

Greetings! Check out our September 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.

NEW! Tenable AI Exposure

We have officially launched the [Tenable AI Exposure platform](#). This platform helps you see, secure and manage how your organization uses AI tools like ChatGPT Enterprise and Microsoft Copilot across your enterprise. Safeguard sensitive data, stop AI-driven attacks and establish governance for safe AI adoption.

Be among the first to try it! Learn more and sign up for the [private customer preview here](#).

Tenable One

August 2025 Release: This month's release delivers faster insights, broader coverage and greater control over your exposure data.

Release highlights:

- **Dashboard enhancements:** With daily data updates, new chart types and dedicated filters for CISA KEV and end-of-life software, Tenable One dashboards now make it easier to analyze specific risks, communicate impact and speed up response.
- **Tenable On-Prem Connector:** Install the Tenable On-Prem Connector to create a secure, encrypted connection to safely bring on-premises exposure data into Tenable One. Get the insights you need without putting your network at risk.
- **Asset information source display:** Deduplication in Tenable One is key to ensuring a clean, accurate view of each asset, without redundant information from multiple sources. With this release, the asset details screen now clearly displays the source that populates findings and property information, so your team fully understands and trusts asset data.
- **Dynamic asset tagging:** Define dynamic rule-based criteria that automatically apply tags to all Tenable One data for easier customization and greater control over tagging rules. This improvement enables smarter segmentation, precise asset management and deeper analysis across the platform.

[Explore all platform enhancements](#)

Tenable Connect

Coming soon: Enhanced support case experience

We're excited to announce a new case creation and management experience. This release will streamline how you open and track cases while leveraging Generative AI to improve search and

help you find answers faster. Stay tuned for enablement resources posted within [Tenable Connect](#) to maximize this new functionality.

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](#).

Read all about it:

- **New Tenable white paper by Analyst IDC:** *“Bridging cloud security and exposure management for unified risk reduction.”* This commissioned piece explores the value of exposure management and Tenable strengths. [White paper](#) • [Blog](#)
- **Featuring fintech customer Snoop.** We are honored to share the Tenable story of Snoop, using CIEM and JIT to enforce least privilege. [Video](#) [Want to tell your Tenable story? Let your Tenable rep know. We’d love to capture it!]
- **Security alert:** Tenable Research detected a [supply chain attack](#) in certain Nx build system packages that [exfiltrated secrets to GitHub](#). GitHub has disabled the repos, yet compromised versions may persist. We’ve flagged any affected packages in your Tenable Console (Vulnerability ID: GHSA-cxm3-wv7p-598c). **Act now:** Update packages and rotate exposed secrets.

Platform:

- **Default Home and Favorite dashboards.** Set a default Home dashboard to see your most important security insights first, and mark frequently used dashboards as Favorites for instant access.

Benefit: These usability updates let you focus on what matters most in your workflow so you can work faster, make informed decisions and keep pace as the platform adapts to your needs.

- **Japanese language support is here.** You can now navigate the full Tenable Cloud Security Console in Japanese (switch via your profile menu), and access our documentation portal in Japanese for a smoother, more localized experience.

Benefit: Japanese customers are the first to benefit from our new language infrastructure, designed to accelerate the rollout of additional languages. Watch this space!

CWP: Workload Protection

- **Clusters filter and column.** Identify vulnerable clusters and all related vulnerabilities more easily. (The column is hidden by default.)

- **Resolved filter.** In the Workload > Vulnerabilities table, quickly display only vulnerabilities marked as resolved.

Benefit: Get clear visibility into cluster-level risks and easily distinguish open from resolved issues to streamline vulnerability management and save time.

CSPM: New and Updated Security Best Practice Support

- Tenable now supports AWS Foundational Security Best Practices, CIS Azure 2.0, CIS Kubernetes 1.8 and CIS OpenShift 1.5.

Benefit: Stay ahead of evolving threats and strengthen your security posture across cloud and container environments. Up-to-date best practices simplify compliance, reduce risk and make it easier to consistently implement proven security controls.

DSPM: AWS RDS Support for Oracle

- Data protection scanning is now available for Oracle on AWS RDS, for both Enterprise and Standard license holders.

Benefit: Extend visibility into sensitive data stored in Oracle RDS to improve protection and compliance across more of your cloud database environments.

Tenable Identity Exposure

Tenable Identity Exposure uncovers Storm-0501's cloud identity threats:

Financially motivated threat actor [Storm-0501](#) is advancing cloud-based ransomware and hybrid identity compromises to move seamlessly between on-premises Active Directory (AD) and Microsoft Entra ID.

Tactics include **initial identity exploitation** that compromises AD and abuses non-human synced Global Admin accounts in Entra ID, along with **malicious persistence**, where they establish backdoors by adding rogue federated domains with tools like AADInternals to gain persistent access and impersonation capabilities.

Attacker tactic	How Tenable Identity Exposure prevents it
Initial compromise	Flags high-privilege, improperly synced Entra ID accounts from on-prem AD, a configuration Microsoft advises against .
MFA bypass	Identifies critical, privileged accounts missing MFA, one of the most exploited gaps in hybrid identity attacks.
Malicious persistence	Detects backdoor federated domains and anomalous signing certificates using multiple indicators of exposure (IOEs), including: Known Federated Domain Backdoor , Federation Signing Certificates Mismatch , Unusual Federation Certificate Validity , Federated Domains List for verification against legitimate IDPs.

Tenable Identity Exposure continuous monitoring of IoEs uncovers and aids remediation of critical identity risks before groups like Storm-0501 can exploit them.

See [Tenable Identity Exposure documentation](#).

Tenable Vulnerability Management

Streamline ACSC Essential 8 compliance with new dashboards

Simplify and strengthen your Essential 8 reporting with Tenable's new ASD Essential 8 dashboards. These dashboards take your risk-mitigation SLAs to the next level, giving you a clear, real-time view of progress toward ACSC Essential 8 compliance.

Quickly spot gaps, track patching and remediation efforts, and demonstrate measurable risk reduction. Monitor internet-facing assets, ensure critical applications are patched, and confidently report on SLA performance, all in one place.

Explore the resources to get started:

- [Applying Tenable's risk-based VM to the ACSC Essential 8](#)
- [ASD Essential 8 – Patch Applications dashboard](#)
- [ASD Essential 8 – Internet-Facing Assets dashboard](#)

Tenable Security Center

Critical security patch 202508.1 now available

Protect your Security Center deployment with the new patch 202508.1, which fixes critical third-party vulnerabilities in Apache, PHP and SQLite, including CVE-2025-23048, a critical Apache flaw. The update applies to versions 6.4 through 6.6 and must be installed manually. If you're running 6.5.0, upgrade to 6.5.1 before applying it.

For full details, see the [release notes](#), [security advisory](#), and [download the patch](#); this update will be included in future Security Center releases.

Tenable OT Security

What's new in Tenable OT Security 4.4

The latest version is now available. It introduces several new features and enhancements to improve visibility, streamline workflows, and expand coverage across your industrial environment.

- **OT asset tag data synchronization:** Asset tags you create in Tenable OT Security will sync with Tenable One and Tenable Security Center to integrate OT context directly into your enterprise-wide reporting and security workflows.
- **Policy violations dashboard:** A redesigned view aggregates disparate alerts and events (e.g. unauthorized access, configuration changes) into unified and actionable Policy Violations to significantly reduce alert fatigue so you can focus on remediating your most critical exposures.

- Check out this [guided demo](#) to see it in action!
- **PLC product file imports:** Import PLC project files (starting with Rockwell Automation) to enrich your asset inventory. This provides deep visibility on live or sensitive OT devices without performing active queries.
- **Merge assets:** A new workflow helps you find and merge duplicate asset entries for a cleaner and more accurate OT asset inventory.
- **Foxboro DCS support:** Gain visibility into Foxboro Distributed Control Systems to extend security monitoring into complex industrial environments.
- **VXLAN support:** Analyze network traffic within Virtual Extensible LANs (VXLAN) to monitor assets and activity in modern virtualized data centers.
- **Multi-interface sensor configuration:** A simplified workflow allows a single sensor to simultaneously listen on multiple network interfaces to reduce deployment time and complexity.

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

Tenable Nessus

Reminder: End of support for Terrascan in all Nessus versions

Tenable announced the End of Life for Terrascan in Nessus. The last day to download the affected product(s) is Sept. 30, 2025. Customers will receive continued support through the Last Date of Support. For more information, please refer to the [bulletin announcement](#).

Reminder: Nessus 10.9 is generally available

Nessus 10.9 introduces several key features to empower your security teams, including offline web application scanning in Nessus Expert. For more information, see the [Nessus 10.9 release notes](#) and [Nessus 10.9 User Guide](#). You can also view [this announcement](#) under Product Announcements in Tenable Connect.

Tenable Connect

Coming Soon: Enhanced Support Case Experience

We're excited to announce a new case creation and management experience. This release will streamline how you open and track cases while leveraging Generative AI to improve search and help you find answers faster. Stay tuned for enablement resources posted within Tenable Connect to maximize this new functionality

Tenable Training and Product Education

Connectors added to Tenable One Intro course

The updated *Introduction to Tenable One* course in Tenable University now shows you how to connect third-party security tools to the exposure management platform, to give you a unified view of risk across your entire attack surface. This no-cost training is open to customers, partners, prospects and the public. Start learning today at [Tenable University](#).

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

- [Oct 1, 2025: Beyond the endpoint: Exposure management that's proactive](#). *Why endpoint-first vulnerability management isn't enough.*
- [Oct. 7, 2025: Nessus customer update](#). *Troubleshooting common Nessus issues.*
- [Oct. 8, 2025: Tenable Vulnerability Management customer update](#). *Mastering asset tagging and introducing AI Aware.*
- [Oct. 9, 2025: Tenable One customer update](#). *Identity security in an exposure management program.*
- [Oct. 10, 2025: Tenable Security Center customer update](#). *In-depth guide to user roles and permissions.*

On-demand

- [September Tenable Nessus customer update](#): *From the ground up – building a custom scan policy in Nessus.*
- [September Tenable Vulnerability Management customer update](#): *Using Nessus agents in Tenable Vulnerability Management.*
- [September Tenable One customer update](#): *Introducing AI Exposure, and other topics.*
- [September Tenable Security Center customer update](#): *Answering the CISO – a guide to Assurance Report Cards.*
- [Ecosystem view of risk](#): *Integrate cloud security with your security stack.*

Customer Office Hours

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 Security Operations blog posts

- [Frequently Asked Questions About Chinese State-Sponsored Actors Compromising Global Networks](#)
- [CVE-2025-54135, CVE-2025-54136: Frequently Asked Questions About Vulnerabilities in Cursor IDE \(CurXecute and MCPoison\)](#)
- [Frequently Asked Questions About SonicWall Gen 7 Firewall Ransomware Activity](#)
- [CVE-2025-54987, CVE-2025-54948: Trend Micro Apex One Command Injection Zero-Days Exploited In The Wild](#)
- [CVE-2025-53786: Frequently Asked Questions About Microsoft Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability](#)
- [Microsoft's August 2025 Patch Tuesday Addresses 107 CVEs \(CVE-2025-53779\)](#)
- [CVE-2025-25256: Proof of Concept Released for Critical Fortinet FortiSIEM Command Injection Vulnerability](#)

- [CVE-2025-7775: Citrix NetScaler ADC and NetScaler Gateway Zero-Day Remote Code Execution Vulnerability Exploited in the Wild](#)

Research release highlights

- [Include/Exclude Path and Tenable Utils Unzip added to Log4j Detection](#)
- [Nutanix Prism v4 API Compatibility](#)
- [Excluding the SUSE Linux Snapshots directory from Language Library enumeration](#)

Content coverage highlights

- Almost 17,000 new [vulnerability plugins](#) published including new **AI Aware** detections!
- Over [25 new audits](#) delivered to customers!

Quick links

- [Join the Tenable Connect community](#)
- [Sign up for on-demand training](#)
- [Watch Tenable product education videos — more than 250 videos now available](#)
- [Check out all upcoming and on-demand Tenable webinars](#)

Read Tenable documentation:

- [Documentation RSS Feed](#)
- [Tenable Vulnerability Management User Guide](#)
- [Vulnerability Management Release Notes](#)
- [Tenable Web App Scanning User Guide](#)
- [Tenable Web App Scanning Release Notes](#)
- [Tenable Cloud Security User Guide](#)
- [Tenable Cloud Security Release Notes](#)
- [Tenable Identify Exposure User Guide](#)
- [Tenable Identify Exposure Release Notes](#)
- [Tenable Security Center Release Notes](#)
- [Tenable Security Center 6.5 User Guide](#)
- [Tenable OT Security Release Notes](#)
- [Tenable OT Security User Guide](#)
- [Tenable Attack Surface Management User Guide](#)
- [Exposure View User Guide](#)
- [Exposure View Release Notes](#)
- [Asset Inventory User Guide](#)
- [Asset Inventory Release Notes](#)
- [Attack Path Analysis User Guide](#)
- [Attack Path Analysis Release Notes](#)
- [Tenable Nessus Release Notes](#)
- [Tenable Nessus 10.8 User Guide](#)
- [Tenable Nessus Agents 10.8 User Guide](#)
- [Tenable Nessus Agents Release Notes](#)
- [Tenable Nessus Network Monitor 6.5 User Guide](#)
- [Tenable Nessus Network Monitor Release Notes](#)