tenable

SOLUTION OVERVIEW

RISK-BASED VULNERABILITY MANAGEMENT

Business challenge

Thanks to the rise of digital transformation, everything is now connected. Cloud and containers, operational technology and mobile devices – something new is popping up every day and it all must be included in the scope of your vulnerability management program. But, your growing attack surface makes the vulnerability overload worse. You know the problem: The more broadly, frequently and thoroughly you assess all your assets (which is the right thing to do), the faster you bury yourself and others under a mountain of vulnerabilities and misconfigurations. It's tempting to do less and just meet the compliance requirements. But, less is less, and it puts your organization at risk. Old approaches to vulnerability management are no longer sufficient. You need a way to identify all the vulnerabilities – and then winnow them down to a manageable quantity.

Solution

A proactive, risk-driven approach delivers comprehensive, continuous visibility and informs technical and business decisions. You need a solution that helps you:

Assess all your assets for vulnerabilities and misconfigurations continuously

Measure the vulnerability's risk to your business using threat intelligence and asset criticality

Predict which vulnerabilities present the most risk to your organization, so you know what to focus on first

Deliver risk-based information to business owners

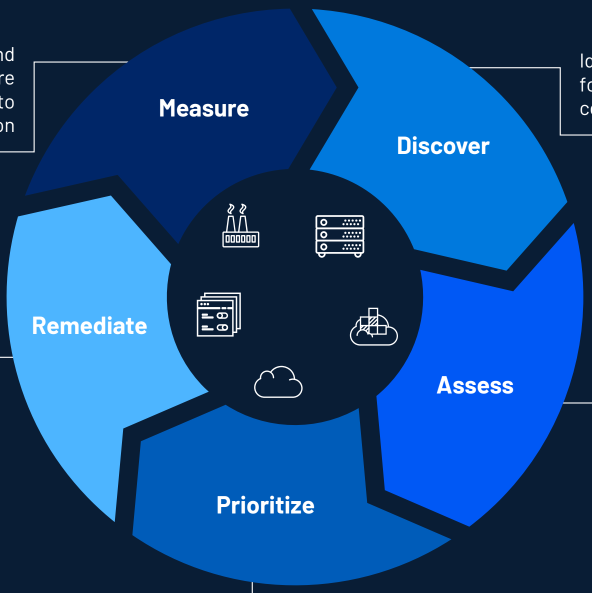
This is risk-based vulnerability management, and it's not optional.

Value

Risk-based VM is the process of reducing vulnerabilities across your attack surface by prioritizing remediation efforts based on risk. With the Tenable Risk-Based Vulnerability Management Solution, you get:

- Full visibility into the converged attack surface: Get the broadest coverage and most thorough assessment of the traditional and modern assets in your attack surface.
- Dynamic and continuous assessment: Assess new and transitory assets as soon as they become active (e.g., integrate assessment into your CI/CD pipeline).
- Prioritization powered by machine learning: Know exactly which vulnerabilities to remediate to reduce risk. Our machine learning models automatically combine vulnerability severity data with threat intelligence and asset criticality to predict each vulnerability's impact on your organization.
- Tailored dashboards: Communicate business system risk, not vulnerability counts, to business stakeholders.

THE CYBER EXPOSURE LIFECYCLE FOR RISK-BASED VULNERABILITY MANAGEMENT



Calculate, communicate and compare Cyber Exposure and key maturity metrics to drive risk reduction

Identify and map every asset for visibility across and computing environment

Prioritize which exposures to fix first to apply the appropriate remediation or mitigation technique

Understand the state of all assets, including vulnerabilities, misconfigurations and other health indicators

Understand exposures in context, to prioritize remediation based on asset criticality, threat context and vulnerability severity

Figure 1. The 5-Step Cyber Exposure Lifecycle for Risk-Based Vulnerability Management

How it works

The Tenable Risk-Based Vulnerability Management Solution is built upon the five-step Cyber Exposure Lifecycle, which helps you continuously improve your security program (see Figure 1). Applying the solution via this lifecycle will help you get complete visibility into your attack surface and prioritize your remediation efforts based on the 3% of vulnerabilities that pose the greatest risk to your organization – reducing your cyber risk over time.

Get started with risk-based vulnerability management today

Upgrade from traditional VM to managing and measuring cyber risk with the Tenable Risk-Based Vulnerability Management Solution. Visit our solution webpage to learn how we can help you evaluate your current VM capabilities, assess gaps in your program and develop a plan to begin adopting risk-based VM best practices today.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

tenable®