WHITE PAPER

RidgeBot®

AI-Enabled Security Validation Platform

Overview

Many organizations utilize security testing (a.k.a penetration testing) to validate the security posture of their network. In such a test, the security tester takes on the role of an attacker and tries his/her best to break into the organization's IT environment. The purpose is to find any vulnerabilities and determine how the vulnerabilities could be exploited in a real-world hacker attack. The underlying idea is that a good security test should reveal how an attacker could work his/her way through the organization's systems before it actually happens. Proper penetration testing helps organizations address issues in a more man-ageable and cost-effective way.

However, nowadays, attackers are always developing new exploits and attack methods, and often using AI-assisted tools to launch attacks automatically. Enterprises' security teams and professional "penetration testers" are under tremendous pressure to keep up. Ridge Security is changing this game with RidgeBot® an intelligent security validation Robot. RidgeBot® is modeled with a collective knowledge of threats, vulnerabilities, and exploits, and equipped with state-of-the-art hacking techniques. RidgeBot® acts like a real attacker, relentlessly locates, exploits, and documents their findings. RidgeBot® automates penetration testing, making it affordable with the ability to run at scale. They work within a defined scope and instantly replicates to address highly complex structures.

Ridge Security enables enterprises and web application teams, DevOps, ISVs, governments, healthcare, education, anyone responsible for ensuring software security, to afford-ably and efficiently test their systems.
RidgeBot® provides continuous security validation services. It assists security testers in overcoming knowledge and experience limitations and always performs at a top-level. The shift from the manual-based, labor-intensive testing to machine-assisted automation alleviates the current severe shortage of security professionals. It allows human security experts to let go of daily labor-intensive work and devote more energy to the research of new threats and new technologies.

- Improve security test coverage and efficiency
- Reduce the cost of security validation
- Continuously protect the IT environment
- Produce actionable and reliable results for different stakeholders

RidgeBot® Key Functions

In a given task, RidgeBot® automates the entire attack process. When it connects to an organization’s IT environment, RidgeBot® automatically discovers all different types of assets on the network and then utilizes the collective knowledge database of vulnerabilities to mine the target system. Once RidgeBot® discovers vulnerabilities, it uses built-in hacking techniques and exploits libraries to launch a real attack against the vulnerability. If successful, the vulnerability is validated, and the entire kill-chain transaction is documented. RidgeBot® provides rich analytics for risk assessment and prioritization, exporting a comprehensive report with remediation advice. RidgeBot® is built with a powerful “brain” that contains artificial intelligence algorithms and an expert knowledge base that guides RidgeBot® in attack pathfinding/selection, launching iterative attacks that are based on learnings along the path to achieve much wider test coverage and deeper inspection. Due to its friendly usability and unlimited scalability, it is RidgeBot® is adopted by both large organizations as well as smaller web application development teams.

- **Asset auto-discovery** RidgeBot® can automatically identify broad types of assets, including networks, hosts, applications, plug-ins, images, IoT devices, and mobile devices are some examples.
- **Vulnerability mining** RidgeBot® leverages RidgeSecurity’s Threat Intelligence platform that includes 2-billion security intelligence data, 100 million attack libraries, and 150K exploit libraries.
- **Vulnerability exploits** The RidgeBot® supports various attack modes that meet customers’ different needs, automatically verifies the efficacy of the vulnerability findings, and ensures that the test outputs are accurate, reliable, and usable.
- **Risk Prioritization** The RidgeBot® visualizes the kill chain and quantifies the risks based on multiple factors that give organizations a clear idea of what to focus on first.

Asset Discovery Based on smart crawl techniques and fingerprint algorithms, discover broad types of IT assets: IPs, domains, hosts, OS, apps, websites, plug-ins, and network devices.

Vulnerability Mining Utilize proprietary scanning tools, our rich knowledge base of vulnerabilities and security breach events, plus various risk modeling.

Iterative Exploit Deploy a PoC payload to exploit vulnerabilities in target systems. Adjust the attack strategy in response to real-time data gathered from those targets.

Risk Prioritization Automatically generate an analytical view, visualize the kill chain, present attack logs, and showcase testing results with supporting evidence.

RidgeBot® System Architecture

The RidgeBot® system is architected in a layered structure. There are a total of six layers: a collection layer, data layer, algorithm layer, extraction layer, cognitive layer, and service layer. Each layer serves its upper layer and makes it functional.

- **The collection layer** imports threat intelligence data from Ridge Security Intelligence Platform or the 3rd party knowledge base.
- **Data layer** The data layer gathers data from the to-be-tested business systems. It labels and analyzes the data by matching with threat intelligence.
- **Algorithm layer** The algorithm layer provides varieties of artificial intelligence algorithms to build models for assets, threats, attacks, and many others.
- **Extraction layer** The extraction layer uses various models that are built from the algorithm layer to identify object fingerprints and vulnerabilities. This layer plans how to attack and exploit under the guidance of the "Expert Knowledgebase."
- **Cognitive layer** The cognitive layer feeds new learnings from a successful attack back to RidgeBot's knowledge map and completes the profile of a target system. This feedback loop evolves RidgeBot's platform.
- **Service layer** The service layer visualizes the result of the test with user-friendly graphics, for example, the Quantified Risk Score helps customers prioritize urgent issues, and the Security Compliance view helps users comply with patch regulations.

In the Continuous Security Vali-dation mode, RidgeBot® decides whether repeated, or iterative validation tests are needed on the fly. Once the predefined condition is triggered, the computer system schedules a thread to restart the task from the very beginning—the collection layer.

Service Layer	Risk Quantification	Security Compliance	Continuous Security Validation	
Corgnitive Layer	NLP	Knowledge Map	Target Profile	
Extraction Layer	Fingerprint	Vulnerability	Exploit Method	Detection Method
Algorithm Layer	Machine Learning	Deep Learning	Augumented Learning	
Data Layer	Data Collection	Data Labeling	Data Analysis	
Collection Layer	Ridge Threat Intelligence Platform	Third-Party Threat Intelligence Platform		

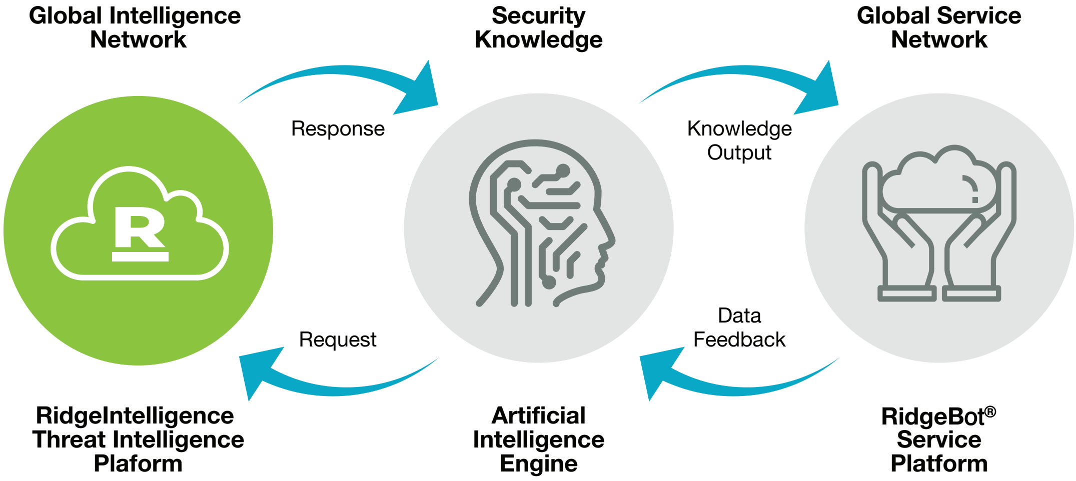
RidgeIntelligence Threat Intelligence Platform

Backend Platform

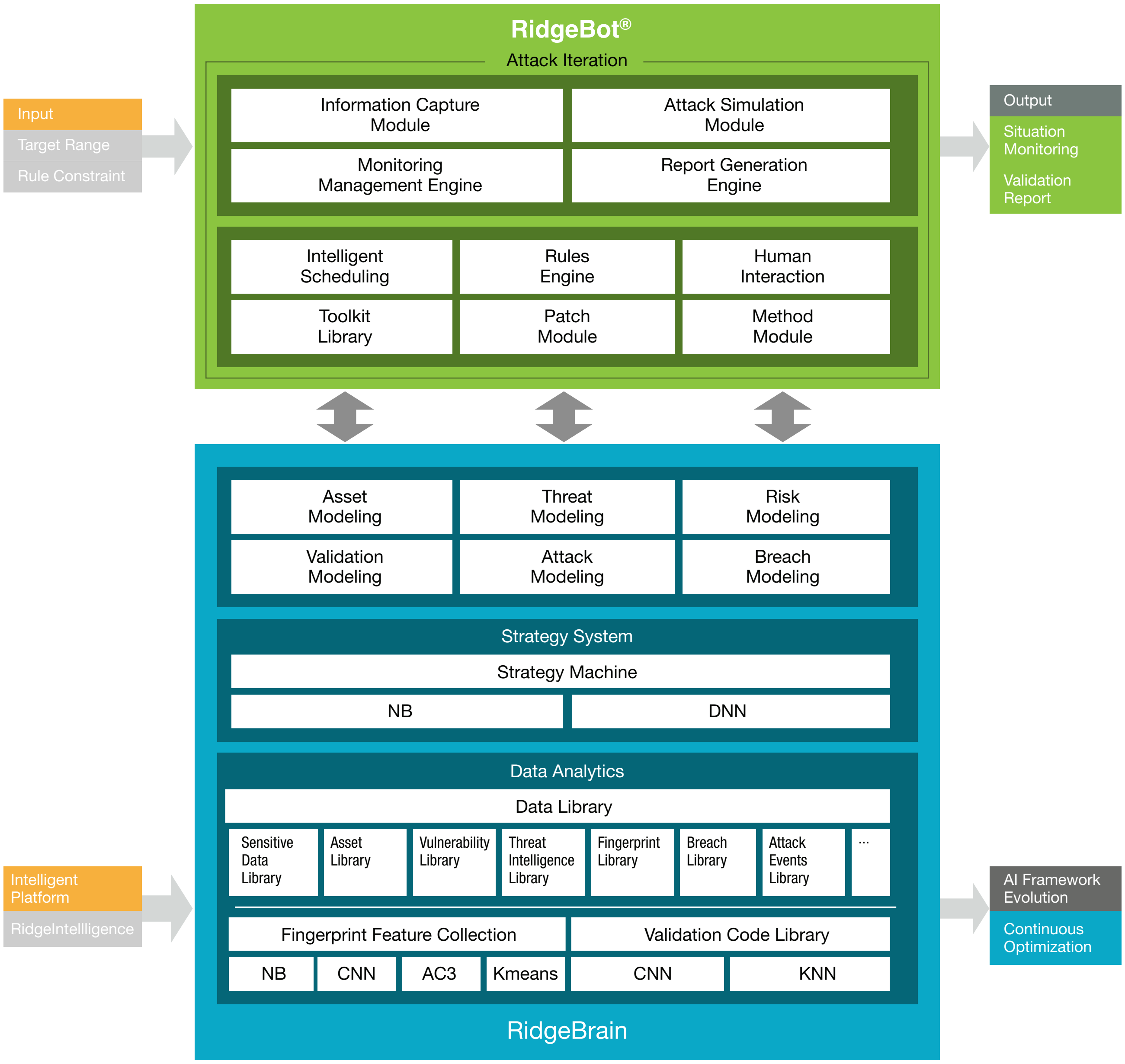
- **RidgeIntelligence Security—Threat Intelligence Platform** A proprietary network with nodes that are deployed around the globe to collect real-time malware and threat information and breach events.

- **RidgeBrain—Artificial Intelligence Engine** A central, decision-making, command center. It's a deep learning system that constructs RidgeSecurity's multi-dimensional and polymorphism knowledge map based on the information gathered from the Intelligence platform. It plans which path to take, which method to use, and what sequence to follow. It exports its security "knowledge" and decisions to the Ridge Service Platform to execute.

- **RidgeBot®—Service Platform** The Ridge Service Platform is the execution arm, RidgeBot®—the Security Validation Robot. It relentlessly pokes and launches real-world attacks and shows how a vulnerability is exploited and its consequences.


Global Intelligence Network
Security Knowledge
Global Service Network
Response
Knowledge Output
R
Request
Data Feedback
RidgeIntelligence Threat Intelligence Plaform
Artificial Intelligence Engine
RidgeBot® Service Platform

- **Machine Learning Framework** RidgeBrain introduces numerous machine learning algorithms in various tasks, including image recognition algorithms (such as CNN, KNN etc.); feature recognition and classifica-tion algorithms (such as NB, CNN, A3C, KMeans, etc.); and decision-making algorithms (NB, DNN, etc.). It supports a wide range of scenarios by using algorithm combinations.



RidgeBot® Differentiations

Higher Precision, More Discoveries

RidgeBot®, built with one of the world's largest exploit database, adopts the open-community's findings, 3rd party intelligence, as well as Ridge Security's global research. Ridge Security has deployed a large number of global nodes, especially in the region where attacks are prolific. Besides its global intelligence network, the RidgeBot® platform supports integration with any 3rd party intelligence system via API.

RidgeBot® is powered by RidgeBrian—an intelligent expert system with patentable machine learning and feature recognition, and AI algorithms. With image recognition algorithms and hacking techniques, RidgeBot® smartly bypasses security checks, obtains credentials, and gains escalated privileges just like an experienced hacker. Also, guided by its knowledge map, RidgeBot® can launch sophisticated attacks such as associated target attacks, later-al movement, and joint vulnerability exploits to achieve multi-layer penetration and iterative attacks on targets and associated IT assets. It maximizes the value of security testing and reports precisely on what and how the vulnerability could be exploited.

Equipped with both RidgeIntelligence and RidgeBrain, RidgeBot® not only discovers more vulnerabilities than traditional scanning tools but also achieves higher precision in vulnerability validation.

Unlimited Scalability, High Efficiency

RidgeBot® provides 24*7 online monitoring services and is ready to accept work orders at any given time. It supports concurrent execution of multiple, continuously running tasks. Its distributed architecture supports linear scalability via clusters and load balancing. Its performance scales with no limit in the cloud platform or virtual machine deployment.

Wider Range of Coverage

RidgeBot® supports asset identification in the broadest range of types in IT domains, including IPs, Networks, Hosts, Applications, Plugins, Web Pages, Operating Systems, Mobile devices, and IoT devices. It also can launch attacks from global or local, from Intranet, Internet or Extranet. As long as the network connection is reachable, RidgeBot® can do the job.

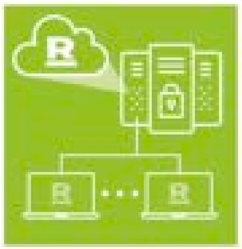
Multi-dimensional Data Analytics, Self-defined Alerts

RidgeBot® conducts quantitative assessments of multiple types of assets from dimensions such as attack surfaces, kill chain, vulnerabilities, and risk scoring, providing multiple views of a security perspective to serve different needs from various levels of stakeholders.

RidgeBot® gives customers immediate feedback on how their networks respond to a specific threat by imitating a real-world attack, allowing customers to protect assets from specific threats and malware proactively. Customers can set self-defined alerts to get informed once a condition is triggered so that they can be on top of security events that are concerned. Customers can also seamlessly integrate this part of RidgeBot‘s capabilities into their existing infrastructure.

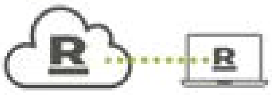
Deployment Scenarios

RidgeBot® can be deployed on-premise or in the cloud platforms.



On-Premise Deployment

Ridge Security offers on-premises deployment options. Users can opt to deploy RidgeBot® on virtual machines or bare metal servers, connecting it into the customer's IT network with the necessary permissions. For the minimum hardware specifications required, please refer to the RidgeBot's data sheet.



Cloud Deployment

RidgeBot® can be deployed on several cloud platforms, including AWS EC2, Microsoft Azure, and Google Cloud. Typically, users set up RidgeBot® within their own VPC or tenant to assess the security posture of their cloud infrastructure.

Company Profile

Ridge Security is revolutionizing Security Validation with RidgeBot®, an AI-Enabled Security Validation Platform. RidgeBot® is designed using techniques drawn from the strategies of countless real-world attacks. Once deployed within a system, RidgeBot® tirelessly seeks out vulnerabilities, exploits them, and meticulously documents the findings. It operates within a set scope and can swiftly adapt to address intricate structures. Ridge Security equips enterprises, web application teams, ISVs, DevOps, governmental agencies, educational institutions, and essentially anyone tasked with ensuring software security, to test their systems both affordably and effectively.

Ridge Security Technology Inc.
www.ridgesecurity.ai