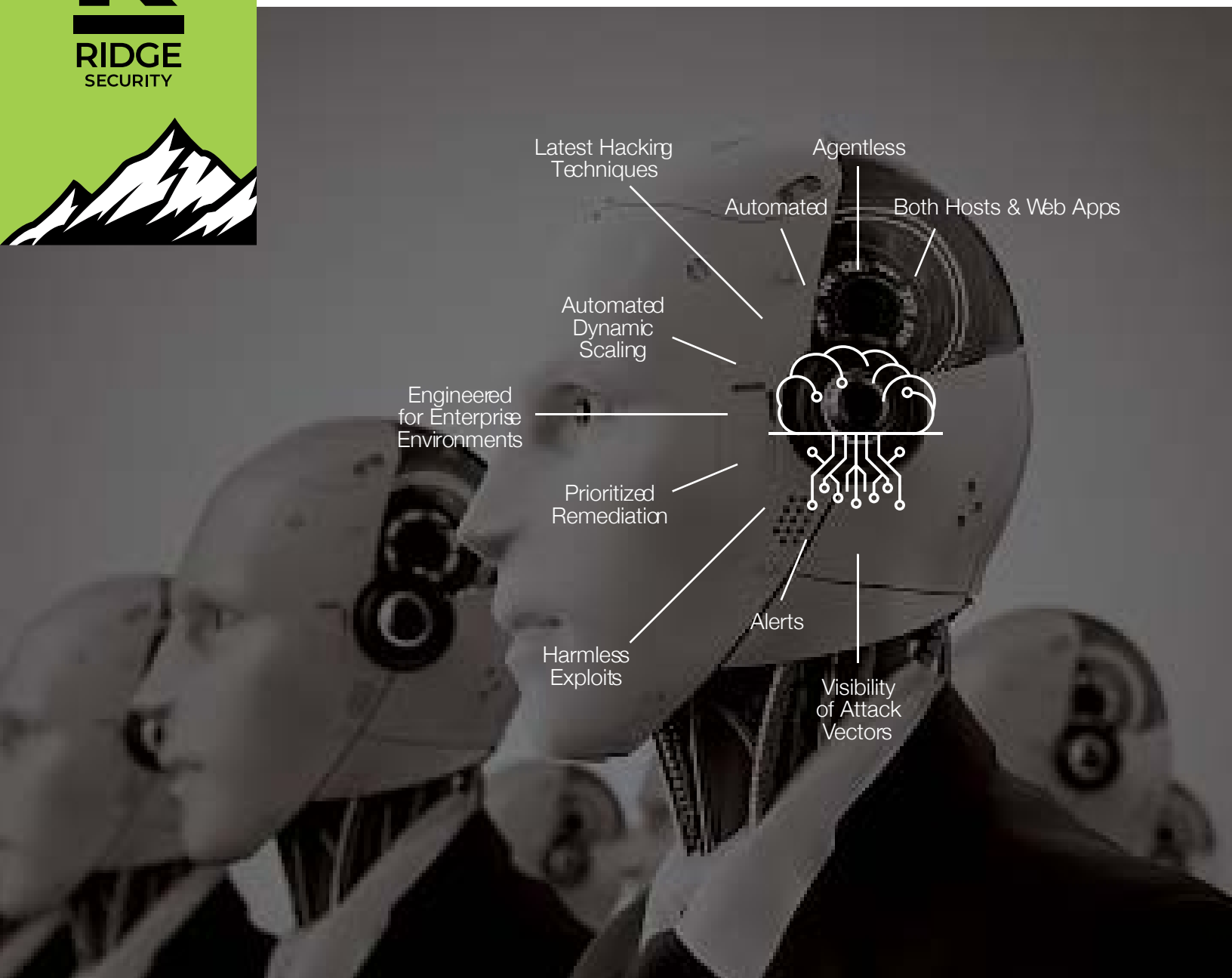
RidgeBot™ Brings Affordable Pen Tests to Your Organization

RIDGE SECURITY

RidgeBot™

Enterprise-Class Automated Penetration Testing Using Intelligent Validation Robots



RidgeBot™ automates the entire ethical hacking process 100x faster than a human tester

Ridge Security is changing the game with **RidgeBot**™, an intelligent security validation robot. Equipped with state-of-the-art hacking techniques, **RidgeBot**™ has a collective knowledge of threats, vulnerabilities, and exploits. Acting like an actual ethical attacker, **RidgeBot**™ relentlessly locates, and documents exploits. Automating penetration testing 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 and web application teams, DevOps, ISVs, governments, healthcare, education—anyone responsible for ensuring software security—to affordably and efficiently test their systems.

Challenges

Most organizations utilize security testing (a.k.a penetration testing) to validate the security posture of their network and systems. In such a test, security testers take on the role of a hacker and try to break into the organization's IT environment to find vulnerabilities and determine how they exploit a real-world hacker attack. The underlying idea is that a good security test should reveal how an attacker could infiltrate an organization's systems before it happens. Proper penetration testing helps organizations address issues in a more manageable and cost-effective manner.

However, attackers are always developing new exploits and attack methods, often using machine learning (ML) to launch attacks automatically. Enterprises' security teams and professional "penetration testers" are under tremendous pressure to keep up.

RidgeBot's Solution and Key Benefit

RidgeBot™ provides automated security validation services. It assists security testers 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 environment
- Produce actionable and reliable results for different stakeholders

RidgeBot™ brings **automated penetration testing** within reach of every organization.

RidgeBot™ Key Functions

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 target system. Once RidgeBot™ identifies vulnerabilities, it uses built-in hacking techniques and exploits libraries to launch an actual ethical 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, giving tools for patch verification.

Asset Profiling—Based on smart crawl techniques and fingerprint algorithms, discover broad types of IT assets: IPs, domains, hosts, OS, apps, websites, plugins, and network devices.

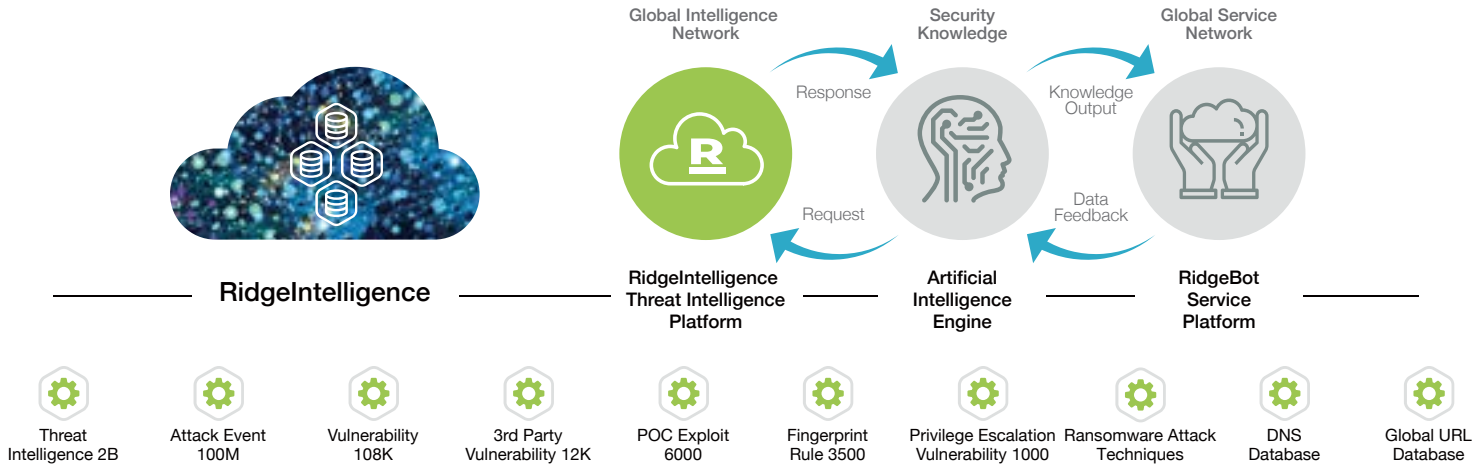
Vulnerability Mining—Utilizing proprietary scanning tools, our rich knowledge base of vulnerabilities and security breach events, plus various risk modeling.

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 escalated privileges from the compromised objects.

Higher Precision and More Discoveries with AI Brain

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

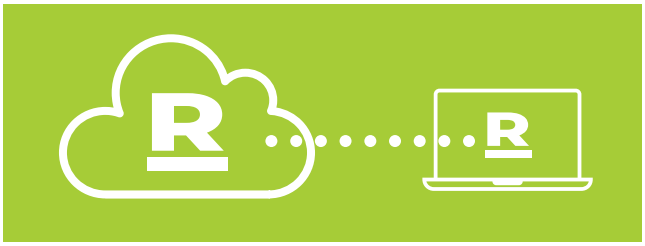


RidgeBot™ Deployments

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 and Microsoft Azure), have better flexibility while minimize the initial CapEx investment

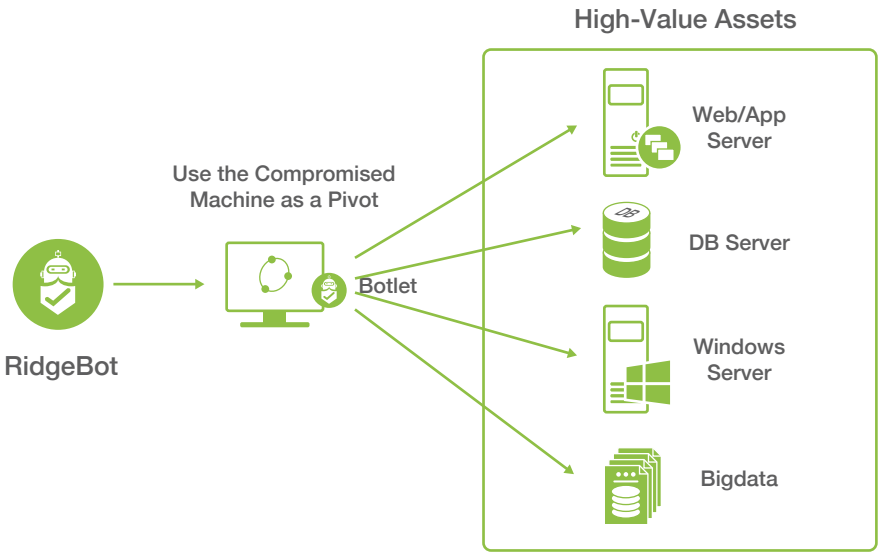
Pentest Scenarios

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 adjacement networks; discover and exploit vulnerabilities on assets deeper in the network.

RidgeBot Lateral Movement



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 4 cores • 32 GB RAM • 1TB SSD • 2 Ethernet interfaces	• Dual Intel Xeon CPUs with a minimum of 6 cores each • 64 GB RAM • 2 X 1TB SSD with RAID controller (RAID 1) • 2 Ethernet interfaces
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 ECC UDIMM) • 960GB SSD vSAS Mixed Use 12Gbps 512e 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 NV Cache, Adapter, Low Profile • 2 X 960GB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYB CARR, 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 • 2 Virtual Network interfaces	• 8 vCPU • 32 GB RAM • 100 GB Storage • 2 Virtual Network interfaces
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 • Amazon AWS EC2 • Microsoft Azure	

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 provide them to relevant modules, so that the entire attack process can continue to run without a manual intervention and achieve the automated process of security validation tasks.
- **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.

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 conntected target marchines, proactively discover and exploit security flaws on target machines to gain access.

  Local attack/Privilege Escalation: After gaining a lower priviledge access on the target machine, exploit additional vulnerabilities from local to gain elevated privilege

  Lateral Movement: Gain control of a compromised asset and use it as a privot to exploit other target machines on adjacent networks

- **Attack Coverage**

  Host Servers (Windows, Unix, Linux, MacOS and Others)
  Web Servers, Applications, Databases
  Virtualization Platforms
  Network Equipment
  IoT Devices
  Bigdata Platforms

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 validatd risks, includes priviledge obtained, screenshots, shell terminal, file manager, database name or database table name etc.
- **Kill-Chain Visualization:** Visulize 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.

Reporting and 3rd Party System Integration

- **Professional Reports:** Provide professional penetration testing reports with detailed asset information, vulnerability and risk analysis data as well as mitigation suggestions. Support multiple report formats and report password protection
- **MSSP Co-branding Reports**: Support report customization, and allow a MSSP(Managed Security Service Provider) customer to add its company logo on penetration testing reports
- **Mutil-Language Reports**: Support English, Spanish and Korean, customer can select a language before generating the penetration testing report.
- **System Integration**: Support RESTful API and CEF-compliant syslog messages, easy to be integrated with 3rd-party security management platforms

About Ridge Security Technology

Ridge Security delivers ethical, efficient and affordable pen testing 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 penetration testing system, fully automates the testing process by coupling ethical hacking techniques to decision-making algorithms. RidgeBots locate, exploit and document business risks and vulnerabilities discovered during the testing process, highlighting the potential impact or damage.

ContactRidge 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