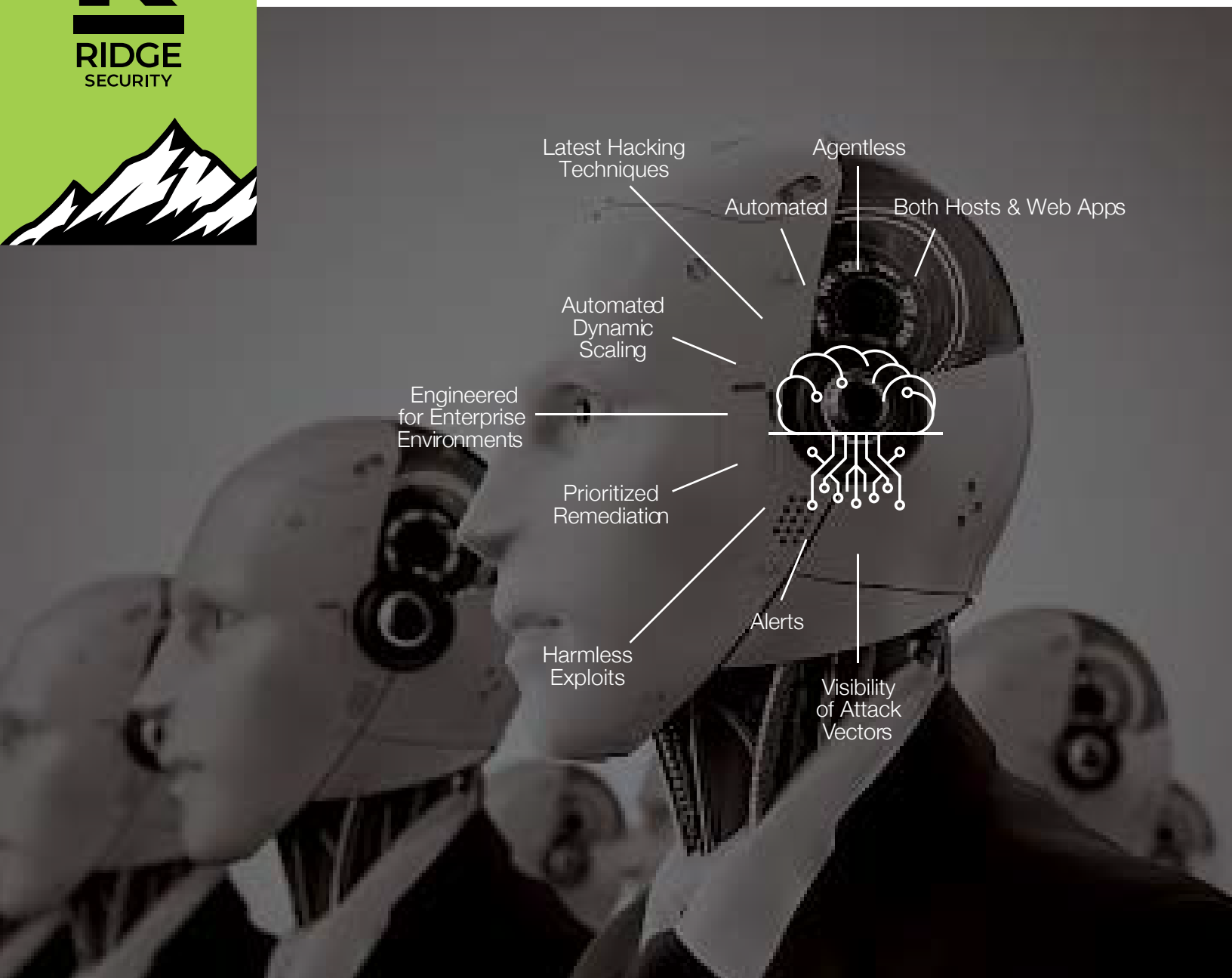
Enterprise Security Validation HyperAutomation

RIDGE SECURITY

RidgeBot®

Intelligent Security Validation Robots to deliver Automated Penetration Testing and Adversary Cyber Emulation



RidgeBot® automates the enterprise IT security validation process 100x faster than a human tester

Ridge Security is changing the game with **RidgeBot®** , an intelligent security validation robot. Unified with state-of-the-art ethical hacking techniques and operationalized threat intelligence, **RidgeBot®** helps enterprises to verify its external risk exposures and internal security controls. **RidgeBot®** has a collective knowledge of threats, vulnerabilities, exploits, adversary tactics and techniques. Acting like an experienced ethical attacker, **RidgeBot®** relentlessly locates, and documents exploits, pinpoint security control failures. Automating enterprise security validation makes it affordable with the ability to run at scale. Working within a defined scope, **RidgeBot®** instantly replicates to address highly complex structures.

Ridge Security enables enterprises, web application teams, DevOps, ISVs, governments, healthcare, education – anyone responsible for ensuring software security – to affordably and efficiently test their systems.

Challenges

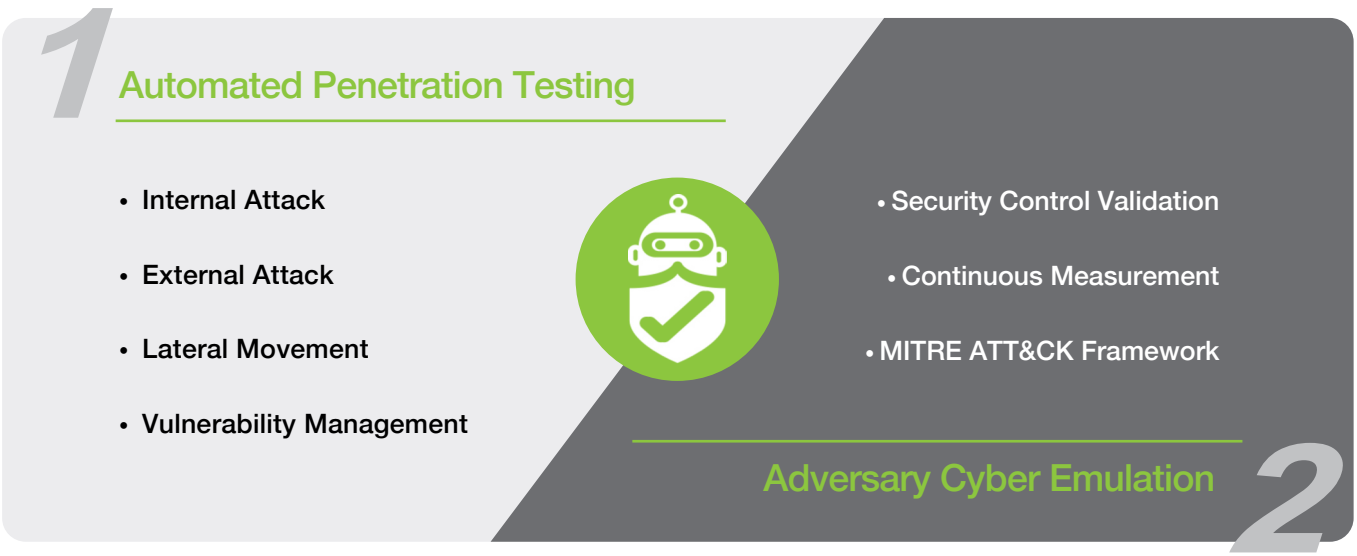
Today's organizations are facing cyber security challenges from multiple angles. Security teams not only need to validate IT infrastructure has no exploitable vulnerabilities which may be leveraged by a hacker or a ransomware to compromise the mission critical data, but also need to verify the expensivee cyber defense solutions deployed can work as expected to detect and mitigate the most current attack techniques used by advanced persistent threats (APTs) and other malicious entities.

Cyberattacks are increasingly sophisticated and forever on the rise, hackers are developing new exploits and attack methods every month, often using tools to launch attacks automatically. In response to cyber security threats, most organizations utilize security testing (a.k.a. penetration testing) for their computer systems, websites, applications and networks, try to find risk exposures before a hacker does. While security teams' internal pen testing expertise are limited and expensive, can't afford to do continuous security validation. Many organizations are looking for an automated penetration testing system to address this challenge in a more manageable and cost-effective manner.

RidgeBot's Solution and Key Benefit

RidgeBot® is a unified system that automates the penetration testing process and emulates adversary attacks to validate an organization's cybersecurity posture. It provides a clearer picture of your security gaps and keeps the windows of opportunity closed for malicious attackers by increasing the frequencies of penetration testing, risk-based vulnerability management and training your defense team with effective exercises RidgeBot® assists security team in overcoming knowledge and experience limitations and always performs at a consistent top-level. The shift from 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 infrastructure
- Produce actionable and reliable results for different stakeholders



RidgeBot® Brings **360-degree security validation** within reach of every organization.

RidgeBot® Key Functions

Automated Penetration Testing

In a given task, RidgeBot® automates the entire ethical hacking 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 attack surfaces of target system. Once RidgeBot® identifies vulnerabilities, it uses built-in hacking techniques and exploit libraries to launch real ethical attack against the vulnerability. If successful, the vulnerability is validated and the entire kill-chain transaction is documented. RidgeBot® provides rick analytics for risk assessment and prioritization, exporting a comprehensive report with remediation advice, giving tools for patch verification.

Asset Profiling—Based on smart crawling techniques and fingerprint algorithms, discover broad types of IT assets,: IP's, domains, hosts, OS, apps, websites, database and network/OT devices

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

Vulnerability Exploit—Use multi-engine technology 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 escalated privileges from the compromised objects.

Adversary Cyber Emulation (ACE)

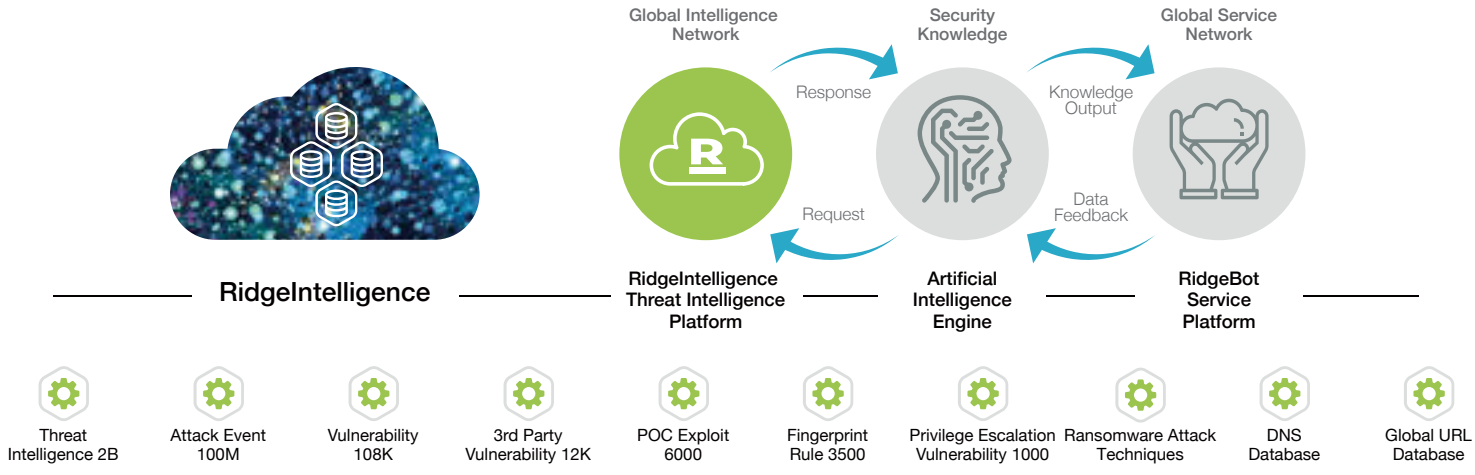
IT security controls are mechanisms used to prevent, detect and mitigate cyber threats and attacks. RidgeBot® ACE emulates the adversary by mimicking the likely attack paths and techniques to generates continuous assessment data to help identify security control failures, resolve structural weaknesses and enable security control optimization. RidgeBot® ACE has aligned itself with the MITRE ATT&CK framework and maps its assessment test scripts to MITRE ATT&CK tactics and techniques. This increases the visibility of potential attack vectors and improves the communication of security control measurements.

Assets Management

RidgeBot® assets management provides a centralized repository to manage enterprise IT assets for security validation, including assets' IP addresses, hostnames, OS versions, service open ports, active applications with app versions, as well as website domain names, DNS resolution and web server versions.

Higher Precision and More Discoveries with AI Brain

RidgeBot® has a powerful "brain" that contains artificial intelligence and an expert knowledge base that guides RidgeBot® in attack path finding/selection. It launches iterative attacks based on learnings along the path, achieving more comprehensive test coverage and deeper inspection.

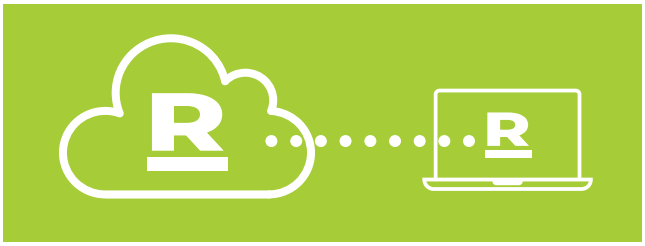


RidgeBot® Deployments

On-Premise Deployment

For enterprise environment—deploy RidgeBot® on the customer's premise, provides the lower Risk of Infosec Data Leakage

Cloud Deployment



For Cloud and SMB customers—deploy RidgeBot® in the Cloud (AWS EC2, Microsoft Azure and Google Cloud), have better flexibility while minimize the initial CapEx investment

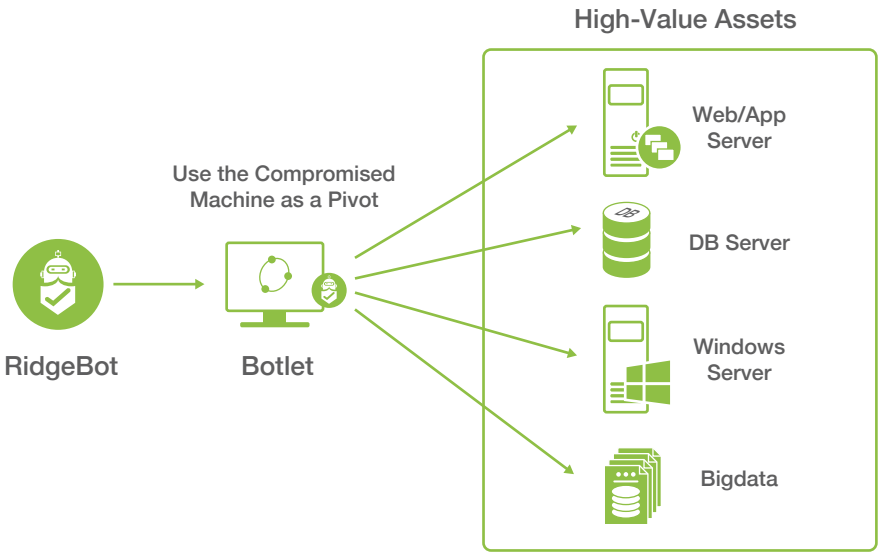
Penetration Testing Scenarios

Internal Attack. Launch attacks from inside of Enterprise network with customer's permission, focusing on exploiting vulnerabilities discovered on local network and systems.

External Attack. Launch attacks from outside of Enterprise network towards publicly accessible assets such as organizations' websites, file shares, or services hosted in public cloud/CDN.

Lateral Movement. Escalate privilege on a compromised asset and use the compromised asset as a pivot to launch attack toward adjacent networks; discover and exploit vulnerabilities on assets deeper in the network.

RidgeBot Lateral Movement



Adversary Cyber Emulation (ACE) Methods

Agent-Based Attack Simulation: RidgeBot® uses agent-based Botlet to simulate adversary attacks. RidgeBot® Botlet can be deployed on multiple OS platforms and in different network segments to simulate real-world cyber threats continuously or on-demand.

Out-of-Box Assessment: RidgeBot® offers pre-built ACE assessment test templates, make it simple for all skill levels to assess the efficacy in different aspects of your security controls. The assessment tests are comprehensive and safeto launch in the production environment

MITRE ATT&CK Framework Alignment: The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used extensivelyby RidgeBot to create meaningful and life-like assessment test scripts for its customers to challenge, assess and optimize their security controls.

RidgeBot System Requirements

The RidgeBot® solution is a software package deployed on specified bare metal servers, virtual machines or in the Cloud. The RidgeBot® software package includes the RidgeIntelligence platform, the RidgeBrain engine, and RidgeBot® plugins. Software upgrades are provided through professional services. We recommend on-premise deployment for organizations to have complete control over test procedures, findings, and sensitive data involved.

Bare Metal Server Deployments	**Essential**	**Advanced**
Minimum Hardware Requirement	• Intel Xeon CPU with a minimum of 4cores with Hyper-Threadin • 32 GB RAM • 1TB SSD • 1 Ethernet Interface Card	• Dual Intel Xeon CPUs with a minimum of 6 cores each • 64 GB RAM • 2 X 1TB SSD with RAID controller (RAID 1) • 1 Ethernet Interface Card
Reference Platforms	**Dell PowerEdge R340 Rack Server** • Intel Xeon E-2278G 3.4GHz, 16M cache, 8C/16T, Turbo (80W) • 32 GB (2 x 16GB 2666MT/s DDR4 ECCUDIMM) • 960GB SSD vSAS Mixed Use 12Gbps512e 2.5in with 3.5in HYB CARR Hot-Plug AG drive,3 DWPD 5256 TBW • https://www.dell.com/en-us/work/shop/productdetailstxn/poweredge-r340	**Dell PowerEdge R540 Rack Server** • Dual Intel Xeon Silver 4208 2.1G, 8C/16T, 9.6GT/s,Turbo, HT (85W) DDR4-2400 • 64 GB (2 X 32GB RDIMM, 3200MT/s, Dual Rank) • PERC H730P RAID Controller, 2GB NVCache,Adapter , Low Profile • 2 X 960GB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYBCARR, 3 DWPD, 5256 TBW, RAID 1 https://www.dell.com/en-us/work/shop/productdetailstxn/poweredge-r540
Concurrent Bots	16	32

Virtual Machine/Cloud Deployments	**Demonstration/Lab**	**Production**
Minimum Hardware Requirement	• 8 vCPU • 16 GB RAM • 100 GB Storage • 1 Virtual Network interface	• 8 vCPU • 32 GB RAM • 100 GB Storage • 1 Virtual Network interface
Concurrent Bots Supported	16	32
Supported Hypervisors and Cloud Platforms	• VMware Workstation 15 Pro or higher • VMware Fusion 11 Pro or higher • VMware ESXi 6.5 or higher • Microsoft Windows/Hyper-V 2019 or higher	• QEMU KVM 7.2 • Amazon AWS EC2 • Microsoft Azure • Google Cloud Platform

RidgeBot® Key Features

Automation Assistance

- **Object recognition:** Through this function module, RidgeBot® automatically identify information such as asset types, data content types, record classification Identifiers and then feed them to relevant modules, so that the entire attack process can continue to run without any manual intervention and achieve the automated process of security validation
- **Sandbox simulation:** Using the sandbox technology, RidgeBot® simulates a variety of operating environments in the validation task, provides an automatic response to interactive scenarios during the attack, so that the automated process of security validation can be done.
- **Embedded Fuzzing Engine:** Generating dynamic payloads for vulnerability detection and exploitation

Artificial Intelligence

- **Turing confrontation:** By using Turing confrontation technology, RidgeBot® can recognize character validation code and simulate manual operations through a smart sandbox to bypass the manual operation inspection required by the system, so that the system can perform an automatic execution of security inspection which improves the efficiency of security testing.
- **Decision brain:** RidgeBot® is built in with many types of artificial intelligence decision-making algorithms to provide optimal decisions such as selection and ranking when executions are going down to branch attack paths.
- **Expert system:** RidgeBot's is embedded with an expert system. During the execution of the security validation, it can always reference "expert experience" for a better decision or a more effective path to penetrate the target system.
- **Vector engine:** The vector engine creates attack vectors and non-linear stitching which enable RidgeBot® to produce more efficient attack with high successful rate toward the targeted system.

Risk Analysis

- **Topology portrait:** Automatically generate a topology map from the information collected during the attack, label the risks identified in each part of the topology, and assist administrators in risk analysis and evaluation.
- **Proactive situational awareness:** Proactively poke the targeted system from multiple perspectives to form a multidimensional analysis view and the real-time graphic models; provide administrators a global view of the security landscape.
- **Real time attack action visibility:** Provide real time visibility to every single step of the attack, from discovery, scanning to exploit attempts for security team to further analyze.

Vulnerability Mining

- **Weakness discovering:** Identify possible weak links on the attack surface and check for vulnerabilities based on the intelligent decision system such as the expert models and RidgeBot brains.
- **Vulnerability scanning:** Access and test the target system by using packet generated by an automatic tool and the payload provided by the attack component, vector engine etc., and the returned results are checked to determine whether there are vulnerabilities that can be exploited.

Vulnerability Exploitation

- **Attack Vector Supported:**
  Network attack: Explore network connected target machines, proactively discover and exploit security flaws on target machines to gain access.
  Local attack/Privilege Escalation: After gaining a lower privilege access on the target machine, exploit additional vulnerabilities from local to gain elevated privilege.
  Lateral Movement: Gain control of a compromised asset anduse it as a pivot to exploit other target machines on adjacent networks.
- **Attack Coverage**
  Host Servers (Windows, Linux, Unix, MacOS and others), Web Servers, Application Servers, Database Servers (Oracle, IBM DB2, MS SQL Server, MySQL, PostgreSQL and others), Virtualization Platforms, Network Equipment, IoT Devices and Bigdata
- **Attack User Intervention Mode**
  Enable experienced pentesters to control the attacks of high impact penetration testing plugins, provide better risk control and attack visibility
- **Application Security Testing**
  Support Dynamic Application SecurityTesting (DAST)
  Support Authenticated Web Penetration Testing with built-in web login sequence recorder and proxy mode.

- **Brute Force Weak Password**
  Dedicated security validation scenario for and OS, application and database weak taking credential exploit.
- **Automatic SQL injection testing**
  Automates the process of detecting exploiting SQL injection flaws and over of database servers.
- **Customizable pentest plugins**
  User customizable application fingerprint, attack vector, vulnerability detection payload, vulnerability exploitation payload (scripts and rules) as well as remediation suggestions

Vulnerability Validation

- **Risk validation:** Validate whether the vulnerability is exploitable in user's real environment by using proof-of-concept payload generated by RidgeBot knowledge base and auto-exploitation engine. Proof of a successful exploitation is provided for validated risks, includes privilege obtained, screenshots, shell terminal, file manager, database name or database table name etc.
- **Kill-Chain Visualization:** Visualize the full attack path with attack sequence information, including target machine information, attack surface exposure, vulnerability discovered and vulnerability exploited.
- **Risk Assessment:** Provide real-time risk assessment for IT assets being tested, including health score rating and vulnerability details & risk analysis
- **Patch validation test:** Retest after patch is installed to verify whether the vulnerability has been fixed.

Adversary Cyber Emulation

- RidgeBot Botlet supports both 32-bit and 64-bit Windows and Linux platforms
- Assessment test scripts are mapped to Threat Groups and MITRE ATT&CK and Techniques

Task Management

- **Task scheduling:** Support 1) Run Now, 2) Run Once, 3) Weekly (Daily) 4) Monthly task scheduling
- Support multiple runs within a weekly/monthly task cycle
- Support scheduled pause for penetration testing tasks to minimize business disruption during a penetration testing
- **Stealth control:** 4-tier penetration testing flow control to control the traffic volume being sent to the target machines and minimize the impact to test targets

Asset Management

- A centralized repository to manage tested host and web targets, active applications/ services, OS and application versions, as well as domain names and DNS resolutions
- Botlet installation and status
- Configure integration connectors

Reporting and 3rd Party System Integration

- Professional Report: Provide professional security validation test reports with detailed asset information, vulnerability and risk data,assessment test results, mitigation suggestions, and historical trend
- Multi-language Reports: Support English, Spanish, Italian and Korean reports. The customer can select a preferred language before generating the reports
- System Integration: Support RESTful API and CEF-compliant syslog messages, easy to integrate
- OWASP Top-10 Compliance Reports. Support 2017 and 2021 versions of OWASP Top-10 definition. Dedicated OWASP Top-10 report templates for web penetration testing tasks
- Support scanning: result validation for Tenable, Nessus Pro and Rapid7 Nexpose VA scanners with 3rd-party security management platform. Support Token-based
- MSSP Co-branding Reports: Support report customization, and allow a MSSP (Managed Security Service Provider)user to add its company logo on testing authentication for API communication.
- DevSecOps Integration: Support Jira Software and GitLab for issue tracking

System Administration

- Support online and offline software updates
- Support user role-base access control for security validation tasks and reports
- Support local management console for system administration and service recovery
- Support two-factor authentication (2FA) or virtual private cloud (VPC) access
- Support OpenVPN for enterprise Intranet for web user login
- Support http/https proxy and SOCKS5 proxy for communication with license server and Jira/GitLab server

About Ridge Security Technology

Ridge Security delivers ethical, efficient and affordable security validation solutions to enterprises, small and large. We ensure our customers stay compliant, alerted and secure at all times in the cyber world. The management team has many years of networking and security experience. Ridge Security is located in the heart of Silicon Valley and is expanding into other areas including Latin America, Asia and Europe.

RidgeBot®, a robotic security validation system, fully automates the testing process by coupling advanced ethical hacking techniques and adversary cyber emulation. RidgeBots locate, exploit and document business risks and vulnerabilities discovered, IT security controls failures during the testing process, highlighting the potential impact or damage.

Contact Ridge Security to learn more.

Sales@RidgeSecurity.ai RidgeSecurity.ai/contact-us

Ridge Security Technology Inc.

www.ridgesecurity.ai

@RidgeSecurityAI

www.linkedin.com/company/ridge-security