



RidgeBot®

AI-powered security validation that never sleeps

The CISO's trusted AI-powered security platform that protects your business 24/7



Expose vulnerabilities before they expose you.

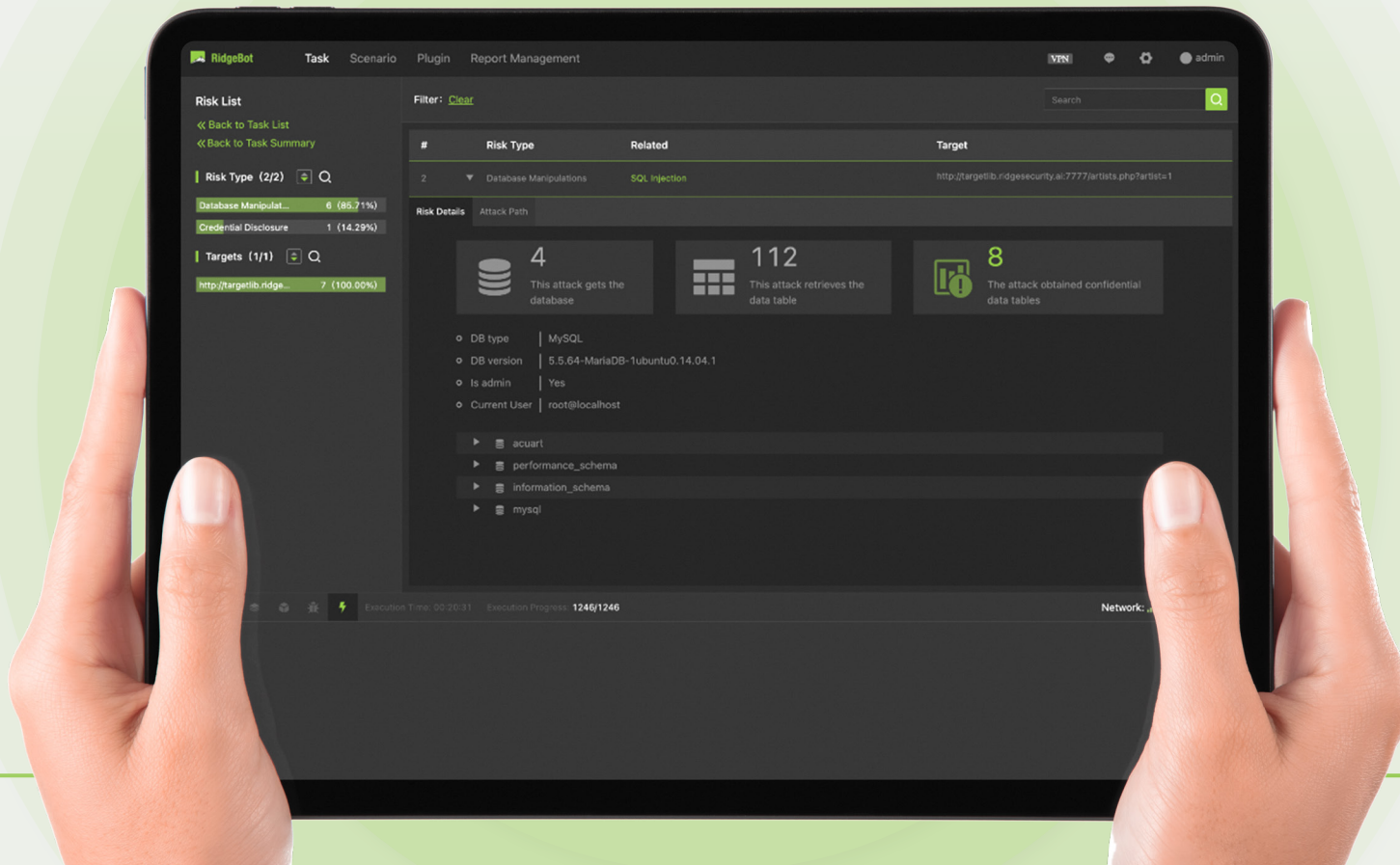
RidgeBot puts you on the offensive, exposing vulnerabilities before attackers can exploit them. Unlike traditional scanners that merely identify risks, RidgeBot goes further—safely executing real-world exploits to provide undeniable proof of compromise.

With AI-powered continuous testing, it replicates hacker tactics, uncovering weaknesses that could lead to a breach.

The result? Actionable insights that help you prioritise and remediate critical threats before they become costly incidents.

See what hackers see—before they strike. RidgeBot® autonomously scans, validates, and safely exploits vulnerabilities across your IT environment, delivering hard evidence of security gaps.

No guesswork, no false positives—just clear, data-backed proof of where your defenses fall short. Stay ahead of cyber threats with RidgeBot®—because waiting for an attack is not a strategy.



Speed matters.
Cyber threats
move fast.
RidgeBot®
moves faster.

Traditional security assessments cannot keep up with the rate of vulnerability exploitation. Point-in-time testing is no longer enough. Organizations need continuous automated validation of their security posture to support CTEM goals.

Continuous Threat Exposure Management (CTEM) helps organizations identify, validate, and remediate security risks before attackers exploit them. RidgeBot® seamlessly aligns with this framework to enhance security and efficiency.

CTEM Goal	RidgeBot's Role	Business Benefit
Asset Discovery & Inventory	Automates attack surface mapping across networks, web apps, OT/IoT, APIs, and cloud.	Eliminates blind spots , ensuring no unmanaged assets remain vulnerable.
Continuous Attack Surface Testing	AI-powered penetration testing & vulnerability exploitation with 36,000+ plugins.	Reduces compliance risk by ensuring security gaps are constantly identified.
Threat Simulation & Risk Validation	Real-world attack emulation (Breach & Attack Simulation + Red Teaming).	Improves efficiency by focusing security teams on real threats, not false positives.
Automated Remediation & Response	Prioritizes risks based on exploitability & business impact ; integrates into DevOps/SecOps.	Speeds up response and lowers breach costs by fixing high-risk vulnerabilities first.
Adaptive Security & Threat Intelligence	AI-powered real-time security validation and MITRE ATT&CK framework mapping	Proactively defends against evolving threats, keeping security one step ahead .

\$23 Trillion

Annual average cost of cyber crime by 2027
US Department of State report 2024

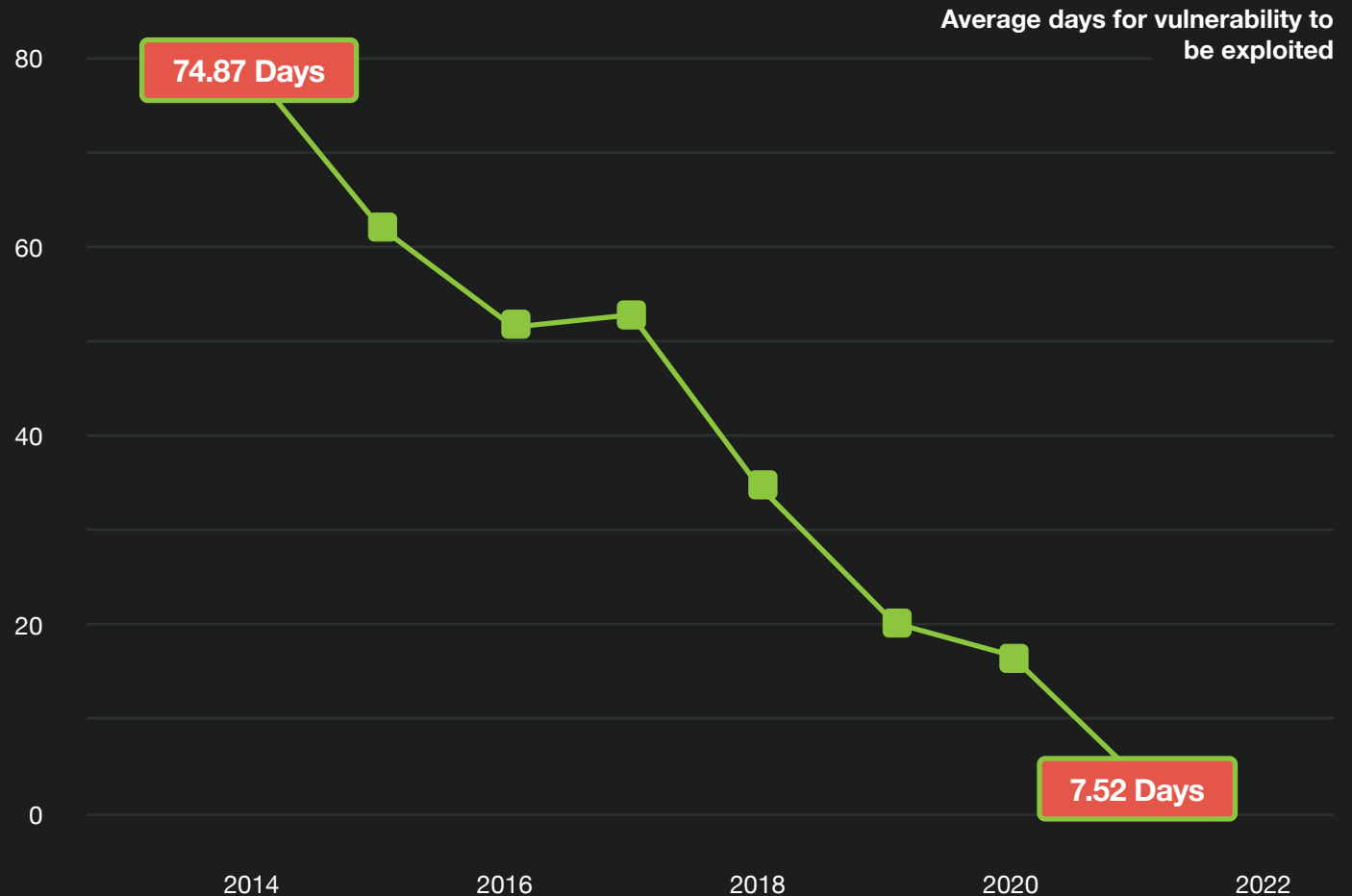
\$4.8 Million

Average cost of data breach globally
Statista 2025

Act Fast. The window for exploitation is closing.

In 2014, organizations had over 74 days before a vulnerability became exploitable. By 2022, that window shrank to less than 8 days. Attackers move fast—can your security team keep up?

Manual risk-based prioritization through traditional vulnerability management platforms slows you down, consuming time you don't have. RidgeBot eliminates the lag, automating identification, validation, and safe exploitation to provide immediate proof of compromise. Act now—because in cybersecurity, delays mean breaches.



48%

Of applications contain critical risks as ranked by OWASP Top 10

Veracode State of Software Security report 2025

5 Million

Shortfall in cyber security personal globally

ISC2 Cyber Security Workforce Study 2024

180%

Increase in exploitation of vulnerabilities – Almost triple of the previous year

Verizon 2024 Data Breach Investigation report

Relentless security without the complexity.

Unlike traditional pen testing or scanning technologies, RidgeBot is continuously assessing, identifying, validating and prioritizing threats across your entire IT estate 24/7. As a fully automated, continuous AI-powered threat management platform, RidgeBot not only discovers vulnerabilities but exploits them to demonstrate their potential harm and prioritises efforts for remediation.

Network & App testing

- > Scans and validates a wide range of plug-ins for operating systems, databases and applications.
- > Identifies exploitable vulnerabilities in network services before attackers do.
- > Validates risk exposure by safely simulating real-world attack scenarios.

Authenticated web app testing

- > Conducts in-depth security assessments by logging in as a real user.
- > Identifies authentication flaws, session hijacking risks, and OWASP Top 10 threats.
- > Simulates real attack paths to provide proof of compromise and prioritization insights.

Authenticated API testing

- > Authenticates and tests APIs to uncover security flaws in endpoints and data exchanges.
- > Detects vulnerabilities like broken authentication, injection attacks, and misconfigurations.
- > Validates exploitability with safe attack simulations, ensuring secure API integrations.

Stay Ahead. Hack yourself first with AI-powered continuous pen testing

RidgeBot automates the entire attack process. When it connects to your organization's IT environment, RidgeBot automatically discovers all different types of assets on your network and then utilises 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.

Close all gaps and secure every asset, comprehensive, autonomous and predictive testing for your entire IT estate.

36 Billion

Total private records breached in 2024

IT Governance report UK



Empowering security teams and strengthening SSDLC with AI-powered testing

RidgeBot transforms security testing by integrating seamlessly into the Secure Software Development Lifecycle (SSDLC), ensuring vulnerabilities are identified and mitigated before applications reach production.

By automating pre-release security testing, RidgeBot enables development teams to identify and validate risks early, reducing costly remediation efforts and accelerating secure software development.

With machine-assisted automation, RidgeBot eases the workload on security teams, allowing them to focus on high-impact threats rather than time-consuming manual testing.

RidgeBot continuously validates code, APIs, and applications throughout development, providing real-time insights into exploitable vulnerabilities.

By shifting security left in the development process, RidgeBot enables organizations to stay ahead of threats, streamline DevSecOps workflows, and build resilient software from the ground up.

100x

Faster than human testing

Key differentiators at a glance

Feature	Traditional Scanners	RidgeBot®
Validation of Exploits	No	Yes
False Positives	Common	Eliminated
Security Posture Improvement	Limited	Continuous

Transforming security challenges into decisive action.



See Everything, Secure Everything

Comprehensive Asset Discovery

Gain full visibility into your IT environment as RidgeBot automatically identifies devices, applications, and websites, ensuring no asset is left unprotected.



Find and Fix Vulnerabilities Before Attackers Do

Proactive Vulnerability Scanning

Uncover hidden weaknesses with RidgeBot's AI-powered detection, ensuring your security team focuses on real threats, not false positives.



Validate Risks with Real-World Testing

Ethical Exploitation & Risk Proofing

Know which vulnerabilities are actually exploitable through safe, AI-powered attack simulations, helping you prioritize what truly needs fixing.



Turn data into actionable insights

Smart Reporting & Remediation Guidance

RidgeBot delivers clear, prioritized insights allowing faster remediation and stronger security outcomes, helping your team respond faster and reduce risk.



Total Attack Surface Awareness

Continuous Exposure Management

Either on-demand or scheduled – RidgeBot monitors your entire IT landscape, including IP's, domains, apps, databases, and OT devices, ensuring no blind spots.



Smarter Threat Detection, Stronger Security

AI-Powered Vulnerability Identification

Leverage advanced payload-based testing and risk modelling to detect real-world attack patterns, so you stay ahead of cyber threats.



Simulated Attacks, Real-World Defense

Realistic Breach Simulation

RidgeBot simulates multi-vector cyberattacks, showing you exactly how a hacker would break in, so you can strengthen defenses before it's too late.



Focus on the Biggest Risks, Not the Loudest Alerts

Automated Risk Prioritization

Instantly visualize the kill chain and hacker's potential path to exploitation, ensuring your team tackles the most critical threats first.

Simple to install, easy to run.

RidgeBot is a software appliance that can be deployed within your organization or cloud environment. RidgeBot does not require extensive training for security teams. The annual subscription license covers a specified number of IP addresses, web applications, and APIs within the tested network.





RidgeBot®

Security you can afford.
Risks you can't afford
to ignore.



Contact your Sales Consultant for more information

Tasks

Scenarios

Plugins

Assets

Reports

Task Operation

Pause

Stop

Res...

Re-run

Proxy

API ...

Add Target

Add Vulnerability

Add Attack Surface

Broken Access and Authorization

Time	Action	Description
The task has been completed		
11/27/2024 12:13:35	Detection	Start with http://192.168.103.211:5000
11/27/2024 12:13:32	Detection	Start with http://192.168.103.211:5000
11/27/2024 12:13:24	Detection	Start with http://192.168.103.211:5000
11/27/2024 12:13:20	Detection	Start with http://192.168.103.211:5000
11/27/2024 12:13:03	Detection	Start with http://192.168.103.211:5000

Close

Execution Time: 00