



# Tenable VM and RidgeBot® Integration Provides Proactive Exposure Management

## Executive Summary

The fast-evolving threat landscape combined with increasing organizational and technological intricacies create an exceedingly complex environment that leaves organizations vulnerable to attack. Combining leading security tools—such as Tenable VM’s asset discovery, asset assessment and vulnerability scanning, with Ridge Security RidgeBot’s automated vulnerability exploitation and validation—continuously assess and probe the resilience of your assets to identify the highest priority exposures that pose the risk of an active breach to your organization.

The integration draws together Tenable’s asset discovery and assessment capabilities with RidgeBot’s automated continuous vulnerability exploitation to provide a dashboard of insightful, actionable, accurate and timely threat intelligence to your SecOps team.

## The Challenge

Attack surfaces continue to expand dramatically due to increasing adoption of cloud workloads and data storage, a significant WFA workforce, virtualization of the network perimeter, and evermore sophisticated cybercriminals and attack resources. To stay a step ahead of the bad

actors, you require an adaptive, automated ecosystem of specialized security tools integrated into an operational dashboard for immediate visibility and situational awareness to maximize rapid SecOps response and action.

## Joint Solution Description

The integration of Tenable’s asset management with RidgeBot’s automated exploitation strengthens your cybersecurity threat intelligence. The combined solution leverages the capabilities of Tenable’s asset discovery and vulnerability assessments, with RidgeBot’s active exploitation validation to distil out the highest urgency real risks among the assets with detected vulnerabilities.

Tenable VM continuously discovers and assesses your assets to provide a list of the vulnerabilities identified. RidgeBot® receives this detailed list and proceeds to test these vulnerabilities with payload to prioritize the active risk that each one poses. RidgeBot® then tag the assets with active risks as validated by RidgeBot®. With this information, your SecOps team can immediately focus on—and remediate—the most perilous vulnerabilities to have the highest impact, in the shortest time, using the least resources, to best protect your assets.

## Solution Components

### Ridge Security RidgeBot®

Security validation AI agent that continuously probes and validates your network and assets. Results prioritize exploitable vulnerabilities and provide remedial steps.

### Tenable VM

Asset and vulnerability discovery and management capabilities to get a asset-based view of your attack surface to quickly identify, investigate and prioritize your most critical assets and vulnerabilities.

## Solution Benefits

### ■ See Everything Visibility

Find hidden vulnerabilities with continuous, always-on asset discovery and assessment of known and unknown assets in your environment, even highly dynamic cloud or remote workforce assets. By integrating RidgeBot® exploitation with Tenable asset management, vulnerabilities detected can be tested for exploitability in real-time, immediately distinguishing between theoretical vulnerabilities and those that pose a real risk.

### Prioritize Vulnerabilities; High-precision

### ■ Remediation

Identify which vulnerabilities to fix first with automated prioritization that combines vulnerability data, threat intelligence and data science. Speed up and focus remediation with real-time visualization of risk, and tracking of vulnerabilities, assets and remediations. Gain higher precision by focusing on critical exploitable vulnerabilities that must be addressed promptly.

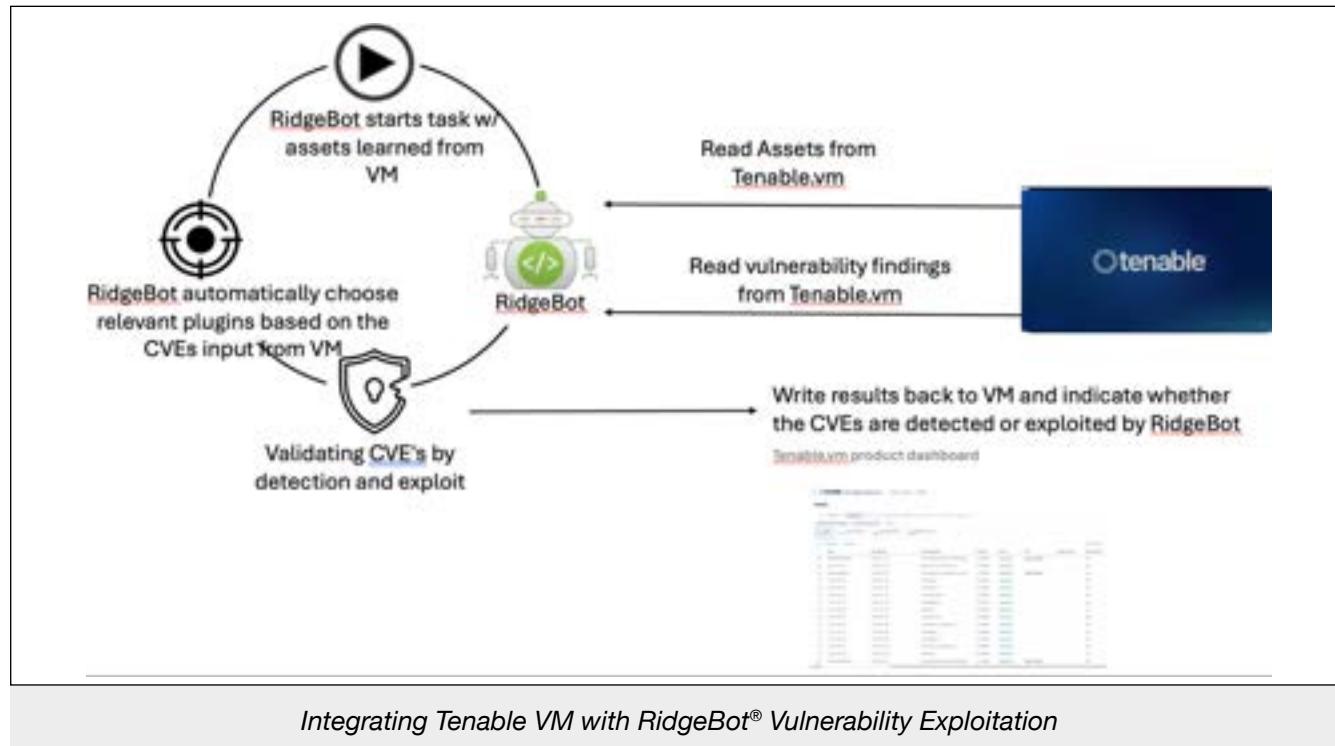
### ■ Reduce Business Risk

Use threat intelligence from Tenable VM to identify assets and vulnerabilities. Integration with RidgeBot® helps to:

- Transform raw data into actionable intelligence to enable your SecOps team to make quicker and better-informed decisions.
- Provide a comprehensive view of your organization's security posture.
- Provide clarity with built-in vulnerability risk scores into how detected vulnerabilities translate into business risk and which ones are most likely to be targeted by attackers.

## Joint Solution Integration

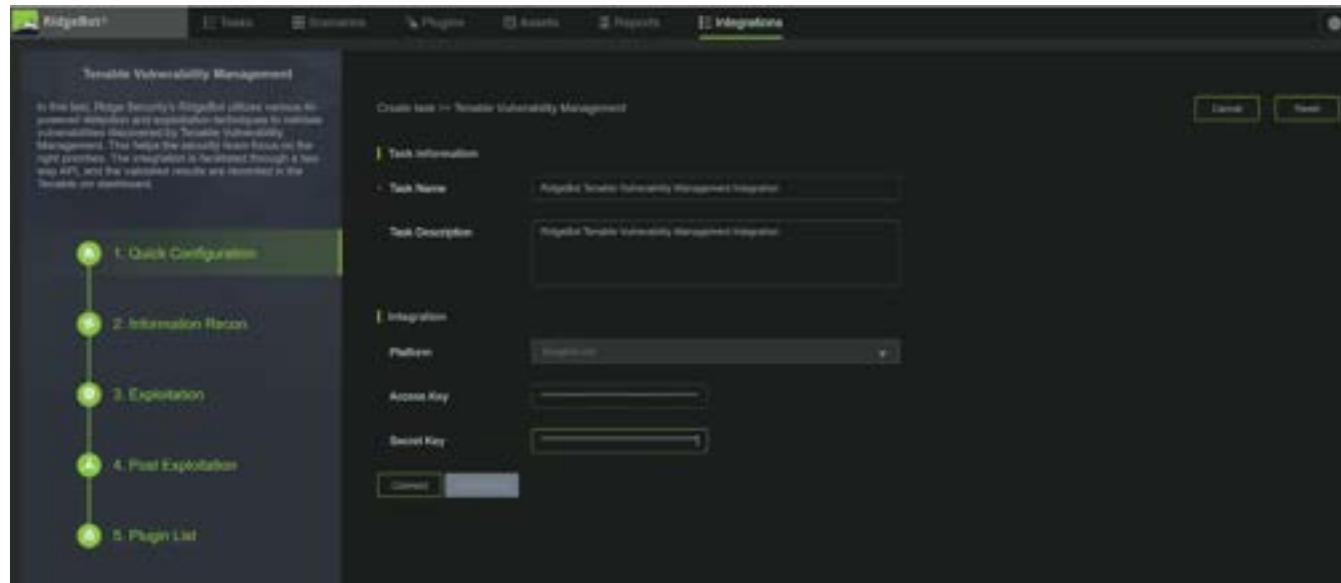
Assets discovered and managed by Tenable VM are tagged with RidgeBot® when vulnerabilities on the assets are validated by RidgeBot®. The combined results provide your SecOps team with a prioritized list of the highest risk items to be remediated.



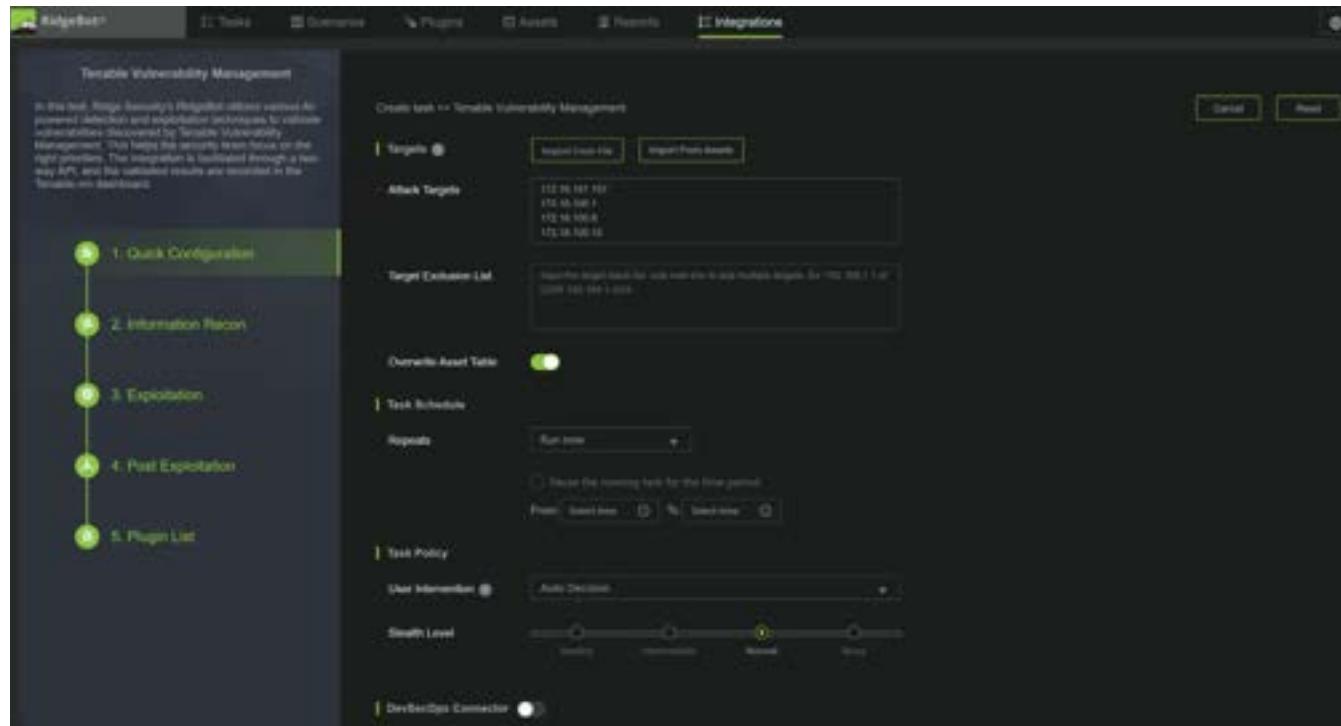
From the RidgeBot® UI, choose the Tenable integration.

The screenshot shows the RidgeBot UI with the "Integrations" tab selected in the top navigation bar. The main content area displays the "Integration" section, which includes a sub-section for "Penetration". A card for "Tenable Vulnerability Management" is shown, featuring the Tenable logo, the title "Tenable Vulnerability Management", and a description: "The test utilizes various AI-powered RidgeSecurity techniques to perform penetration testing to validate the vulnerabilities being scanned from Tenable VM." A "Select" button is visible at the bottom right of the card.

Configure the Tenable platform with Access Key and Secret Key, then select “Connect”. Once authenticated, you can also click the “Synchronize” button to collect the latest assets discovered by Tenable.



On the next screen, you can click the “Import From Assets” button to import a view of all assets discovered by Tenable.



On the next screen, you can select the asset targets to be validated by RidgeBot®.

The RidgeBot interface is shown with the 'Available Assets' dialog open. The sidebar on the left lists five steps: 1. Quick Configuration, 2. Information Recon, 3. Exportation, 4. Post Exploitation, and 5. Plugin List. The 'Available Assets' dialog lists 14 nodes, all of which are 'Susceptible' to the 'Windows' plugin. The nodes are numbered 1 through 14 and have IP addresses ranging from 172.16.101.30 to 172.16.101.81.

| Node | IP            | Plugin  | Status      |
|------|---------------|---------|-------------|
| 1    | 172.16.101.30 | Windows | Susceptible |
| 2    | 172.16.101.34 | Windows | Susceptible |
| 3    | 172.16.101.38 | Windows | Susceptible |
| 4    | 172.16.101.56 | Windows | Susceptible |
| 5    | 172.16.101.57 | Windows | Susceptible |
| 6    | 172.16.101.58 | Windows | Susceptible |
| 7    | 172.16.101.59 | Windows | Susceptible |
| 8    | 172.16.101.69 | Windows | Susceptible |
| 9    | 172.16.101.80 | Windows | Susceptible |
| 10   | 172.16.101.81 | Windows | Susceptible |
| 11   | 172.16.101.82 | Windows | Susceptible |
| 12   | 172.16.101.83 | Windows | Susceptible |
| 13   | 172.16.101.84 | Windows | Susceptible |
| 14   | 172.16.101.85 | Windows | Susceptible |

RidgeBot® automatically picks plugin groups based on the vulnerabilities discovered by Tenable.

Template Vulnerability Management

In this area, Ringle monitors a large collection of various, as-powered detection and exploitation techniques to monitor vulnerabilities discovered by Template Vulnerability Management. This helps the operator focus on the most critical findings. The detection is based on the OWASP API, and the returned results are reviewed in the Timeline dashboard.

1. Quick Configuration

2. Information Review

3. Exploitation

4. Post Exploitation

5. Plugin List

Choose tool for Template Vulnerability Management

Plugin List

OWASP API

Level Selection

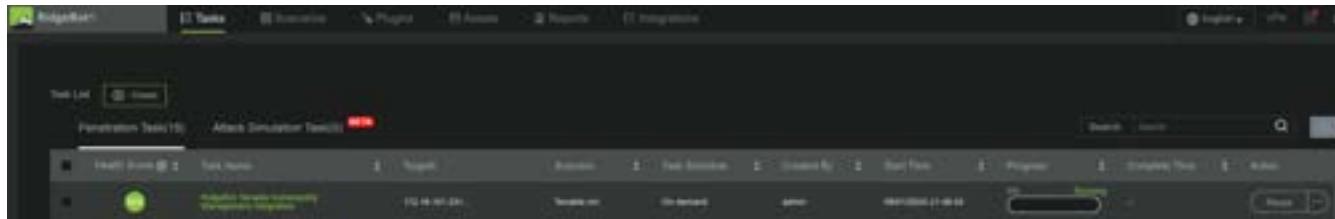
OWASP

Filter

Selected Plugins (0)

| Severity Level | Vulnerability Name                    | CVE           | Vulnerability ID |
|----------------|---------------------------------------|---------------|------------------|
| High           | Root Web Password                     | CVE-2011-3191 | 001              |
| High           | Root Web Password                     | CVE-2011-3191 | 002              |
| High           | Root Web Password                     | CVE-2011-3191 | 003              |
| High           | FTP Root Password                     | CVE-2011-3191 | 004              |
| High           | PHP User Execution                    | CVE-2011-3191 | 005              |
| High           | Remote Desktop Services Root Password | CVE-2011-3191 | 006              |
| High           | Linux Root Sshping                    | CVE-2011-3191 | 007              |
| High           | SSH Root Password                     | CVE-2011-3191 | 008              |

Once the RidgeBot®/Tenable integration task is started, you can see task status and progress in the task view pane.



When RidgeBot® completes its exploitation task, you can generate and download a report. The vulnerability validation results are also automatically exported back to the Tenable VM server for display.

 A screenshot of the Tenable Vulnerability Management interface. The top navigation bar includes 'Tenable' and 'Vulnerability Management'. Below it is a breadcrumb trail: 'Explore Overview > Assets'. The main area is titled 'Assets' with a sub-section '39 Assets'. There are filters for 'Advanced', 'Saved Filters', and a search bar. Below the filters are buttons for 'Hosts' (75), 'Cloud Resources' (5), 'Web Applications' (0), and 'Domain Inventory' (0). A '39 Assets' link and a 'Refresh' button are also present. The main table lists 39 assets with columns: 'Name', 'IPV4 Address', 'Operating System', 'Last Seen', 'Source', and 'Tags'. The 'Tags' column for the first two assets is highlighted with a green box. The table has a header row with sorting arrows for each column.
 

| Name                | IPV4 Address   | Operating System                           | Last Seen  | Source    | Tags                 | Resource Tags | Cloud Provider |
|---------------------|----------------|--|------------|-----------|----------------------|---------------|----------------|
| 0000-0000-0000-0000 | 172.16.101.107 | Microsoft Windows Server 2016 Standard     | 07/06/2024 | Household | HighRisk, vulnerable | N/A           | N/A            |
| 172.16.101.101      | 172.16.101.101 | Ubuntu 18.04 Linux Kernel 4.18             | 07/06/2024 | Household | HighRisk, vulnerable | N/A           | N/A            |
| ubuntukeepit102     | 172.16.101.102 | Linux Kernel 5.3.0-44 generic on Ubuntu... | 07/06/2024 | Household | HighRisk, vulnerable | N/A           | N/A            |
| 172.16.101.103      | 172.16.101.103 | Linux Kernel 5.1                           | 07/06/2024 | Household | N/A                  | N/A           | N/A            |
| 172.16.101.105      | 172.16.101.105 | Linux Kernel 3.1                           | 07/06/2024 | Household | N/A                  | N/A           | N/A            |
| 172.16.101.173      | 172.16.101.173 | FE Networks BIG-IP                         | 07/06/2024 | Household | N/A                  | N/A           | N/A            |
| 172.16.101.178      | 172.16.101.178 | Linux Kernel 2.6                           | 07/06/2024 | Household | N/A                  | N/A           | N/A            |
| 172.16.101.180      | 172.16.101.180 | Aruba EOS                                  | 07/06/2024 | Household | N/A                  | N/A           | N/A            |

## About Ridge Security RidgeBot®

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity solutions designed to protect organizations from advanced cyber threats. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation. With a focus on automation, intelligence, and actionable insights, Ridge Security enables security teams to proactively defend against and respond to evolving cyber challenges.