tenable | Data Sheet

Tenable One for Government

The only FedRAMP authorized exposure management platform

Get ahead of attackers

If you're a threat actor, you don't honor security silos. You look for any weakness to exploit and move laterally. Yet the tools we rely on to secure the attack surface remain focused on individual technologies: cloud, identity, IT, OT, IoT, applications — and generate a tremendous amount of noise. They lack the critical 'attacker perspective' — a cross domain view of asset, identity and risk relationships that enable every breach; and more importantly, the impact on the agency, be it revenue, data sovereignty, compliance or other critical measurement.

As the only FedRAMP authorized end-to-end exposure management platform, Tenable One for Government radically unifies security visibility, insight and action across the attack surface. It equips agencies to isolate and eradicate priority cyber exposures from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. With Tenable One for Government, agencies can distinguish which risk combinations constitute true exposure from a sea of noisy findings. The result is greater productivity from existing staff, and more informed investments that help optimize overall security posture and compliance.

Key benefits

- Easily communicate risk posture to leadership, business units, and teams.
- Measurably reduce cyber exposures while demonstrating compliance to industry standards and regulations such as NIST, CISA BOD mandates, Executive Orders and more.
- Consolidate tools and prioritize investments where they have the greatest impact.
- Optimize productivity, reduce staff churn, and scale limited resources and expertise.
- Accelerate zero trust with foundational visibility into all assets, users and vulnerabilities.
- FedRAMP authorized and CDM approved.

A unified platform for federal agencies

As malicious cyberattacks on our government's infrastructure increase in number, impact and sophistication, federal agencies must manage cyber risk amid scattered products, siloed views and disjointed teams. That's where Tenable One comes in. Tenable One for Government is FedRAMP moderate authorized, providing a singular platform built to solve the central challenge of modern security: a deeply divided approach to seeing and doing battle against cyber risk.

Unify visibility

Bring agency views of cyber risk across the attack surface together as one, exposing the gaps that leave you vulnerable to attack across all types of assets and pathways.

Unify insight

Analyze cyber risk context and insights from across the attack surface as one, connecting dots to identify the true exposures threatening your agency.

Unify action

Unite agency leaders and security teams to do battle as one, mobilizing all organizational resources to find and fix exposures with the highest likelihood of attack and business impact.

Unify visibility

Discover the complete attack surface

Eliminate blind spots with comprehensive discovery of your attack surface, including externally and internally facing assets: cloud, IT, OT, IoT, containers, Kubernetes, applications, and unseen assets — as well as human and machine identities.

Identify asset and identity-related risks

Assess your assets and identities and gain a comprehensive view of the three varieties of risk that enable every breach — vulnerabilities, misconfigurations and excess privileges — on prem and across all your clouds.

Unify your asset inventory

See the assets and identities across your end-to-end attack surface in one central view, along with deep asset intelligence, including asset configuration details, weaknesses, tagging, Asset Criticality Rating (ACR), overall Asset Exposure Score (AES), and more.

Unify insight

Normalize risk scoring across domains

Leverage a consistent approach to measure risk across risk types and asset classes. A Vulnerability Priority Rating (VPR) assesses static and dynamic variables in the changing threat landscape, including availability of exploit code, and frequency of use by attackers to constantly adapt risk scores. VPR is combined with ACR, to calculate an overall AES for each asset, enabling teams to quickly assess which assets pose the greatest risk to the agency for prioritized remediation.

Unify action

Get business-aligned views of exposure

Global and custom exposure cards within Lumin Exposure View enable focused security efforts by providing a clear, business-aligned view of security posture for the overall agency, by domain, or by any logical grouping of assets. For example, agencies can build custom exposure cards for a critical business service or process, or by vendor, such as device manufacturer. A Cyber Exposure Score (CES) aggregates the individual AES scores for all assets in an exposure card, providing a tailored quantification of security posture.

Track trends and optimize investments

Trend Views, SLA tracking, and Tag Performance help answer critical questions, such as:

- How has our security posture changed over time?
- What domains or functional areas require more investment?
- Are we meeting our remediation commitments?

This enables better communication and strategic alignment of objectives and budget spend with stakeholders and teams.

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at tenable.com.

Contact Us

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

COPYRIGHT 2024 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, NESSUS, LUMIN, ASSURE, AND THE TENABLE LOGO ARE REGISTERED TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.