Focus on security risks that matter most
Drive faster vulnerability response,
from detection to remediation.

Closing the remediation gap remains a key challenge for today’s security organizations. The typical enterprise attack surface is expanding in scope and constantly targeted with a growing number of vulnerabilities that threaten the security of critical business assets. Security and IT teams must not only be aligned in their workflows, but also possess the data to prioritize vulnerabilities based on business context when deciding which vulnerabilities to remediate first.

6 key components for a vulnerability response platform

1. Identify assets and summarize vulnerabilities by assets/services
2. Prioritize vulnerabilities by criticality of affected services
3. Group and assign vulnerabilities based on ownership
4. Remediate vulnerabilities via patching
5. Validate remediation with a re-scan
6. Report on progress and closed vulnerabilities

How we solve this better, together
ServiceNow and Tenable™ combine powerful vulnerability management insights with a security orchestration, automation, and response engine to quickly and effectively remediate security weaknesses. This integrated solution enables customers to have a single response platform for continuous visibility and critical context across the enterprise. It allows for decisive actions and granular remediation process control to protect your organization from risk, exposure, and loss.

Access Vulnerability Response Integration with Tenable in the ServiceNow Store

1 “Persistent Vulnerabilities, Their Causes and the Path Forward,” Tenable Research, June 2020
2 The Rise of the Business-Aligned Security Executive, a commissioned study conducted by Forrester Consulting on behalf of Tenable, August 2020
3 Costs and Consequences of Gaps in Vulnerability Response, an independent survey conducted by Ponemon Institute LLC on behalf of ServiceNow, October 2019