RidgeBOT

Intelligent Security Validation Robot

RIDGE SECURITY

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 a hacker 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 manageable and cost-effective way.

However, nowadays, attackers are always developing new exploits and attack methods, and often using machine learning (ML) 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 affordably 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.

Vulnerability Exploit Use a smart sandbox to simulate real-world attacks with toolkits. Collect more data for a further attack in a post-breach stage.

Risk Prioritization Automatically form an analytic view, visualize a kill chain and display a hacker's script. Show hacking results like data and esca-lated privileges from the compromised objects.

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.

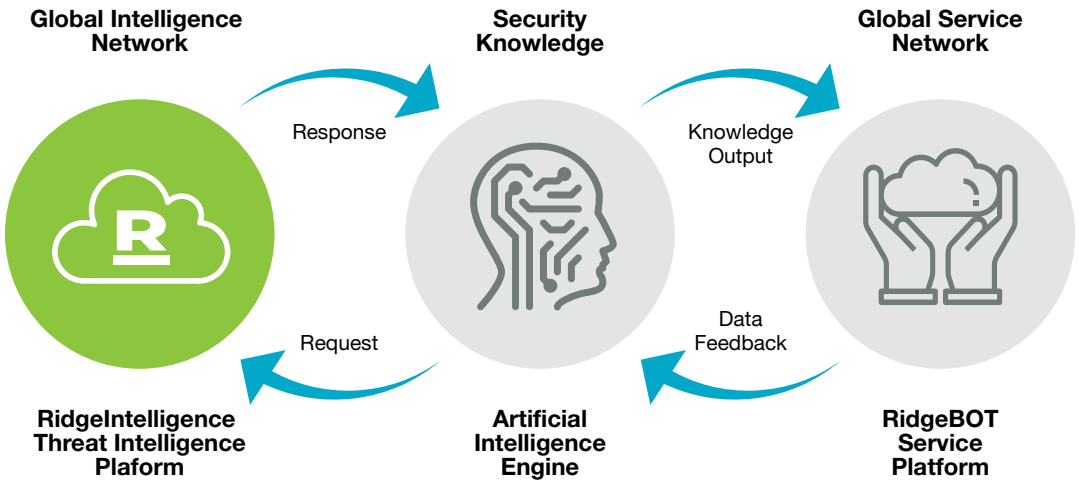
- **The collection layer** imports threat intelligence data from Ridge Security Intelligence Platform or the 3rd party knowledge base.
- **Data layer** The data layer gathers data from the to-be-tested business systems. It labels and analyzes the data by matching with threat intelligence.
- **Algorithm 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 Validation 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 Portrait	
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

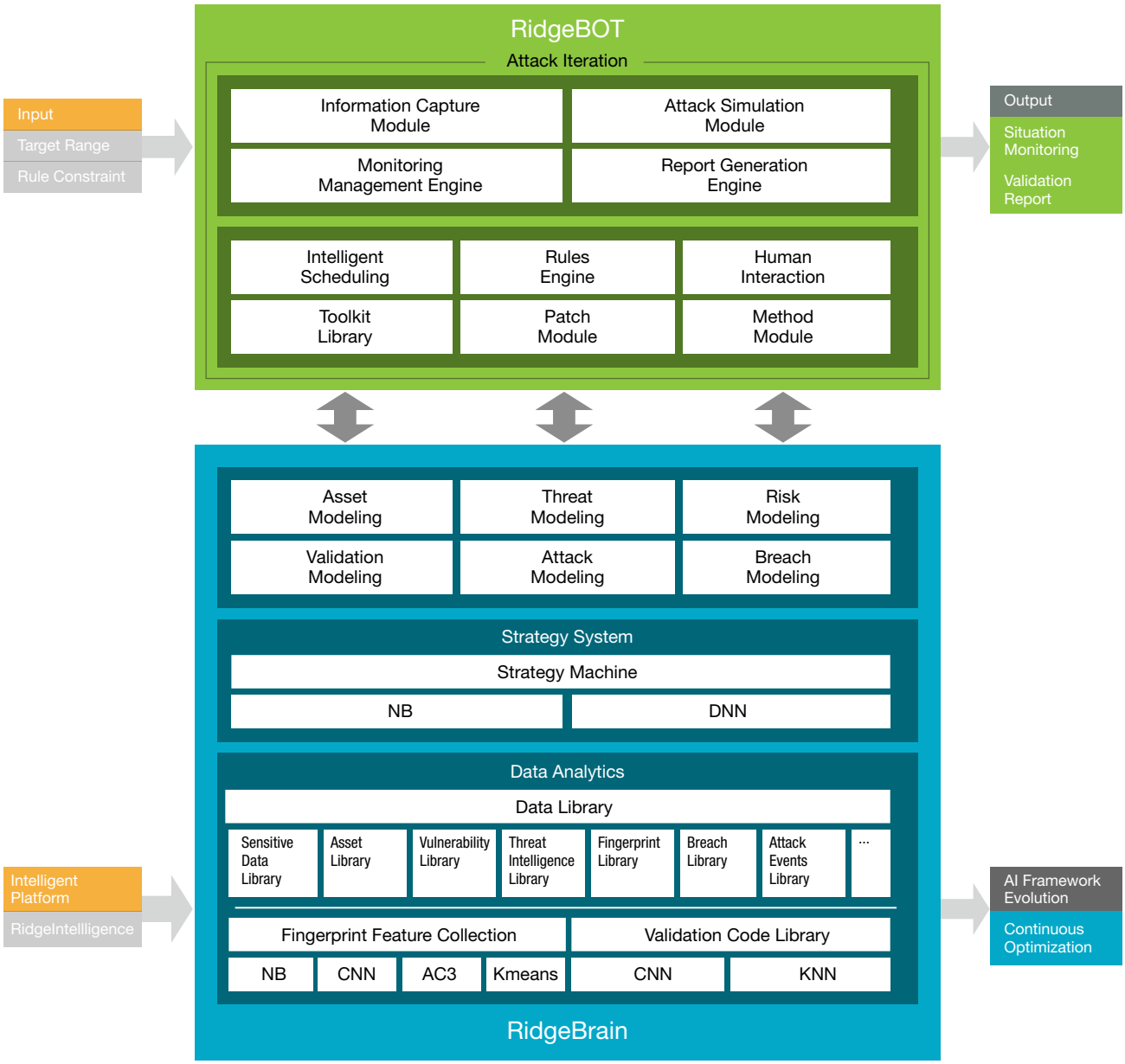
Backend Platform

- **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.



Machine Learning Framework

RidgeBrain introduces numerous machine learning algorithms in various tasks, including image recognition algorithms (such as CNN, KNN etc.); feature recognition and classification 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 patented 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, lateral 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 7x24 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

There are three ways to deploy RidgeBOT: SaaS mode, VPN mode or On-premise mode.

SaaS Mode

RidgeSecurity offers security validation as a service from its cloud platform. Customers can subscribe to its service and use it as needed.

VPN Mode

Ridge Security RidgeBOT SaaS cloud platform supports a Virtual Private Network (VPN) configuration option. Users connect to the RidgeBOT SaaS platform via designated VPN tunnels and initiate security validation service on their networks and systems. RidgeBOT SaaS cloud platform also supports the combined use of the SaaS and the VPN Modes.

On-Premise Mode

Due to security compliances or regulations, remote access via the cloud platform or VPN tunnel is not allowed, or specific business-critical systems are restricted to access from an external network. In this scenario, Ridge Security provides on-premises deployment. The RidgeBOT system can be offered in a specialized hardware appliance or as a software image to run on any virtual machines with on-premise servers.

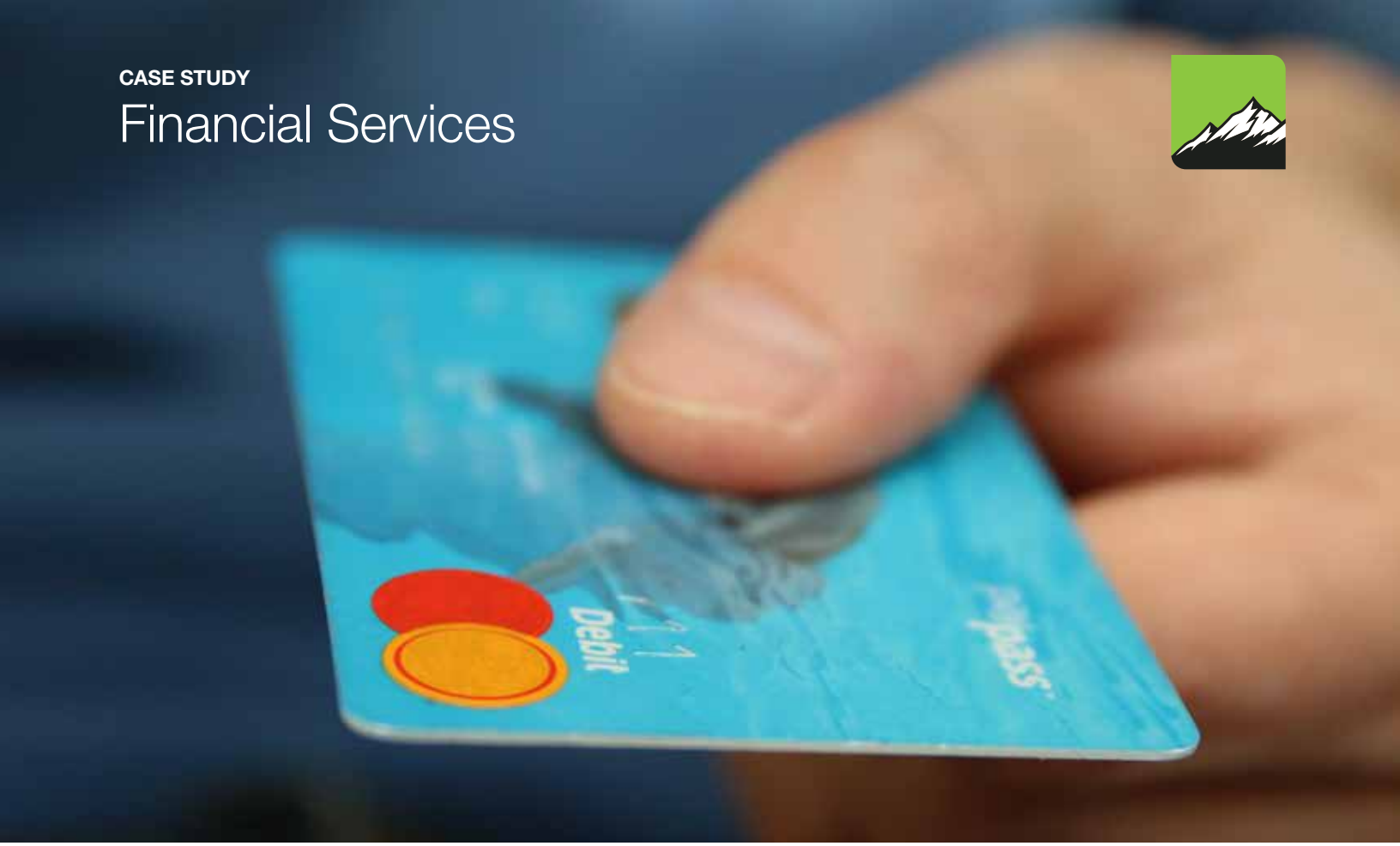
The RidgeBOT hardware appliance or software image is preloaded with the RidgeThreat Intelligence database and RidgeBrain algorithms. With a purchased license, the hardware appliance or virtual image is activated.

The RidgeBOT system is deployed in the location specified by the customer and with an approved configuration. It connects to the customer’s IT network with appropriate authorization.

One or multiple hardware appliances/virtual machines form the RidgeBOT platform, which accomplishes various security validation tasks based on the user’s needs.

CASE STUDY

Financial Services



Ridge Security Solution

The organization chose to deploy the RidgeBOT64 hardware platform on-premise with Ridge Security professional service. A senior security consultant from Ridge Security conducted penetration testing and reported the result with remediation suggestions.

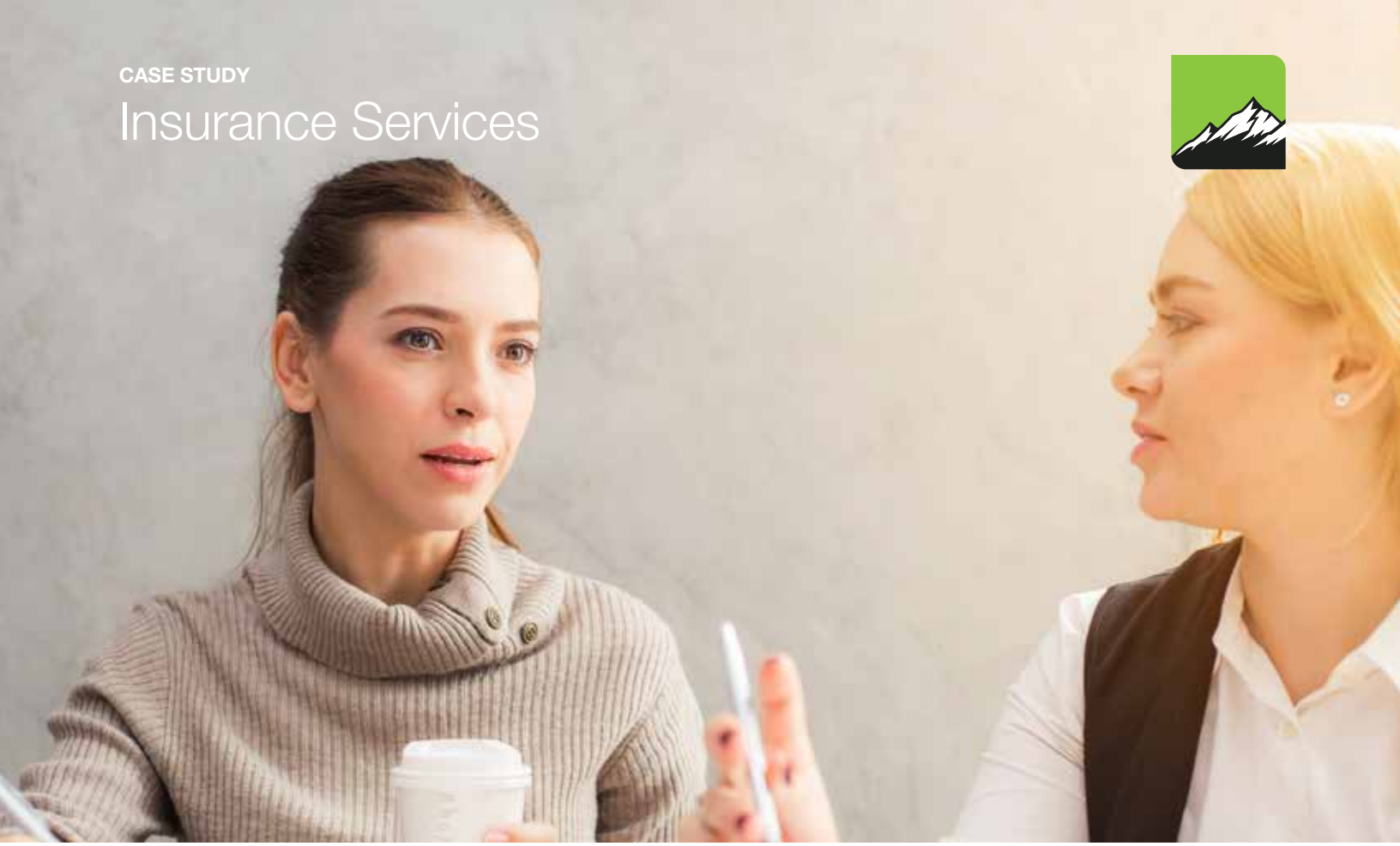
Customer Benefits

RidgeBOT solution benefits the customer in the following ways

1. RidgeBOT's platform-based services can be "on call" 7*24, the customers can get the testing running at any given time and keep continuous monitoring. And, with intelligent machine learning algorithms built-in, RidgeBOT keeps digging deeper to uncover more potential issues than other system used before. It maximizes the value of the testing. Its self-evolving approach keeps up with the change of the security landscape as well as the customers' IT environment. It delivers high-quality testing with consistency.
2. RidgeBOT is easy to configure. Its usability and scalability make it suitable for this large organization to adopt it through the entire company. RidgeBOT's machine-based test program followed a defined process and generated a standardized report with different levels of details and from multiple perspectives. The report's consistency in formats and various choices in contents made conversations easier across organizations and different levels of stakeholders.
3. Data was in full control during the test; no loss happened. RidgeBOT prevents data loss:
   - Kept a full logging during the test. RidgeBOT logged every step during the test and stored the information in a database available for audit. Each operation was traceable and can be thoroughly analyzed.
   - RidgeBOT was installed in a secured and controlled physical environment designated by the customer. During the test, the RidgeBOT platform was the sole entry connecting to the customer's network; all the information and data were recorded and stored in a RidgeBOT server. The RidgeBOT server resided in a secured physical area and was in full control of the customer.
   - RidgeBOT is a proprietary platform; RidgeSecurity has full control over how it works. Therefore, RidgeSecurity can assure the customer that there is no connection beyond the customer's premise and that data is is secure.

CASE STUDY

Insurance Services



Customer Profile

Some of this insurance company's businesses are web-based applications offered via the Internet. They were facing several challenges in cybersecurity before using RidgeBOT:

1. Their security infrastructure was quite weak; no complete defense system was established.
2. They lacked security personnel: only "a few hands in the security team."
3. Their security team was under extreme time pressure when there were new software upgrades and updates. And It is easy to imagine such releases are quite frequent.

Business Goal

To overcome the above challenges, the customer needed to achieve the following goals with security validation service:

1. Minimize mitigation efforts by putting the best efforts to prevent before their software was released. The test shall cover both breadth and depth.
2. Minimize the workload of their security personnel
3. A good ROI that balances between investment and return.

Ridge Security Solution

The customer deployed the RidgeBOT in SaaS mode. The test was performed via the Internet, but the entire process was initiated, tracked, viewed then terminated by the customer's security team. With RidgeBOT's SaaS mode, the service can be ordered and launched whenever needed.

Customer's Benefits

As the platform is cloud-based, it satisfied the customer with the convenience of use and high cost-performance. It presented a great ROI. RidgeBOT reduced the efforts required from the customer's security team by automating the whole testing process and providing many ease-of-use features such as a one-click retest, and auto-generated reporting with remediation strategies. RidgeBOT performed multi-layered iterative attacks that ensured a thorough inspection of any software before its release to the market.

CASE STUDY

Manufacturing

Customer Profile

The customer is a leading brand of home appliances. It has multiple plants and product lines in different physical locations. In their modern factories, scheduling, planning, and supply management have been making their IT systems more and more complex. However, security was not a priority in the past, and cyber risk is high.

Customer Top Priority

1. Build internal security validation capabilities rather than use temporary external security services.
2. Be able to identify a wide range of assets, including IT systems, mobile devices, and IoT devices. Also, they need to inspect a large number of assets in a short time frame.
3. Provide accurate validation and effective remediation

Ridge Security Solution

The customer deployed a combination solution of RidgeScan and RidgeBOT128 on their corporate intranet. Through the unified management interface, RidgeScan and RidgeBOT can coordinate task distribution. They worked in parallel and streamlined the vulnerability of mining and validating. The inspection of the customer's large number of assets were completed in time.

Company Profile

RidgeSecurity is transforming Security Validation with RidgeBOT, an Intelligent Security Validation Robot. RidgeBOT's is modeled using the techniques utilized by literally millions of hackers that penetrate systems. When deployed within a system, RidgeBOT's are relentless in their quest to locate, exploit, and document their findings. They work within a defined scope and instantly replicate to address highly complex structures. RidgeSecurity enables enterprise and web application teams, ISVs, DevOps, governments, education, anyone responsible for ensuring software security to affordably and efficiently test their systems.

Ridge Security Technology Inc.
2010 El Camino Real PMB 3017
Santa Clara, CA 95050
www.ridgesecurity.ai