**Revision History**

**Use Cases Document**

**Security Innovation Alliance**

**Author: Ridge Security**

****

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Comments** |
| **29-Jul-2023** | **1.0** | **Lydia Zhang** | **Use case document for Ridge security integration with Trellix ePO** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Company Info 4](#_Toc141372208)

[2 Company Contacts 4](#_Toc141372209)

[3 Product Backgrounder 4](#_Toc141372210)

[4 Trellix Products Being Proposed for Integration 5](#_Toc141372211)

[5 Platform 5](#_Toc141372212)

[6 Use Cases 5](#_Toc141372213)

[7 Integration Points 5](#_Toc141372214)

[8 Integration Architecture 6](#_Toc141372215)

[9 Implementation Phases 6](#_Toc141372216)

[10 Benefit to customer 6](#_Toc141372217)

[11 Effort 6](#_Toc141372218)

# 

This Use Case Document is used to help Partners and Trellix identify and refine the integration points, products and strategy between our companies. It forms the basis for the Functional Specification Document and must be signed off by SIA before proceeding with the development effort. Upon completion, please send it to the SIA Technology Team with whom you’ve been collaborating. After we complete its initial review, we’ll schedule a meeting between the primary contacts you’ve listed and the SIA Engineering team.

# Company Info

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity products that benefit CISOs and security teams by reducing risk through validation and using automation to improve efficiencies. Ridge Security’s products incorporate advanced artificial intelligence to deliver comprehensive security validation, powerful workload protection and cloud security monitoring.

# Company Contacts

*<Key Company Contacts: name, title, e-mail, phone numbers, time zone>*

*Lydia Zhang, President & Co-Founder, Ridge Security Technology Inc.*

*e-mail:* [*lydia@ridgesecurity.ai*](mailto:lydia@ridgesecurity.ai)

*Business Phone: + (408)8006883*

*Mobile Phone: + (408)8812738*

*Time Zone: Pacific Time (UTC -8:00) California, USA*

# Product Backgrounder

Ridge Security’s RidgeBot product is a fully automated penetration testing that discovers and flags validated risks for remediation by SOC teams. The test does NOT require highly skilled personnel. RidgeBot is a tireless software robot, it can run security validation tasks every month, every week or every day with a historical trending report provided. Provides a continuous peace of mind for our customers. Evaluate the effectiveness of your security policies by running emulation tests that follow Mitre Att&ck framework. Prioritize those vulnerabilities that are exploited in your organization with clear evidence. It is zero-false positive.

# Trellix Products Being Proposed for Integration

Select products (double-click to toggle checkbox):

ePO

ESM

DXL

MAR

TIE

ATD

MWG

NSP

CASB Connect

Others (please mention here)

# Platform

RidgeBot is a software solution that can be deployed on-premise or in the cloud with virtual machines or bare medal servers. We offer rich UI platform to manage all security operations for RidgeBot. Apart from UI we also provide REST endpoints to achieve the same.

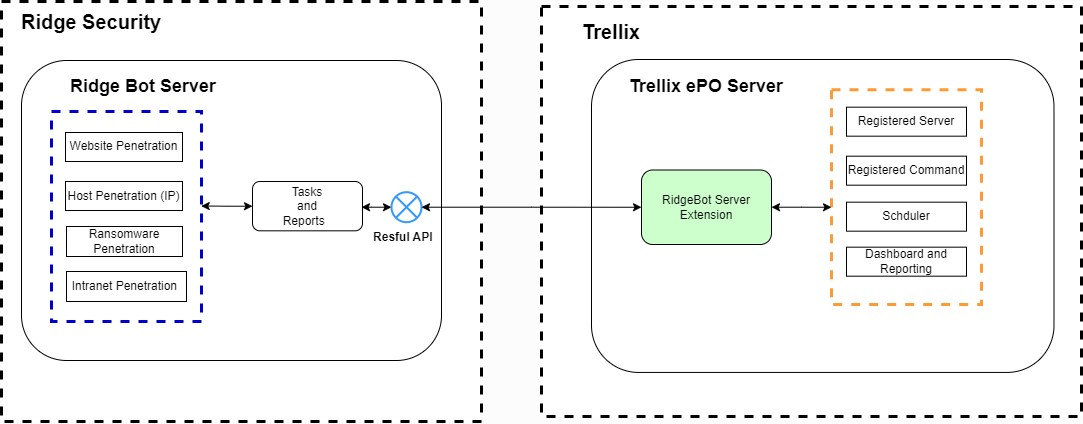
# Use Cases

1. Configure RidgeBot server details as part of ePO’s registered sever UI to establish the communication between ePO server and RidgeBot Security RESTful API.
2. Create an ePO Registered Command to pull penetration testing and task details from RidgeBot server to ePO. The retrieved information will be saved as part of ePO custom tables that are created for RidgeBot integration.
3. Create an ePO Scheduler task to pull penetration testing and task details periodically from RidgeBot server.
4. Create dashboard to show the penetration testing and task details of RidgeBot server as part PO reports and manage the same from ePO.
5. Import the server IP addresses managed by ePO to RidgeBot, so that RidgeBot can perform a pentest towards these servers.

# Integration Points

To Implement use cases #1 to #4 we use ePO’s registered server, Registered Command, Scheduler and Dashboard integration points.

# Integration Architecture



# Implementation Phases

Phase 1: Registered Server

Using ePO’s Registered server, Registered Command, Scheduler, Dashboard and Reporting to integrate and mage RidgeBot server from ePO server.

# Benefit to customer

1. Customer can use ePO as single management console to manage all the security products including RidgeBot.
2. Customer can launch the penetration testing towards the endpoints it manages by clicking one-key, so that it can provider better protection for their end points.
3. Better event management and reporting options.

# Effort

Partner: 60 to 90 days to create a Registered server, Registered Command, Scheduler, Dashboard and Reporting.