



Empower your Cyber Defenders for Unmatched Protection.

Ridge Security's AI-Driven Security Validation Gives Unparalleled Power to Cyber Defenders

About this eBook

As organizations face evolving threats, integrating AI into cybersecurity brings an intelligent, iterative, and continuous learning force with unparalleled opportunities to enhance defense mechanisms, streamline processes, and mitigate risks more effectively.

This eBook articulates how the AI engine works on Ridge Security's security validation platform and explores the pivotal role of RidgeBot's AI-driven approach in cybersecurity validation. It clarifies its significance in augmenting offensive security, automating DevSecOps practices, enabling continuous threat and exposure management, and refining threat intelligence.



The AI-decision engine continuously updates attack strategies

When RidgeBot's AI-powered security validation platform starts working on a given asset, such as a Linux or Windows server or a website, it starts with a clean slate. To begin with, the smart decision engine only has access to an extensive knowledgebase of threats, attack libraries, etc.

The AI engine starts by launching jobs to discover the attack surface on the target systematically. For example, it scans ports and finds all open ports. It then sends probes to each open port and discovers the protocol behind it. It also does fingerprinting and discovers the specific app providing a specific service on a given port.

If the target is a website, the smart decision engine discovers all visible POST and GET URLs for that website. It also discovers as much information about the website as possible, such as which web app framework it uses, whether it is protected by a WAF, and more.

As pieces of the attack surface are discovered, the smart decision engine keeps processing and learning from the result. It launches new jobs to find new information based on what's been discovered. For example, it looks for relevant vulnerabilities, given that it knows the attack surface. If such a vulnerability is found, it then tries to exploit it.



By thinking like a sophisticated threat actor, AI empowers RidgeBot to efficiently identify and exploit critical vulnerabilities to fortify defenses against potential breaches.

This feedback loop is critical for the smart decision engine's work. It keeps learning from what it discovers and updates its attack strategy accordingly. So, it keeps re-strategizing based on what it learns from the new data points in the feedback loop.

After discovering new information, such as a partial attack surface and a few newly discovered vulnerabilities, the smart decision engine acquires more learning, which helps it predict more potential attack vectors. It then broadens its focus to exploiting the relevant vulnerabilities.

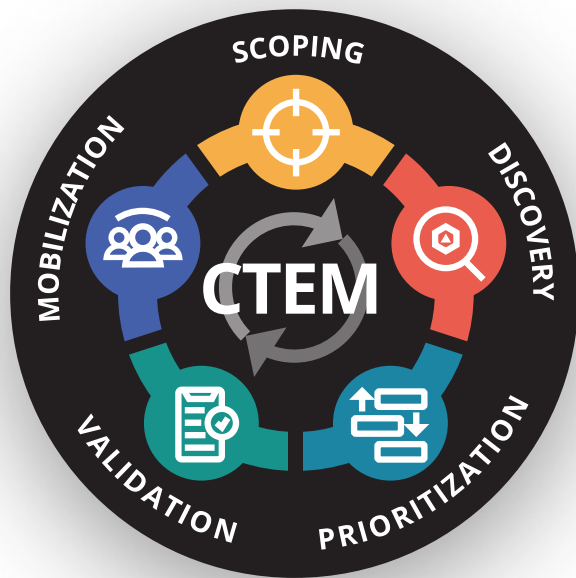
Refining threat intelligence with AI

The synergy between ethical hacking, automated penetration testing, and AI-driven security validation transforms threat mitigation strategies. While automation is a cornerstone, AI adds a layer of intelligence for mimicking threat actors' tactics. It enables more intelligent automated security validation that adapts dynamically to evolving attack surfaces and prioritizes vulnerabilities strategically. By thinking like a sophisticated threat actor, AI empowers RidgeBot to efficiently identify and exploit critical vulnerabilities to fortify defenses against potential breaches.

AI's role in threat intelligence extends beyond reactive measures to proactive prediction and prevention of cyber threats. By harnessing AI-powered solutions, organizations gain deeper insights into potential cyberattacks, enabling preemptive mitigation strategies. Many examples underscore AI's efficacy in predicting and mitigating cyber threats before they materialize, safeguarding sensitive infrastructure and data.

Request a demonstration of
RidgeBot and see it for yourself





- ✓ AI-powered Asset Discovery
- ✓ Vulnerability Prioritization
- ✓ Risk Validation

Ensuring consistent, continuous threat exposure management

Continuous Threat Exposure Management (CTEM) is a holistic approach to cybersecurity that emphasizes the importance of continuous security validation in mitigating threats. The RidgeBot AI-powered security validation platform is pivotal in CTEM because it facilitates proactive risk discovery and vulnerability assessment. By augmenting human expertise and increasing testing frequency, this new AI-driven security validation enables organizations to stay ahead of adversaries and safeguard their digital assets more effectively.


Cybercriminals, including ransomware actors, also utilize AI in their attacks, leading to more frequent cyberattacks. Corporate defenders must utilize AI-powered automated security validation to combat these threat actors and stay ahead of them. Without it, they will be in a losing battle trying to match the increasing sophistication of cybercriminals.

Given an organization's infrastructure, where assets and apps continue to evolve, exposure management has to be continuous. Gartner has coined the term Continuous Threat Exposure Management, or CTEM, which has gained much momentum.

However, continuous security validation of the assets without AI to speed up and focus on what matters is not practical in today's threat landscape. Artificial intelligence and cybersecurity convergence are forging an unyielding shield against relentless cyber threats. As organizations defend against evolving dangers, integrating AI into cybersecurity unleashes a dynamic and relentless force that learns incessantly, iterates tirelessly, and operates with unparalleled intelligence.

This symbiosis transforms defense mechanisms, streamlines processes, and effectively mitigates risks through continuous observation and adaptation to turn the tables on threat actors.

Request a demonstration of
RidgeBot and see it for yourself



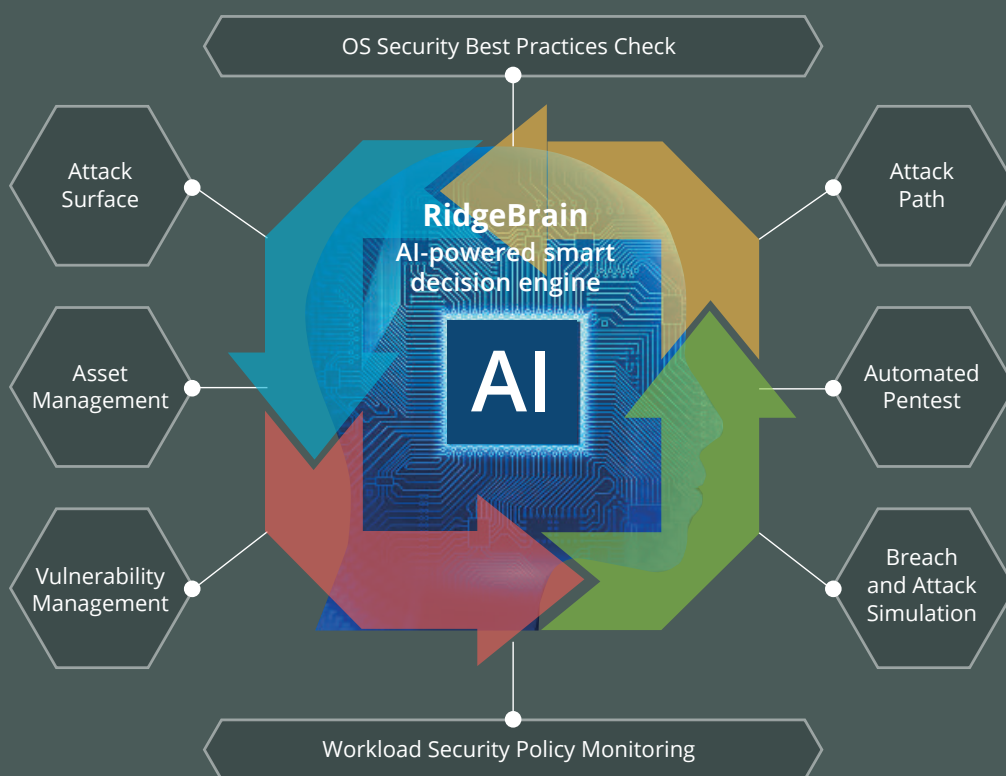
Automated security validation without AI is an incomplete offensive strategy

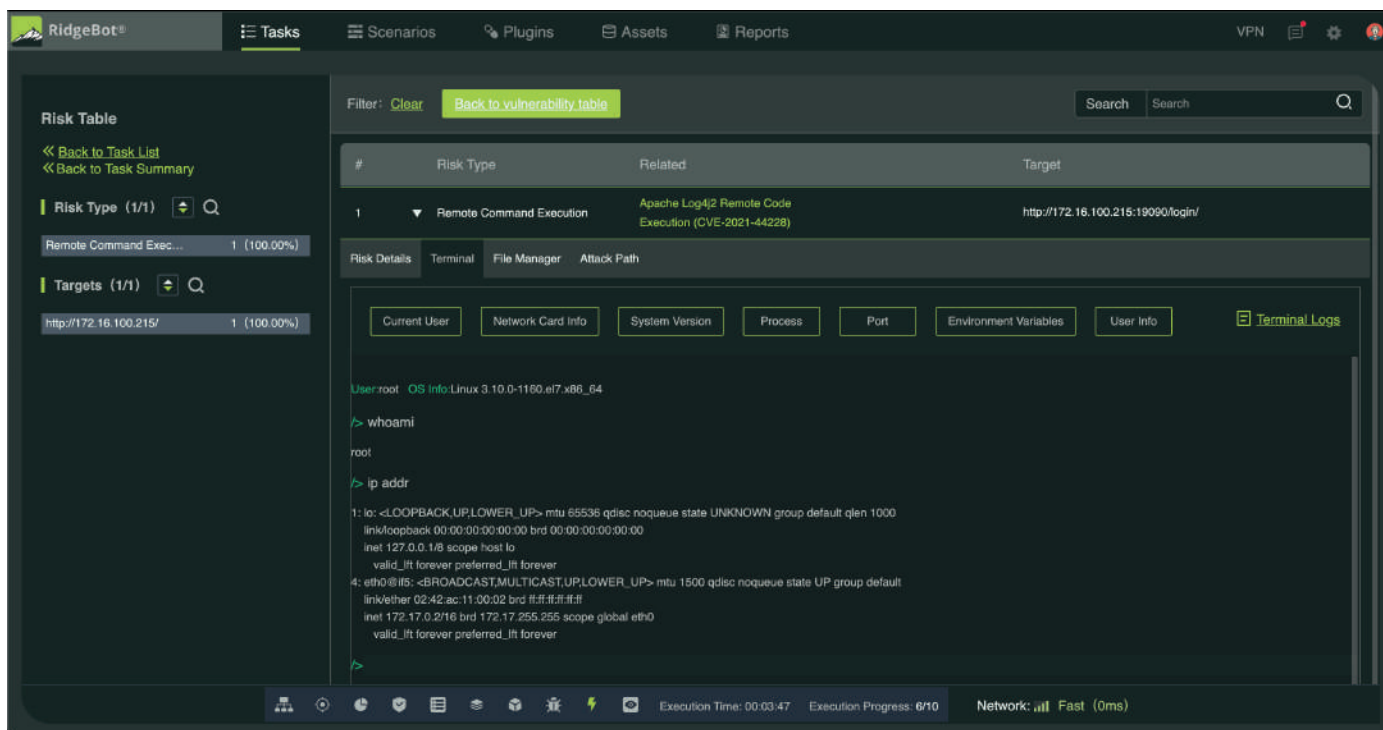
When automation is coupled with AI, magic happens. Automated security validation mimics how threat actors think and work. At any point, RidgeBot will automatically use whatever information it has discovered up to that point and assess what attacks have the most priority regarding potential negative impacts on the organization.

Without AI, automation becomes less valuable. AI is the crucial factor that empowers automated pentesting and security validation to think like a sophisticated attacker. Knowing what vulnerabilities make the most sense to exploit is essential based on the attack surfaces discovered. Once additional attack surfaces, such as POST URLs, are discovered, the AI-powered decision engine will reassess and re-strategize.

To drive this point home, let's consider an example. The best type of exploitation a threat actor can hope for is remote command execution (RCE). An RCE attack occurs when an attacker runs malicious code on an organization's computers or network. The ability to execute attacker-controlled code can be used for various purposes, including deploying malware or stealing sensitive data. Examples of RCE are buffer overflow, deserialization, and SQL injection.

RCE allows threat actors to access the target fully, such as a shell session where they can browse the file system and execute whatever command they want. When examining all available possibilities given the discovered attack surface and vulnerabilities, RidgeBot's AI-driven automated security, just like a threat actor, will focus first on those vulnerabilities that lead to the most severe damage and bring serious business risk to the organization. When an RCE is discovered, the threat is real and severe; users must take immediate action to eliminate the risk.





AI is significant in attaining a balance between speed of risk validation and accurate DevOps security

DevOps emphasizes tearing down walls between the development team and IT operations. It increases the speed of delivery and continues innovation through rapid iteration. Therefore, speed is of the utmost importance for DevOps's success. When security is integrated into DevOps to deliver DevSecOps, it's imperative that:

- Security validation meets the required speed of DevOps
- Security is not sacrificed as a result of the required speed

Without AI, speed and accuracy typically form a trade-off. However, with AI, both can be supported. Shift-left security improves the protection of the final product, reducing costs and delivering a faster time to market. Ridge Security has worked with many

banks that deployed the RidgeBot AI-powered security validation platform within their DevOps process; that is, they can integrate RidgeBot into their CI/CD pipeline. This has become part of their shift-left strategy to perform security tests earlier in the software development process.

Every time they have a build for their online banking app, in addition to the automated unit test and feature test modules, RidgeBot also performs automated security validation. This approach enables developers to find security vulnerabilities and coding errors reliably and accurately before releasing the software.

RidgeBot's AI capabilities play a crucial role by using all the available data points and focusing on what matters most. RidgeBot's exploit library is updated regularly, enabling it to cover the latest vulnerabilities within the context of the discovered attack surfaces and make intelligent decisions.

Request a demonstration of RidgeBot and see it for yourself



Automated security validation with AI eliminates non-essential data points

Security validation platforms consume massive data sets, including irrelevant data. An automated security validation platform requires a lot of information to do its job successfully, including:

- An extensive knowledgebase that continuously grows
- A library of attacks, i.e., POC scripts to exploit vulnerabilities that continue to grow
- Continually updated threat intelligence, like vulnerabilities currently being exploited in the wild

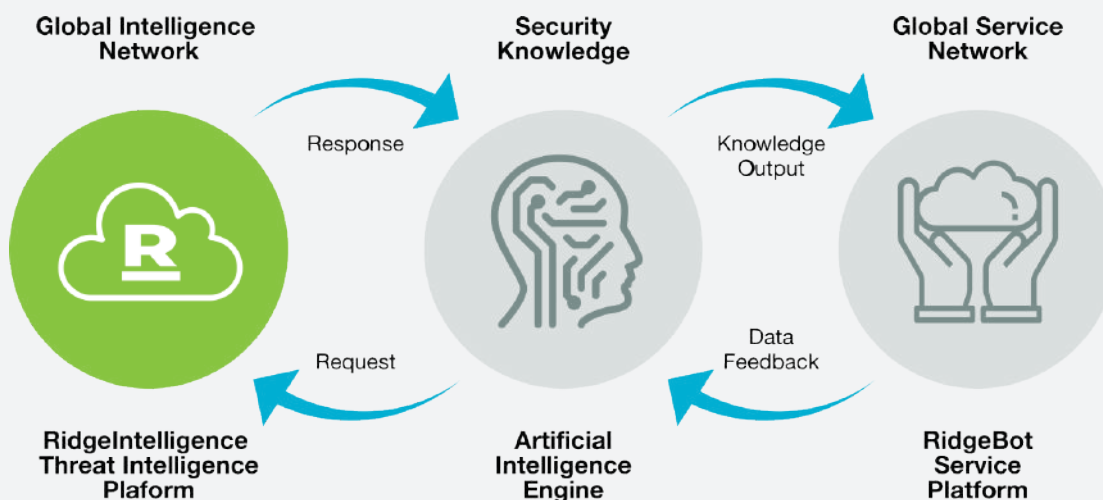
Automation without AI tends to become a brute force exercise of automatically consuming all this information. AI adds a new dimension to the process.

For example, it can provide a feedback loop of all the information discovered, such as the attack surface, the list of vulnerabilities found, and a list of vulnerabilities exploited. This helps intelligently eliminate data points that have zero or negligible impact.

AI also helps focus on the vulnerabilities that would have the most significant impact. For example, if a vulnerability can be exploited to gain Remote Command Execution, it is given a higher value than a vulnerability that leads to database manipulation. During the time it takes for the pentesting to complete, each AI-powered engine discovers new data points, from which they learn and apply that new knowledge with all the other data points discovered up to that point.

Key characteristics that enable AI-powered security validation to think like a threat actor

- Constant learning from new information discovered enables constant re-strategizing re-strategizing the security validation and attack plans.
- The smart decision engine, like a threat actor, attempts to get the biggest bang for the buck by finding the most impactful risks, such as RCE.
- The smart decision engine looks for vulnerabilities that can lead to lateral movement. Exploiting this vulnerability on a given target, leading to privilege escalation, enables it to use that target as a pivot point for launching attacks on other assets.



About Ridge Security

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity products that benefit CISOs and security teams by reducing risk through validation and using automation to improve efficiencies. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation, powerful workload protection and cloud security monitoring.

The RidgeBot AI-powered automated security validation platform empowers organizations to fortify their defenses, mitigate risks, and safeguard their digital assets effectively. With RidgeBot, organizations can seamlessly integrate security into their DevOps pipelines, accelerate threat detection and response, and uphold the highest standards of cybersecurity resilience in today's dynamic threat landscape.

RidgeBot helps organizations discover risks and vulnerabilities ahead of the attacker

The goal is not to replace human testers with AI-powered solutions like RidgeBot. Instead, RidgeBot helps:

- Scale operations to compensate for the shortage of security engineers within enterprises and MSSPs
- Increase productivity of the security engineers for organizations with existing red teams
- Increase frequency of testing, from once or twice annual testing by humans versus once a month automated testing

RidgeBot enables rapid discovery, identification, and reporting of vulnerabilities and exposures. Automated reports show validated vulnerabilities and exposures, provide remediation, and support compliance. Organizations can prioritize and correlate risk severity with context for an accurate picture of their digital environment.



Request a demonstration of

RidgeBot[®]

Designed for enterprises



Ridge Security Technology Inc.

www.ridgesecurity.ai

© 2024 All Rights Reserved Ridge Security Technology Inc.
RidgeBot is a registered trademark of Ridge Security Technology Inc.

Follow us online

