



## 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 only end-to-end 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 risks 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.

## Key benefits

- Easily communicate risk posture to the board, business units, and teams.
- Measurably reduce cyber exposures while demonstrating compliance.
- Consolidate tools and prioritize investments where they have the greatest impact.
- Optimize productivity, reduce staff churn, and scale limited resources and expertise.



# Unify visibility

## Discover the complete attack surface

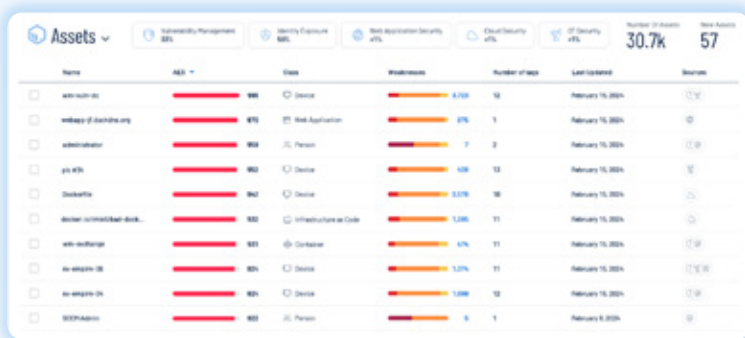
Eliminate blind spots with comprehensive discovery of your attack surface, including externally and internally facing assets: cloud, IT, OT, IoT, containers, Kubernetes, applications, and unseen assets — as well as human and machine identities.

## 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), related attack paths, and more.



Name	AES	Class	Weaknesses	Number of tags	Last scanned	Actions
www.example.com	98%	Device	2,128	12	February 15, 2024	🔍
webapp1.example.org	85%	Web Application	15%	1	February 15, 2024	🔍
admin@corp.com	95%	Person	7	2	February 15, 2024	🔍
ip:10.0.0.1	90%	Device	108	12	February 15, 2024	🔍
dbserver1	92%	Device	2,278	18	February 15, 2024	🔍
docker://localhost:8080	88%	Infrastructure as Code	1,100	11	February 15, 2024	🔍
api-server-01	91%	Container	14%	11	February 15, 2024	🔍
server-02	89%	Device	1,174	11	February 15, 2024	🔍
server-03	93%	Device	1,088	12	February 15, 2024	🔍
SSHAdmin	90%	Person	6	1	February 8, 2024	🔍

“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 and 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 access choke points details with remediation guidance. With visibility into attack paths and choke points, security staff 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

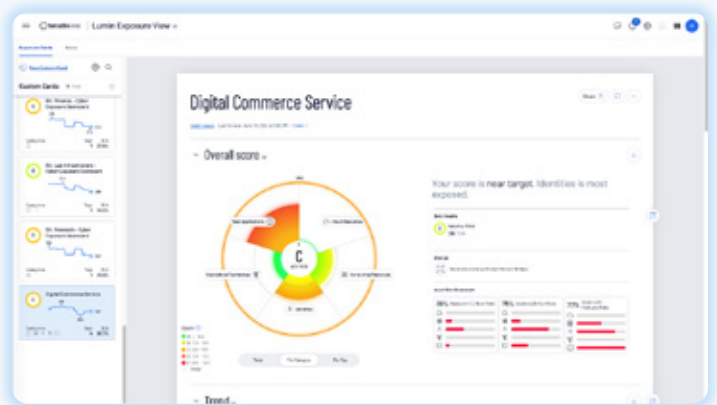
Global and custom exposure cards within Lumin Exposure View enable focused security efforts by providing a clear, business-aligned view of security posture for the overall organization, by domain, or by any logical grouping of assets. For example, organizations can build custom exposure cards for a critical business service or process, or by vendor, such as 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 more than 44,000 customers around the globe.