

RISK-BASED VULNERABILITY MANAGEMENT FOR FEDERAL AGENCIES

Cloud computing continues to evolve and revolutionize the way government agencies operate. Federal agencies face escalating pressure to manage security and compliance and adopt a Zero Trust security policy. Agencies need a unified solution to deliver continuous visibility, critical context and actionable insight in order to protect complex networks and sensitive data, while adhering to compliance standards and regulations.

Tenable has over 20 years of experience working with government agencies and commercial organizations. Our FedRAMP authorized solutions provide a unified security and compliance platform that gives federal agencies the necessary visibility to maintain control and security of their complex network.

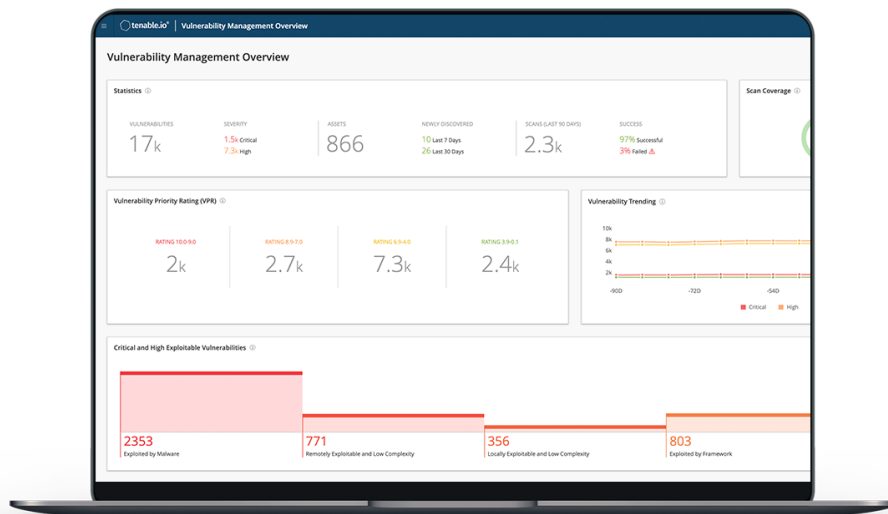


Figure 1:

Tenable.io provides an accurate view of assets and vulnerabilities across your environment to help you prioritize remediation based on actual cyber risk.



KEY BENEFITS

- **FedRAMP** authorized risk based vulnerability management platform
- **Prioritize Remediation** and speed up incident response with easy to understand vulnerability risk scores.
- **Automate Processes** with a fully documented API and pre-built integrations.
- **Secure Your Remote Workforce.** Extend visibility into the expanded attack surface and quickly assess new, unprotected assets like laptops, phones and more
- **Eliminate Blind Spots** with coverage for more than 60K vulnerabilities and more than 109,000 plugins across applications and operating systems.

FEDRAMP AUTHORIZED

Tenable.io received FedRAMP authorization in 2021, after completing a lengthy and rigorous testing process. Tenable.io's authorization streamlines the assessment and approval process for federal agencies' and accelerates the road to secure cloud adoption. Tenable.io WAS is also FedRAMP authorized. Tenable.io is also on the approved products list of the General Services Administration's (GSA) Continuous Diagnostics & Mitigation (CDM) program.

ZERO TRUST SECURITY

Zero Trust is a multi-year journey, but there are several key principles to help accelerate your strategy. Access control, lateral movement detection and foundational cyber hygiene practices are essential in the world of Zero Trust. Tenable can help you build on your Risk-based Vulnerability Management platform to jumpstart your Zero Trust journey. For more information visit: <https://www.tenable.com/solutions/zero-trust>

TOTAL CLOUD PROTECTION

Tenable.io provides the security necessary for federal customers to move their workloads to the cloud and ensure they are compliant across cloud platforms. The federal government has some of the highest standards for cloud security in the world. FedRAMP authorization validates Tenable.io's security controls meet the stringent standards of US Federal agencies to protect government systems, sensitive data and critical infrastructure. Tenable.io also has a fully documented API and pre-built integrations to help you leverage other existing investments to streamline workflows.

COMPREHENSIVE VISIBILITY

Tenable.io's FedRAMP uses a diverse array of sensors to continuously gather and analyze security and vulnerability data. You get a real-time, continuous view of all your assets- both known and previously unknown. Centrally managed and self-updating, Tenable.io leverage Nessus sensors, a mix of active scanners, lightweight agents and passive network monitoring to maximize scan coverage. You get a complete view of your attack surface and security and compliance posture with Tenable.io's web-based UI.

SINGLE PANE OF GLASS VIEW

Eliminate complexity from managing multiple, siloed solutions, with full visibility of IT, cloud and web application vulnerabilities in a single platform. Integrated with Tenable Web Application Security (WAS), you can view vulnerable web app components and custom code vulnerabilities alongside your IT and cloud assets.

VULNERABILITY PRIORITIZATION

Tenable.io combines vulnerability data, threat intelligence and data science to give you easy to understand risk scores to quickly assess risk and know which vulnerabilities to fix first.

PROTECT SENSITIVE DATA AND CRITICAL INFRASTRUCTURE

Tenable.io incorporates industry leading threat intelligence from the Tenable Research team to strengthen our national cybersecurity program. The Tenable Research Team delivers world-class Cyber Exposure intelligence, data science insights, alerts and zero day discoveries. Tenable.io also uses Tenable's Exposure.ai technology to continuously analyze over 20 trillion aspects of threat, vulnerability and asset information with machine learning algorithms to predict critical exposure points before they can be leveraged in an attack.

For More Information: Please visit tenable.com

Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact

