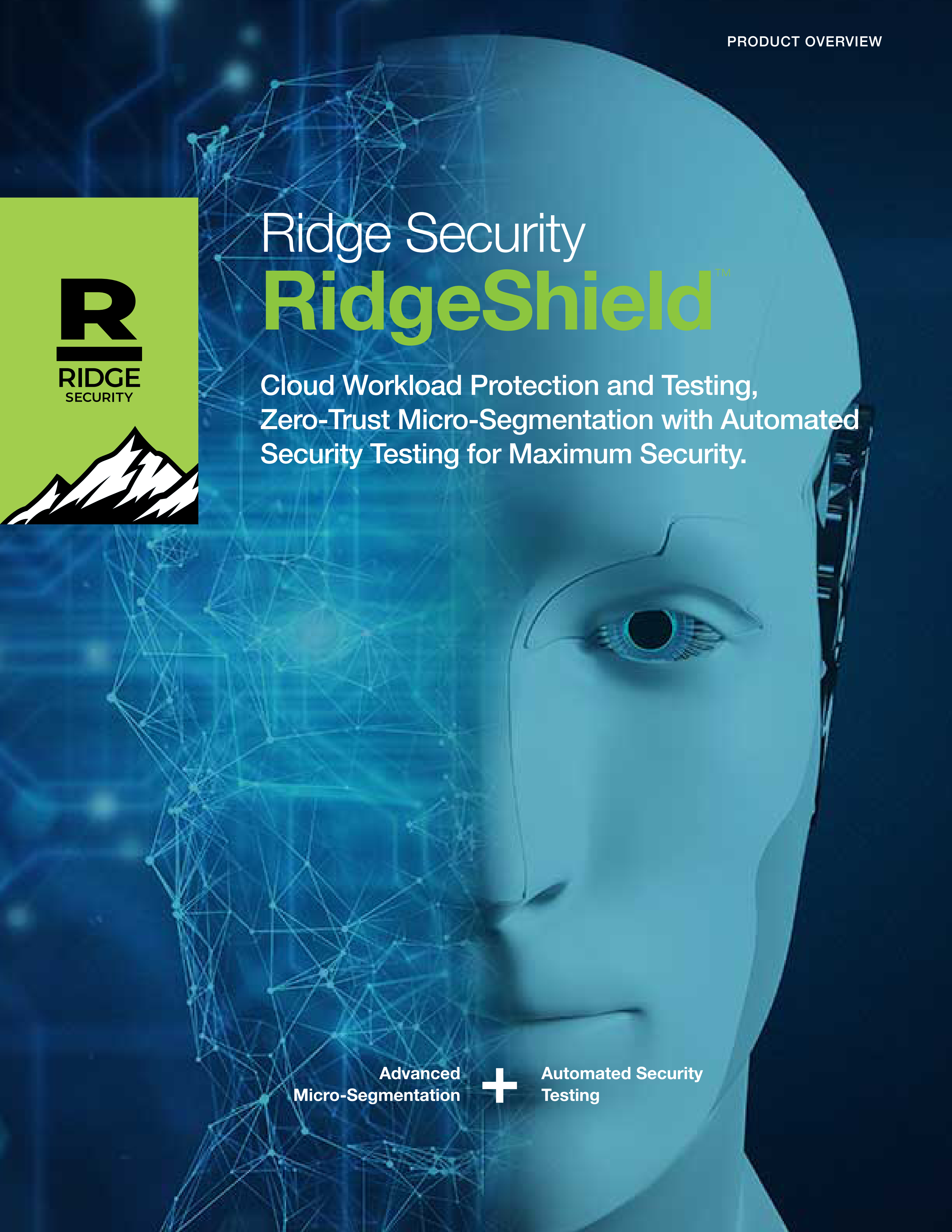
PRODUCT OVERVIEW



RIDGE
SECURITY

Ridge Security
RidgeShield™

Cloud Workload Protection and Testing, Zero-Trust Micro-Segmentation with Automated Security Testing for Maximum Security.

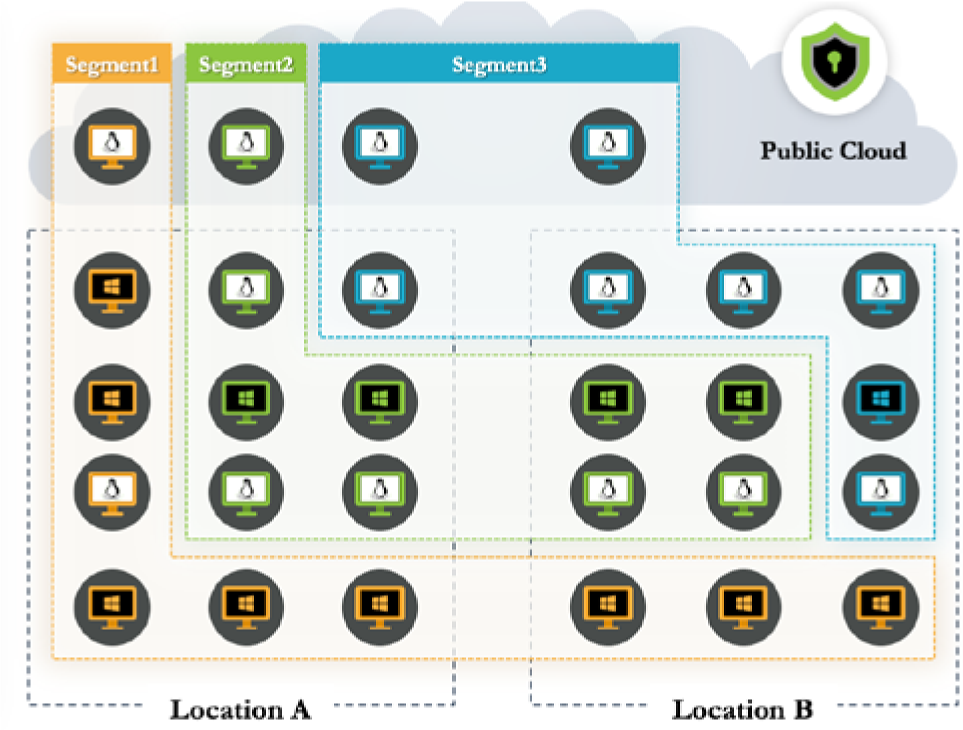
Advanced Micro-Segmentation + Automated Security Testing

Cloud Worklaod Protection and Testing

RidgeShield™

The Ridge Security Cloud Workload Protection solution, RidgeShield is your first line of defense, providing zero-trust Microsegmentation technology to protect cloud workloads, regardless of whether they are deployed on-premises, in hybrid cloud, or multi-cloud environments. With RidgeShield, organizations can ensure the security posture of their network against sophisticated security threats.

As an innovative host based micro-segmentation platform, RidgeShield supports a wide range of operating systems and workloads, continuously monitoring traffic across workloads and enforcing unified security policies across any environment.



Label-based Microsegmentation

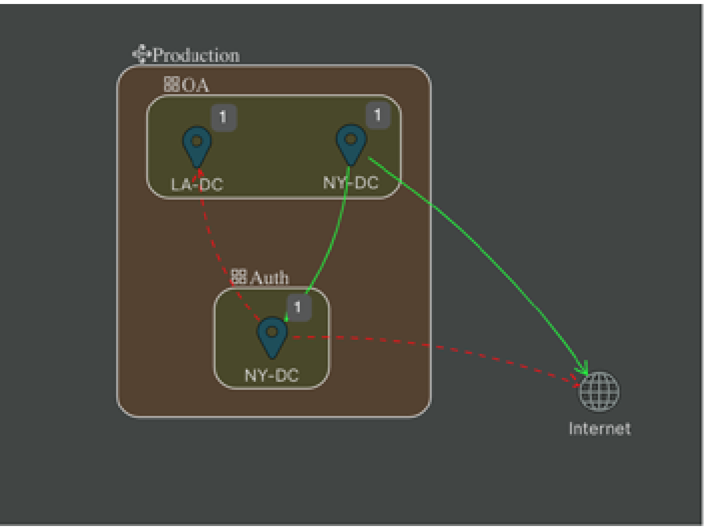
Label-based micro-segmentation is a technique that divides networks into smaller, isolated segments based on labels applied to the workload or data. These labels can be based on attributes such as application type, user group, sensitivity level, compliance requirement, or any relevant parameter. This offers a more dynamic and context-aware way of controlling access and traffic flow within a network.

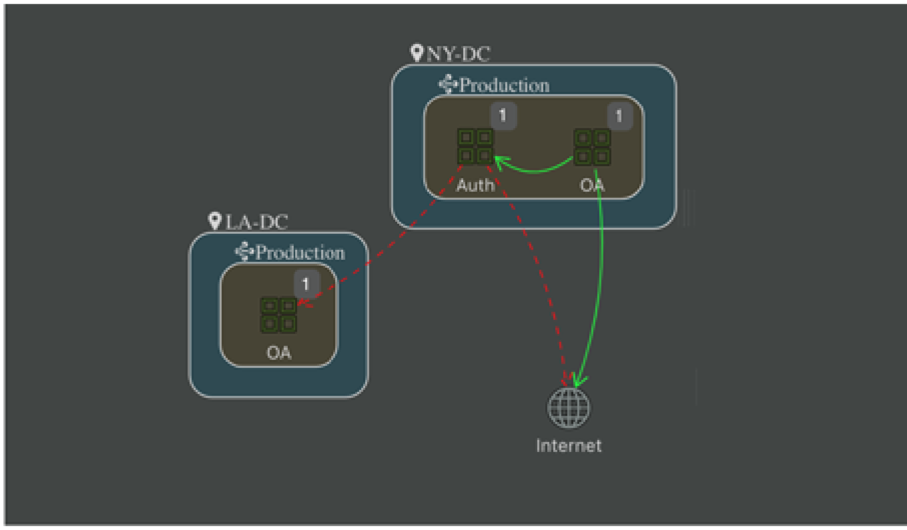
RidgeShield's label-based Microsegmentation approach allows organizations to create secure zones around applications and workloads. This approach ensures that only authorized traffic is allowed to reach those applications, limiting the scope of potential breaches by reducing the attack surface, and preventing lateral movement within the network.

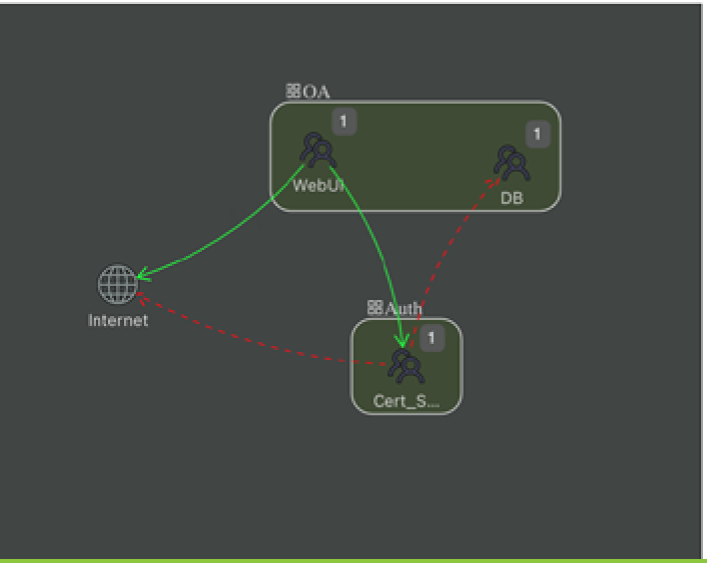
Business-oriented Flow View

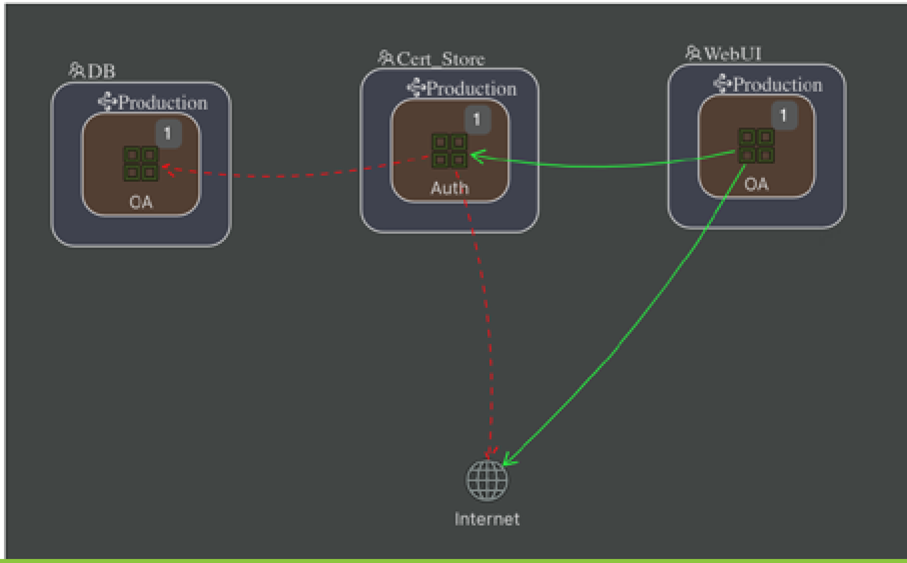
Today's IT environments are complex and typically hybrid in deployment mode. Ensuring zero-trust security is a big challenge if an IT organization does not have visibility into the business processes that make up network operations. A Business-oriented Flow View provides a high-level, visual understanding of how different assets and services are connected within a network, and how they interact with each other. It can greatly help to identify potential attack vectors and vulnerabilities, and to prioritize security controls and remediation efforts.

RidgeShield's Business-oriented Flow View allows organizations to visualize communications between workloads and monitor and enforce security policies in real-time. It provides a simplified, business-focused view of the network architecture, highlighting critical assets and services, and their dependencies and relationships. The information can be used to identify potential security risks, such as unauthorized access, data breaches, or service disruptions, and helps organizations proactively remediate them before they can be exploited by attackers.

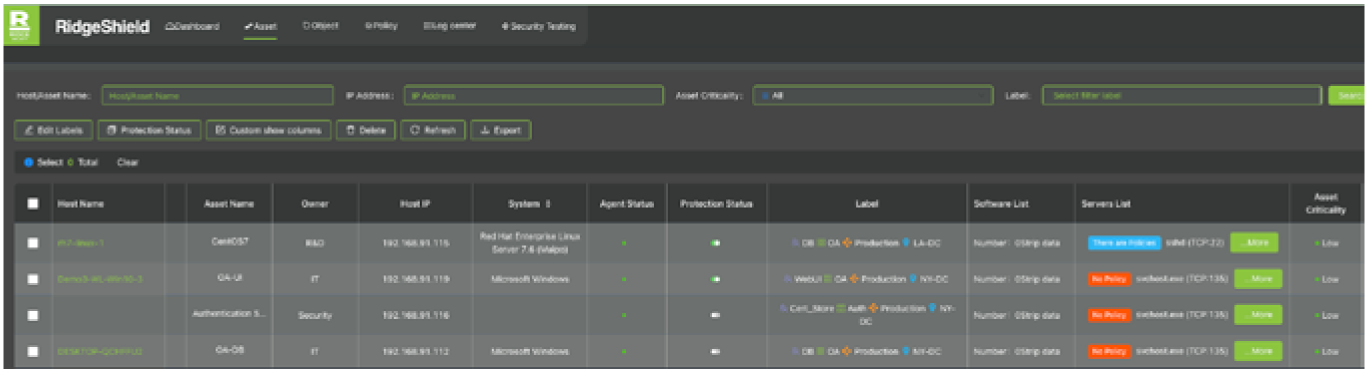








Only RidgeShield Combines Automated Security Testing with Cloud Workload Protection



Host/Asset Name: Host/Asset Name IP Address: IP Address Asset Criticality: All Label: Select filter label

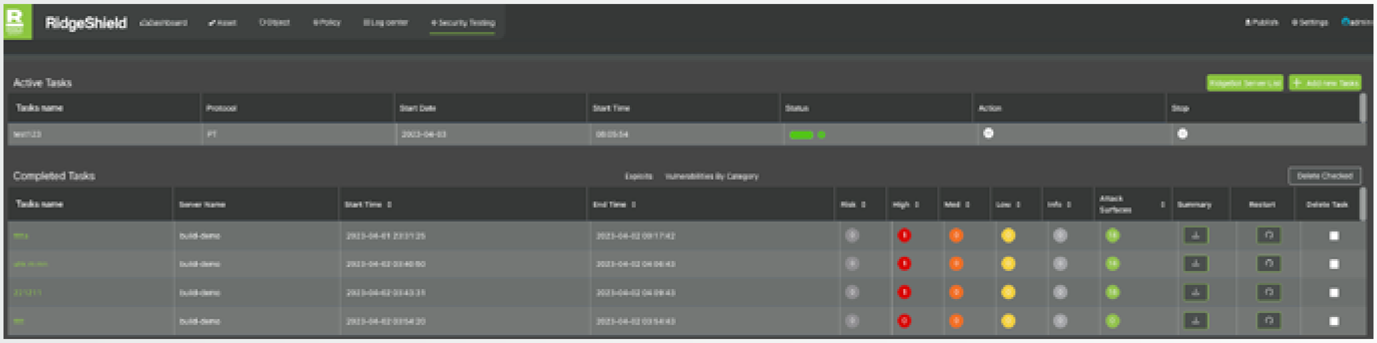
● Select 0 Total Clear

□	Host Name	Asset Name	Owner	Host IP	System	Agent Status	Protection Status	Label	Software List	Servers List	Asset Criticality
□	[illegible]	CentOS7	R&D	192.168.91.115	Red Hat Enterprise Linux Server 7.6 (Maipo)	●	●	DB OA Production LA-DC	Number : 0Strip data	There are Policies sshd (TCP:22) ...More	● Low
□	[illegible]	OA-UI	IT	192.168.91.119	Microsoft Windows	●	●	WebUI OA Production NY-DC	Number : 0Strip data	No Policy svchost.exe (TCP:135) ...More	● Low
□		Authentication S...	Security	192.168.91.116		●	●	Cert_Store Auth Production NY-DC	Number : 0Strip data	No Policy svchost.exe (TCP:135) ...More	● Low
□	DESKTOP-[illegible]	OA-DB	IT	192.168.91.112	Microsoft Windows	●	●	DB OA Production NY-DC	Number : 0Strip data	No Policy svchost.exe (TCP:135) ...More	● Low

Asset Management

Asset management is a critical component of any penetration testing solution. It helps to ensure that all assets are properly inventoried, tracked, and secured to minimize potential vulnerabilities and risks in each network.

RidgeShield provides asset management capabilities that help organizations identify and manage their assets and workloads across all environments. It uses various techniques and tools to discover and inventory digital assets, helping organizations ensure that their workloads are properly secured and compliant with regulatory requirements.



Active Tasks

Tasks name	Protocol	Start Date	Start Time	Status	Action	Stop
test123	PT	2023-04-03	08:05:54	●	○	○

Completed Tasks

Tasks name	Server Name	Start Time	End Time	Risk	High	Med	Low	Info	Attack Surfaces	Summary	Restart	Delete Task
[illegible]	build-demo	2023-04-01 23:31:25	2023-04-02 00:17:42	0	1	0	0	0	14			□
[illegible]	build-demo	2023-04-02 03:40:50	2023-04-02 04:06:43	0	1	0	0	0	14			□
221211	build-demo	2023-04-02 03:43:31	2023-04-02 04:09:43	0	1	0	0	0	14			□
[illegible]	build-demo	2023-04-02 03:54:20	2023-04-02 03:54:43	0	0	0	0	0	0			□

Complete DevSecOps Cycle with Integrated Security Testing

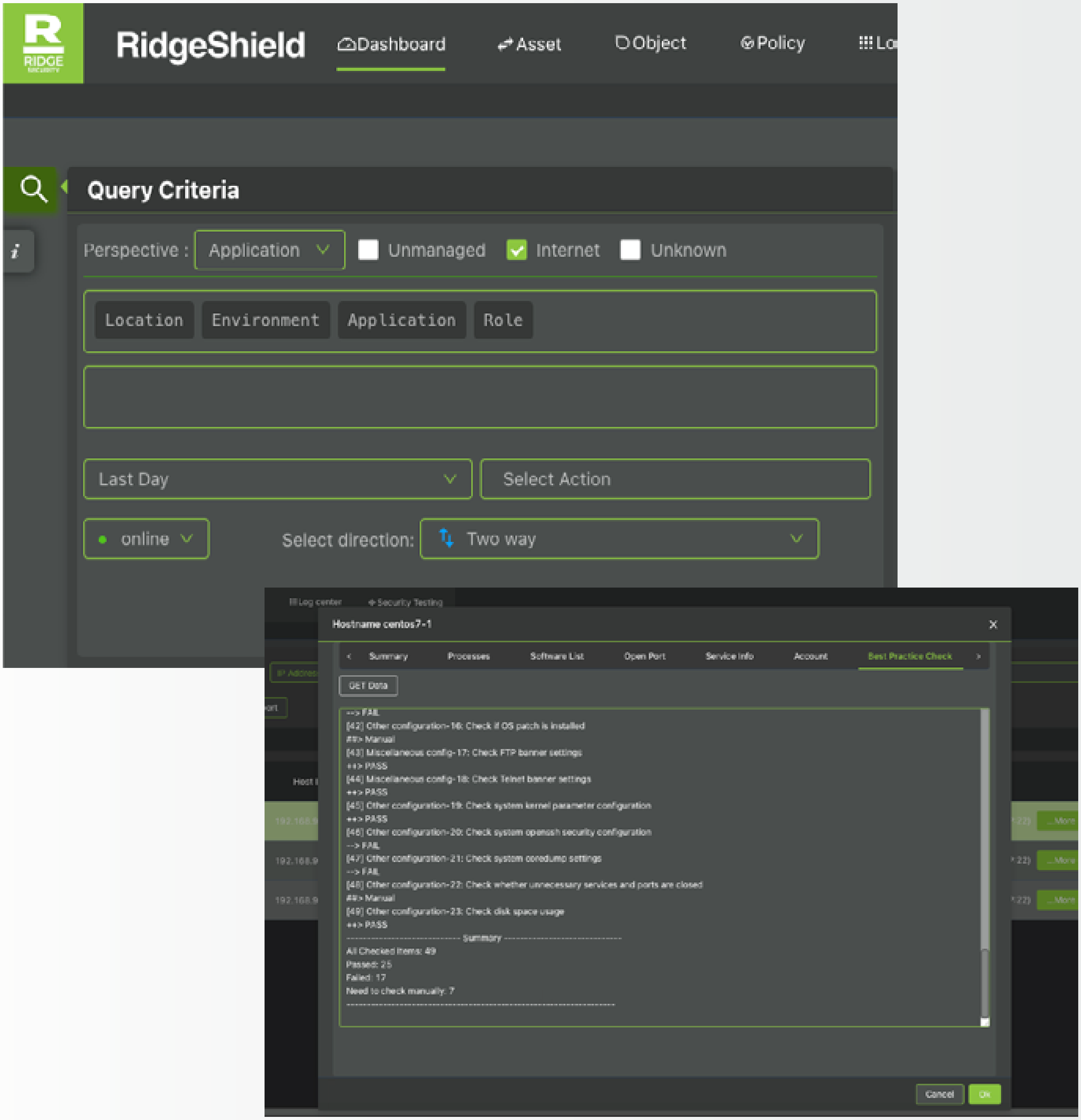
RidgeShield integrates the core security testing capabilities of RidgeBot, allowing organizations to perform Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST) over their workloads. In addition, the integration also enables the organizations to test their overall security posture across cloud, servers, applications, and networks from one platform. This feature helps organizations identify potential security gaps and proactively remediate them before they can be exploited by attackers.

RidgeShield is a comprehensive security solution that provides zero-trust Microsegmentation and protects workloads across different environments, delivering tangible business benefits:

- Security operations efficiency across environments
- Cost savings with automation and integration
- Real-time multi-dimension visibility of network assets
- Improved security posture with reduced infrastructure downtime

Workload Operating System Baseline Security Check to Minimize Risks

The Workload Operating System Baseline Security Check provided by RidgeShield is a critical step in minimizing cybersecurity risks for Windows and Linux systems. By running a baseline security check, RidgeShield identifies configuration discrepancies between the running system and the vendor's recommended best practices. Any misconfigured or non-secure settings are flagged as alerts, allowing customers to quickly address any potential vulnerabilities and strengthen their overall security posture. By proactively identifying and addressing these configuration issues, RidgeShield helps to mitigate potential security risks and ensure that workloads are operating securely.



Perspective : Application
☐ Unmanaged ☑ Internet ☐ Unknown

Last Day

● online

Select direction: Two way

Hostname centos7-1

```
--> FAIL
[42] Other configuration-16: Check if OS patch is installed
##> Manual
[43] Miscellaneous config-17: Check FTP banner settings
++> PASS
[44] Miscellaneous config-18: Check Telnet banner settings
++> PASS
[45] Other configuration-19: Check system kernel parameter configuration
++> PASS
[46] Other configuration-20: Check system openssh security configuration
--> FAIL
[47] Other configuration-21: Check system coredump settings
--> FAIL
[48] Other configuration-22: Check whether unnecessary services and ports are closed
##> Manual
[49] Other configuration-23: Check disk space usage
++> PASS
------------------------------ Summary ------------------------------
All Checked Items: 49
Passed: 25
Failed: 17
Need to check manually: 7
-----------------------------------------------------------------------
```

Highlights

- **Increased Security:** RidgeShield provides a comprehensive security solution that protects workloads against modern security threats. With its label-based micro-segmentation, business-oriented flow view, and operating system baseline security check, organizations can ensure that their workloads are secure and compliant.
- **Reduced Risk:** RidgeShield reduces the attack surface by creating secure zones around applications and workloads. This approach prevents lateral movement within the network and reduces the risk of data breaches and other security incidents.
- **Simplified Security Operations:** RidgeShield uses automation to simplify security operations and reduce the burden on IT teams. With automated policy enhancement and instant security checks, organizations can reduce the time and resources required to maintain their security posture.
- **Improved Compliance:** RidgeShield provides a comprehensive security solution that helps organizations meet regulatory requirements and industry standards. With RidgeShield, organizations can maintain compliance across all their environments and avoid costly fines and penalties.

Gartner
Peer Insights™

Read what customers are saying about Ridge Security

The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Garter Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates.

Contact Ridge 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