Tenable One Adoption Roadmap

Quick Reference Guide

Last Revised: December 05, 2025

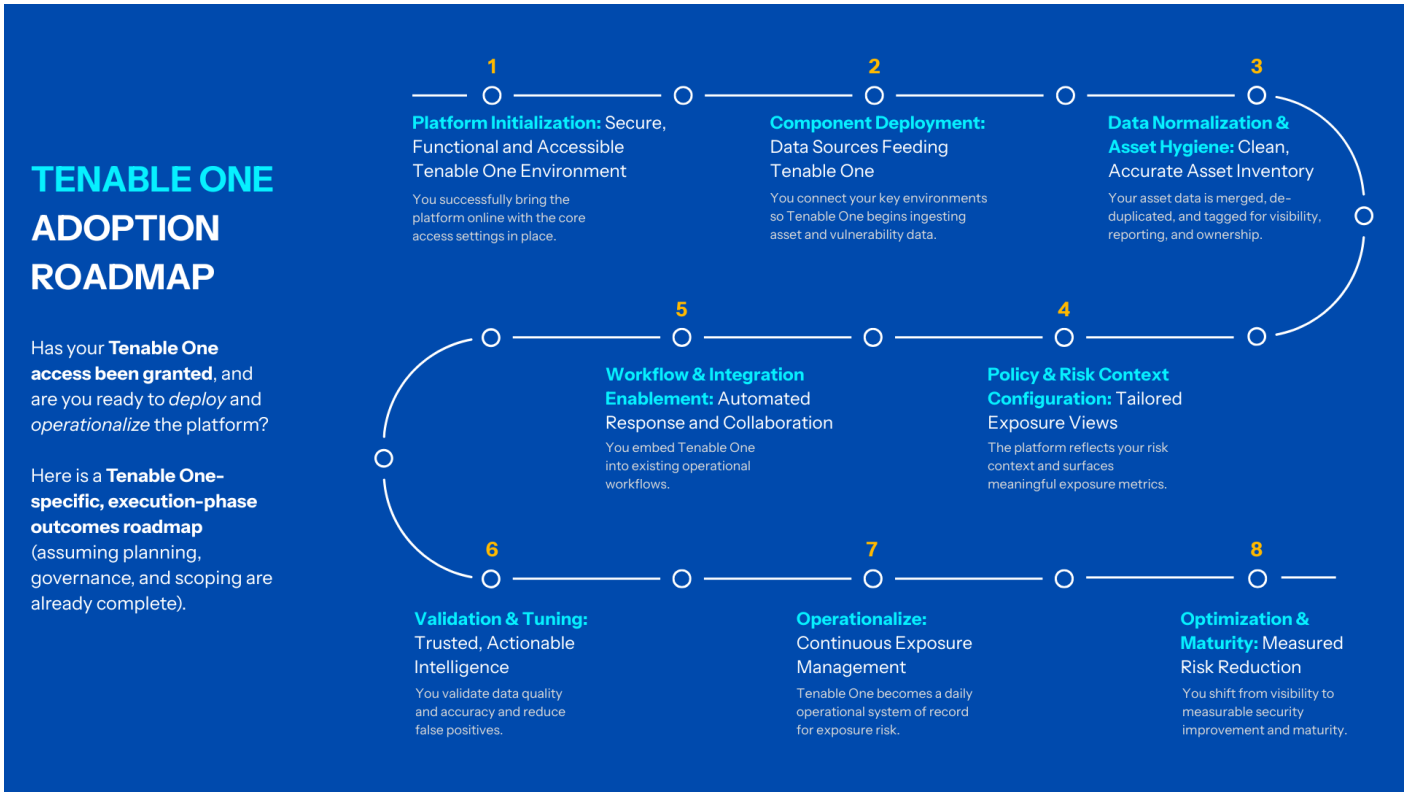
Table of Contents

Welcome to the Tenable One Adoption Roadmap

Last updated: December 05, 2025

The Tenable One Adoption Roadmap provides a repeatable, outcome-driven framework to help you successfully deploy, operationalize, and mature the Tenable One platform. This guide outlines eight key phases, each focused on a specific platform-level outcome that every customer experiences on their Tenable One journey.

> **Tip:** Click each step to view more information.



This roadmap scales across use cases and maturity levels, guiding you from initial platform activation through measurable risk reduction.

The Eight Phases of Adoption

This guide is broken into eight conceptual phases. Tenable recommends you approach them in order, as each phase builds the foundation for the next.

- **Phase 1: Platform Initialization** — Establish a secure, functional, and accessible Tenable One environment.
- **Phase 2: Component Deployment** — Connect your data sources to Tenable One.
- **Phase 3: Data Normalization and Asset Hygiene** — Create a clean and accurate asset inventory.
- **Phase 4: Policy and Risk Context Configuration** — Configure tailored exposure views.
- **Phase 5: Workflow and Integration Enablement** — Set up automated workflows with third-party integrations.
- **Phase 6: Validation and Tuning** — Achieve trustworthy and actionable vulnerability intelligence.
- **Phase 7: Operationalize**— Create repeatable operations that meet your exposure management needs.
- **Phase 8: Optimization and Maturity** — Optimize your exposure platform and achieve measurable risk reduction.

Before You Begin

This execution-phase roadmap assumes that your organization's initial planning, governance, and scoping are already complete. It also assumes your Tenable One access has been granted (one administrator has access at minimum) and you are ready to deploy and operationalize the platform.

What to do next:

Proceed to Phase 1: Platform Initialization.

Phase 1: Platform Initialization

Platform Initialization is the first phase of your Tenable One adoption. This phase focuses on bringing the platform online and establishing the core security, access, and structural settings for a functional and accessible environment.

Expected Outcomes

During this phase, you successfully bring the platform online with the core access settings in place. This includes:

- Validating that your platform is active and in the correct region. For more information, see Tenable Cloud Region Availability.
- Confirming administrator login credentials and configuring multi-factor authentication (MFA) and/or single sign-on (SSO) via SAML. For more information, see Configure Two-Factor Authentication and SAML.
- Creating and testing your user groups and role-based access control (RBAC) structure (for example, Admins, Analyst, Read-Only). For more information, see User Groups.
- Ensuring all licensed components (for example, Tenable Vulnerability Management, Tenable Cloud Security) are accessible under the **Workspace**. For more information, see View the Workspace Page.

Why This Is Important

Completing this phase ensures that your Tenable One environment is secure from the start, that user access is correctly governed by roles, and that your licensed components are visible and ready for configuration. This foundation is essential before ingesting data.

Verification

You can verify the success of this phase by confirming the following:

- At least one administrator and one standard user can successfully log in. For more information, see Log In to Tenable and Create a User Account.

- The **License Information** page reflects your expected asset allocation and deployed region. For more information, see License Information.
- Your expected components are visible under the **Workspace**. For more information, see View the Workspace Page.

> **Note:** Tenable OT Security and Tenable Identity Exposure require additional configuration before they are accessible in the **Workspace**. For more information, see Configure SAML Integration for Tenable One (Tenable OT Security and Access the Workspace (Tenable Identity Exposure).

What to do next:

Proceed to Phase 2: Component Deployment.

Phase 2: Component Deployment

Component deployment is the second phase of your Tenable One adoption. This phase focuses on connecting your key environments so Tenable Exposure Management can begin ingesting asset and vulnerability data from all your data sources.

Depending on the deployment resources at your disposal, you may choose to focus on achieving these outcomes sequentially or concurrently. You may also proceed to the next phase after just one or two outcomes are completed, and plan to return later to focus on another application.

Expected Outcomes

In this phase, you configure data sources to feed into Tenable Exposure Management. This includes connecting Tenable applications (components) and third-party connectors.

The expected outcomes include the following, depending on what applications your organization allocated licenses to:

- **Tenable Vulnerability Management** scans are configured, and assets and findings are syncing.
- **Legacy Tenable Cloud Security** is configured, with environments syncing their workloads.
- **Tenable Security Center** is configured and syncing asset and vulnerability data.
- **Tenable Web App Scanning** scans are configured, with web app data syncing.
- **Tenable Patch Management** is configured and syncing asset, risk context and patch data.
- **Tenable Attack Surface Management** domains are configured, with records syncing.
- **Tenable AI Exposure** is integrated and syncing enterprise AI LLMs (for example, Copilot or ChatGPT).
- **Tenable OT Security** is integrated and syncing OT asset data.
- **Tenable Identity Exposure** is integrated and syncing identity data.
- **Tenable Third-Party Data Connectors** are configured, with asset and risk data syncing.

> **Tip:** For more information on how to deploy each Tenable component, see the *Tenable One Platform Deployment Guide*.

Why This Is Important

This phase is critical for populating Tenable Exposure Management with comprehensive data from across your attack surface. This data ingestion is the foundation for all exposure analysis, attack path visualization, and reporting.

Verification

You can verify the success of this phase by confirming the following within at minimum 24 hours of component enablement:

> **Note:** Keep in mind that Tenable Exposure Management updates data using a specific cadence. For more information, see Data Timing.

- Assets appear in the Tenable Exposure Management views. For more information, see Assets.
- No errors are reported for third-party data connectors. For more information, see Connector Data Status.
- An initial exposure score and letter grade are generated. For more information, see Exposure View.
- Attack paths are beginning to populate. For more information, see Attack Path.

What to do next:

Proceed to Phase 3: Data Normalization and Asset Hygiene

Phase 3: Data Normalization and Asset Hygiene

Data normalization and asset hygiene is the third phase of your Tenable One adoption. This phase focuses on merging, de-duplicating, and tagging your asset data to create a clean, accurate, and searchable asset inventory.

Expected Outcomes

During this phase, Tenable Exposure Management processes your raw asset data to ensure accuracy and provide business context. The expected outcomes are:

- Asset tags are standardized and applied (for example, business unit, owner, or environment) for visibility and reporting.
- Asset tags are applied on QA and/or developer assets so they can be filtered in and out when needed.
- Asset coverage is validated against your expected inventory.

Why This Is Important

Clean and accurate asset data is essential for trustworthy reporting, effective prioritization, and clear asset ownership. This phase ensures that the data you see in Tenable One reflects your environment, allowing you to confidently build policies and workflows based on it.

Verification

You can verify the success of this phase by confirming the following:

- Asset coverage in Tenable One is near your expected inventory count. For more information, see Assets.
- Tagging is completed and visible in both Tenable Exposure Management and in the respective components (where applicable). For more information, see Manage Tags.

What to do next:

Proceed to Phase 4: Policy and Risk Context Configuration.

Phase 4: Policy and Risk Context Configuration

Policy and risk context configuration is the fourth phase of your Tenable One adoption. This phase focuses on tailoring the platform to reflect your organization's specific risk context and business priorities, enabling more meaningful exposure metrics.

Expected Outcomes

During this phase, you apply your business logic and risk appetite to the platform. The expected outcomes include:

- Exposure views are customized for priority areas (for example, Cloud, Identity, Internet-facing).
- Attack path analysis is returning valid paths based on your data.
- Exposure signals are customized for combination and identity risks.
- Visible benchmarking is configured to compare against industry peers or internal baselines.
- The exposure card SLA is set for each criticality level.
- Business context is added to identify critical assets, "crown jewels," and compliance domains.

Why This Is Important

This phase transforms Tenable Exposure Management from a data repository into a tailored risk management solution. By configuring policies and adding business context, you ensure the platform surfaces the most relevant and high-priority exposures, allowing your teams to focus on what matters most.

Verification

You can verify the success of this phase by confirming the following:

- Exposure cards, attack paths, and signals are visible, customized, and populated with data. For more information, see Exposure Card Library, Attack Path Dashboard, and Exposure Signals.

- Benchmarking is configured against the correct industry. For more information, see Configure Exposure View Page Settings.
- Contextual dashboards are created and accessible to each stakeholder group. For more information, see Analytics Dashboard.
- Where possible, the Asset Criticality Rating (ACR) is reviewed and configured for critical systems. For more information, see Edit Asset ACR.

What to do next:

Proceed to Phase 5: Workflow and Integration Enablement.

Phase 5: Workflow and Integration Enablement

Workflow and integration enablement is the fifth phase of your Tenable One adoption. This phase focuses on embedding Tenable One into your existing operational workflows to automate response and collaboration.

Expected Outcomes

During this phase, you connect Tenable One to your broader security and IT ecosystem. The expected outcomes include:

- Ticketing integrations (for example, ServiceNow or Jira) are operational and mapping fields correctly.
- Ownership and workflows for exposure signals are configured.
- Any additional integrations (for example, Splunk or other SIEMs) are active and functioning. For more information, see Tenable Technology Partners.

Why This Is Important

Integrating Tenable One with your existing tools, such as ticketing systems and SIEMs, is key to operationalizing exposure management. This phase ensures that prioritized findings are automatically routed to the correct teams for remediation, reducing manual effort and mean time to remediate (MTTR).

Verification

You can verify the success of this phase by confirming the following:

- Exposures assigned through a workflow automatically appear in the appropriate ticketing queue. For more information, see ServiceNow Integration Guide (PDF) or Jira Cloud Integration Guide (PDF).
- Ticket closure in your external system syncs back to Tenable One, updating the exposure status.

What to do next:

Proceed to Phase 6: Validation and Tuning.

Phase 6: Validation and Tuning

Validation and tuning is the sixth phase of your Tenable One adoption. This phase focuses on validating the data quality and accuracy within the platform and reducing noise to ensure you are receiving trusted, actionable intelligence.

Expected Outcomes

During this phase, you fine-tune the platform to align with your organization's specific environment and operational realities. The expected outcomes include:

- A sample of potentially known exposures is confirmed to be present in Tenable One.
- The exposure score trendline behaves predictably after an intentional remediation activity (in other words, the score improves).
- Potential false positives are tuned using recast or accept rules. For more information, see Recast Rules.
- Platform performance validation is complete, ensuring dashboards and queries load within expected timeframes.

Why This Is Important

This phase builds trust in the platform. By validating data, tuning potential false positives, and ensuring performance, you give your security and IT teams confidence that the information from Tenable One is accurate, reliable, and actionable.

Verification

You can verify the success of this phase by confirming the following:

- Your organization's internal procedures are used to validate that findings align with expected vulnerabilities.
- The exposure score trendline is growing, mapping days (or weeks/months) of change. For more information, see Exposure View and Remediation SLA.

> **Note:** Keep in mind that Tenable Exposure Management updates data using a specific cadence. For more information, see Data Timing.

What to do next:

Proceed to Phase 7: Operationalize.

Phase 7: Operationalize

Operationalization is the seventh phase of your Tenable One adoption. This phase focuses on making Tenable One a daily operational system of record for managing exposure risk across the organization.

Expected Outcomes

During this phase, you fully integrate Tenable One into your security program's regular cadence. The expected outcomes may include:

- A weekly or bi-weekly exposure review cadence is established.
- Roles are formally assigned for platform ownership, data validation, and reporting.
- A monthly executive exposure summary is automated and delivered.
- Key Performance Indicators (KPIs) are defined and tracked, for example:
    - Increased percentage of total assets covered.
    - Reduced percentage of critical exposure.
    - Improved Mean Time to Remediate (MTTR) for exposures.

Why This Is Important

This phase marks the transition from *implementing* Tenable One to *using* Tenable One. By establishing a regular operational cadence and defining clear KPIs, you create a sustainable and continuous exposure management program.

Verification

You can verify the success of this phase by confirming the following:

- Exposure reviews are documented in tickets or reports. For more information, see Analytics Dashboard.
- Regular trend reports show measurable improvement against your KPIs. For more information, see Exposure View.

- Attack paths are actively leveraged to inform and prioritize remediation. For more information, see Attack Path.

What to do next:

Proceed to Phase 8: Optimization and Maturity.

Phase 8: Optimization and Maturity

Optimization and maturity is the eighth and final phase of the Tenable One adoption roadmap. This phase focuses on shifting from day-to-day visibility to long-term, measurable security improvement and program maturity.

Expected Outcomes

During this phase, you leverage the full capabilities of Tenable One to drive strategic risk reduction. The expected outcomes include:

- Tenable One is used to set and drive exposure reduction goals across IT/OT, cloud, AI, and identity teams.
- Attack path reductions are measured over time.
- Remediation timelines (MTTR) demonstrably decrease quarter-over-quarter.
- Executive dashboards are used for board-level or compliance reporting.
- A periodic review of Tenable Exposure Management configurations is scheduled to ensure they remain aligned with business goals.

Why This Is Important

This phase represents a mature exposure management program. Your organization is no longer just finding and fixing vulnerabilities; you are proactively reducing risk, measuring improvement, and using platform insights to inform your overall security strategy.

Verification

You can verify the success of this phase by confirming the following:

- The Exposure Score trend demonstrates consistent, measurable advancement and out-performance of industry peers. For more information, see Exposure View.
- A quarterly maturity review is performed. For more information, see View Assessment Maturity Details and View Remediation Maturity Details.
- Platform insights are actively used to inform and adjust your exposure management strategy.

What to do next:

Review the adoption roadmap: Welcome to the Tenable One Adoption Roadmap.