tenable | Data Sheet

Tenable One Exposure Management Platform

The only all-enterprise 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 organization, be it revenue, data sovereignty, compliance or other critical measurement. As the world's leading AI-powered exposure management platform, Tenable One radically unifies security visibility, insight and action across the attack surface. It equips modern organizations to isolate and eradicate priority cyber exposures from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. With Tenable One, organizations 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.

Win with one

Tenable One is 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 enterprise 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 business value, reputation and trust.

Unify action

Unite business 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, unseen assets, as well as assets discovered by other security tools — and human and machine identities.

Identify asset and identity-related risks

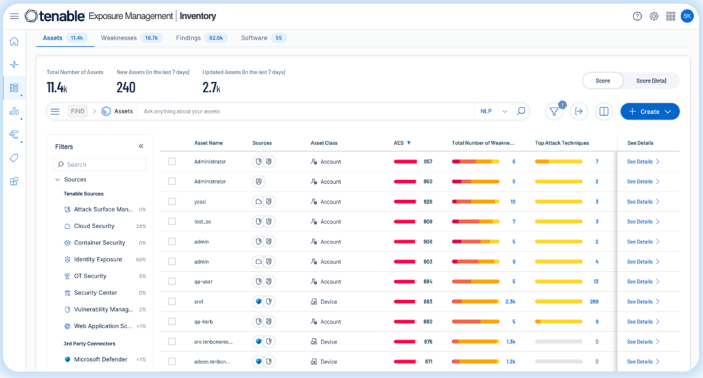
Assess your assets and identities and gain a comprehensive view of the three varieties of risk that enable every breach — vulnerabilities, misconfigurations and excess privileges — on prem and across all of your cloud platforms.

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), related attack paths, and more.

Unify exposure data for complete risk context

Seamlessly integrate data across your security tool ecosystem — including vulnerability management, cloud security, endpoint security, OT security, application security, CMDBs, and more — alongside native Tenable findings to gain a truly unified view of assets and exposures. This comprehensive approach enables full risk context, helping you prioritize what matters most and act with confidence.



“Being able to see our security exposure under one common view is very important. Tenable One helps us consolidate expensive point solutions and gain better comprehensive visibility across our attack surface under a single pane of glass. The reporting capability in Tenable One is a business enabler, as well. Whether communicating our cybersecurity posture to the board or generating a detailed action plan for the team, we can push the ‘easy button’ to deliver reports suitable for any audience.”

Deputy CISO,
Fortune 500 Enterprise

Unify insight

Normalize risk scoring across domains

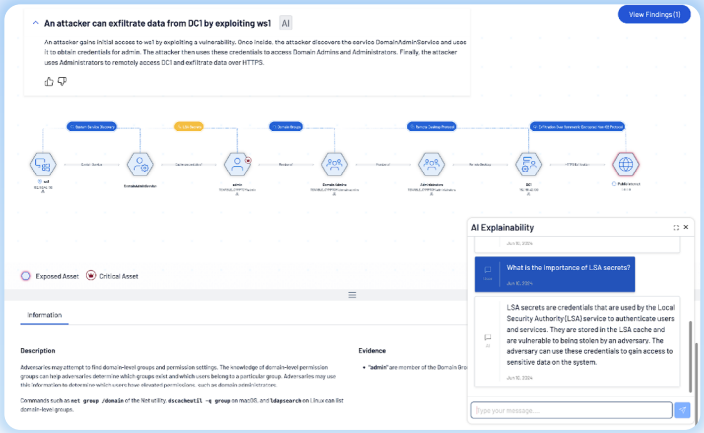
Leverage a consistent approach to measure risk across risk types and asset classes. A Vulnerability Priority Rating (VPR) assesses static and dynamic variables in the changing threat landscape, including availability of exploit code and frequency of use by attackers to constantly adapt risk scores. VPR 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 organization for prioritized remediation.

Prioritize attack paths leading to crown jewels

Attack path analysis provides a detailed understanding of asset, identity and risk relationships which can be exploited by attackers to compromise crown jewel assets — assets with high potential for material impact on the organization. See a prioritized list of attack paths, and easily search for common attack path signatures used in high profile breaches (e.g., SolarWinds), see specific MITRE techniques and get clear explanations for each step with generative AI and natural language query.

Scale remediation with choke points

Rather than investigate and remediate every finding or each step in an attack path, quickly assess choke point details with remediation guidance. With visibility into attack paths and choke points, you can see which remediation will remove the most potential attack paths leading to crown jewels, reducing unnecessary noise which leads to churn and reduced productivity.



Unify action

Get business-aligned views of exposure

Global and custom exposure cards within Exposure View enable focused security efforts by providing a clear, business-aligned view of security posture for the overall organization, by domain, or by any logical grouping of assets. For example, organizations can build custom exposure cards for a critical business service or process, or by vendor, such as a 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.

Analyze and communicate exposure risk

Tenable One dashboards offer a unified view of your organization's exposure by combining native Tenable insights with data from third-party security tools. This integrated view allows security teams to track, analyze, and communicate cross-domain risks across the attack surface. With Tenable One dashboards, customers can:

- Leverage pre-built dashboards for best-practice insights.
- Use a widget library to create customized dashboards for any use case or audience.
- Build custom widgets to meet unique needs.

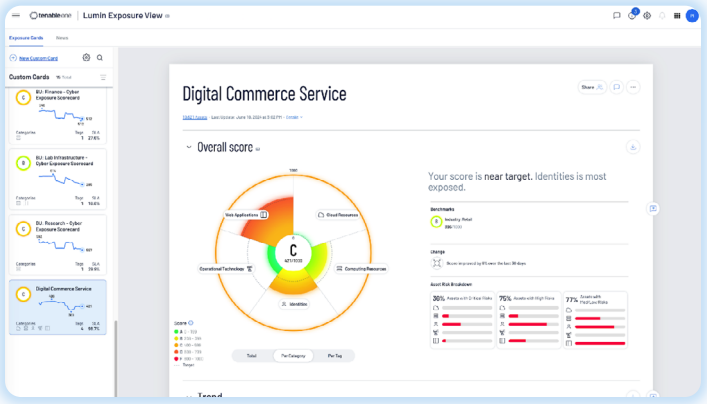
This enables better communication and strategic alignment of objectives and budget spend with stakeholders and teams.

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 more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us

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

COPYRIGHT 2025 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.

051225