tenable

YOUR ANSWER TO THE VULNERABILITY OVERLOAD PROBLEM:

RISK-BASED VULNERABILITY MANAGEMENT

Overwhelmed by the number of new vulnerabilities across your expanding attack surface? You're not alone.

Here's the problem: Legacy vulnerability management tools are no match for today's complex IT landscape – which includes cloud, mobile, web, IoT and OT assets. They fail to deliver a unified, real-time view of your attack surface. And more frustratingly, they flood you with vulnerability data, forcing you into technical details – instead of telling you which ones pose the greatest risk to your organization. It's time to change the conversation.

With risk-based vulnerability management, you'll not only gain foundational visibility into your entire business environment, but you'll also know exactly which vulnerabilities to fix first. Use machine learning to go beyond CVSS ratings and unveil the real threat potential of every vulnerability. Prioritize remediation based on whether the vulnerability is being exploited in the wild and how critical the asset is to the business.

Here's a quick look at how risk-based vulnerability management differs from legacy vulnerability management.

"By 2020, organizations that use the risk-based vulnerability management method will suffer from **80% fewer breaches**."
– Gartner[1]

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. • 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.) • When the press reports a new headline-grabbing vulnerability, staff scrambles to determine if they are susceptible, and if so, to address it. Reactive is insufficient because scramble drills are error-prone and often ignore other high-risk vulnerabilities.	• Provides utmost focus – optimized, automated processes identify and address the few high-risk vulnerabilities. • Staff adheres to optimized and automated processes to identify and address the few truly high-risk vulnerabilities. These processes minimize error-prone, unplanned work.

Proactive or reactive – the choice is yours

Risk-based vulnerability management removes the guesswork. Instead of wondering which vulnerabilities to tackle first, you'll have clear answers.

If you're tired of wading through the never-ending vulnerability backlog, take the next step toward risk-based vulnerability management today. Visit the webpage to get started.

[1]Gartner, *A Guide to Choosing a Vulnerability Assessment Solution*, Prateek Bhajanka, Mitchell Schneider, Craig Lawson, April 3, 2019.