Continuous Threat Exposure Management

RIDGE SECURITY

Powered by RidgeBot – AI Agent for Security Validation

Ridge Security Presence

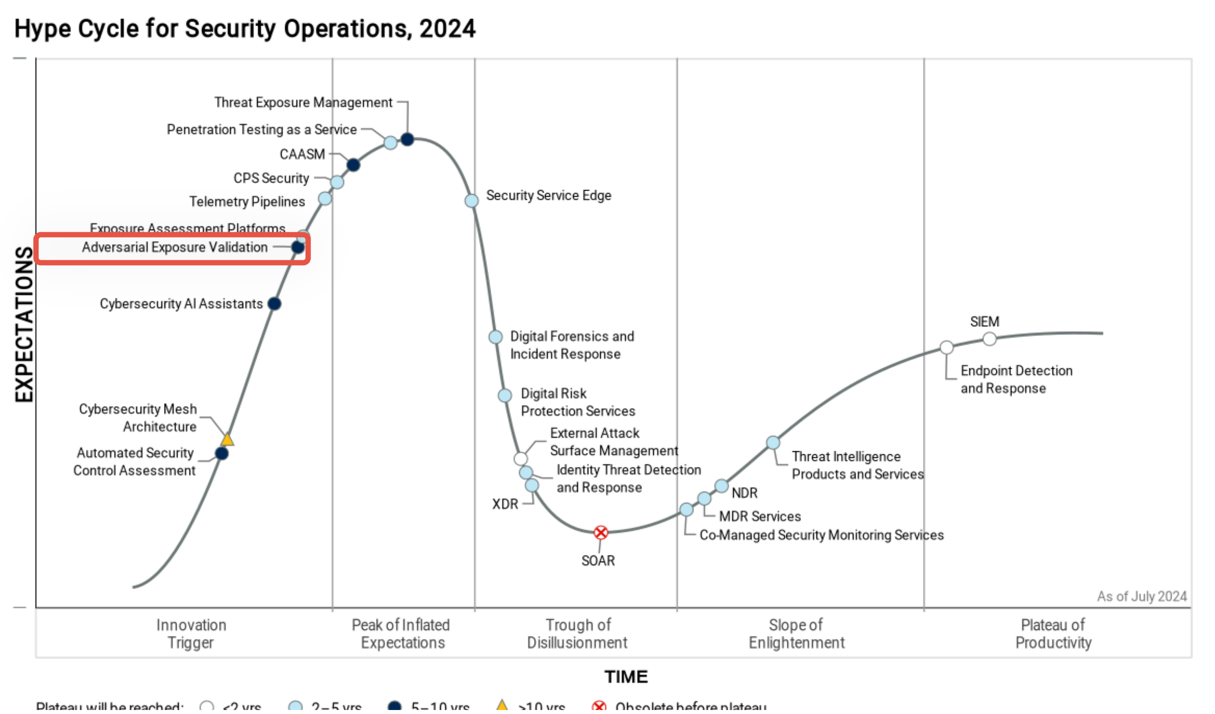
250+ Customers across North & South America , Europe, Asia and Africa

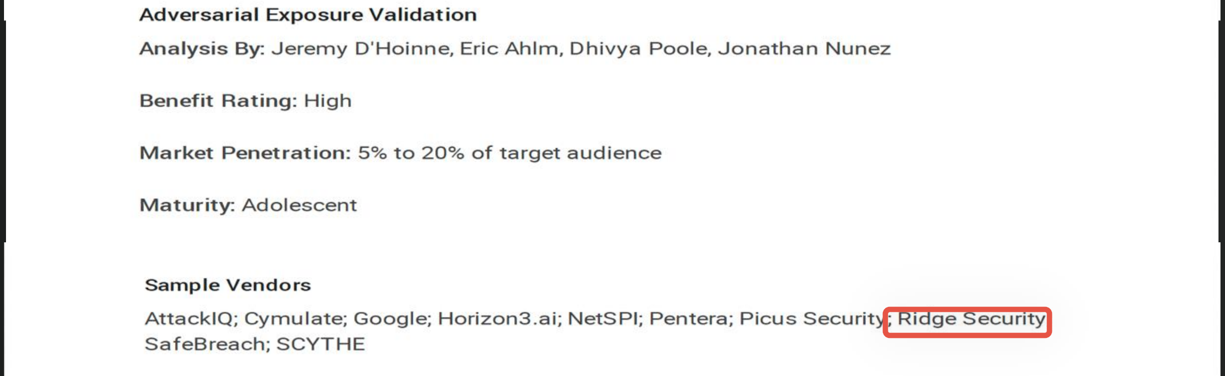
200+ active channel partners
700+ registered channel partners

FSI, Government, Telcom and MSSPs

Silicon Valley
TACTICS
forecight
COREIT
ASSURA
Securin
trulcap
BRAVESOFT
ArmorPoint.
NDC
PROACTIVERISK
PRIANTO
cips
micronet
ABS
nxtHop
BROAD
ESTC
GENESI
NETT7
whIP solutions
ETCOMMUNICATIONS INC
FYRA CONSULTING
NETier
Experis ManpowerGroup
multibyte
CIRTEC
3XPERTIUS
Solcomp
CPNNET
SYNNEX
MEGADVANTAGE
micronet
CP CORP
APLIDIGITAL
INFINYCORE
PROTECTY
ART2SEC
XCLOUD
BSECURE
Imperia
GDLsa
multisoft
AVEERE
DDM
Ona Systems
redvoiss
AKTI
BOCH systems
OSCAR SEVEN
BITRATE
NETSEC
MBONENI
DataGr8
REVEZ
BitCyber
ALFA SIBER TEKNOLOGI
SYSWARE
itSdi
ELITECH
SMARTDATA
BlueZebra Network Security
SDS
IshanTech
TGS
NESSAR
securXcess
CQ CyberQuote
Bumi Optimus
FirstCambodia
TECHNOPATH Solutions Inc.
TeleScience
iNS
WIKI LABS
N-TEK
nexgen

Recognized by Gartner





Adversarial Exposure Validation

Analysis By: Jeremy D'Hoinne, Eric Ahlm, Dhivya Poole, Jonathan Nunez

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

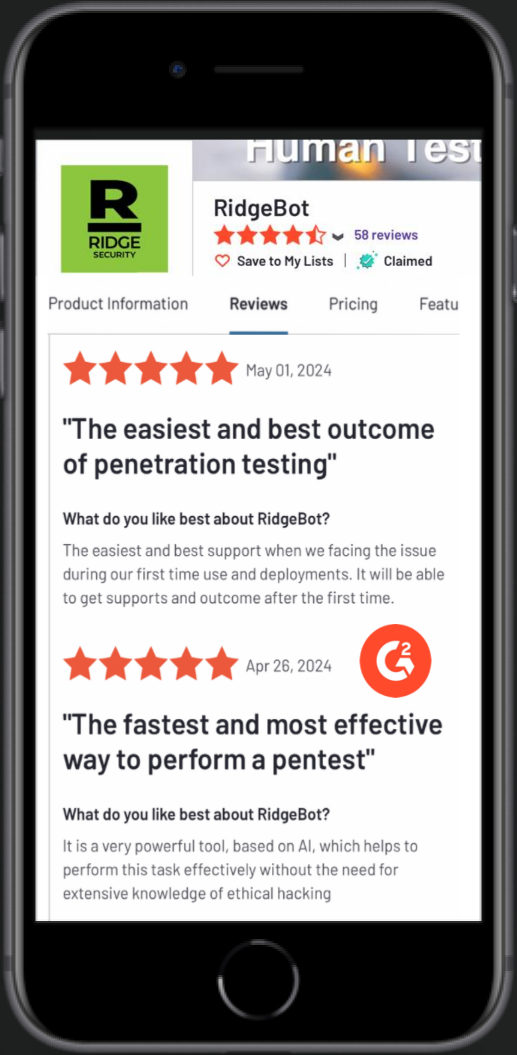
Sample Vendors

AttackIQ; Cymulate; Google; Horizon3.ai; NetSPI; Pentera; Picus Security; Ridge Security; SafeBreach; SCYTHE

★★★★★

Ridge Security is included by Gartner as a sample vendor for Adversarial Exposure Validation

Recommended by Customers



Human Test

RidgeBot
★★★★½ 58 reviews
Save to My Lists | Claimed

Product Information Reviews Pricing Featu

★★★★★ May 01, 2024

"The easiest and best outcome of penetration testing"

What do you like best about RidgeBot?

The easiest and best support when we facing the issue during our first time use and deployments. It will be able to get supports and outcome after the first time.

★★★★★ Apr 26, 2024

"The fastest and most effective way to perform a pentest"

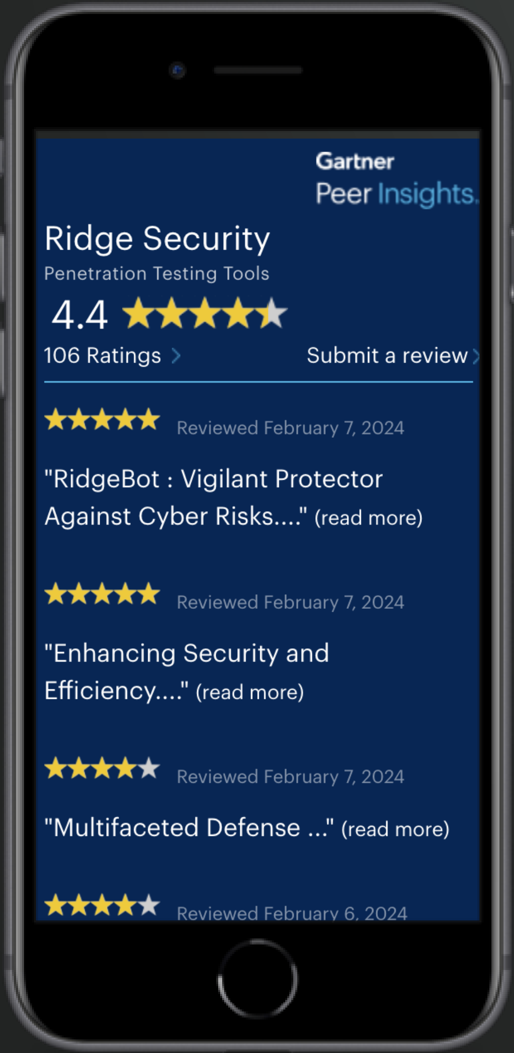
What do you like best about RidgeBot?

It is a very powerful tool, based on AI, which helps to perform this task effectively without the need for extensive knowledge of ethical hacking

Users Love Us

The full product reviews & rating insights

Click to read



Gartner
Peer Insights.

Ridge Security
Penetration Testing Tools
4.4 ★★★★½
106 Ratings › Submit a review ›

★★★★★ Reviewed February 7, 2024

"RidgeBot : Vigilant Protector Against Cyber Risks...." (read more)

★★★★★ Reviewed February 7, 2024

"Enhancing Security and Efficiency...." (read more)

★★★★☆ Reviewed February 7, 2024

"Multifaceted Defense ..." (read more)

★★★★☆ Reviewed February 6, 2024

Strongly Performing in the Vulnerability Assessment Market

Recognized in the 2024 Gartner Peer Insights™ "Voice of the Customer" for Vulnerability Assessment

Leading In User Interest and Adoption of Penetration Testing Tools

Recognized in the 2024 Gartner Peer Insights™ "Voice of the Customer" for Penetration Testing Tools

The full product reviews & rating insights

Click to read

Global Acclamation in 2024

Top 10
Penetration
Testing Provider
2024

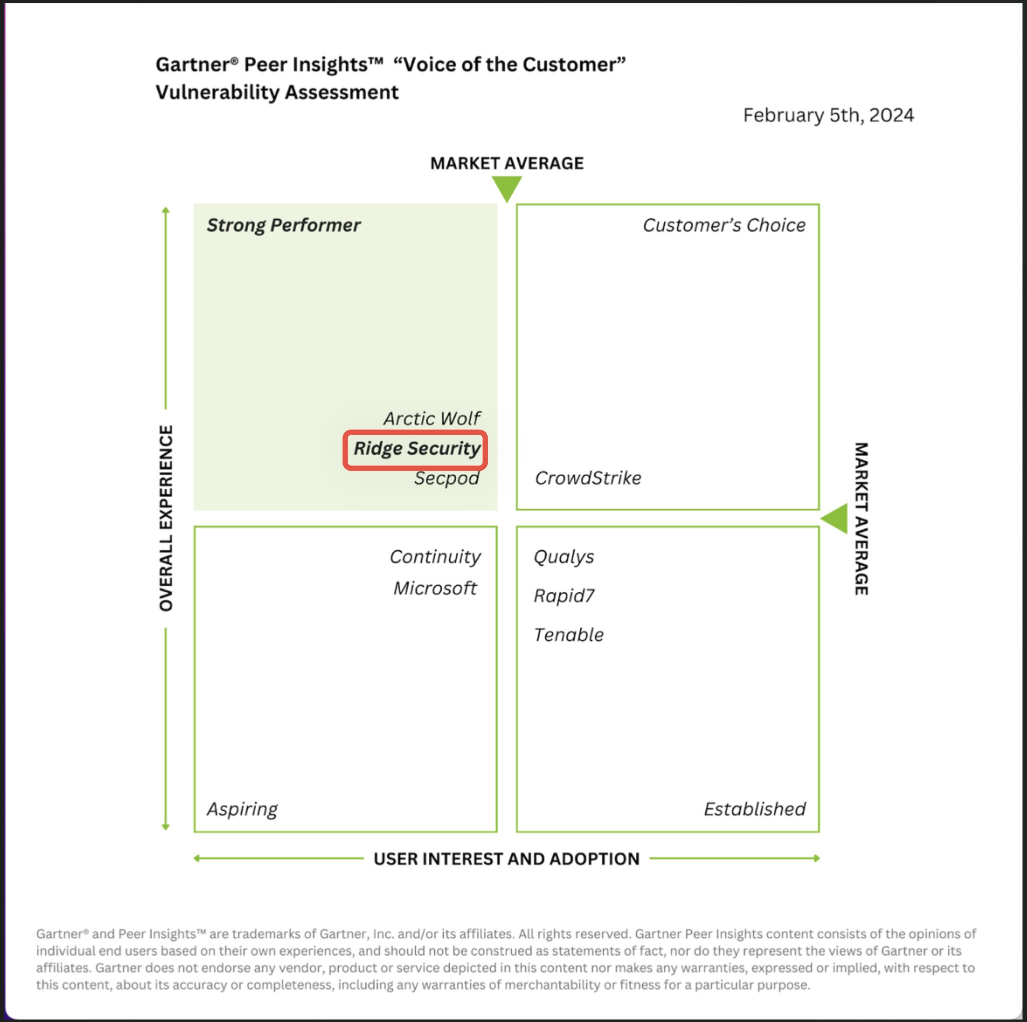
Publisher's Choice
DevSecOps
Vanguard
2024

The Most Promising
Cybersecurity
Startup
2024

Breakthrough
Award AI in
CTEM
2024

Strong Performance from "Voice of Customers"

Strong Performers in Vulnerability Assessment



Gartner® Peer Insights™ "Voice of the Customer"
Vulnerability Assessment

February 5th, 2024

MARKET AVERAGE

Strong Performer

Arctic Wolf
Ridge Security
Secpod

Customer's Choice

CrowdStrike

Continuity
Microsoft

Aspiring

Qualys
Rapid7
Tenable

Established

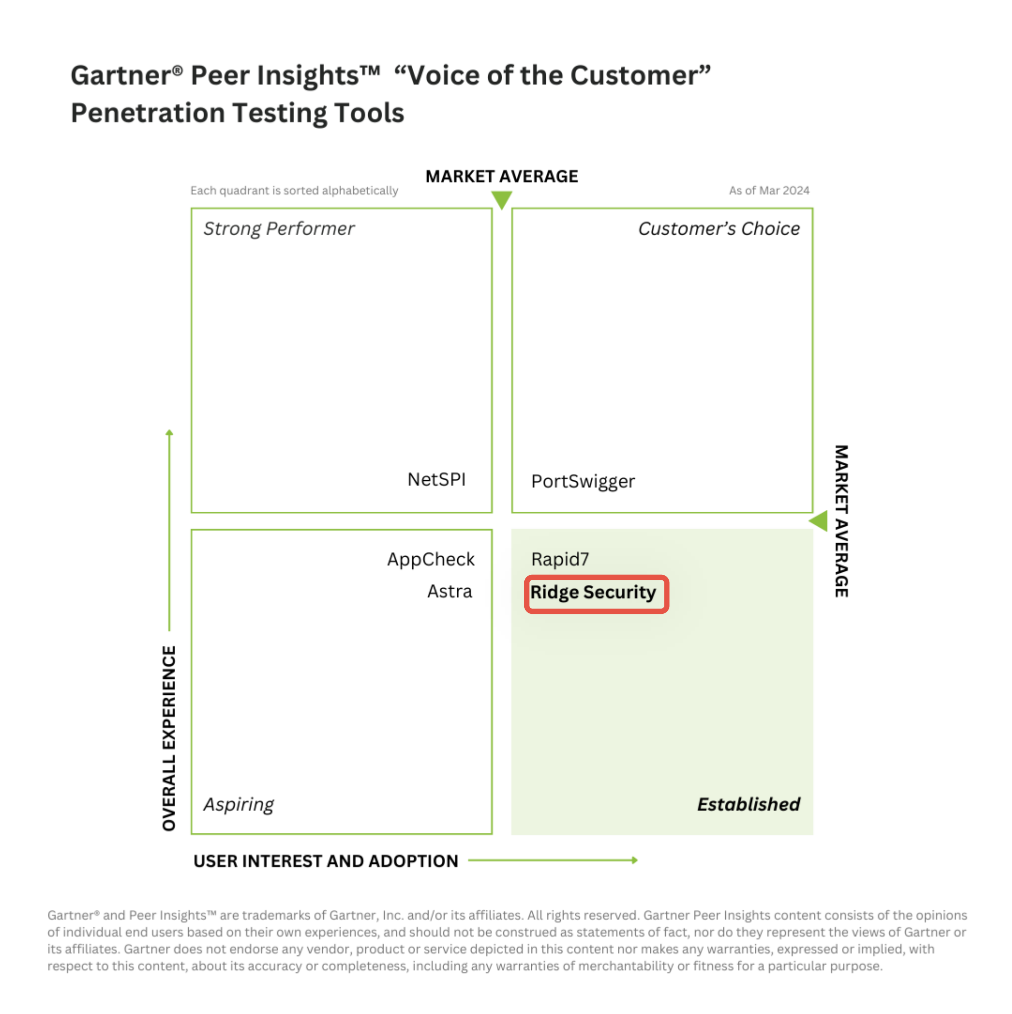
OVERALL EXPERIENCE

MARKET AVERAGE

USER INTEREST AND ADOPTION

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Leading in User Interest and Adoption in Penetration Testing Tools



Gartner® Peer Insights™ "Voice of the Customer"
Penetration Testing Tools

Each quadrant is sorted alphabetically

MARKET AVERAGE

As of Mar 2024

Strong Performer

NetSPI

Customer's Choice

PortSwigger

AppCheck
Astra

Aspiring

Rapid7
Ridge Security

Established

OVERALL EXPERIENCE

MARKET AVERAGE

USER INTEREST AND ADOPTION

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Strategic Partnership

STELLAR CYBER®

Trellix

tenable®

Azure

RAPID7

FORTINET®

IBM

aws

splunk>®

Microsoft Sentinel

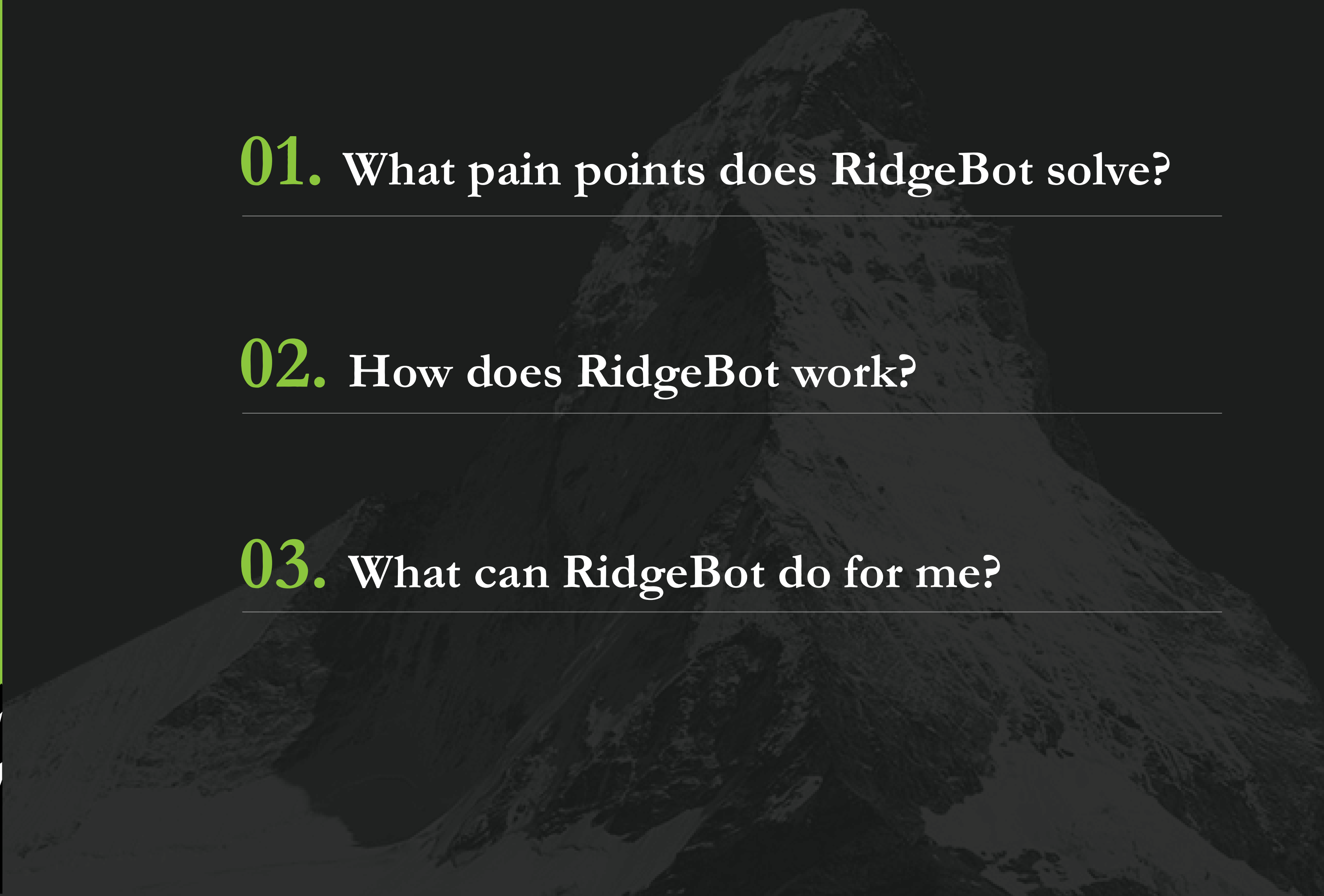
RidgeBot

- RESTful API
- CEF-Compliant Syslog
- Raw Data Export

Manage Cybersecurity Threat Exposure with

AI-Powered RidgeBot

RIDGE
SECURITY



01. What pain points does RidgeBot solve?

02. How does RidgeBot work?

03. What can RidgeBot do for me?

01

What painpoints does RidgeBot solve?

RIDGE SECURITY

PAIN POINT 1

Too Much Data to Effectively Manage

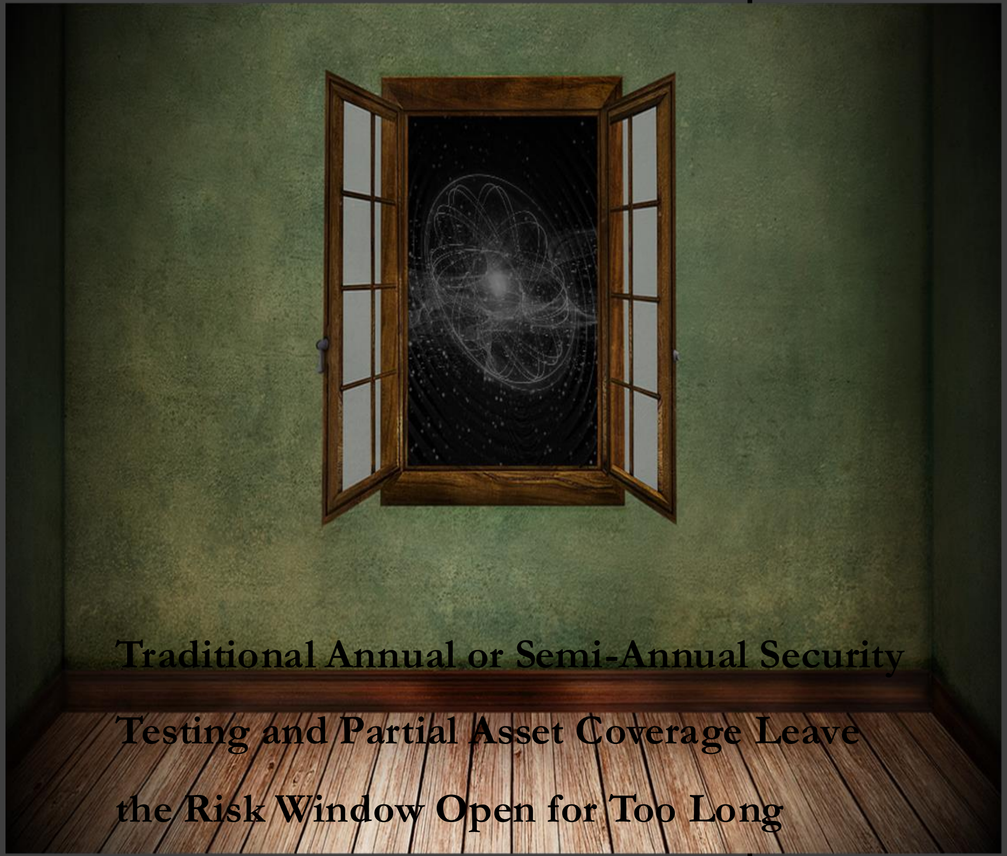
Security Leaders Suffer from Information Overload & Alert Fatigue

- Lots of telemetry but difficult to make sense of it all
- Ongoing growth of attack surface
- Overwhelming volume of vulnerabilities reported by VM solutions
- Very high false-positive rate
- Patch priority not based on exploit possibility

Cannot effectively manage too much data. Security Validation is required to help.

PAIN POINT 2

Traditional Security Validation vs. Threat Exposure Risk



Traditional Annual or Semi-Annual Security Testing and Partial Asset Coverage Leave the Risk Window Open for Too Long

- Traditional security validation, such as manual testing, no longer a good fit:
  - Too expensive
  - Too time-consuming
  - Require highly skilled experts
  - Typically miss the latest exploits
- As a result, traditional security validation:
  - Only performed ad-hoc, not continuously
    - → Gaps in Time
  - Only focuses on critical assets, not all IT assets
    - → Gaps in IT Assets

Traditional security validation is simply not able to keep up with ever-evolving threat landscape and leaves the risk window open for too long.

Continuous & Automated Security Validation is required.

PAIN POINT 3

Sophisticated Attacks Require Sophisticated Solution

- With continued rise of threat exposure risk, organizations experience the security staff shortage more than ever before
- Match the increasing sophistication of cyber criminals
- AI-driven cyber attacks require AI-powered solutions to detect them
- Without the help of AI, it’s indeed a losing battle against cyber attacks in today’s threat landscape

Complement your existing security staff with an AI-Powered Security Validation solution.

RidgeBot is Positioned to Address These Pain Points

1

By performing risk mining, help CISOs understand overall cyber risks and reduce security team's workload by prioritizing critical exposures

2

Perform continuous and automated management of threat exposures and security posture

3

Alleviate the security staff shortage & ever-increasing sophistication of cyber attacks with AI-powered and automated security validation

RIDGE
SECURITY

RidgeBot

Security Validation AI Agent

- 1st AI Agent for Security Validation
- Powered by AI Engine & genAI based Expert Knowledge
- Easy to use, no specialized expertise required

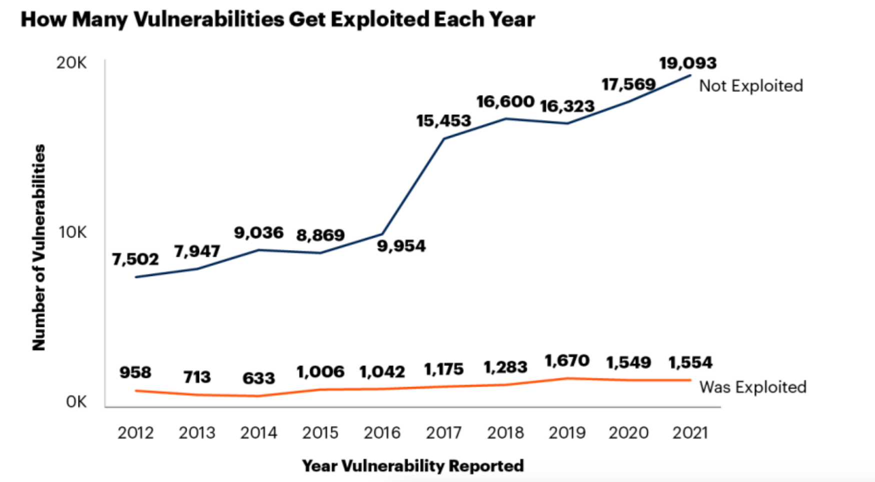
- Do less but achieve more by focusing validated exploitable risks.
- Shorten risk windows from years/months to days/hours
- Cover all IT assets compressively, leaving no gaps.
- Utilize AI to defend against sophisticated hackers.

Periodical manual penetration testing
=>
Automated Continuous Threat Exposure Mgmt

Informational, high false positive
=>
Actionable, zero false positive

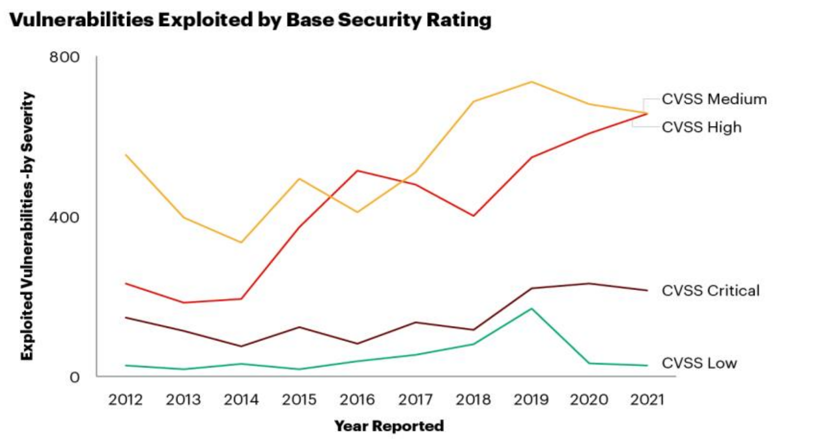
Shortcomings of Vulnerability Management

- Vulnerabilities keep growing year over year
- VM deals with volume, not quality
- Very high false-positive rate
- Not possible to patch all vulnerabilities
- Vulnerability scoring does not reflect likelihood of being exploited by attackers
- Patching vulnerabilities in vacuum does not necessarily reduce Threat Exposure or the risk of a breach



How Many Vulnerabilities Get Exploited Each Year

Source: Gartner (data drawn from the IBM X-Force vulnerability databa

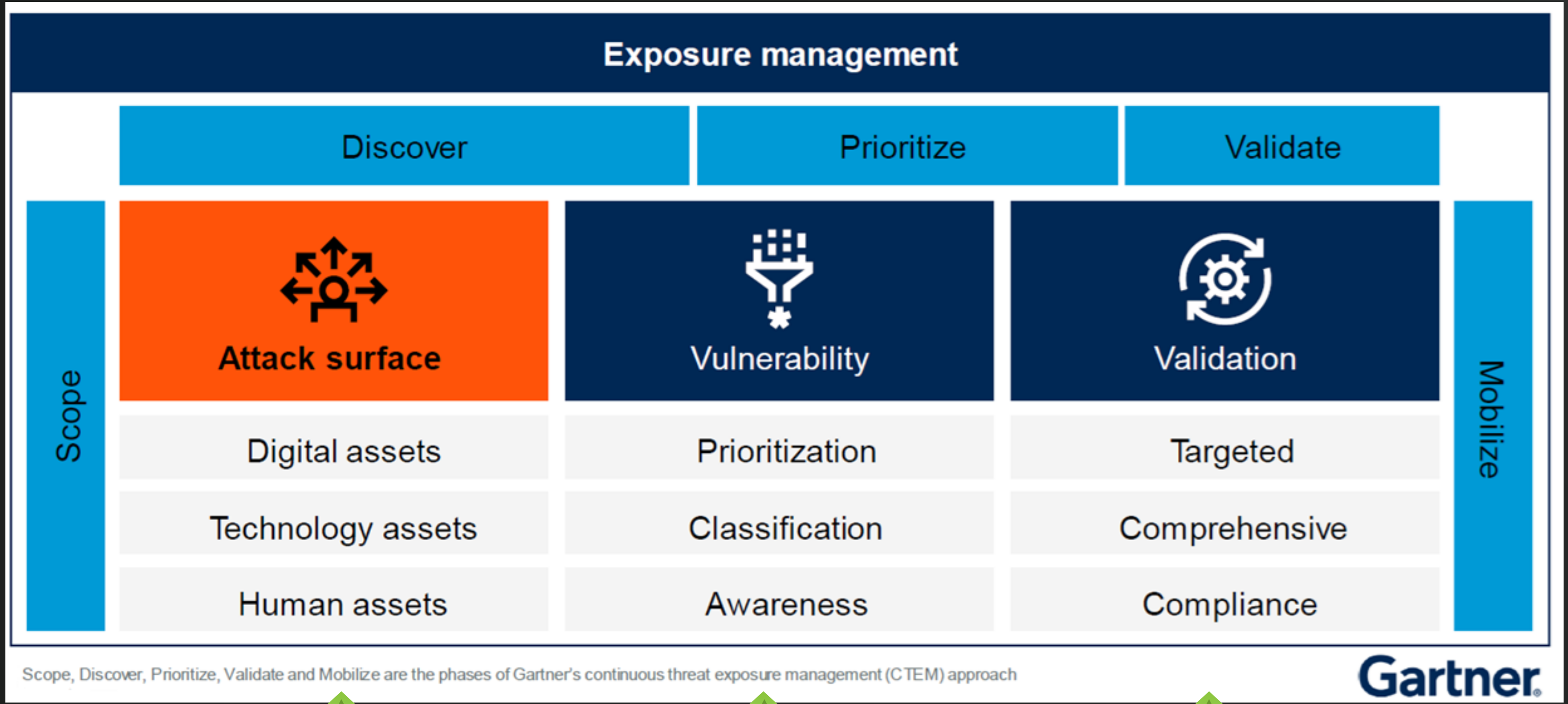


Vulnerabilities Exploited by Base Security Rating

CVSS = common vulnerability scoring system

Source: Gartner (data drawn from the IBM X-Force vulnerability database)

RidgeBot Supports Threat Exposure Management

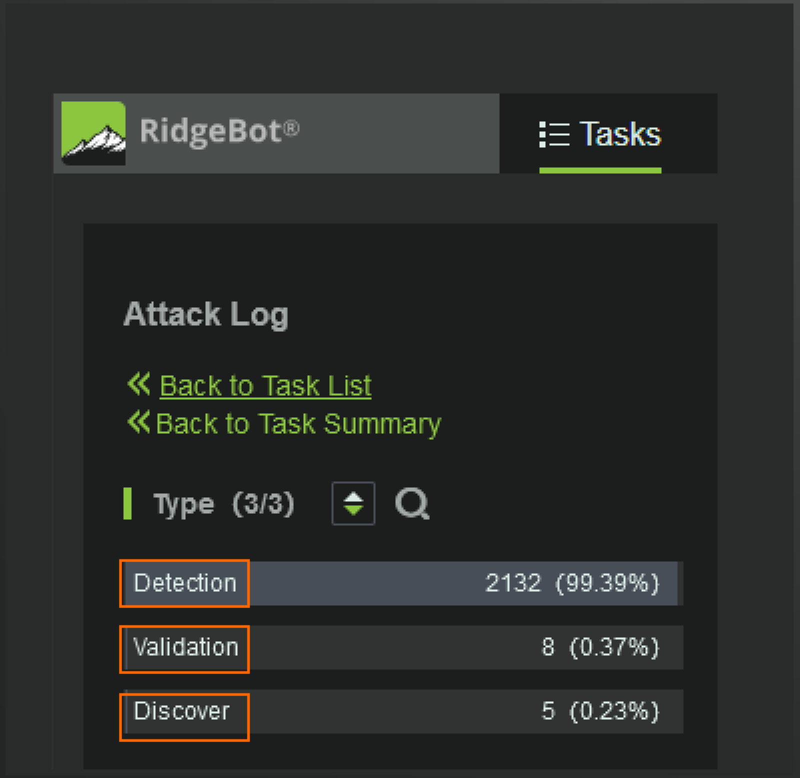


Exposure management

	Discover	Prioritize	Validate	
Scope	**Attack surface**	Vulnerability	Validation	Mobilize
	Digital assets	Prioritization	Targeted	
	Technology assets	Classification	Comprehensive	
	Human assets	Awareness	Compliance	

Scope, Discover, Prioritize, Validate and Mobilize are the phases of Gartner's continuous threat exposure management (CTEM) approach

Gartner.



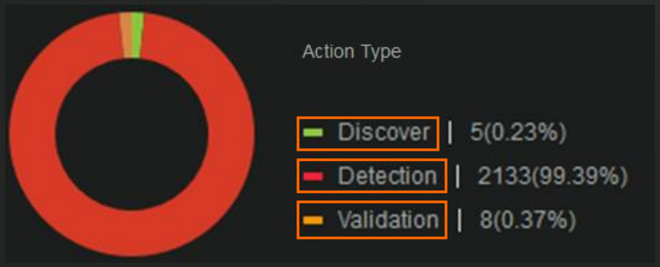
Attack Log

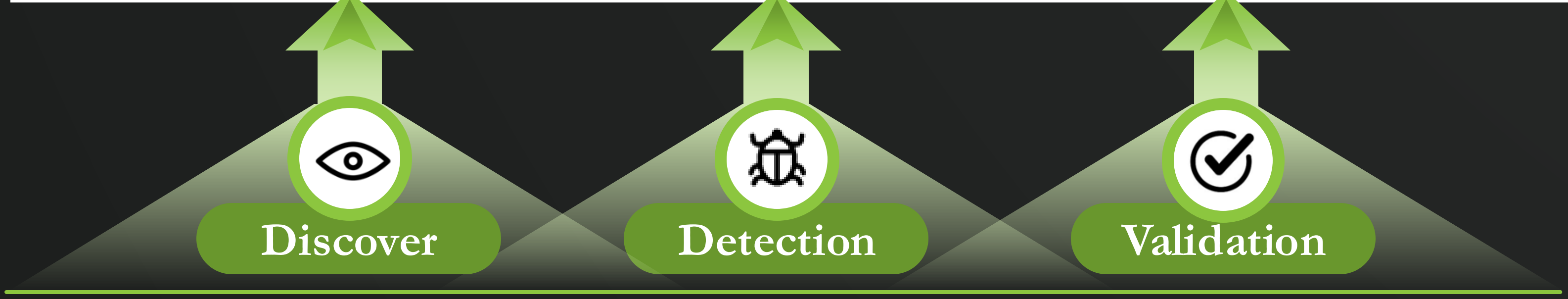
« Back to Task List

« Back to Task Summary

Type (3/3)

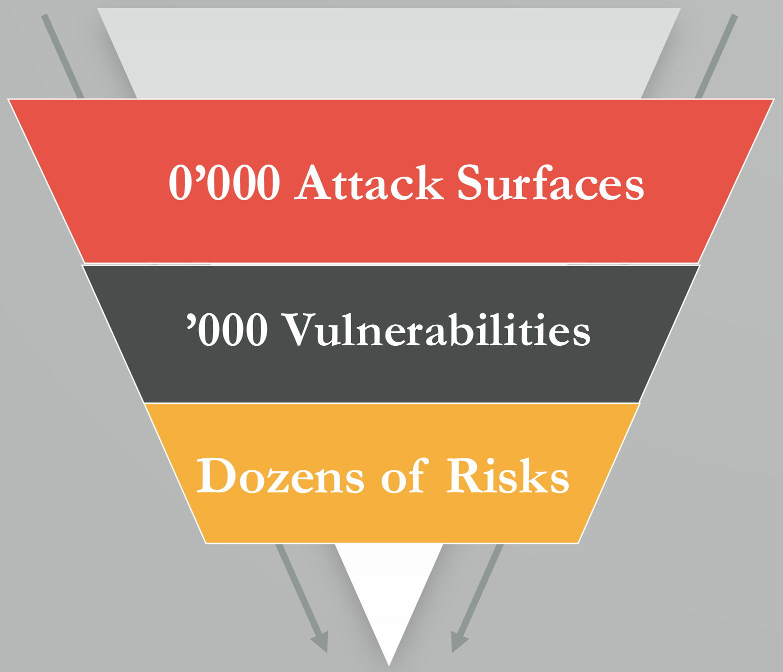
Detection	2132 (99.39%)
Validation	8 (0.37%)
Discover	5 (0.23%)





Smart Threat Exposure Mgmt Leads to Risk Mining

	Question Addressed	Actionable Insight
Attack Surface	What is visible?	What the attackers may target
Vulnerability Detection	What is vulnerable?	We understand our inherent risks
Validation	Is it possible?	Are our security investments working?



0’000 Attack Surfaces

’000 Vulnerabilities

Dozens of Risks

Risk Mining:

out of large number of potential vulnerabilities,
identify and **prioritize**
small number of exploitable & validated vulnerabilities
requiring immediate **action**

RIDGE
SECURITY

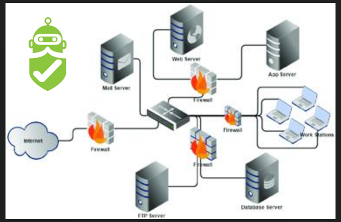
HOW DOES RIDGEBOT WORK?

RIDGE SECURITY

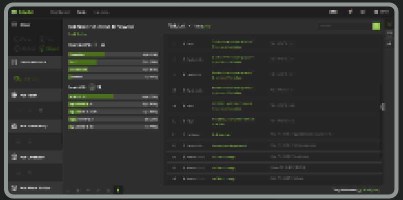
RidgeBot – Easy to Operate

Minutes with RidgeBot vs Days/weeks of manual labor

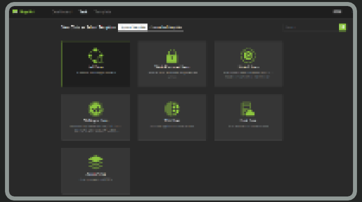
Deploy RidgeBots on bare metal servers, VMs or Clouds



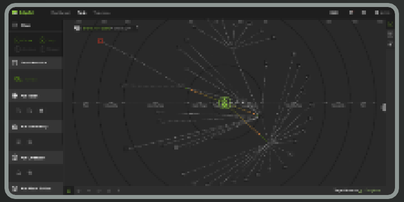
Choose test approach Pentest or ACE



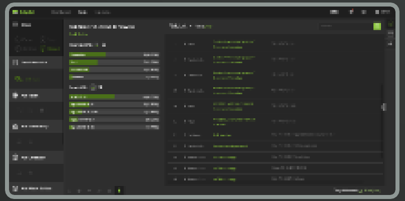
Start or Schedule a Task

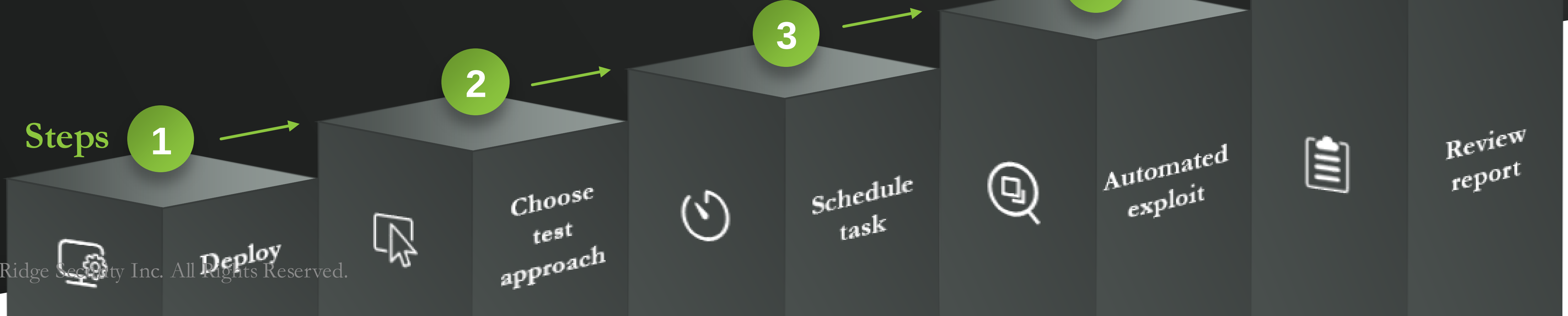


Automated Testing

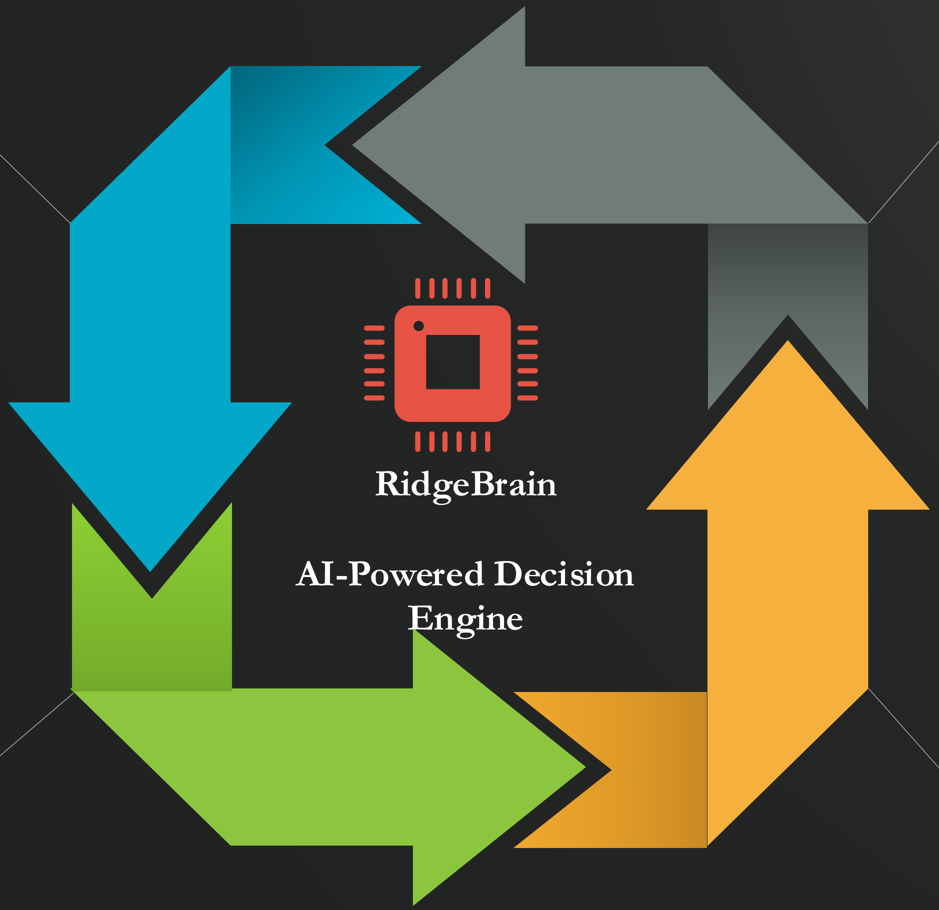


Review & Download Risk Report





100% Automated



Asset and Attack Surface Discovery

- Asset Fingerprinting
- Open ports / applications
- OS/Framework
- Domains/Subdomains
- URLs/

Vulnerability Detection

- Vulnerability information including CVE#, CVSS score
- Remediation suggestions

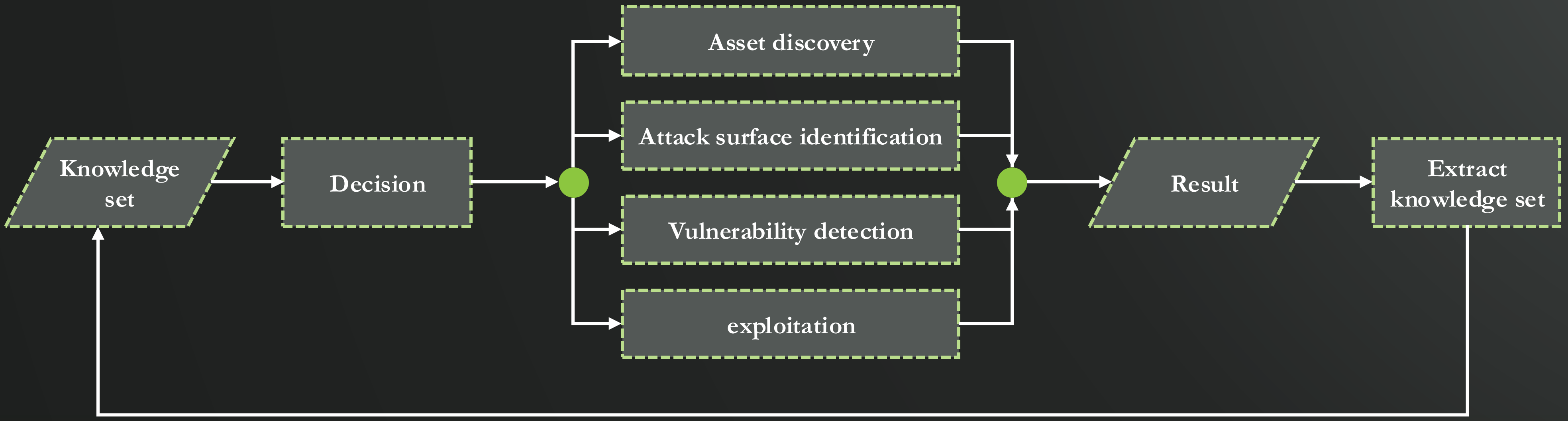
Validation with Exploits

- Autonomously choose attack path
- Perform independent testing
- Launch multi-vector iterative attacks
- Show proof

Lateral Movement

- Privilege Escalation
- Lateral Movement

AI-Powered Security Validation

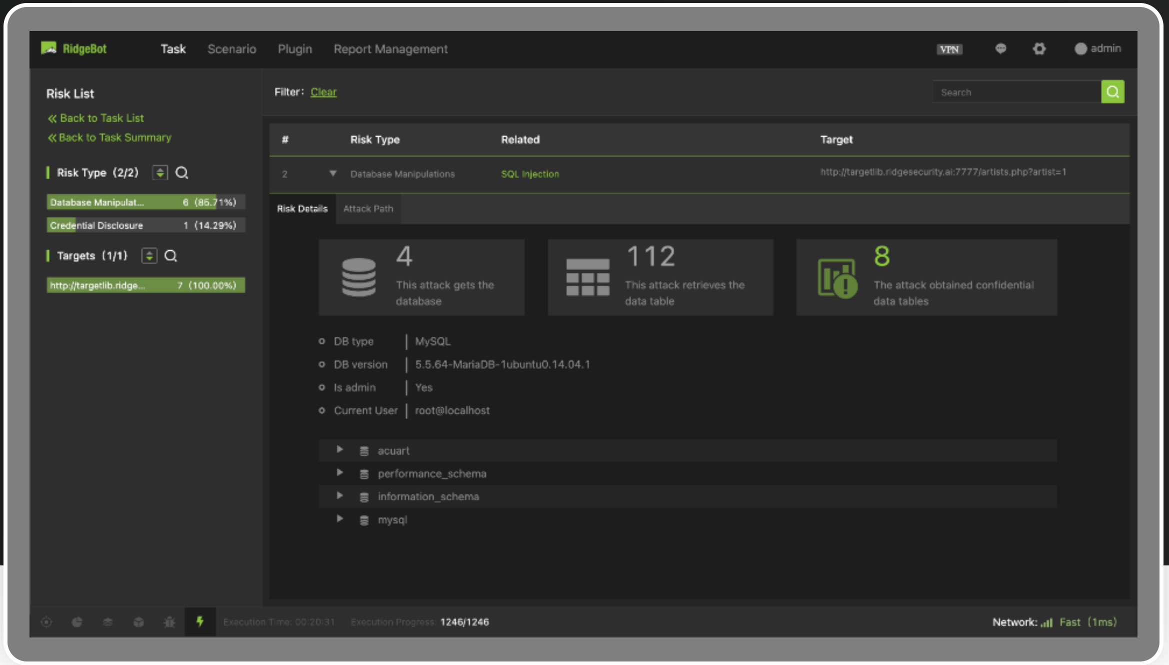


Iterative attack

Decision Making

Technology which simulates human thoughts in penetration attacks, build in an iterative attack model, connecting various data and information produced during the attack process, establishing continuous iterative attack capabilities, and jointly exploiting multiple vulnerabilities to build a three-dimensional attack capability.

Risk Findings with Proof



Risk List

« Back to Task List

« Back to Task Summary

Risk Type (2/2)

Database Manipulat...	6	(85.71%)
Credential Disclosure	1	(14.29%)

Targets (1/1)

http://targetlib.ridge...	7	(100.00%)

Filter: Clear

#		Risk Type	Related	Target
2	▼	Database Manipulations	SQL Injection	http://targetlib.ridgesecurity.ai:7777/artists.php?artist=1

4 This attack gets the database

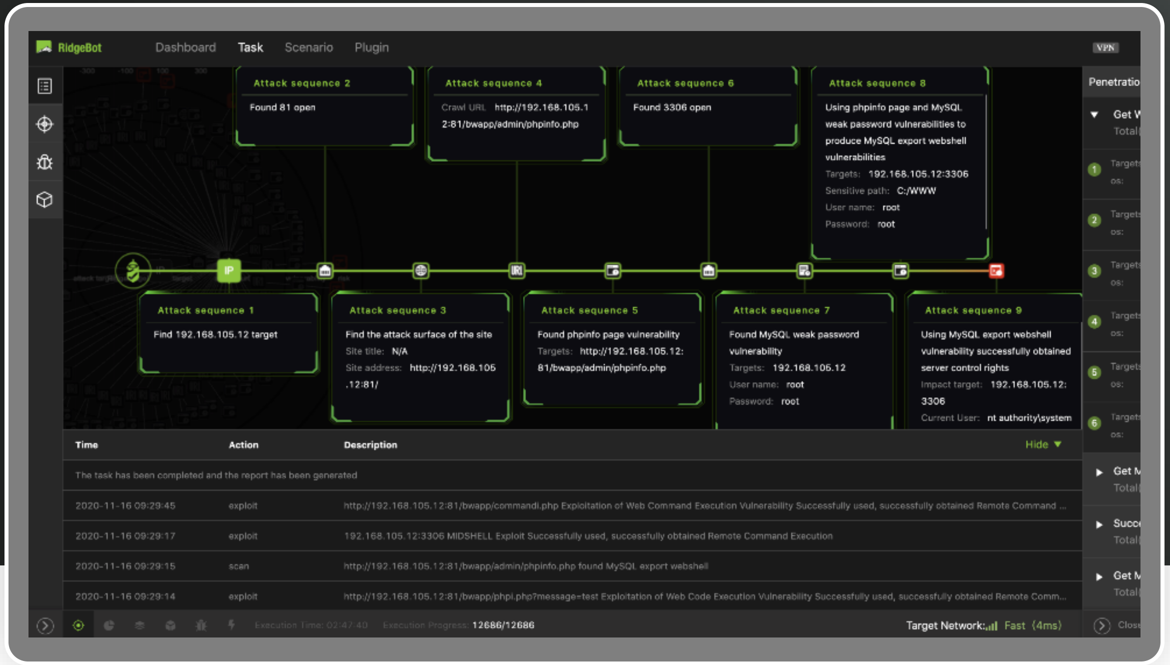
112 This attack retrieves the data table

8 The attack obtained confidential data tables

DB type	MySQL
DB version	5.5.64-MariaDB-1ubuntu0.14.04.1
Is admin	Yes
Current User	root@localhost

- acuart
- performance_schema
- information_schema
- mysql

Execution Time: 00:20:31 Execution Progress: 1246/1246 Network: Fast (1ms)



Attack sequence 1
Find 192.168.105.12 target

Attack sequence 2
Found 81 open

Attack sequence 3
Find the attack surface of the site
Site title: N/A
Site address: http://192.168.105.12:81/

Attack sequence 4
Crawl URL http://192.168.105.12:81/bwapp/admin/phpinfo.php

Attack sequence 5
Found phpinfo page vulnerability
Targets: http://192.168.105.12:81/bwapp/admin/phpinfo.php

Attack sequence 6
Found 3306 open

Attack sequence 7
Found MySQL weak password vulnerability
Targets: 192.168.105.12
User name: root
Password: root

Attack sequence 8
Using phpinfo page and MySQL weak password vulnerabilities to produce MySQL export webshell vulnerabilities
Targets: 192.168.105.12:3306
Sensitive path: C:/WWW
User name: root
Password: root

Attack sequence 9
Using MySQL export webshell vulnerability successfully obtained server control rights
Impact target: 192.168.105.12:3306
Current User: nt authority\system

Time	Action	Description
The task has been completed and the report has been generated		
2020-11-16 09:29:45	exploit	http://192.168.105.12:81/bwapp/commandi.php Exploitation of Web Command Execution Vulnerability Successfully used, successfully obtained Remote Command ...
2020-11-16 09:29:17	exploit	192.168.105.12:3306 MIDSHELL Exploit Successfully used, successfully obtained Remote Command Execution
2020-11-16 09:29:15	scan	http://192.168.105.12:81/bwapp/admin/phpinfo.php found MySQL export webshell
2020-11-16 09:29:14	exploit	http://192.168.105.12:81/bwapp/phpi.php?message=test Exploitation of Web Code Execution Vulnerability Successfully used, successfully obtained Remote Comm...

Hide ▼

Execution Time: 02:47:40 Execution Progress: 12686/12686 Target Network: Fast (4ms)

Exploit vulnerabilities

How could this happen ?

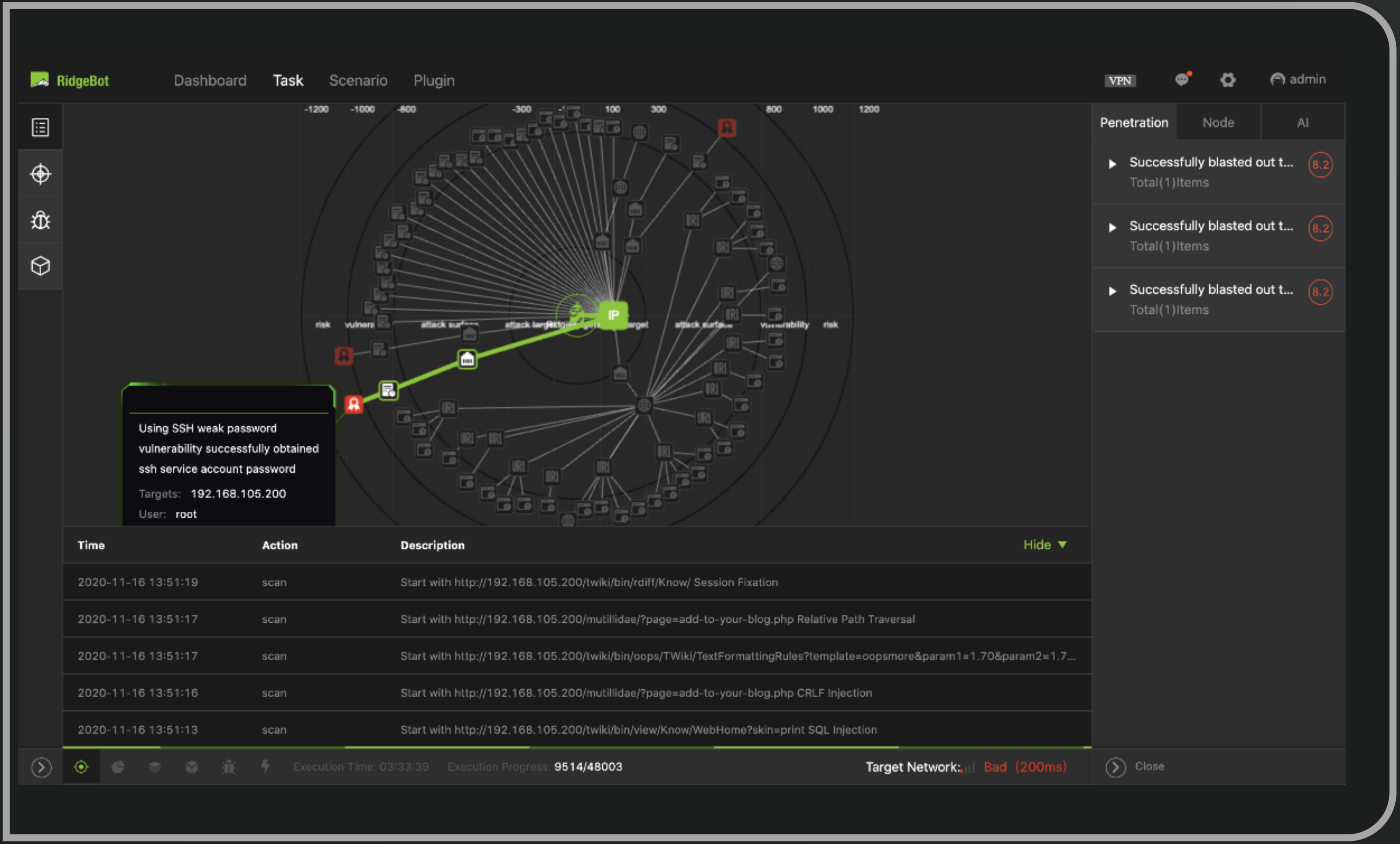
Show risk expose with evidence

What might be exposed ?

Provide remediation suggestion

What shall I do about it ?

Realtime Attack Action Visibility



Using SSH weak password vulnerability successfully obtained ssh service account password

Targets: 192.168.105.200

User: root

Time	Action	Description
2020-11-16 13:51:19	scan	Start with http://192.168.105.200/twiki/bin/rdiff/Know/ Session Fixation
2020-11-16 13:51:17	scan	Start with http://192.168.105.200/mutillidae/?page=add-to-your-blog.php Relative Path Traversal
2020-11-16 13:51:17	scan	Start with http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.70&param2=1.7...
2020-11-16 13:51:16	scan	Start with http://192.168.105.200/mutillidae/?page=add-to-your-blog.php CRLF Injection
2020-11-16 13:51:13	scan	Start with http://192.168.105.200/twiki/bin/view/Know/WebHome?skin=print SQL Injection

Hide ▼

Execution Time: 03:33:39 Execution Progress: 9514/48003 Target Network: Bad (200ms)

Successfully blasted out t... (8.2)
Total(1)Items

Successfully blasted out t... (8.2)
Total(1)Items

Successfully blasted out t... (8.2)
Total(1)Items

Auto Topology Drawing

- Shows relationships of assets and attack surfaces
- Map out vulnerabilities and risks

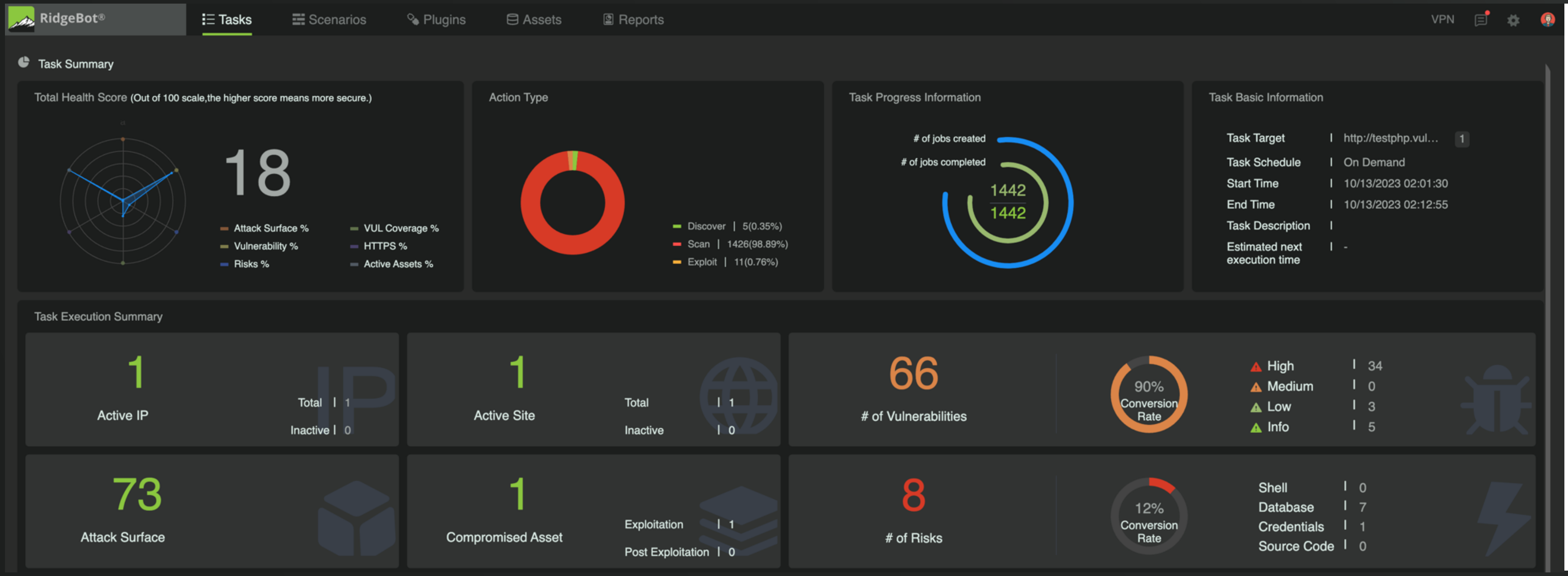
Full Attack Path Visibility

- Track the attack source and show the attack details

Show the realtime actions on dashboard

- Discover
- Scan
- Exploit

Realtime Reports



Task Summary

Total Health Score (Out of 100 scale,the higher score means more secure.)

18

- Attack Surface %
- VUL Coverage %
- Vulnerability %
- HTTPS %
- Risks %
- Active Assets %

Action Type

Discover	5(0.35%)
Scan	1426(98.89%)
Exploit	11(0.76%)

Task Progress Information

# of jobs created 1442

# of jobs completed 1442

Task Basic Information

Task Target	http://testphp.vul... 1
Task Schedule	On Demand
Start Time	10/13/2023 02:01:30
End Time	10/13/2023 02:12:55
Task Description	
Estimated next execution time	-

Task Execution Summary

1 Active IP — Total | 1, Inactive | 0

1 Active Site — Total | 1, Inactive | 0

66 # of Vulnerabilities — 90% Conversion Rate

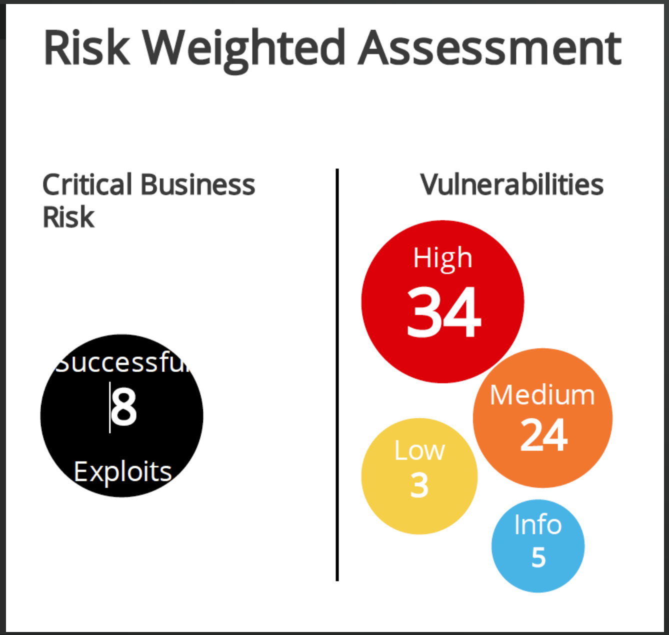
High	34
Medium	0
Low	3
Info	5

73 Attack Surface

1 Compromised Asset — Exploitation | 1, Post Exploitation | 0

8 # of Risks — 12% Conversion Rate

Shell	0
Database	7
Credentials	1
Source Code	0



Risk Weighted Assessment

RidgeBot Can Work Independently or in Conjunction with Vulnerability Management Solutions

RIDGE SECURITY

RAPID7 insightVM

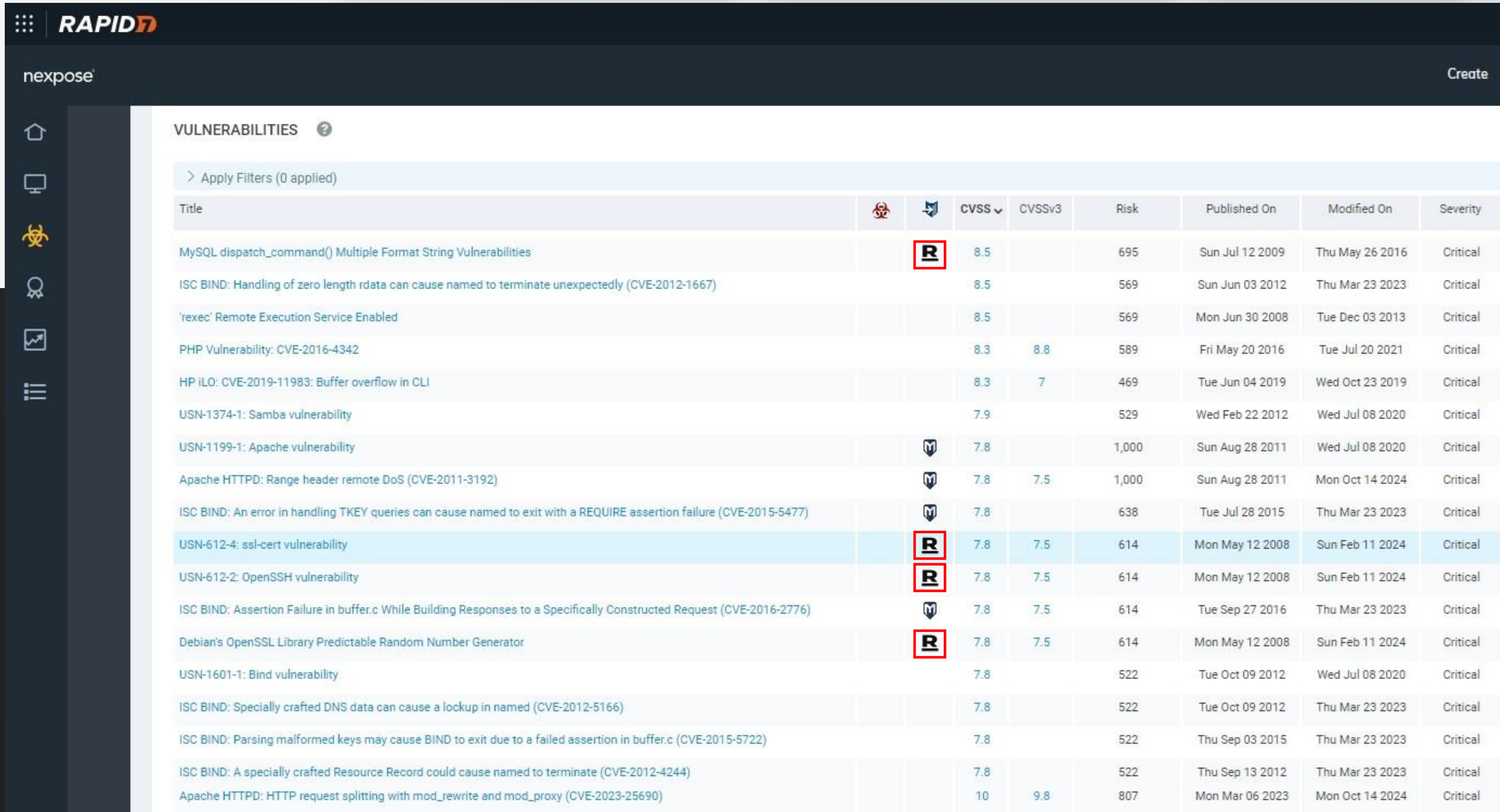
tenable Vulnerability Management

Qualys.

RidgeBot **complements** Vulnerability Management solutions’ findings.

RidgeBot identifies vulnerabilities that are both exploitable and visible by threat actors. It reports such vulnerabailities as **validated vulnerabilities** that are business **risks** and immediately actionable.

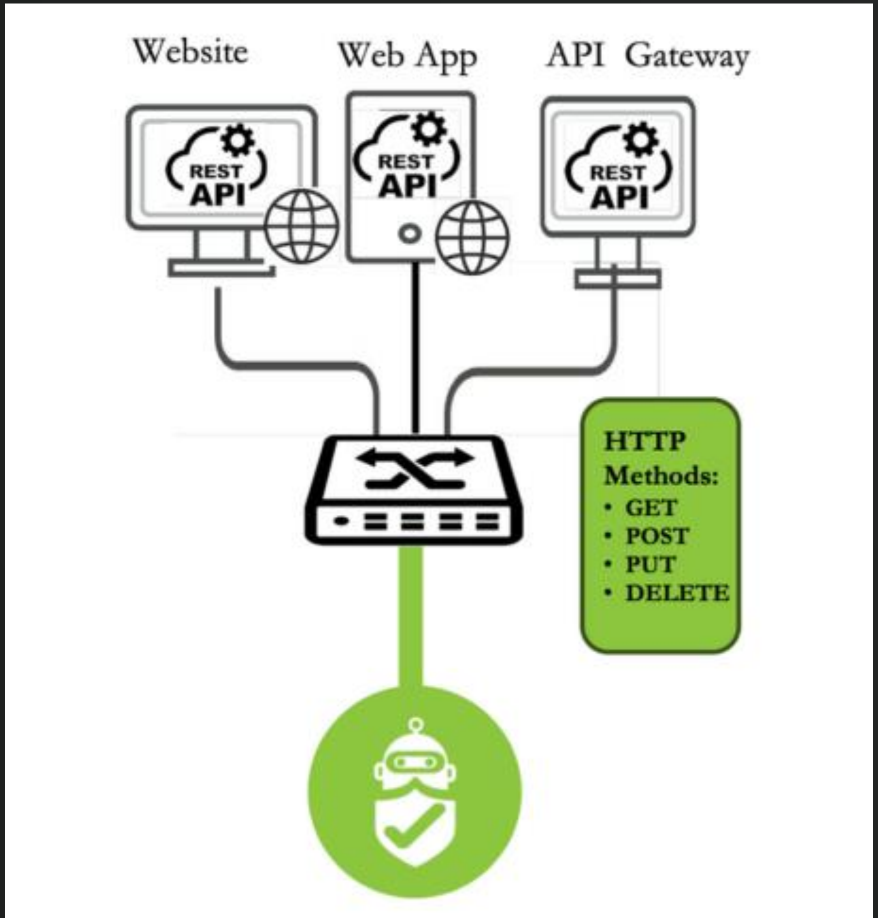
RidgeBot’s vulnerability validation results are now integrated into popular Vulnerability Management solutions’ dashboards, such as Rapid7 InsightVM and Tenable VM.



VULNERABILITIES

Title	☣		CVSS	CVSSv3	Risk	Published On	Modified On	Severity
MySQL dispatch_command() Multiple Format String Vulnerabilities		R	8.5		695	Sun Jul 12 2009	Thu May 26 2016	Critical
ISC BIND: Handling of zero length rdata can cause named to terminate unexpectedly (CVE-2012-1667)			8.5		569	Sun Jun 03 2012	Thu Mar 23 2023	Critical
'rexec' Remote Execution Service Enabled			8.5		569	Mon Jun 30 2008	Tue Dec 03 2013	Critical
PHP Vulnerability: CVE-2016-4342			8.3	8.8	589	Fri May 20 2016	Tue Jul 20 2021	Critical
HP iLO: CVE-2019-11983: Buffer overflow in CLI			8.3	7	469	Tue Jun 04 2019	Wed Oct 23 2019	Critical
USN-1374-1: Samba vulnerability			7.9		529	Wed Feb 22 2012	Wed Jul 08 2020	Critical
USN-1199-1: Apache vulnerability		M	7.8		1,000	Sun Aug 28 2011	Wed Jul 08 2020	Critical
Apache HTTPD: Range header remote DoS (CVE-2011-3192)		M	7.8	7.5	1,000	Sun Aug 28 2011	Mon Oct 14 2024	Critical
ISC BIND: An error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure (CVE-2015-5477)		M	7.8		638	Tue Jul 28 2015	Thu Mar 23 2023	Critical
USN-612-4: ssl-cert vulnerability		R	7.8	7.5	614	Mon May 12 2008	Sun Feb 11 2024	Critical
USN-612-2: OpenSSH vulnerability		R	7.8	7.5	614	Mon May 12 2008	Sun Feb 11 2024	Critical
ISC BIND: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request (CVE-2016-2776)		M	7.8	7.5	614	Tue Sep 27 2016	Thu Mar 23 2023	Critical
Debian's OpenSSL Library Predictable Random Number Generator		R	7.8	7.5	614	Mon May 12 2008	Sun Feb 11 2024	Critical
USN-1601-1: Bind vulnerability			7.8		522	Tue Oct 09 2012	Wed Jul 08 2020	Critical
ISC BIND: Specially crafted DNS data can cause a lockup in named (CVE-2012-5166)			7.8		522	Tue Oct 09 2012	Thu Mar 23 2023	Critical
ISC BIND: Parsing malformed keys may cause BIND to exit due to a failed assertion in buffer.c (CVE-2015-5722)			7.8		522	Thu Sep 03 2015	Thu Mar 23 2023	Critical
ISC BIND: A specially crafted Resource Record could cause named to terminate (CVE-2012-4244)			7.8		522	Thu Sep 13 2012	Thu Mar 23 2023	Critical
Apache HTTPD: HTTP request splitting with mod_rewrite and mod_proxy (CVE-2023-25690)			10	9.8	807	Mon Mar 06 2023	Mon Oct 14 2024	Critical

RidgeBot Web APIs Testing: Preventing Horizontal Escalation



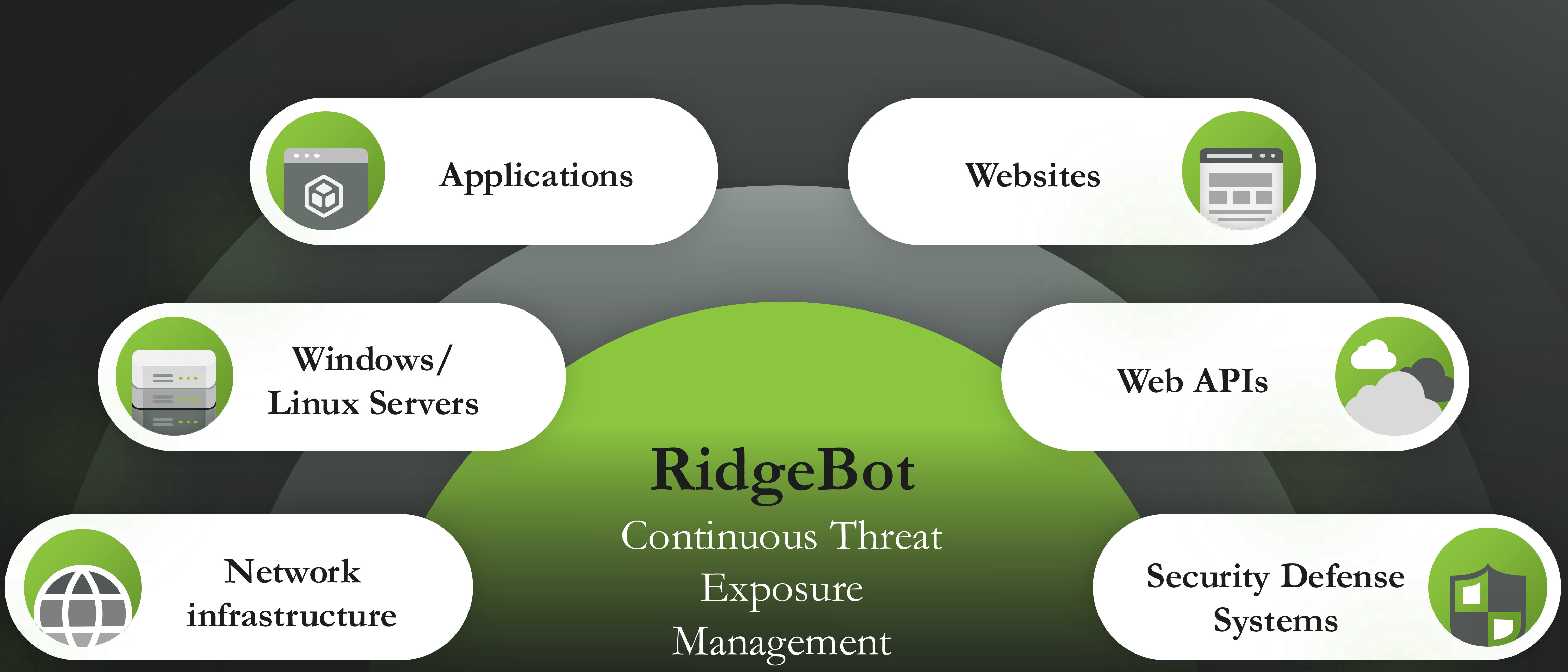
- Uncover OWASP Top 10 API vulnerabilities such as broken authorization to prevent horizontal escalation attacks

- Provide both black-box and gray-box testing to identify API vulnerabilities and risks

Safety Control – No Damage to System

- Clean up the path
- Being stealthy – rate limit
- Disable damaging plugins
- User intervention

Wider Coverage



Applications

Websites

Windows/
Linux Servers

Web APIs

Network
infrastructure

Security Defense
Systems

RidgeBot

Continuous Threat
Exposure
Management

Business Model – Software Subscription

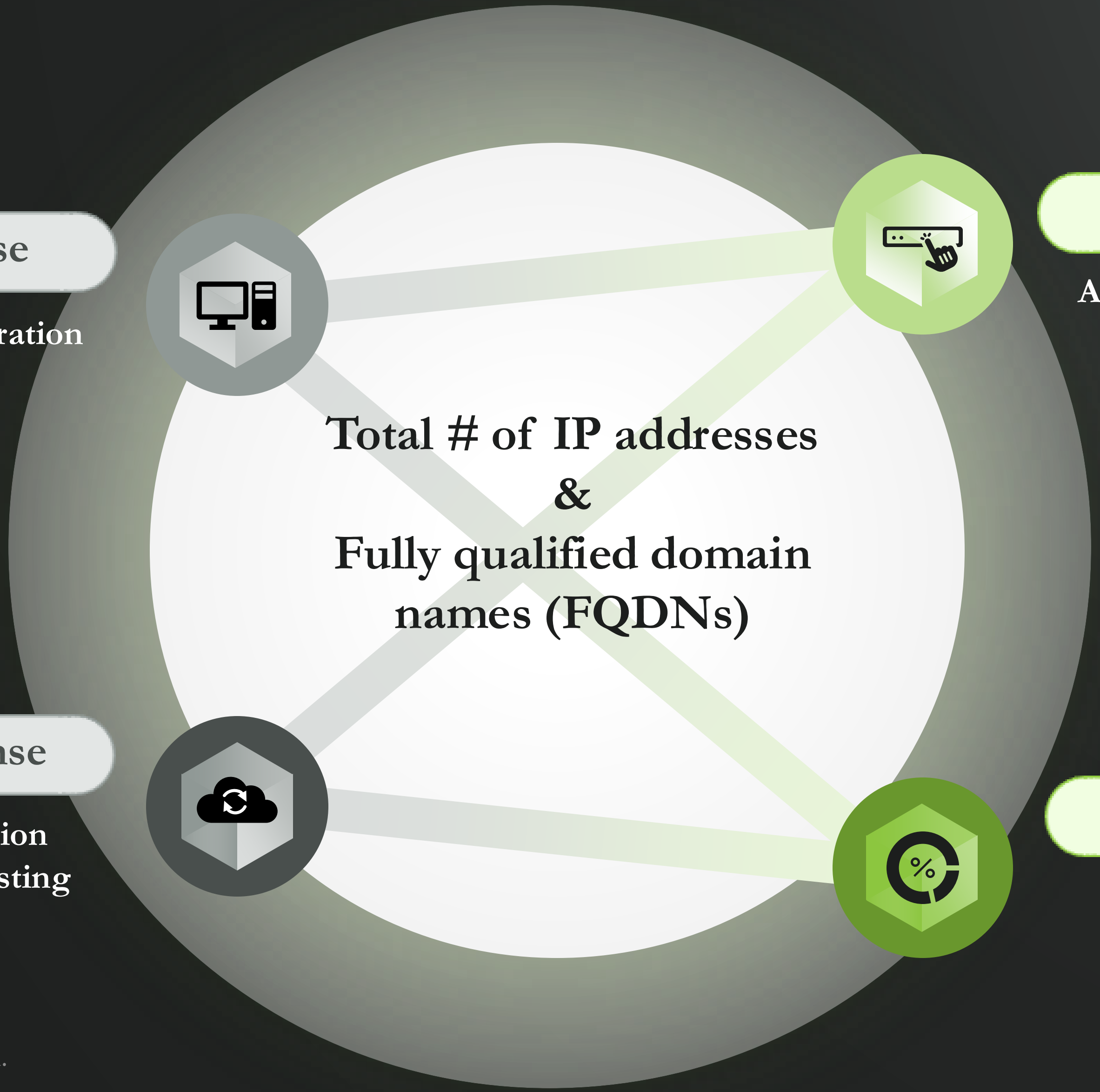
What to Test

IP License

Network Penetration Testing

Web License

Web Application Penetration Testing



Total # of IP addresses & Fully qualified domain names (FQDNs)

End-User

Annual Subscription

MSV

Annual Quota
One-Time Usage

Who Owns RidgeBot

03

WHAT CAN RIDGEBOT DO FOR ME?

RIDGE SECURITY

RidgeBot Benefits

1

Help CISO understand overall the cyber risks

2

Reduce workload for security team by pinpointing the critical risks

3

Alleviate the problem of resource shortage with automation

4

Continuous manage the risks and security posture

Value Proposition

Automated and Continuous

Agentless and Plug and Play

Zero False-Positive Risk Findings

Scheduled and On Demand

No high-skilled Personnel required

RidgeBot

Security Validation AI Agent

Use Cases

Continuous Security Control Validation
for Large Enterprises

Vulnerability Validation
For all Enterprises

Cybersecurity Hyperautomation

for Small and Medium Business

Automated Pentest Tools
for Banking and Government Agencies

Enable Pentest as a Service for
MSSPs

AUTOMATED PENETRATION TESTING

2 Testing Methodologies

Application 1

ADVERSARY CYBER EMULATION

Contact Us!

Inquiry@ridgesecurity.ai

Ridge Security Technology Inc.

www.ridgesecurity.ai

- **LinkedIn** https://linkedin.com/company/ridge-security/
- **Facebook** https://facebook.com/RidgeBot/
- **Twitter** https://twitter.com/RidgeSecurityAI
- **YouTube Channel** https://youtube.com/ridgesecurity

Thanks

Innovative approach to Security Validation Service