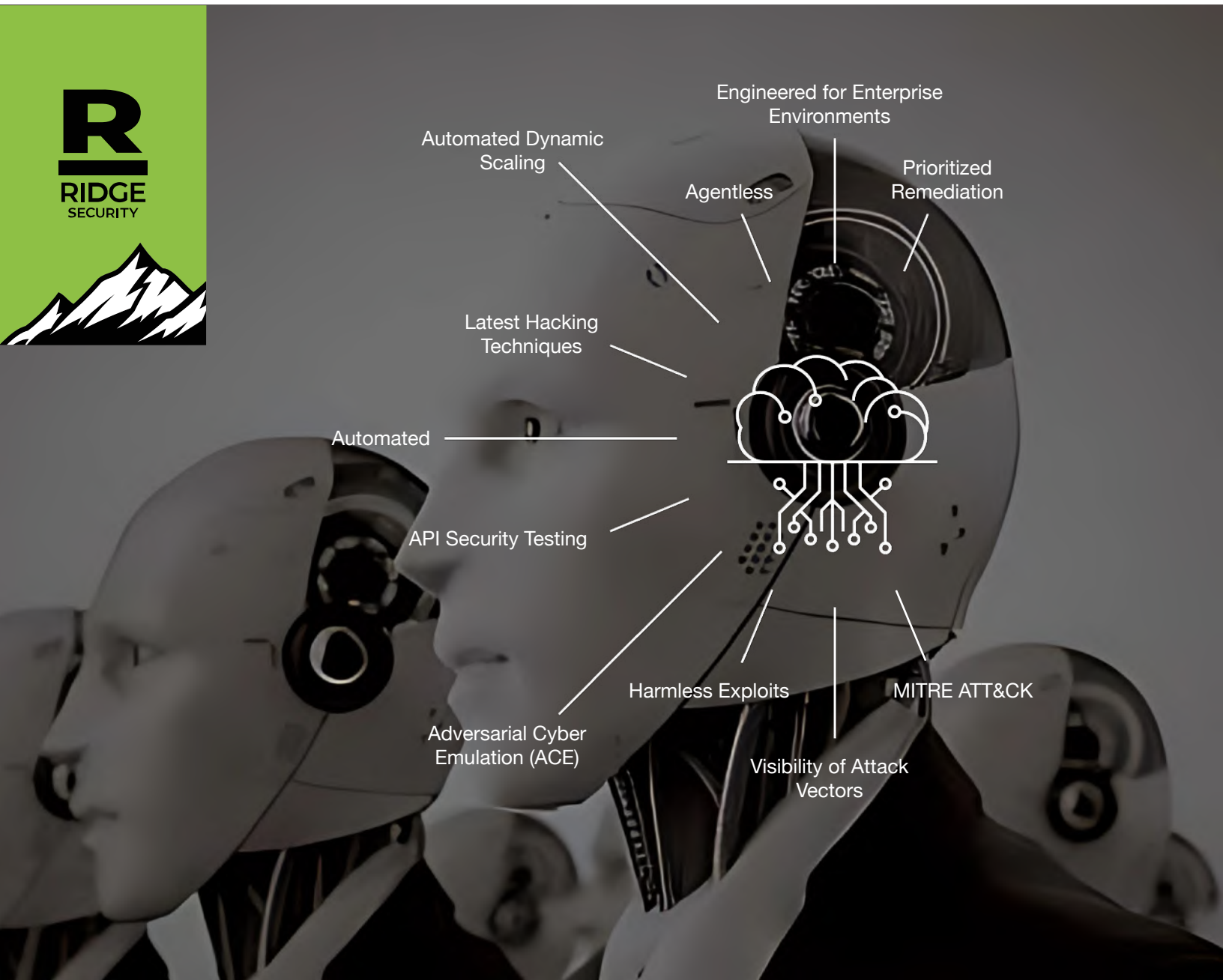


# AI-Powered Offensive Security Platform

RidgeBot®: AI Agent for Continuous Security Validation



Automated Dynamic Scaling

Engineered for Enterprise Environments

Agentless

Prioritized Remediation

Latest Hacking Techniques

Automated

API Security Testing

Harmless Exploits

MITRE ATT&CK

Adversarial Cyber Emulation (ACE)

Visibility of Attack Vectors

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

RidgeBot® is an AI agent designed for continuous security validation. It autonomously performs tests based on the goals set by your security team. RidgeBot® can discover attack surfaces, prioritize vulnerabilities based on exploitability, automate penetration testing, and emulate adversary attacks. This continuous process validates your organization's cybersecurity posture and offers remediation suggestions.

RidgeBot® provides a clearer picture of your security gaps. By increasing the frequency of penetration testing, continuous threat exposure management, and training your defense team with effective exercises, RidgeBot® helps keep malicious attackers at bay. It assists your security team in overcoming knowledge and experience limitations, consistently performing at a top level.

RidgeBot® alleviates the shortage of security professionals by shifting from manual, labor intensive testing to machine-assisted automation. This allows human security experts to focus their energy on researching new threats and technologies.

## 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 expensive 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.

Request a demonstration of  
RidgeBot and see it for yourself



## RidgeBot's® Solutions and Key Benefits

RidgeBot® is an AI powered 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, continuous threat exposure management and training your defense team with effective exercises.

RidgeBot® assists security teams 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 laborintensive 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

### 1 Automated Penetration Testing

- Internal Attack
- External Attack
- Authenticated Penetration
- Lateral Movement
- API Security Testing
- Vulnerability Validation



- Security Control Validation
- Continuous Measurement
- MITRE ATT&CK Framework

Adversary Cyber Emulation 2

RidgeBot® brings 360-degree security validation within reach of every organization

# RidgeBot® Key Functions

## Automated Penetration Testing

---

Automated penetration testing replicates the actions of ethical hackers to identify and exploit vulnerabilities in your systems. RidgeBot® follows a comprehensive process:

- **Attack Surface Discovery:** RidgeBot® utilizes smart crawling techniques and fingerprint algorithms to discover broad types of IT assets, including IPs, domains, hosts, operating systems, applications, websites, databases, and network/OT devices.
- **Vulnerability Detection:** RidgeBot® employs a proprietary payload-based testing approach, a rich knowledge base of vulnerabilities and security breach events, and various risk modeling techniques.
- **Vulnerability Exploitation:** RidgeBot® employs built-in attack techniques to launch ethical attacks against identified vulnerabilities. Successful exploits are documented for further analysis.
- **Risk Prioritization:** RidgeBot® automatically generates an analytical view, visualizes the kill chain, and displays the hacker's script. It presents results such as compromised asset data and escalated privileges.
- **Reporting and Remediation:** RidgeBot® provides a comprehensive report with risk assessments, remediation advice, and tools for patch verification.

## Automated Penetration Testing Scenarios

- **Internal Attack:** Launches attacks from inside the enterprise network with customer permission, focusing on exploiting vulnerabilities discovered on local networks and systems.
- **External Attack:** Launches attacks from outside the enterprise network towards publicly accessible assets such as websites, file shares, or services hosted in public cloud/CDN.
- **Authenticated Penetration:** Simulate attacks by an insider or an external attacker who has obtained some level of authenticated access. This is particularly valuable for identifying how far an attacker could penetrate or how much damage they could inflict, starting from a position of partial system access.
- **API Security Testing:** Perform Swagger file-based API Security Testing to detect and validate vulnerabilities, including the OWASP Top 10 API security risks, hidden paths, and other issues. This helps organizations prevent horizontal privilege escalation.
- **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.

- Cloud Cluster Penetration Testing : Automatically discover Cloud Cluster's nodes information, and then conduct thorough penetration testing on cluster assets. This process enables customers to quickly pinpoint potential security vulnerabilities, facilitating a more efficient subsequent security assessment for cluster.
- Website Penetration Testing: Intelligently crawl for static and dynamic websites, including Single-Page Applications (SPAs), to identify potential vulnerabilities.

## Adversary Cyber Emulation (ACE)

---

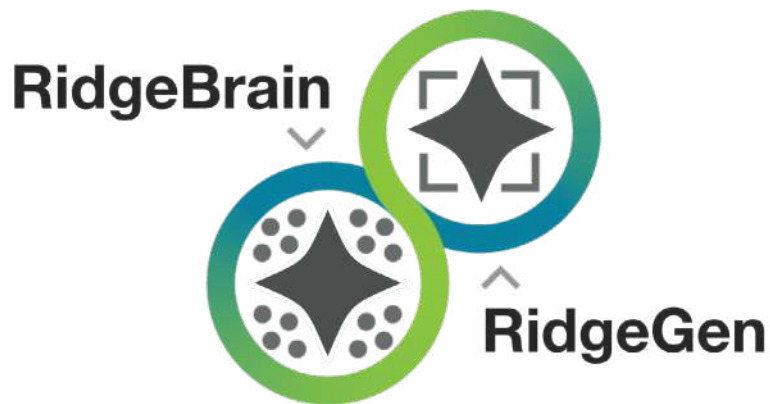
IT security controls are mechanisms used to prevent, detect and mitigate cyber threats and attacks. RidgeBot® ACE emulates the adversary by mimicking the likely attack paths and techniques to generate continuous assessment data to help identify security control failures, resolve structural weaknesses 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.

### Adversary Cyber Emulation (ACE) Methods

- Agent-Based Attack Simulation: RidgeBot® uses an agent-based Botlet to simulate adversary attacks. RidgeBot's® 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, making it simple for all skill levels to assess the efficacy in different aspects of your security controls. The assessment tests are comprehensive and safe to 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 extensively by RidgeBot® to create meaningful and life-like assessment test scripts for its customers to challenge, assess and optimize their security controls.

Request a demonstration of  
RidgeBot and see it for yourself





## RidgeBot's® Dual AI Engine

RidgeBot® integrates two powerful AI engines—RidgeBrain and RidgeGen—to deliver intelligent and autonomous security testing. RidgeBrain is responsible for executing advanced offensive operations, mimicking real-world attacker behavior by automating the full attack lifecycle, from reconnaissance to exploitation. It uses AI-driven logic to adapt and iterate attacks based on results, ensuring persistent and precise threat validation.

Complementing this, RidgeGen is a context-aware, GenAI-based model that enhances detection capabilities across various languages and data formats. It operates entirely onboard RidgeBot®, maintaining strict privacy while enabling nuanced analysis such as identifying sensitive data and contextual vulnerabilities with exceptional accuracy.

## RidgeBot® Deployments

### On-premise deployment



For enterprise environments—deploy RidgeBot® on the customer's premises to reduce the risk of information security data leakage.

### Cloud deployment



For Cloud and SMB customers—deploy RidgeBot® in the cloud (AWS EC2, Microsoft Azure, or Google Cloud) to gain greater flexibility while minimizing initial CapEx investment.

## 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 platform, the dual AI engine, and the 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 Requirements	<ul style="list-style-type: none"><li>• Intel Xeon CPU with a minimum of 4 cores with Hyper-Threading</li><li>• 32 GB RAM</li><li>• 1TB SSD</li><li>• 1 Ethernet Interface Card</li></ul>	<ul style="list-style-type: none"><li>• Dual Intel Xeon CPUs with a minimum of 6 cores each</li><li>• 64 GB RAM</li><li>• 2 X 1TB SSD with RAID controller (RAID 1)</li><li>• 1 Ethernet Interface Card</li></ul>
Virtual Machine / Cloud Deployments	Demonstration/Lab	Production
Minimum Hardware Requirements	<ul style="list-style-type: none"><li>• 8 vCPU</li><li>• 32G RAM</li><li>• 100 GB Storage</li><li>• 1 Virtual Network interface</li></ul>	<ul style="list-style-type: none"><li>• 8 vCPU</li><li>• 32G RAM</li><li>• 100 GB Storage</li><li>• 1 Virtual Network interface</li></ul>
Supported Hypervisors and Cloud Platforms	<ul style="list-style-type: none"><li>• VMware Workstation 15 Pro or higher</li><li>• VMware Fusion 11 Pro or higher</li><li>• VMware ESXi 7.0 or higher</li><li>• Microsoft Windows/Hyper-V 2019 or higher</li><li>• QEMU KVM 7.2</li><li>• Amazon AWS EC2</li><li>• Microsoft Azure</li><li>• Google Cloud Platform</li></ul>	<ul style="list-style-type: none"><li>• VMware Workstation 15 Pro or higher</li><li>• VMware Fusion 11 Pro or higher</li><li>• VMware ESXi 7.0 or higher</li><li>• Microsoft Windows/Hyper-V 2019 or higher</li><li>• QEMU KVM 7.2</li><li>• Amazon AWS EC2</li><li>• Microsoft Azure</li><li>• Google Cloud Platform</li></ul>

Request a demonstration of  
RidgeBot and see it for yourself



# RidgeBot® Detailed Features

## Automation Assistance

- **Object recognition:** Through this function mode, RidgeBot® automatically identify information such as asset types, data content types, record classification identifiers and then feed them into 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 codes and simulate manual operations through smart sandbox to bypass manual operation inspection required by the system, so that the system can perform an automatic execution of the security inspection with improved efficiency of security testing.
- **Decision brain:** RidgeBot® is built in with many pieces of artificial intelligence logic, making RidgeBot® run faster when executing the attack and knowing when executions are going down the branch address.
- **Expert system:** RidgeBot® is embedded with an expert system, allowing RidgeBot to determine if a “successful” condition can be achieved for a target exploitation to perform the next action.
- **Vector engine:** The vector engine analyzes attack vectors and non-linear connections which enable RidgeBot® to make more efficient attacks with higher hit rate toward the target system.
- **RidgeGen:** an offline GenAI engine module to enhance efficiency and accuracy in Penetration testing results.

## Risk Analysis

- **Topology portrait:** Automatically generate a topology map from the information collected during the attack, label the risks identified in each point in the topology, and assist administrators in risk analysis and evaluation.
  - **Proactive situational awareness:** Identify the target systems from the attacker’s perspective and show the most vulnerable assets based on the location and value of the security landscape.
  - **Real time attack action visibility:** Provide real time visibility to every single step of the attack, from topology scanning to exploit launching, 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 of the target model and the RidgeBot® brain.
  - **Vulnerability scanning:** Access and test the target systems by using plugins and scripts to perform vulnerability scanning and return results once the vulnerabilities were checked: to determine whether there are vulnerabilities that can be exploited.
- 

## Vulnerability Exploitation

- **Attack Vector Supported:** Network attack: Explore network connection of target machines, receive/discover and exploit security flaws on the machines to gain access.
- **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.
- **Local Attack/Privilege Escalation:** After gaining a lower privilege access to a target machine, exploit additional vulnerabilities from local to gain elevated access.

- **Testing:** Launch attack to test web application programming interfaces (APIs).
  - **Identify Vulnerabilities:** Detect weaknesses in API design, implementation and configuration.
  - **Exploit Vulnerabilities:** Attempt to manipulate or exploit identified vulnerabilities.
  - **Lateral Movement:** Gain control of a compromised host and use it as a springboard to other target machines in internal networks.
  - **Application Security Testing:** Support Dynamic Application Security Testing (DAST) Support Testing Launch via web application 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 option.
  - **Automatic SQL injection testing**  
Automates the process of detecting exploitable SQL injection flaws and over database servers.
  - **Customizable pentest plugins**  
User customizable application exploitation: attack vector, vulnerability being deployed, vulnerability modules with payload scripts and automation engine, as well as remediation.
- 

## Vulnerability Validation

- **Risk validation:** Validate whether the vulnerability is exploitable in the 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, including 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.
- 

## Task Management

- **Task scheduling:**
    1. Run Now
    2. Run Once
    3. Weekly (Daily)
    4. Monthly task scheduling.
  - Support multiple runs within a weekly/monthly task cycle.
  - Assessment test scripts are mapped to Threat Groups and MITRE ATT&CK and Techniques.
  - 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 reports with detailed asset information, vulnerability and risk data, assessment test results, mitigation suggestions, and historical trend.
- **Multi-language Reports:** Support English, Spanish, Portuguese, Japanese, Italian and Korean reports. The customer can select a preferred language before generating the reports.
- **OWASP Top-10 Compliance Reports:** Support 2017 and 2021 versions of OWASP Top-10 definition. Dedicated OWASP Top-10 report template for web penetration testing tests.
- Support scanning result validation for Qualys, Tenable Nessus Pro and Rapid7 security management platform. Support ticket-based issue tracking.
- **DevSecOps Integration:** Support Jira Software, ServiceNow and GitLab for issue tracking.
- **MSSP Co-branding Reports:** Support report customization, and allow an MSSP (Managed Security Service Provider) user to embed its company logo on the report. Provide documentation for API integration.
- **Reporting Automation Platform:** Integration with PlexTrac to display RidgeBot test results on the reporting platform.
- **System Integration:** Support RESTful API, CEF-compliant and LEEF-compliant syslog messages, easy to integrate.
- **Vulnerability Scanner Integration:** Seamlessly integrates with third-party scanners including Nessus and Qualys, allowing seamless validation of scanner results and cumulative risk evaluation.

## System Administration

- Support online and offline software updates.
- Support user role-base access control for security validation tasks and reports.
- Support Modern IM integration, allowing it to connect with third-party IM like Slack. This enables timely notifications to be posted to the chatroom, keeping users informed about system updates and tasks.
- **Multi-language UI:** English, Spanish, Portuguese, Japanese, Italian, Korean.
- Support multiple log formats: CEF and LEEF.
- Support two-factor authentication (2FA) login.
- Support single sign-on (SSO) with OKTA for Web UI login.
- Support OpenVPN for enterprise intranet or virtual private cloud (VPC) access.
- Supports https/https proxy and authentication proxy for communication with license server and Jira/GitLab integration.
- Support Shell &Clish Access Hardening with Two-Factor Authentication.
- Support SNMP v2c trap and MIB for sending the SNMP trap to server and polling the system status from RidgeBot

### **About Ridge Security Technology Inc.**

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity solutions designed to protect organizations from advanced cyber threats. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation. With a focus on automation, intelligence, and actionable insights, Ridge Security enables security teams to proactively defend against and respond to evolving cyber challenges.



Request a demonstration of

## **RidgeBot<sup>®</sup>**

*Designed for enterprises*



**Ridge Security Technology Inc.**

<https://ridgesecurity.ai/>

© 2025 All Rights Reserved Ridge Security Technology Inc.  
RidgeBot is a registered trademark of Ridge Security Technology Inc.

Follow us online

