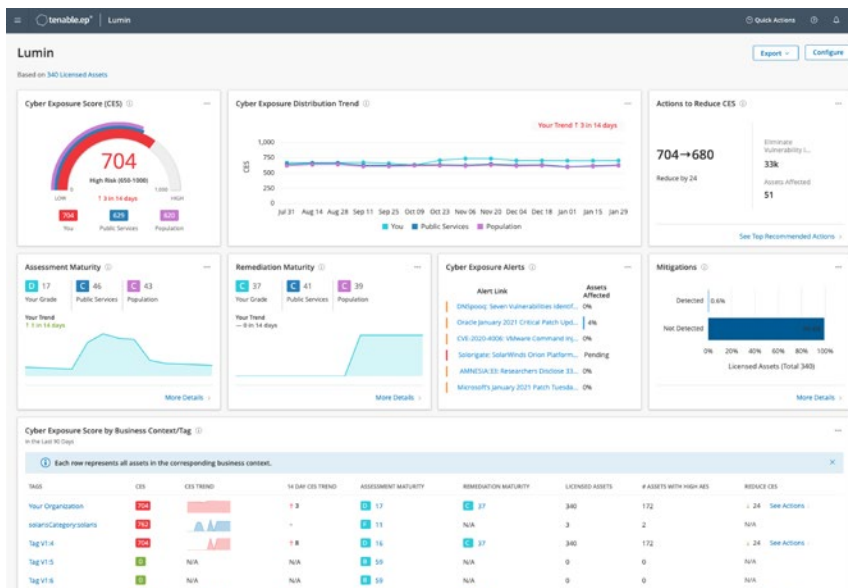


# THE TENABLE EXPOSURE PLATFORM

## SEE EVERYTHING. ACT TO ADDRESS RISK. ALL IN A SINGLE PRODUCT.

Tenable.ep provides complete and continuous visibility into your cyber risks in a single, unified platform. For the first time, you can identify every asset and exposure, predict which vulnerabilities are most likely to be exploited on your critical assets, and act to address critical risks and improve process maturity to secure your organization. All without the need to purchase separate products and manage different licensing models.

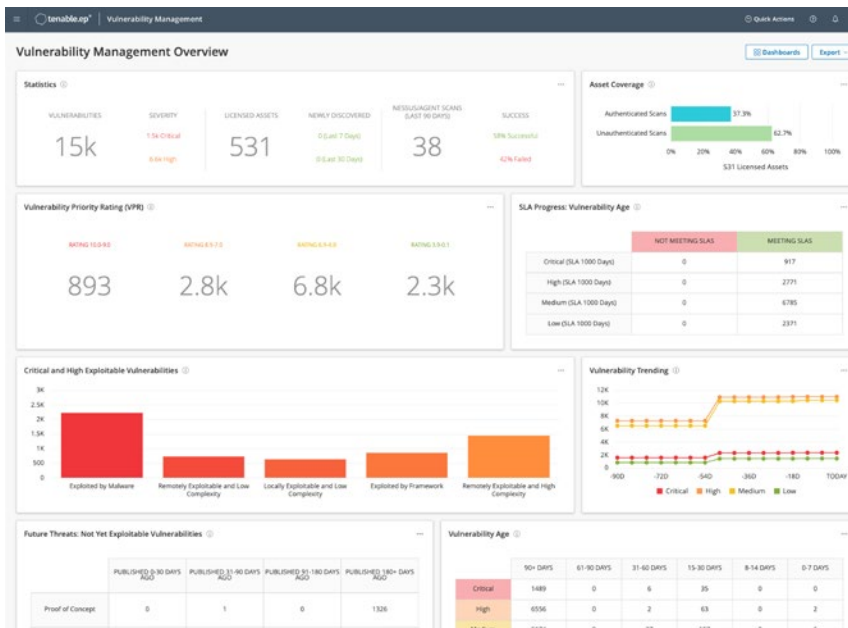
Tenable.ep combines Tenable.io Vulnerability Management, Tenable.io Web Application Scanning, Tenable.cs, Tenable.ad and Tenable Lumin – all in a single platform. Take advantage of a single, flexible asset-based licensing model for simple procurement and easy deployment. Get a unified, risk-based view of all your vulnerability data in a single dashboard to accurately prioritize the vulnerabilities and remediations that matter most. Gain insights into how you are performing on your mission to reduce cyber risk over time. And measure the maturity of your organization's security processes to understand problem areas and improve efficiency.



Tenable.ep provides an objective measure of cyber risk across your organization and enables you to benchmark risk against industry peers.

## KEY BENEFITS

- Deliver Unified Visibility**  
 Eliminate blind spots to see your entire attack surface – including IT assets, cloud services, Active Directory domains, operational technology (OT) devices, modern web apps and containers.
- Understand Cyber Risk**  
 Provide an objective measure of cyber risk across the organization to make more informed decisions.
- Improve Effectiveness**  
 Identify areas of process improvement by comparing your cyber risk and vulnerability management maturity metrics to industry peers.
- Prioritize Security Issues**  
 Reduce the number of vulnerabilities requiring immediate attention by up to 97% with Predictive Prioritization.
- Flexible Licensing**  
 Allocate product licenses according to your unique attack surface needs, and modify that allocation whenever necessary or desired.



Tenable.ep enables you to see and assess all assets and vulnerabilities from across your attack surface – including IT, cloud, container, and web apps – in a single, unified view.

# KEY CAPABILITIES

## Flexible Asset-Based Licensing

Tenable.ep is managed by a single license that simplifies the definition of an asset to help streamline operations. Whether it's a web application, a cloud instance, an Active Directory user, a container image, or a physical server, each asset counts exactly the same based on the unique Tenable.ep licensing model. This model is extremely flexible and enables you to allocate licenses according to your specific needs, and modify that allocation as your attack surface evolves.

## Comprehensive Assessment Options

Tenable.ep is built on Nessus technology and leverages active scanners, web application scanners, agents, passive network monitoring, and cloud connectors to help maximize scan coverage across your infrastructure and reduce vulnerability blind spots. This mix of data sensor types helps you track and assess both known and unknown assets and their vulnerabilities, including hard-to-scan assets like laptops and sensitive systems like industrial control systems.

## Secure Cloud Infrastructure

Continuously discover and assess cloud resources without the need to install agents, configure a scan or manage credentials. Detect security issues quickly as new vulnerabilities are disclosed and as your cloud environment changes with instances spinning up and down. Assess and document compliance to industry standards and established best practices such as CIS, PCI, GDPR. Take advantage of over 1,800 policies across 20 standards for comprehensive assessment. You can also create custom policies based on your individual needs.

## Secure Infrastructure as Code

Assess Infrastructure as Code (IaC) templates, including Terraform, AWS CloudFormation, Azure Resource Manager and Kubernetes, for policy violations. Integrate cloud infrastructure security into the DevOps pipeline to prevent security issues from reaching production. Quickly remediate IaC misconfigurations directly in development tools to enforce policies in both build-time and runtime. Identify discrepancies between IaC and your running cloud Environment to prevent cloud posture drift.

## Automated Web Application Scanning

With the scarcity of application security professionals, it's important to find solutions that offer automation to help alleviate the lack of security resources. Tenable.ep allows you to simply and rapidly assess all of your web applications with a highly automated solution that reduces your manual work effort. Gain visibility into OWASP Top 10 and web app component vulnerabilities, and provide detailed remediation instructions to developers.

## Kubernetes & Container Security

Gain visibility into the secure posture of your container images and infrastructure. Integrate security testing of new container images and Kubernetes configurations into DevOps pipelines to ensure new builds and IaC are compliant with enterprise policies. View vulnerability data, package inventories and misconfigurations of all your container images and Kubernetes infrastructure. Sync container images from third-party registries to continuously assess them for newly discovered vulnerabilities. Keep Kubernetes deployments secure and prevent configuration drift.

## Simplified Risk-Based Vulnerability Management

Through a modern interface with intuitive dashboard visualizations, Tenable.ep makes common tasks, such as configuring scans, running an assessment, and analyzing results, easier than ever. Pre-defined scan templates and configuration audit checks that follow best practices frameworks, such as CIS and DISA STIG, help you protect your organization with a fraction of the effort otherwise needed. Customize your reporting and analysis with pre-configured, out-of-the-box dashboards or quickly build your own from a blank canvas to meet organizational needs.

## Vulnerability Prioritization Based on Actual Risk

Tenable.ep prioritizes vulnerabilities based on the probability that they will be leveraged in an attack by combining over 150 data sources, including Tenable and third-party vulnerability and threat data. A proprietary machine learning algorithm is used to identify vulnerabilities with the highest likelihood of exploitability to help you focus first on the security issues that matter most to your organization.

## Secure Active Directory to Disrupt Attacks

Proactively discover and prioritize weaknesses within your existing Active Directory domains and reduce your exposure with step-by-step remediation guidance. Continuously monitor and detect Active Directory attacks like Golden Ticket, DCShadow, brute force, password spraying, DCSync and more. Securing your Active Directory can help stop attackers in their tracks, eliminate their potential movements and ensure that fewer breaches result in escalated privileges, lateral movement or malware execution.

## Remediation Guidance Based on Actual Risk

Tenable.ep provides security teams with a list of the top recommended actions that reduce the most cyber exposure, to translate business decisions on risk appetite to technical guidance for teams to take action. For additional information, teams can drill down into specific vulnerabilities or assets for business and risk context to enable more effective remediation.

## Calculate and Communicate Cyber Exposure

Tenable.ep provides an objective measure of cyber risk via the Cyber Exposure Score (CES), which combines vulnerability data with other risk indicators, such as threat intelligence and asset criticality. The score is automatically generated through machine learning algorithms that factor in the likelihood of vulnerability exploitability and the business criticality of the impacted asset. CES can be applied to any group of assets, from a single asset to all assets across the entire organization, for detailed analysis and decision-making.

## Process Maturity Metrics

Tenable.ep provides key Assessment and Remediation Maturity metrics to help improve program effectiveness and cyber hygiene. The product provides detailed analysis of your organization's assessment frequency, assessment depth, remediation responsiveness and remediation coverage to highlight shortcomings, benchmark against peers, and identify actionable recommendations to improve your scores.

## External and Internal Benchmarking

Tenable.ep enables organizations to benchmark themselves against industry peers and internal operational groups to quickly identify shortcomings and strengths. The product benchmarks a number of key metrics, such as CES, Assessment Maturity and Remediation Maturity, based on industry and overall averages to analyze how organizations compare. Tenable.ep benchmarking is based on the industry's most extensive vulnerability intelligence, processing over 20 trillion aspects of threat, vulnerability and asset data and coupled with data science to provide comprehensive and accurate insights.

## Pre-Built Integrations and a Documented API and Integrated SDK

Tenable.ep has pre-built integrations available for popular credential management, SIEM, ticketing systems and other complementary solutions, so you can easily build an efficient vulnerability management process. A complete listing can be found here: <https://www.tenable.com/partners/technology>. Additionally, you can easily create your own integrations to Tenable.ep by leveraging a fully documented API set and SDK. There is no extra cost to use these tools to maximize the value of your vulnerability data.

## SLA with Uptime Guarantee

Tenable provides the vulnerability management industry's first and only uptime guarantee through a robust service level agreement (SLA) for Tenable.ep. Service credits are offered if the SLA is not met, just like leading cloud vendors, such as Amazon Web Services.

## Backed by Tenable Research

Tenable.ep is backed by Tenable Research, delivering world class Cyber Exposure intelligence, data science insights, alerts, and security advisories. Frequent updates from Tenable Research ensure the latest vulnerability checks, zero-day research, and configuration benchmarks are immediately available to help you secure your organization.

---

For More Information: Please visit [tenable.com](https://tenable.com)

Contact Us: Please email us at [sales@tenable.com](mailto:sales@tenable.com) or visit [tenable.com/contact](https://tenable.com/contact)

