

Ridge Security RidgeBot® and Trellix ePO Integration

Executive Summary

The fast-evolving threat landscape combined with increasing organizational and technological intricacies create an exceedingly complex environment that leaves an organization vulnerable to attack. Automated security tools, such as Ridge Security's RidgeBot® penetration testing and exploitation, continuously probe the resilience of your assets and report on vulnerabilities detected as well as documenting successfully exploited attack vectors.

It is imperative to integrate streamlined, continuous testing into your SecOps policy enforcement toolchest to provide immediate and accurate remedial action for any detected vulnerabilities.

The Challenge

Attack surfaces continue to expand dramatically due to increasing adoption of cloud workloads and data storage, a significant WFA workforce, growing 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 exemplary dashboard for immediate situational awareness to drive rapid SecOps response and action.

The early decisions you make when responding to a potential security incident often make the difference between containing it or a crisis occurring. Unfortunately, most organizations are still using manual processes or custom code without full security automation and response dashboards.

Trellix ePolicy Orchestrator (ePO) is a centralized, scalable, extensible platform for security policy orchestration and enforcement to manage all your endpoints.

The RidgeBot®—ePO integration delivers cost-effective continuous automated penetration testing of your endpoints, automated asset inventory and profiling, automated security validation, and risk-based vulnerability management using intelligent robots. RidgeBot® pentest results as well as task management and control are integrated into Trellix ePO's dashboards.



Trellix ePO allows you to:

1. Create automated workflows between your security and IT operations systems, allowing you to quickly remediate issues
2. Customize and enhance your security posture by integrating via APIs to 3rd party security tools
3. Simplify security management through a central, graphical security posture dashboard with role-based access control and a summary view of risks for the entire digital terrain
4. Focus on security posture and keeping ahead of threats, instead of maintaining/updating security infrastructure

Ridge Security and Trellix ePO have partnered to deliver an industry-leading policy orchestration solution to address these challenges. The RidgeBot®—ePO integration delivers cost-effective continuous automated penetration testing of your endpoints, automated asset inventory and profiling, automated security validation, and risk-based vulnerability management using intelligent robots. RidgeBot® pentest results as well as task management and control are integrated into Trellix ePO's dashboards.

Solution Components

Ridge Security RidgeBot®

Cost-effective automated test & exploit that provides continuous automated penetration testing and an exploitation software robot that continuously probes and validates your network and assets. The results prioritize exploitable vulnerabilities and provides remedial steps. RidgeBot® also automatically inventories and profiles your assets.

Trellix ePO

Eliminates the need to maintain security management infrastructure, reducing the potential for error and enabling your team to manage security more efficiently and with higher efficacy across geographies. Trellix ePO manages and schedules RidgeBot® tasks, and integrates the results into the ePO dashboards.

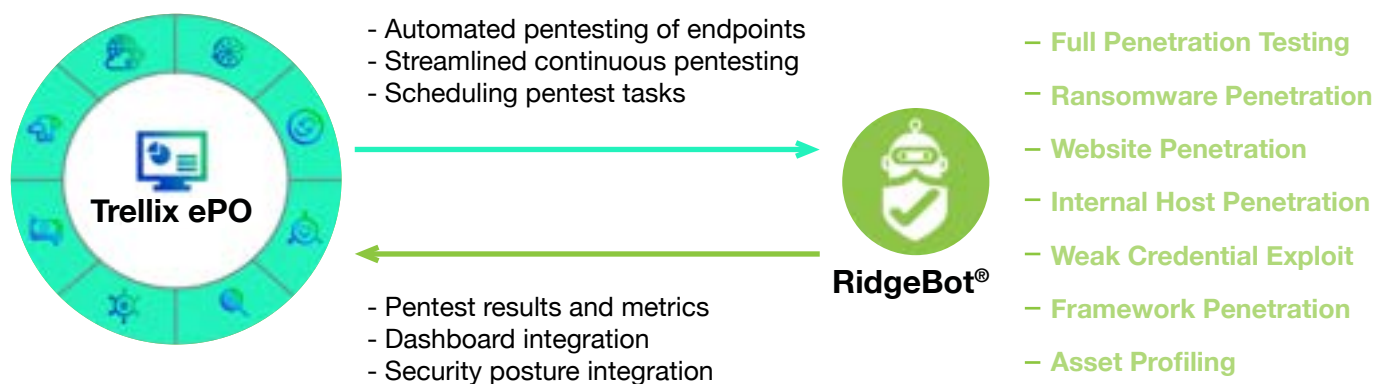
Solution Benefits

A	RidgeBot® performs continuous, automated pentesting and exploitation of endpoints in your network.
B	RidgeBot® streamlines Trellix ePO's threat response capabilities with RidgeBot's elastic at-scale security pentesting.
C	RidgeBot's automation tests 100x faster than human testers, and instantly replicates to address complex infrastructure. RidgeBot® task results integrate with Trellix ePO's dashboard to enable instant, proactive threat detection, focused investigation and response decision making.
D	The Trellix ePO dashboard provides a single management console to manage all your security tools including RidgeBot®.

E	You can launch with a single click pentesting of managed endpoints to provide more immediate protection for your assets.
F	The Trellix ePO dashboard provide enriched management and reporting options. A RidgeBot® dashboard inside Trellix ePO shows pentesting status, results and task details.
G	The integrated solution reduces risk through continuous validation and uses automation to improve efficiencies.

Joint Solution Integration

The Ridge Security RidgeBot® and Trellix ePO integrated solution provides users with a comprehensive, validated and always up-to-date view of endpoint vulnerabilities and risks. The integrated solution streamlines the probing of endpoint compliance with enterprise policies through automated pentesting and an integrated dashboard of results. The RidgeBot® Task Manager inside ePO facilitates automated interactions—such as creating, scheduling and executing pen-testing tasks.



Integrating RidgeBot® pentest tasks and results with Trellix ePO

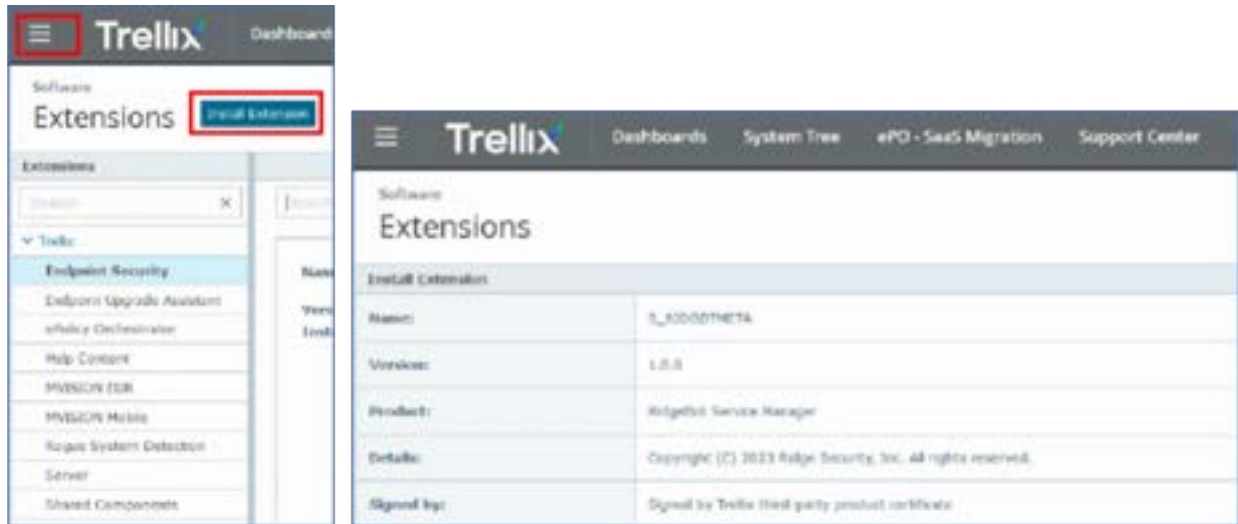
Configuration and Use

The Trellix ePO interface allows you to register a Ridge Security RidgeBot® server. The RidgeBot® Service Manager allows you to define and schedule RidgeBot® pentest tasks to probe your endpoints. Results from the RidgeBot® tasks are displayed in the RidgeBot® dashboard display as shown below. Mousing over any of the candles in the display allows you to drill down on the details of that task result.



RidgeBot® Dashboard Results

Ridge Security RidgeBot® version 4.2.2 or later integrates with Trellix ePO on-prem as of version 5.10.0. To set up RidgeBot® integration with Trellix ePO, you install the RidgeBot® Server Manager 1.0.0 as an extension into ePO.



After the installation of the extension, click on “Registered Servers” in the ePO menu to register the RidgeBot® server, provide its key and then connecting.

The figure shows the 'Registered Servers' configuration page in Trellix ePO. The page has a 'Configuration' header and a 'Registered Servers' title. Below the title, there is a table with columns for 'Registered Server Builder' and 'Description'. The 'Registered Server Builder' column has a dropdown menu set to 'RidgeBot® Server'. The 'Description' column has a text input field containing 'RidgeBot® Server'. There is also a 'Notes' section with a text area.

Registered Server Builder	Description
RidgeBot® Server	RidgeBot® Server

[illegible]

RidgeBot® is now installed as a “RidgeBot® Server Manager” in ePO. You can use the “RidgeBot® Task Manager” to create and schedule tasks. These tasks can run pentests and upload results into the ePO dashboard.

Automation

Server Tasks

Server Task Builder	1 Description	2 Actions	3 Schedule
Name:	RidgeNet server task		
Notes:			
Schedule status:	☒ Enabled ☐ Disabled		

Automation

Server Tasks

Server Task Builder

Description

Actions

Schedule

What actions do you want the task to take?

1. Actions

RidgeBot Server: Pull Task Details

Select RidgeBot Server Name :

RidgeBot Server

Automation

Server Tasks

Server Task Builder

1 Description

2 Actions

3 Schedule

Schedule type: Advanced

Start dates: 08 / 01 / 2024

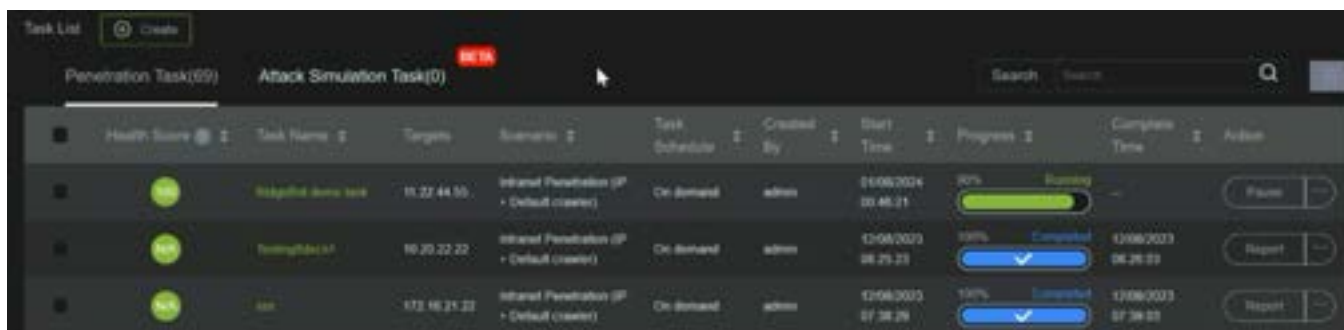
End dates: ☐ 09 / 01 / 2024
☒ No end date

Schedule: Cron Syntax:

Task status can be viewed and controlled (start, restart, pause, stop, delete) from the ePO interface.



Task status can also be viewed from the RidgeBot® interface.



About Ridge Security RidgeBot®

Ridge Security enables enterprise and web application teams, ISVs, governments, education, DevOps, SecOps and anyone else responsible for ensuring software security, to affordably and efficiently test their systems before and after deployment. Ridge Security improves the efficiency of your SecOps team by providing risk-based vulnerability management through continuous automated testing, exploitation, prioritization and remedial guidance.