, so you can address vulnerabilities that have exploits known to be available in the wild.

2. **Remediate vulnerabilities most likely to be exploited in the next few weeks.** Predictive models provide insight into the likelihood that a given vulnerability will be exploited based on certain characteristics (e.g., past threat patterns, NVD data as well as threat intelligence).

3. **Address assets tagged as critical.** Critical assets are worth attending to since an attack on them could have broad-scale impacts on the business. Assets open to the internet should be of particular concern.

Next Steps

The above approach will dramatically reduce the list of vulnerabilities you need to remediate, enabling you to gain structure and control in a pursuit that's otherwise charged with unknowns.

And when you're able to prioritize vulnerabilities, you'll have time to focus on even more strategic initiatives, like evolving toward a comprehensive Cyber Exposure program – across technologies, systems, and departments.

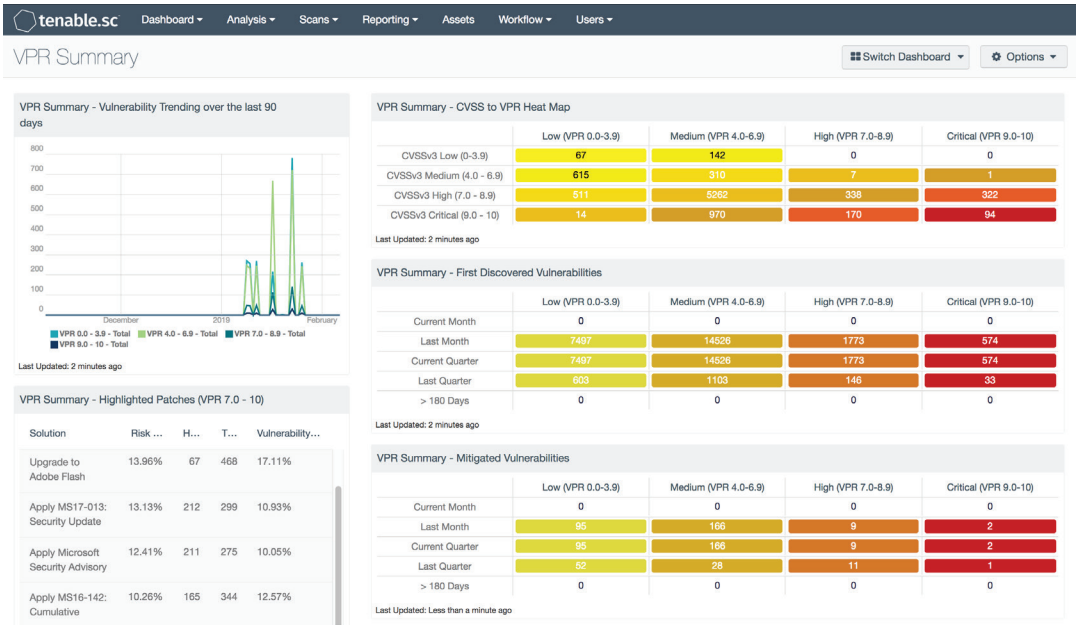
With more predictability, less guesswork, and fewer ad hoc practices, your organization is better protected – and your job is saner, more rewarding, and dare we say it, fun again.

> **Tenable is taking vulnerability management to a whole-new level with Predictive Prioritization.**

WHAT SHOULD WE FIX FIRST?

Predictive Prioritization combines data and threat intelligence across multiple sources, and analyzes them all with a data science algorithm that uses machine learning to anticipate the probability of a vulnerability being leveraged by threat actors.

You get real-time insights to help you differentiate between real and theoretical risks, and a prioritized, custom list of which vulnerabilities to remediate first – resulting in a massive 97% reduction in the number of critical and high vulnerabilities you need to patch.



Focus on the true risks to your business.

Predictive Prioritization is avaliable now for cloud or on-premises deployment:

- Cloud: **Start free trial of Tenable.io**
- On-premises: **Request demo of Tenable.sc**

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

04/12/19 V03