

# Tenable Product Newsletter

## November 2025

Greetings! Check out our November newsletter to learn about the latest product and research updates, upcoming and on-demand webinars and educational content — all to help you get more value from your Tenable solutions.

## Tenable One

### What's new in Tenable One: October 2025 release

This month's release delivers greater visibility, faster analysis, and more flexibility across APA and Inventory to help you manage risk with ease.

- APA enhanced public APIs: We've improved our public APIs with a higher chunk limit and standardized naming conventions for smoother integrations and a more consistent experience.
- Inventory export: Easily export asset and finding information to CSV or JSON, so it's simpler to share insights and collaborate across teams.
- APA new filters: Analyze paths and techniques more efficiently with new filtering options, including MITRE ID and "Archived by User," for faster, more focused investigations.
- Create tickets in inventory findings: Drive action across all your assets in Tenable One by creating a direct link between security findings and workflows to improve collaboration and accelerate response times.

[See all platform enhancements.](#)

### Tenable is named a Leader in the first-ever Gartner® Magic Quadrant™ for Exposure Assessment Platforms

We believe Tenable's [recognition as a Leader](#), positioned highest in Ability to Execute and furthest in Completeness of Vision among all vendors evaluated, is validation of the path we've forged together with our customers. Together, we're redefining exposure management. This exciting report comes on the heels of both the [IDC MarketScape: Worldwide Exposure Management 2025 Vendor Assessment](#) and [The Forrester Wave™: Unified Vulnerability Management, Q3 2025](#). Tenable is the only vendor recognized as a Leader across all three of these trusted industry reports.

# Tenable Cloud Security

Reminder: Tenable Cloud Security requires that you log in to view [documentation](#) and release notes. To try/see the product, contact your account manager or request a [demo](#).

## Accelerate your cloud security maturity!

- **Now launched:** [Tenable Cloud Vulnerability Management](#)! This new offering, part of Tenable One, delivers foundational risk prevention and container security for hybrid environments, granting vulnerability management stakeholders key capabilities to:
  - Achieve an agentless inventory of all cloud virtual machines, images and containers
  - Unify vulnerability risk visibility across on-premises and multi-cloud environments
  - Receive clear remediation steps for closing risk while laying the foundation for a holistic exposure management program tomorrow[Tenable Cloud Vulnerability Management](#) extends the power of Tenable's leading vulnerability management expertise directly into the cloud for consistent security controls across your entire attack surface.
- **New, actionable use cases** to accelerate your cloud security program:
  - [Enforce least privilege across cloud identities](#)
  - [Mitigate the blast radius of vulnerabilities](#)
- **New Tenable research/accolades:**
  - New AI discovery: [7 novel AI vulnerabilities in ChatGPT](#)
  - New insights [brief](#) from our *State of the Cloud and AI Security* [research](#)
  - [Named CTEM Leader](#) in *Latio's 2025 Cloud Security Market Report*

## Console

- **New finding insights widgets:** See risk and response at a glance. Get sharper visibility into your cloud risk posture with new widgets for findings, trending, mean time to resolve (MTTR), and resolved findings. Quickly spot patterns, track progress, and measure response efficiency, all from your dashboard. These new measurement tools equip you to better assess and quantify your cloud security program's progress and response efficiency.
- **Smarter, custom dashboards for deeper, side-by-side insights:** Go beyond static views. Apply granular filters to dashboard widgets, further customization of your dashboards to address your specific needs. Add the same widget multiple times with different filters to instantly reveal insights such as severity trends, without navigating away.
- **Bulk resource labeling:** Organize at scale in seconds. Save time and maintain a clean cloud inventory. Apply one or more custom labels to multiple resources at once, like tagging all Production EC2 instances in a single action, for faster organization, enriched context, and more efficient reporting.

These features contribute to an ever-more tailored solution, giving you the flexibility to secure your dynamic cloud environment while meeting your operational needs.

## Data

- **Snowflake data scanning:** Find sensitive data fast, now in Snowflake. Tenable Cloud Security now supports inventory and data protection for Snowflake, scanning the platform to detect and classify sensitive data, and give visibility into where critical data lives and if it's at risk. Reduce your exposure across this popular cloud data platform. Learn more in the Snowflake FAQ in the Documentation.

## Workload

- **Smarter Linux vulnerability detection:** No more noise. Tenable now improves Linux vulnerability detection by ignoring unused kernel versions left after upgrades. Expect fewer unnecessary findings and a clearer picture of the real risks affecting your Linux workloads.

## Identity

- **IAM access visibility:** Spot high-risk resources fast. The IAM Access Level column in Inventory now covers both Azure and AWS. See the highest (maximum) access level any principal has to a resource across your multicloud environment, quickly identify publicly or externally exposed resources, and reduce the risk of over-permissioned accounts.

## Upcoming changes

- **New network scanning:** We're excited to inform all Tenable Cloud Security users that, starting in December, a powerful new network scanner capability will be available, activated by default. This feature improves your cloud visibility by actively verifying which resources are truly reachable from the internet. It also helps prioritize verified risks more effectively and reduce false positives, so your teams can focus on what truly matters. No further configuration needed. Find results under Inventory > Network Endpoints. To opt out, please go to Settings > Cloud Security > Network > Scanner.

# Tenable Vulnerability Management

## Accelerate your plugin deployment

Significantly speed up plugin testing and deployment using the new Accelerated Plugin Updates toggle in agent profiles. When enabled, your agents check in more frequently, about every 33 minutes, to rapidly detect changes to the "Select Plugin set from the last 30 days" scheduling setting. This allows you to quickly push the latest plugins to production systems to minimize deployment latency. For more information, see [documentation](#).

## Centralized management with scanner profiles

Streamline scanner management using new Scanner Profiles, mirroring the functionality of Agent Profiles. Access this feature on the Sensors page under the Scanners menu. Profiles enable you to centrally control:

- Disabling scanner software version updates
- Pinning the scanner software version
- Configuring declarative plugin scheduling options

This control simplifies maintenance and ensures consistency across your deployment. Note that Nessus scanners version 10.10.0 and above support this feature. For details, see the [Release Note](#) and [User Guide](#).

## Nessus

### Tenable Nessus 10.10 now available

We released Tenable Nessus 10.10, which includes a new global scan timeout setting so you can define a maximum duration for a host scan for greater control over scan windows. See the [release notes](#) for more details on new features and performance enhancements.

Additionally, Terrascan has been removed from all standalone Nessus products. It is no longer supported. Refer to the [Tenable Nessus Terrascan End-of-Service FAQ](#) for more information.

## Tenable Security Center

### What's new in Tenable Security Center 6.7

See your environment more clearly and act faster on what matters most. This release delivers a modern, intuitive experience that improves usability, scalability, and efficiency across your operations.

*Here's what's new:*

- **Explore – Assets (Preview):** Get a [modern view of your assets](#) with advanced filtering and improved navigation that helps you identify risks faster.
- **Triggered Agent Scanning:** [Automate Tenable Agent scans](#) based on conditions you define, so you can catch vulnerabilities sooner and respond confidently.
- **Credential Verification Scan Policy:** Quickly validate Windows and Unix credential pairs with a [built-in template](#) that confirms authentication success.
- **Performance and Reporting Enhancements:** Experience faster scan ingestion, faster reporting, and improved backend performance that keeps pace with your team.

*Before you upgrade:* Tenable Security Center 6.7 supports upgrades from version 6.3.0 and later. Hardware specifications are updated for this release. Systems below the new recommendations will still upgrade successfully, but performance may vary.

Upgrade now to take advantage of these improvements and keep your environment running at peak performance. [Read the release notes](#) or [upgrade now](#).

### Patches for Tenable Security Center

Address recent vulnerabilities by applying two security patches: 202509.2.1 (resolves Critical SimpleSAML CVEs) and 202509.1 (resolves High PostgreSQL CVEs). You need manual installation for both. The Software Updates feature is not compatible with these patches.

### Key requirements:

- *Compatibility:* Patch 202509.2.1 applies to SC 6.4 through 6.6. Patch 202509.1 applies to SC 6.5.1 and 6.6.0.

- *Prerequisite:* If you are on SC 6.5.0, you must first upgrade to 6.5.1.
- *Upgrade Note:* Patch 202509.2.1 may impact future SC upgrades. [See this KB article](#) for more information.

See the [Release Notes](#) and advisories ([TNS-2025-20](#) and [TNS-2025-18](#)) for full details and download the patches [here](#).

## Tenable Patch Management

### Tenable Patch Management now available in the cloud!

We're excited to announce that Tenable Patch Management is now available in the cloud. It's easily accessible through your Tenable Workspace. This version includes all the great features you've grown to love in the on-premises version of Tenable Patch Management.

**Please note:** if you're currently on an on-premises version of Tenable Patch Management and would like to migrate to the cloud version, please contact your account team.

See a list of third-party applications covered [here](#) and note that we are always adding more.

For more information, please read the Tenable [documentation](#) and [release notes](#).

## Tenable OT Security

### Fortify your CPS security posture with Tenable OT Security 4.4

The latest version of Tenable OT Security is now available, designed to give you a more integrated, efficient, and comprehensive view of your operational environment.

New features and enhancements in this release include:

- **Unified enterprise reporting for your exposure management program:** Sync OT asset tags directly to Tenable One and Tenable Security Center to enrich your enterprise-wide security workflows with critical OT context.
- **Reduced alert fatigue:** A [new Policy Violations dashboard](#) unifies disparate alerts into actionable insights to help you focus on your most critical exposures first.
- **Deep visibility for specialized environments:** Gain granular asset details on sensitive devices by importing PLC project files (starting with Rockwell Automation) without active queries. We've also added support for Foxboro DCS and VXLAN environments.
- **Streamlined workflows and sensor configuration:** A new workflow helps you easily [find and merge duplicate assets](#) for a more accurate inventory, while a simplified sensor configuration reduces deployment complexity.

[Review the full release notes](#) to learn more about what's new and how to upgrade.

## Tenable Identity Exposure

### Tenable Identity Exposure (SaaS) v3.106 available now

With this release, we're strengthening our ability to surface the identity hygiene issues most likely to enable privilege abuse. The enhanced Password Weaknesses Indicator of Exposure

now delivers deeper analysis and clearer guidance, so your teams can move faster from discovery to risk reduction.

For full details, please review the release notes:

<https://docs.tenable.com/release-notes/Content/identity-exposure/saas/2025.htm>

## **Tenable Identity Exposure (On-Prem) v3.77.14 now shipping**

To support customers running complex or regulated environments, this update focuses on resilience and operational integrity. Improvements to RabbitMQ recovery and identity telemetry processing help ensure consistent, dependable analysis, so teams always have the visibility they need to act with confidence.

Full release notes are [available here](#).

## **Tenable Ecosystem**

### **Tenable App for Microsoft Sentinel v3.1.1**

This update for the Tenable App for Microsoft Sentinel v3.1.1 includes:

- Azure Gov Cloud support with a dedicated link on the Data Connector UI for Azure Gov Cloud.
- Update to the Azure Sentinel Tenable Vulnerability Management Connector's Function Extension Bundle to the latest version.
- Improved performance and general bug fixes.

For more details, check out the Tenable [documentation](#) and visit the [Azure Marketplace](#) to download. Note: this application is also available via Microsoft Azure Gov Cloud marketplace.

## **Tenable Web Application Scanning**

### **Scan management just got smarter**

Two features, Scan by Tag and Add New Application, are now available. These fundamentally change how you manage and scan your web application portfolio, shifting your focus from individual scans to application-centric security.

- **Scan by Tag:** Now use your established tagging structure to define scan targets. You no longer need to manually enter or maintain extensive lists of web applications for every scan. By leveraging tags, you ensure consistency, making it easier to manage RBAC and efficiently filter and organize your scan data. Tags are configured in the "Settings" page.
- **Add New Application:** You have the power to define your applications manually or via the API before scanning them. This lets you define targets with greater precision, using criteria like port, protocol, or path in addition to the FQDN. By defining your application targets upfront, you ensure scan results consolidation into the correct, cumulative application data, for more accurate and meaningful findings.

For more details, please refer to the [Documentation](#) and the [Release Notes](#).

## Tenable Enclave Security

### **Tenable Enclave Security: Now available as a hosted FedRAMP High and IL5 offering**

Tenable Enclave Security is now available as a hosted and managed solution for high security environments, delivered in partnership with Tenable partner, UberEther. This new offering brings the power of Tenable Security Center and container security to the cloud with full FedRAMP High and DoD IL5 compliance.

For more information review the [UberEther FedRAMP Marketplace listing](#), or read our latest [blog](#) to learn why container security is critical in restricted environments.

## Tenable Connect

### **New in Tenable Connect: Innovators Roundtable**

We're excited to announce the launch of a new Tenable Connect group designed to foster a stronger community and enhance knowledge sharing: [Innovators Roundtable](#).

This group is dedicated to maximizing the value and success of our platform through active collaboration and the sharing of knowledge. A central hub for our most forward-thinking users to exchange cutting-edge resources, share best practices, and collectively push the boundaries of platform utilization.

Join the conversation! Join the groups today to learn and grow with your peers.

## Tenable Training and Product Education

### **No-cost course: Introduction to Tenable Web Application Scanning**

Learn how to secure your web applications with Tenable's new free, interactive on-demand course. You'll explore how Tenable Web App Scanning differs from traditional vulnerability management, discover its key capabilities and sensors, and see demos of scan setup and results analysis in Tenable Vulnerability Management and the Tenable One Exposure Management Platform. Available now on [Tenable University](#) for everyone!

## Tenable Webinars

Tune in for product updates, demos, how-to advice, and Q&A. See all upcoming live and on-demand webinars at <https://www.tenable.com/webinars>.

### **Live customer workshops:**

- [November 25 & 26, 2025 \(EMEA\)](#): Hands-on workshops on Tenable One Connectors.
- [December 3, 2025: From fundamentals to focus \(EMEA\)](#): Strengthening identity and access management in the Cloud.

## On-demand

- [Escape the patching cycle](#). A guide to autonomous risk-based patching.
- [Securing the future of AI in your enterprise](#). Policy frameworks that balance opportunity and oversight.
- [Beyond the endpoint: Exposure management that's proactive \(EMEA\)](#). Why endpoint-first vulnerability management isn't enough. (EMEA session)
- [Nov. 4, 2025: Nessus customer update](#). Web application scanning with Nessus Expert.
- [Nov. 4, 2025: Tenable OT Security customer update](#). What's new in Tenable OT Security 4.4 and a sneak peek of Tenable OT Security 4.5.
- [Nov. 5, 2025: Tenable Vulnerability Management customer update](#). Best practices for role-based access control (RBAC).
- [Nov. 5, 2025: Tenable Web App Scanning Management customer update](#). Using WAS to identify and assess AI in your web applications.
- [Nov. 6, 2025: Tenable One customer update](#). Third-party data in Tenable One.
- [Nov. 6, 2025: Tenable Security Center customer update](#). How to automate reporting and remediation with alerts.

## Customer Office Hours - Live

These are recurring ask-me-anything sessions for Tenable Security Center, Tenable Vulnerability Management, Tenable Cloud Security, Tenable Identity Exposure, and Tenable OT Security. Time zone-appropriate sessions are available for the Americas, Europe (including the Middle East and Africa), and Asia Pacific (APJ). Learn more and [register here](#).

## Tenable Research

### Research blog posts

- [Why Early Visibility Matters: Risk Lurks in the Vulnerability Disclosure Gaps](#)
- [F5 BIG-IP Breach: 44 CVEs That Need Your Attention Now](#)
- [Frequently Asked Questions About The August 2025 F5 Security Incident](#)
- [CVE-2025-61882: Frequently Asked Questions About Oracle E-Business Suite \(EBS\) Zero-Day and Associated Vulnerabilities](#)
- [Oracle October 2025 Critical Patch Update Addresses 170 CVEs](#)
- [Microsoft's October 2025 Patch Tuesday Addresses 167 CVEs \(CVE-2025-24990, CVE-2025-59230\)](#)
- [Tenable Discovers Critical Vulnerabilities in SimpleHelp Tool: CVE-2025-36727 and CVE-2025-36728](#)

### Content coverage highlights

- Almost 6,000 new [vulnerability plugins](#) published, including new detections for the recent F5 BIG-IP Breach!
- More than [90 new audits](#) delivered to customers!

# Documentation

[Read Tenable documentation.](#)