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.

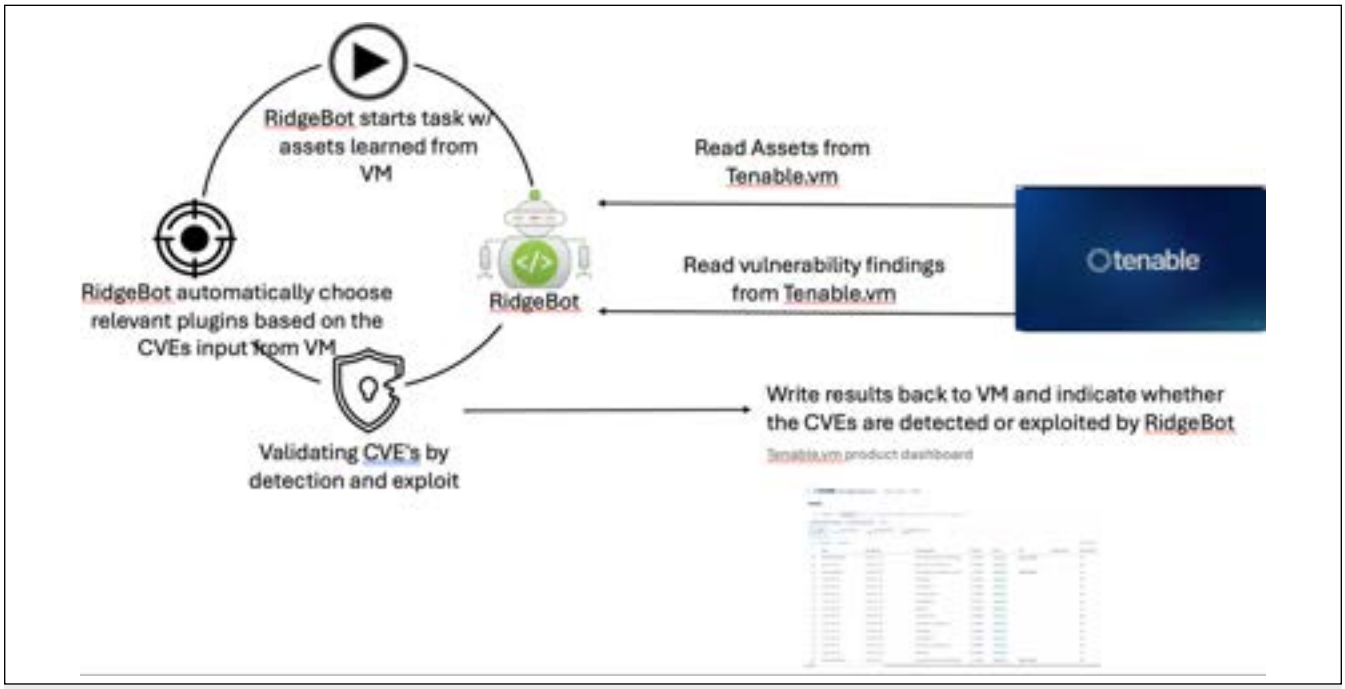
- **Prioritize Vulnerabilities; High-precision Remediation**
  Identify which vulnerabilities to fix first with automated prioritization that combines vulnerability data, threat intelligence and data science. Speed up and focus remediation with real-time visualization of risk, and tracking of vulnerabilities, 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.

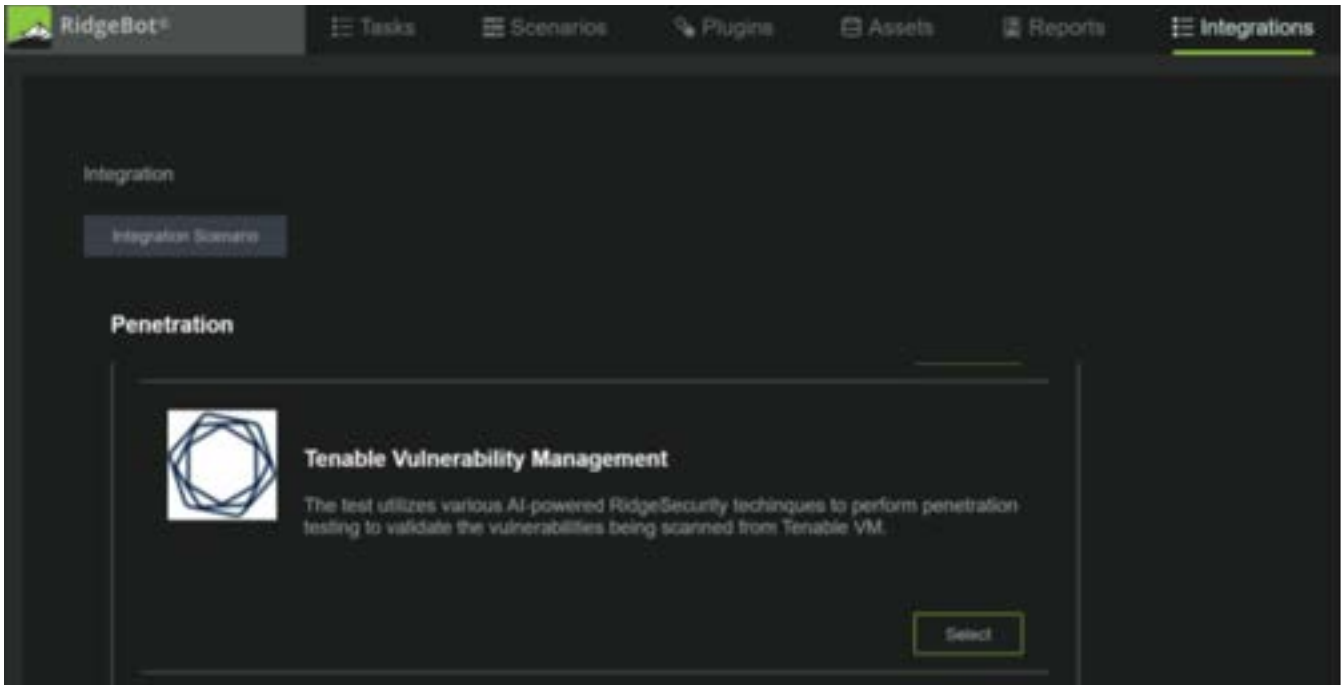
Joint Solution Integration

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.

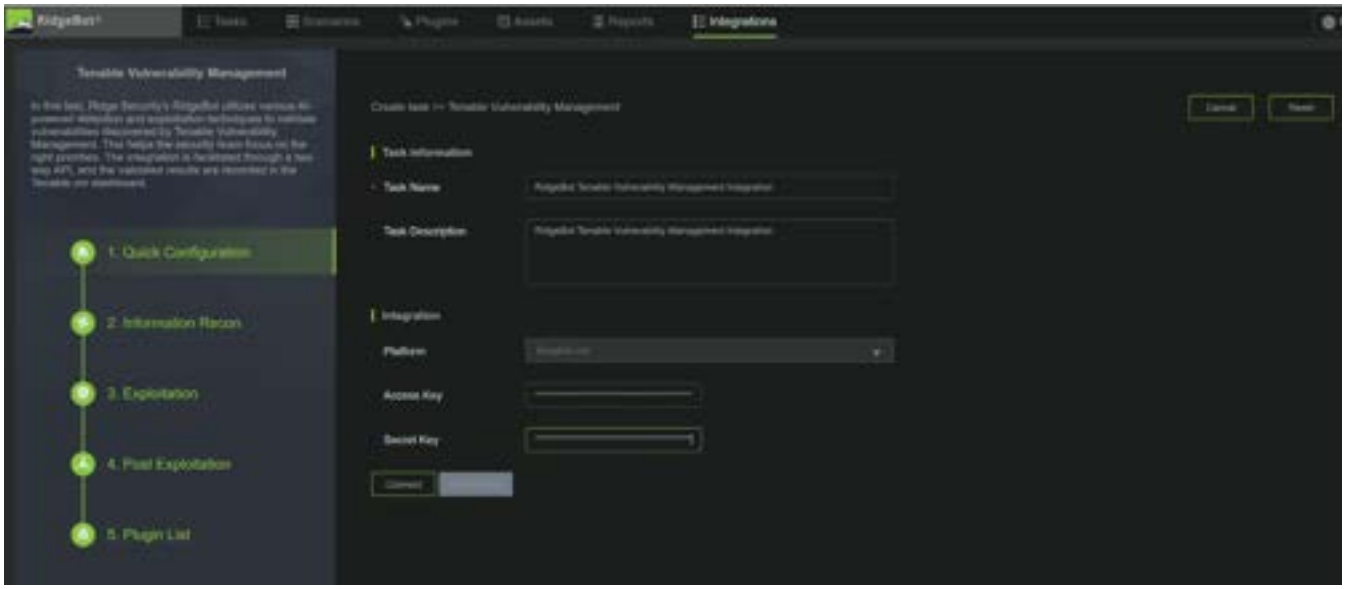


Integrating Tenable VM with RidgeBot® Vulnerability Exploitation

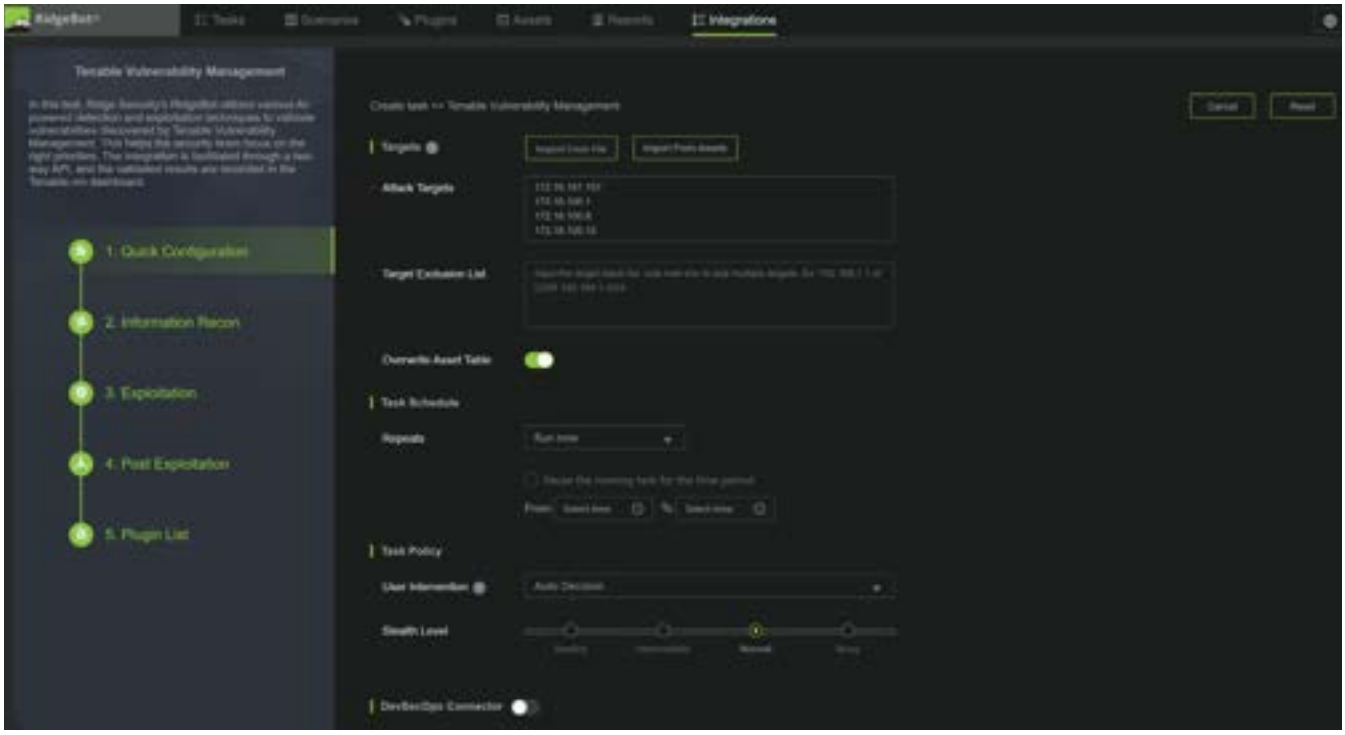
From the RidgeBot® UI, choose the Tenable integration.



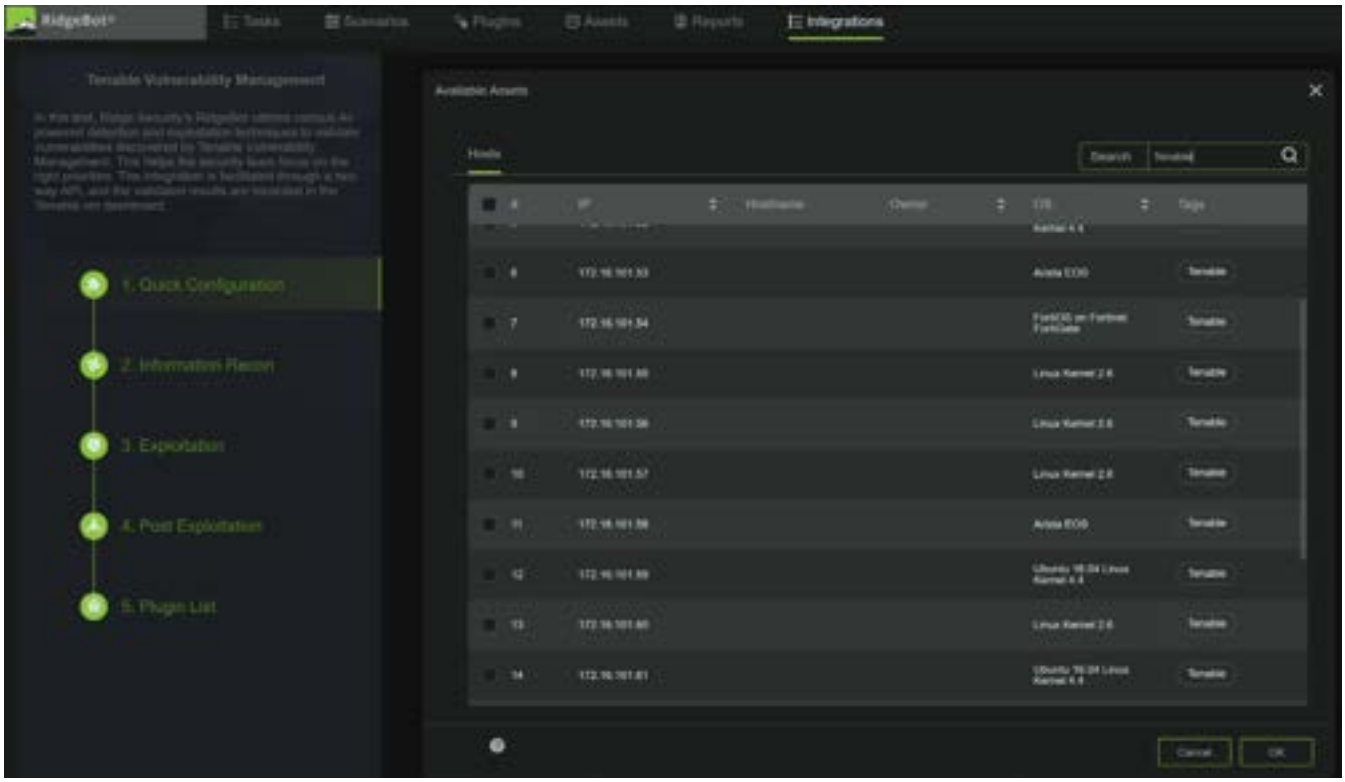
Configure the Tenable platform with Access Key and Secret Key, then select “Connect”. Once authenticated, you can also click the “Synchronize” button to collect the latest assets discovered by Tenable.



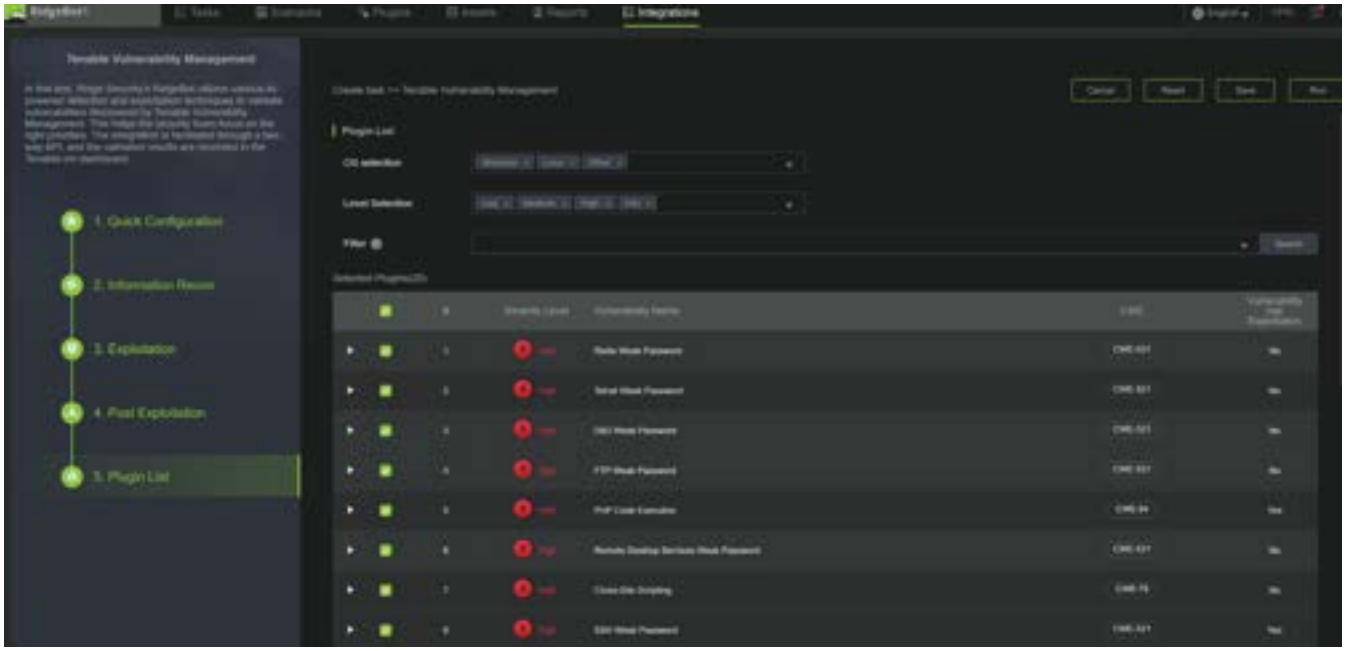
On the next screen, you can click the “Import From Assets” button to import a view of all assets discovered by Tenable.



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

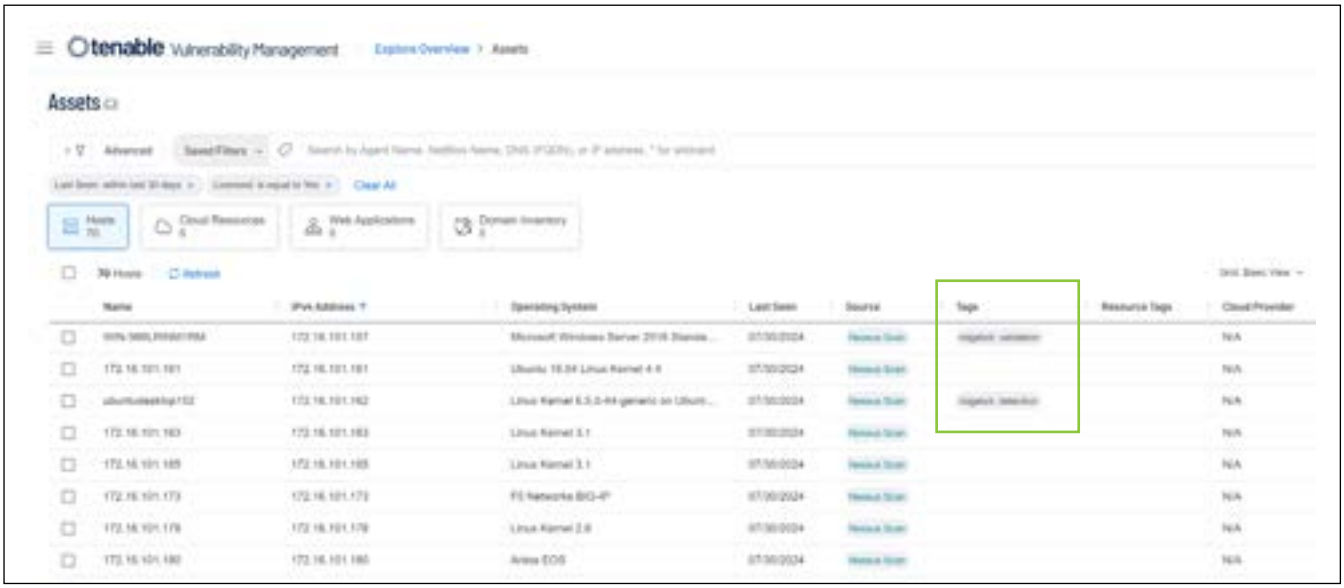


RidgeBot® automatically picks plugin groups based on the vulnerabilities discovered by Tenable.



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.



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.