Tenable Vulnerability Management 1.x User Guide

Last Revised: July 17, 2026

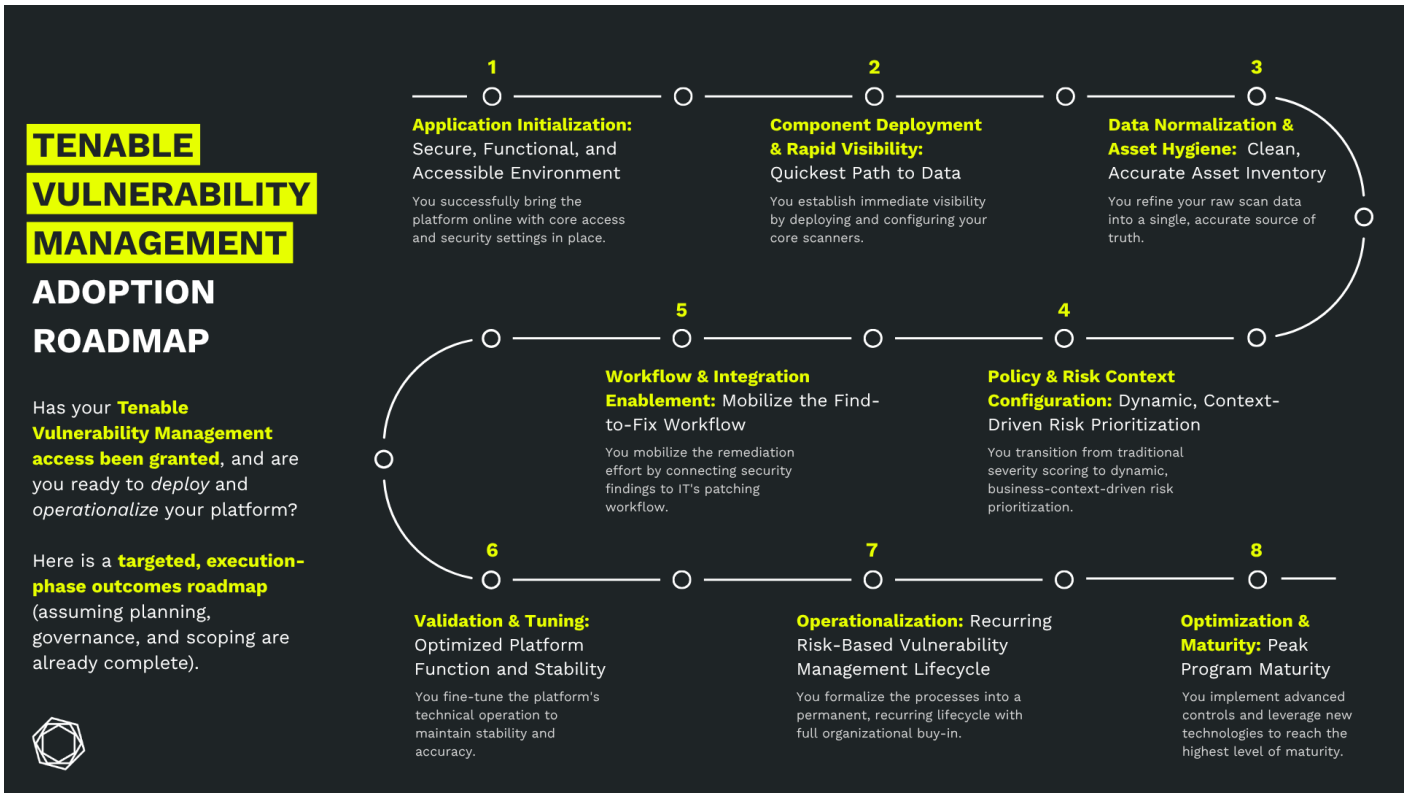
Table of Contents

Welcome to the Tenable Vulnerability Management Adoption Roadmap

Last updated: July 17, 2026

The *Tenable Vulnerability Management Adoption Roadmap* provides a repeatable, outcome-driven framework to help you successfully deploy, operationalize, and mature Tenable Vulnerability Management. This guide outlines eight key phases, each focused on a specific platform-level outcome that every customer experiences on their Tenable Vulnerability Management 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: Application Initialization – Bring the platform online and establish core security, access controls (like MFA and RBAC), and structural settings for a functional environment.
- Phase 2: Component Deployment & Rapid Visibility – Deploy core scanners to establish immediate visibility of external-facing assets and begin basic asset tagging.
- Phase 3: Data Normalization & Asset Hygiene – Refine raw scan data into an accurate source of truth by achieving high credentialed scan success rates and cleaning up your asset inventory.
- Phase 4: Policy & Risk Context Configuration – Transition from static severity scoring to dynamic, business-context-driven risk prioritization using Vulnerability Priority Rating (VPR) and–with Advanced tier of Tenable One–Asset Criticality Rating (ACR).
- Phase 5: Workflow & Integration Enablement – Connect security findings to your IT Service Management (ITSM) platforms to automate and mobilize the discovery-to-remediation workflow.
- Phase 6: Validation & Tuning – Fine-tune platform operations by optimizing scan performance, implementing exclusions, and systematically validating data to ensure stability and accuracy.
- Phase 7: Operationalization – Formalize these refined processes into a permanent, recurring Risk-Based Vulnerability Management (RBVM) lifecycle with full organizational alignment and SLA tracking.
- Phase 8: Optimization & Maturity – Implement advanced automation, precise access controls, and strategic integrations to future-proof your program and transition toward the unified Tenable One platform.

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 Vulnerability Management 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: Application Initialization.

Phase 1: Application Initialization

Application initialization is the first phase of your Tenable Vulnerability Management 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 Tenable Vulnerability Management platform is active and in the correct region.
- Confirming administrator login credentials and configuring Multi-Factor Authentication (MFA) or Single Sign-On (SSO) via Security Assertion Markup Language (SAML). For more information, see SAML Configuration.
- Creating user accounts and assigning them to specific user groups. For more information, see Users and Permissions.

Why This Is Important

Establishing a secure, multi-user environment ensures that data segments are correct from day one. Without proper Role-Based Access Control (RBAC), you risk data sprawl where unauthorized users view sensitive vulnerability data.

Verification

Verify the success of this phase by confirming the following:

- At least one administrator and one standard user successfully log in.
- The License Information page reflects your expected asset allocation and deployed region. For more information, see License Information.
- All user groups and roles (for example, Administrator, Read-Only, and Analyst) assign correctly and function with a dedicated test user to validate the expected scope and permissions. For more information, see Access Control.

What to do next:

Proceed to Phase 2: Component Deployment & Rapid Visibility to begin your external-facing discovery.

Phase 2: Component Deployment & Rapid Visibility

Establish comprehensive visibility by deploying external and internal assessments: start with external-facing asset discovery for rapid, credential-free visibility into your internet-facing perimeter, then validate and expand coverage with internal scans using credentialed assessments. Deploy your initial set of sensors (network scanners and agents) to cover both external and internal assets. The specific order of internal component deployment varies based on your environment's scope and readiness, but the goal is to start efficiently and ensure complete coverage.

Expected Outcomes

During this phase, you establish rapid visibility by deploying and configuring your internal sensors and setting up initial scans. This includes:

- Completing external perimeter scans successfully to establish rapid visibility of internet-facing assets.
- Creating and applying an initial set of tags to assets for basic grouping and context. For more information, see Tags.
- Deploying and configuring Tenable Nessus scanners for network-based asset discovery and vulnerability enumeration. For more information, see Nessus Scanners.
- Deploying Tenable Agents to remote or transient workstations, as needed based on scope. For more information, see Tenable Agents.
- Creating and running scans against internal assets. For more information, see Scan Templates.
- Populating the Explore page successfully with asset results. For more information, see Explore Assets.

Why This Is Important

You cannot protect what you cannot see. Starting with external scans provides immediate benefits by rapidly identifying your most exposed assets with zero credential management or internal network changes. However, external scans alone provide only partial visibility. Internal assessments—especially credentialed scans—validate external findings, uncover configuration weaknesses, and discover assets not visible from outside your network. Together, external and internal scans ensure complete visibility and accurate vulnerability data before moving to Phase 3: Data Normalization & Asset Hygiene, where asset hygiene and data accuracy are refined.

Verification

Verify the success of this phase by confirming the following:

- At least one external network scan completes successfully with no errors. For more information, see Scan History.
- At least one internal credentialed scan completes successfully with no authentication errors. If authentication errors occur, see Troubleshooting Plugins for resolution guidance.
- The Last Seen attribute in the asset workbench is current, and results show in the Explore page.

What to do next:

Once you establish the external-facing view, move to Phase 3: Data Normalization & Asset Hygiene to refine the internal data quality.

> Note: If internal credential or agent deployment is not ready, you may proceed to Phase 3: Data Normalization & Asset Hygiene to focus on data normalization. However, you must prioritize internal component deployment before moving to Phase 4: Policy & Risk Context Configuration.

Phase 3: Data Normalization & Asset Hygiene

Ensure a high-quality data set by optimizing scan data, achieving high authentication success, and maintaining a clean asset inventory. Aligning with public documentation and consulting your internal teams (for example, your network team) is critical, as results depend on your environment's complexity.

Expected Outcomes

During this phase, you refine your raw scan data into a single, accurate source of truth. This includes:

- Achieving high success rates for credentialed scans (plugins 21745, 110095, and 19506) to ensure maximum visibility. For more information, see Credentials.
- Maintaining clean and accurate asset records, purging decommissioned IP addresses and inactive assets, and capturing all relevant asset attributes correctly. For more information, see Asset Age Out.
- Ensuring networking teams allowlist scanners to guarantee complete scan results.

Why This Is Important

This phase is the foundation of a successful vulnerability management program. High-quality authentication (credentialed scans or agent-based scans) ensures complete and deep visibility across your entire asset base. A clean asset inventory allows you to focus remediation efforts efficiently and accelerates your Mean Time to Remediate (MTTR).

Verification

Verify the success of this phase by confirming the following:

- Review the Vulnerability Operations dashboard for Authentication Success metrics. For more information, see Dashboards.
- Discuss findings with your teams (for example, the network team) to ensure the data is complete and accurate.

What to do next:

With clean data, begin prioritizing risk in Phase 4: Policy & Risk Context Configuration.

Phase 4: Policy & Risk Context Configuration

Shift focus from static severity scoring, such as the Common Vulnerability Scoring System (CVSS), to Tenable's dynamic, data science-driven risk scores: Vulnerability Priority Rating (VPR) and—with Advanced tier of Tenable One—Asset Criticality Rating (ACR).

Expected Outcomes

During this phase, you transition from traditional severity scoring to dynamic, business-context-driven risk prioritization. This includes:

- Tuning default scan policies to prioritize remediation efforts using VPR. For more information, see Vulnerability Priority Rating (VPR).
- Creating custom filters or saved searches to quickly identify high-priority vulnerabilities (Critical Risk, VPR 9.0+). For more information, see Saved Searches and Tenable Queries.
- Using Vulnerability Intelligence to identify trending Common Vulnerabilities and Exposures (CVEs) that attackers actively exploit.
- (Tenable One Advanced tier only) Editing Asset Criticality Ratings (ACRs) on business-critical systems to add business context to risk. For more information, see Asset Criticality Rating (ACR).

Why This Is Important

Traditional CVSS is static. VPR evolves daily based on the threat landscape, helping your team focus on the small percentage of vulnerabilities that pose the greatest risk. If you use Tenable Vulnerability Management within Tenable One, integrating ACR ensures that you prioritize risk based on the threat and the business importance of the affected asset.

Verification

Verify the success of this phase by confirming the following:

- Ensure your remediation lists sort by VPR, rather than solely by severity.

What to do next:

Integrate this prioritized data into your IT ticketing systems in Phase 5: Workflow & Integration Enablement.

Phase 5: Workflow & Integration Enablement

Connect Tenable Vulnerability Management to your IT Service Management (ITSM) platform and define the Service Level Agreement (SLA) process to mobilize the discovery-to-remediation workflow.

Expected Outcomes

During this phase, you mobilize the remediation effort by connecting security findings to the patching workflow. This includes:

- Generating API keys for ITSM integrations (for example, ServiceNow or Jira). For more information, see API Keys.
- Documenting Exposure Response workflows to outline the steps for investigation and remediation.
- Setting automated accept or recast rules for vulnerabilities with mitigating controls. For more information, see Recast and Accept Rules.
- Granting remediation teams access to the Tenable Vulnerability Management dashboards.

Why This Is Important

Security identifies the risk, but IT remediates it. This phase mobilizes the remediation effort. Automation via Jira or ServiceNow reduces friction between teams and speeds up the MTTR by clearly defining the Exposure Response process.

Verification

Verify the success of this phase by confirming the following:

- A critical vulnerability in Tenable Vulnerability Management automatically generates a ticket in your ITSM tool.
- Relevant security and IT teams formally review, communicate, and acknowledge the documented Exposure Response workflow.

What to do next:

Optimize the platform settings in Phase 6: Validation & Tuning.

Phase 6: Validation & Tuning

Refine scan performance and implement exclusions to ensure optimal platform function and zero impact on production. This phase makes the technical operation of the program efficient, accurate, and stable.

Expected Outcomes

During this phase, you fine-tune the platform's technical operation to maintain stability and accuracy. This includes:

- Creating exclusion windows for scheduled maintenance periods or sensitive systems to ensure no disruption to business-critical operations. For more information, see Exclusions.
- Optimizing scan performance settings (for example, maximum hosts and checks, or network congestion settings) for each network segment and sensor type to achieve the fastest scan times possible without causing network issues. For more information, see Scan Performance.
- Investigating, validating, and recasting potential false positives with supporting evidence systematically.
- Auditing and pruning scan templates to remove unnecessary customizations.
- Establishing an ongoing process to audit and maintain credentialed scan success rates.

Why This Is Important

Stability and accuracy are paramount. Tuning ensures that deep credentialed scans do not disrupt sensitive legacy devices or consume excessive network bandwidth. Validation confirms that the data used for prioritization is accurate, which prevents the remediation team from wasting effort on non-existent vulnerabilities and builds trust in the program.

Verification

Verify the success of this phase by confirming the following:

- Review scan logs for a reduction in scan interference or network congestion warnings over time.
- Confirm you periodically review the number of recast (accepted risk) vulnerabilities to ensure appropriate risk acceptance. For more information, see View Rules.
- Track and reduce scan completion times to an acceptable target (for example, all scans complete within a 4-hour window).

What to do next:

Move to Phase 7: Operationalization to formalize these refined processes into permanent operations.

Phase 7: Operationalization

Align stakeholders and formalize the refined processes to establish a permanent, recurring Risk-Based Vulnerability Management (RBVM) lifecycle.

Expected Outcomes

During this phase, you formalize the processes into a permanent, recurring lifecycle with full organizational buy-in. This includes:

- Aligning all teams on expectations for roles, responsibilities, and timelines in the vulnerability management process.
- Adopting the complete RBVM lifecycle fully as a recurring process.
- Publishing, approving, and actively following Standard Operating Procedures (SOPs) for the discovery-to-remediation cycle.
- Tracking and reporting SLA compliance via dashboards to establish a Key Performance Indicator (KPI) for remediation performance. For more information, see Service Level Agreement (SLA) Dashboards.
- Establishing monthly or quarterly risk reviews with executive leadership to communicate program status and risk posture.

Why This Is Important

Vulnerability management is a lifecycle, not a one-time project. This phase ensures you document the program so it remains resilient to organizational changes. Tracking SLA compliance drives continuous improvement and accountability.

Verification

Verify the success of this phase by confirming the following:

- Escalation processes trigger correctly for overdue vulnerabilities according to your internal policy.
- Security and IT leadership formally sign off on the published SOPs and SLA targets to signal cross-functional alignment.

What to do next:

Advance toward full program maturity in Phase 8: Optimization & Maturity.

Phase 8: Optimization & Maturity

Implement advanced automation and cloud-native visibility to reach the peak of program maturity.

Expected Outcomes

During this phase, you implement advanced controls and leverage new technologies. This includes:

- Establishing a strategic roadmap to leverage the overarching Tenable One platform.
- Utilizing custom scan templates (for example, specific zero-day, compliance audits, or Operational Technology (OT) assets). For more information, see Scan Templates.
- Establishing advanced, bi-directional integrations to leverage the existing tool stack.
- Optimizing agent and scanner profiles for bandwidth and check-in frequency. For more information, see Agent Profiles and Scanner Profiles.
- Implementing custom roles for advanced least-privilege access. For more information, see Custom Roles.
- Fine-tuning scan performance settings using throttling controls to maintain optimal platform performance.

Why This Is Important

As your environment shifts to the cloud, traditional visibility must evolve. Maturity means frictionless visibility that adapts as fast as your infrastructure does.

Advanced integrations increase security and IT collaboration, while custom roles enable precise access controls. The transition to a unified platform like Tenable One future-proofs your program and integrates risk context across your entire attack surface.

Verification

Verify the success of this phase by confirming the following:

- Evaluate your existing tool stack and non-IT assets to understand how Tenable One assists with overall exposure management.
- Review scan completion times to ensure they remain stable and efficient, demonstrating the effectiveness of throttling controls.
- Verify that key integration workflows trigger and execute automatically.
- Confirm that different user types (for example, audit teams and remediation teams) have access only to the data and features defined by their custom permissions.

> Note: Engage with a Tenable representative or accredited partner for strategic optimization training and maturity conversations.