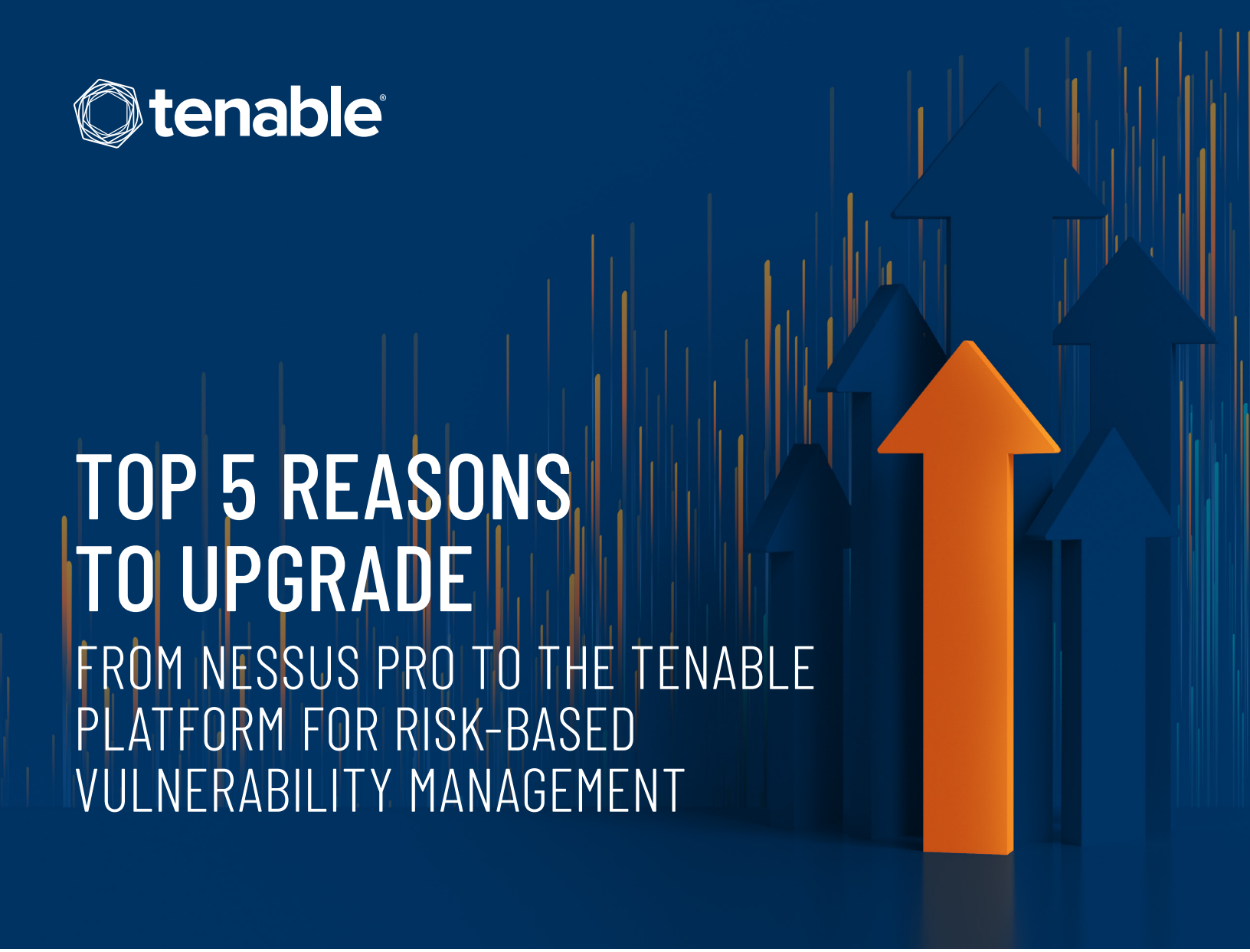


TOP 5 REASONS TO UPGRADE

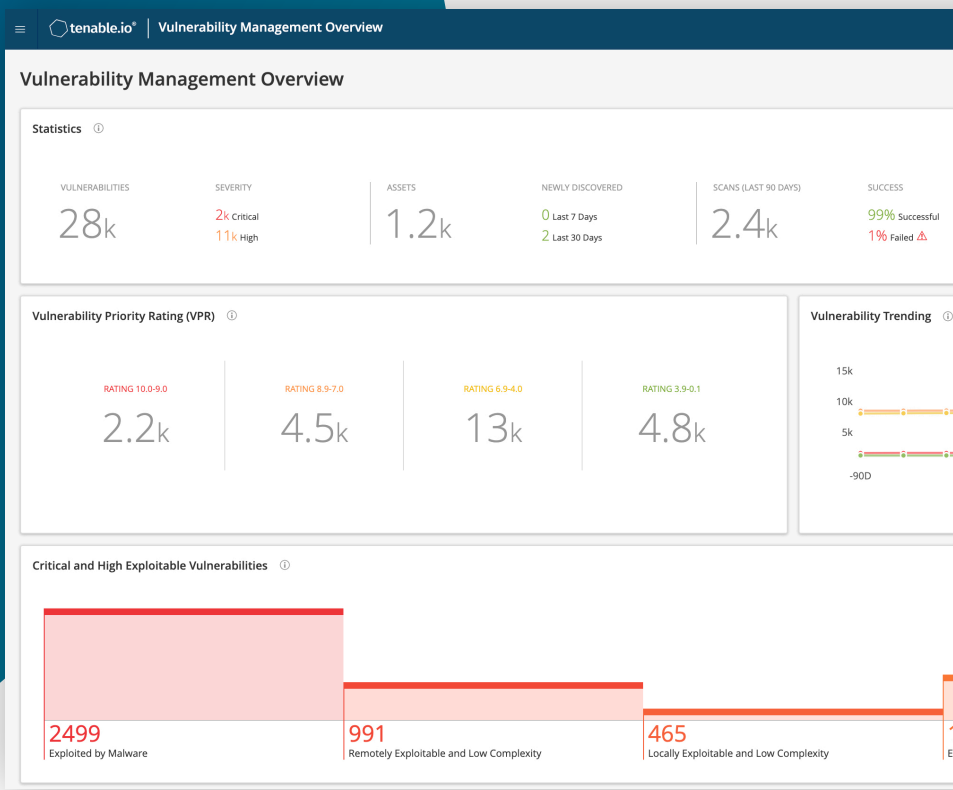
FROM NESSUS PRO TO THE TENABLE PLATFORM FOR RISK-BASED VULNERABILITY MANAGEMENT

Nessus® Professional customers already have one of the most comprehensive vulnerability assessment (VA) tools on the market. But even the best VA tools weren't designed to handle the modern attack surface and its growing number of threats. Instead, their visibility is limited to traditional IT environments, so they completely miss any vulnerabilities that are present in the most dynamic aspects of the modern attack surface, including cloud, operational technology and container environments.

VA tools are also limited to using Common Vulnerability Scoring System (CVSS) base scores to determine which vulnerabilities to remediate. CVSS is an imperfect system that can bury your team with thousands more vulnerabilities each month than they can possibly manage and lead them to waste the majority of their time chasing after vulnerabilities that don't pose much business risk.

To solve these challenges, you need to evolve your VA program to one that takes a risk-based approach to vulnerability management (VM).

Upgrading from Nessus Professional to the full Tenable platform will enable you to:



1. Modernize your security program

You need more than a monthly list of vulnerabilities that just continues to grow. The Tenable platform enables you to actively manage vulnerabilities, so you can reduce the greatest amount of risk with the least amount of effort. Prioritize the assets and vulnerabilities that matter most, effectively manage risk by taking the appropriate action, and measure key performance indicators (KPIs) to understand and communicate the value of your risk-based VM program.

2. See your entire attack surface

Passing an audit isn't the same as being secure. You need to upgrade from infrequent scans of only those network assets that fall within audit scope to continuous assessments of all known assets. In addition, you need to immediately discover and assess any new assets as soon as they appear on your network. By continuously addressing your entire attack surface, the Tenable platform eliminates the blind spots that plague legacy tools and enables security teams to discover and assess all their vulnerabilities together.

3. Predict risk based on full vulnerability context

CVSS base scores, alone, won't help you determine what needs to be fixed. The Tenable platform bolsters CVSS base scores with extensive contextual data, including the criticality of asset(s) affected, threat and exploit intelligence and a prediction of which vulnerabilities are likely to be exploited in the next 30 days. By understanding the true business risk of each vulnerability, you can focus your remediation efforts on what matters most.

4. Act quickly and confidently

Save time and gain confidence with automated analyses. The Tenable platform employs machine learning automation to continuously correlate, process and analyze petabytes of security data, so you always have the most current analysis of the evolving threat landscape. This helps security teams know they're fixing the right things, instead of wasting valuable time manually analyzing every vulnerability to determine its level of risk.

5. Measure using clear success metrics

The number of patches you deploy is meaningless if you're fixing the wrong things. The Tenable platform enables you to measure the team's success by tracking risk exposure for critical assets over time, so you'll know you're actually making a difference. And with robust, configurable reporting, you'll be able to effectively communicate the team's efficiency to a wide range of stakeholders and gain and maintain management's confidence in your abilities.