



# Ridge Security **RidgeShield™**

Protezione e test del Workload in cloud, Micro-Segmentazione Zero-Trust e test di sicurezza automatizzati per la massima sicurezza

Micro-Segmentazione  
avanzata



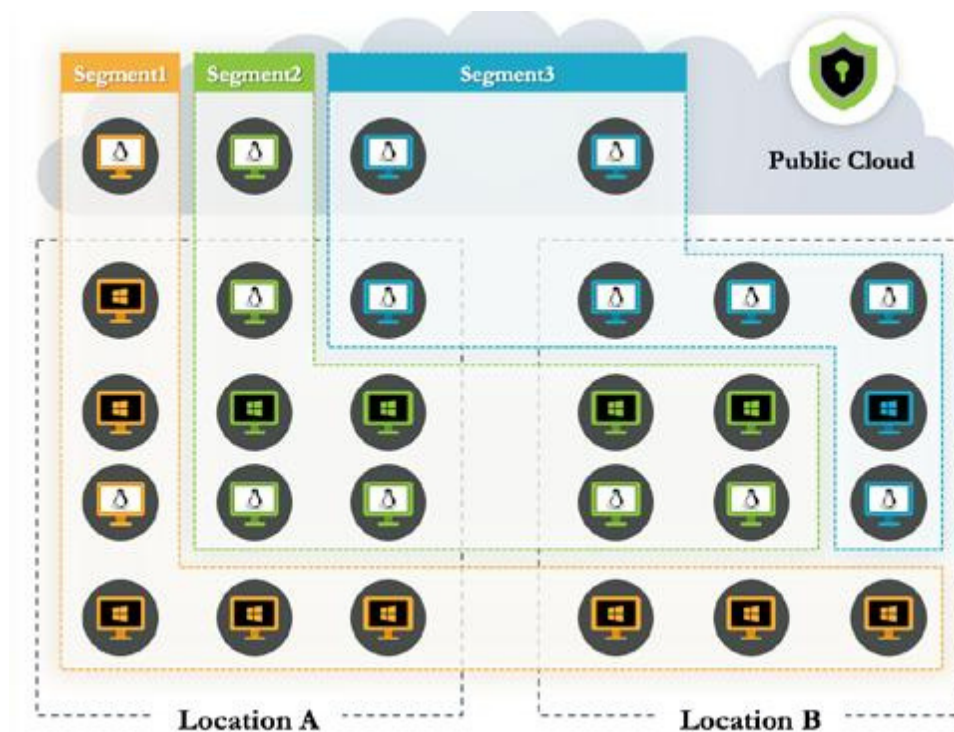
Test di sicurezza  
automatizzati

## Protezione e test del Workload in cloud

# RidgeShield™

La soluzione di protezione e test del Workload di Ridge Security, RidgeShield, è la tua prima linea di difesa in quanto offre una tecnologia di micro-segmentazione zero-trust per proteggere i Workload in cloud, indipendentemente dal fatto che siano distribuiti on-premise, in ambienti cloud ibridi o multi-cloud. Con RidgeShield, le organizzazioni godono di un ottimo livello di sicurezza di rete, in grado di fronteggiare le minacce.

Come innovativa piattaforma di micro-segmentazione basata su host, RidgeShield supporta un'ampia gamma di sistemi operativi e Workload, monitorando continuamente il traffico tra essi e applicando criteri di sicurezza unificati in qualsiasi ambiente.



### Micro-Segmentazione basata su Label

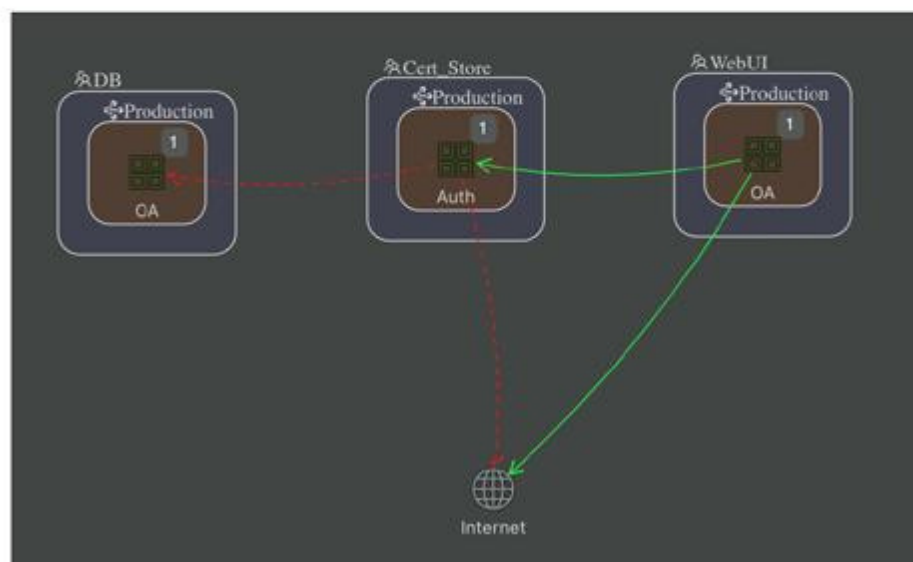
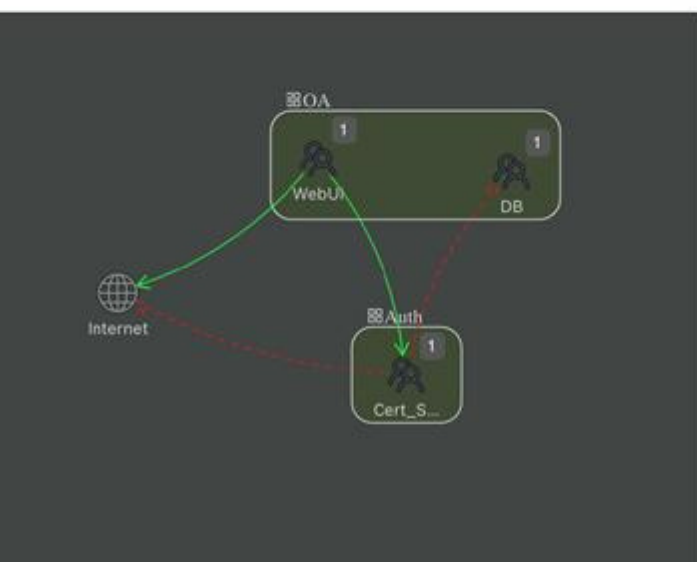
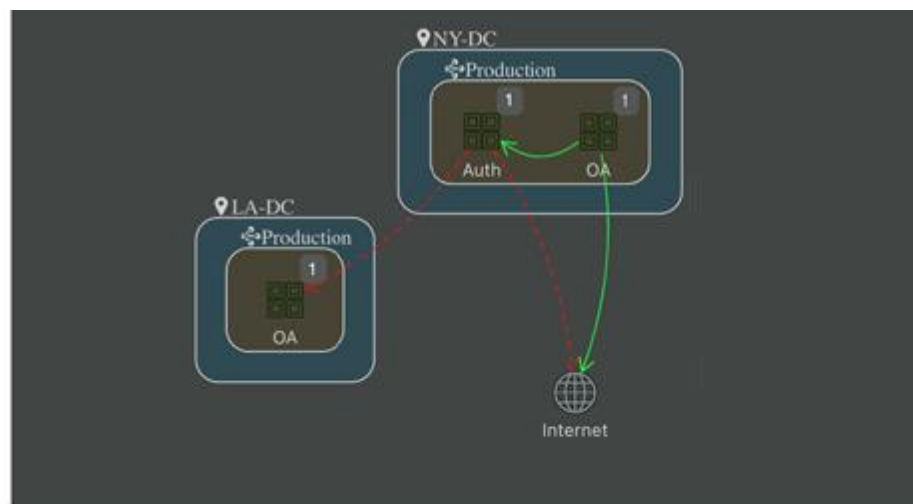
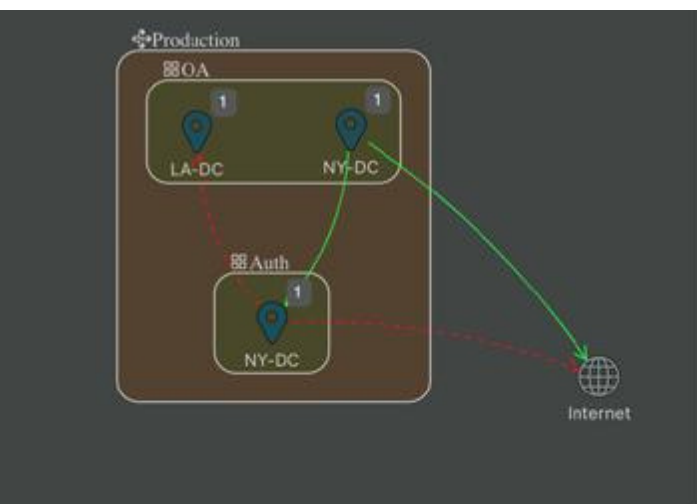
Questo tipo di micro-segmentazione è una tecnica che consiste nella divisione delle reti in segmenti più piccoli e isolati, basati su Label applicate al Workload o ai dati. Le Label possono essere basate su attributi come il tipo di applicazione, il gruppo di utenti, il livello di sensibilità, i requisiti di conformità o qualsiasi altro parametro rilevante. Tutto ciò offre una modalità di controllo degli accessi e del traffico di rete, più dinamica e sensibile.

Questo approccio di micro-segmentazione fa in modo che le organizzazioni possano creare zone sicure intorno alle applicazioni e ai Workload. In questo modo è possibile garantire che solo il traffico autorizzato possa raggiungere tali applicazioni, in quanto vengono limitate potenziali violazioni riducendo la superficie di attacco e impedendo il movimento laterale all'interno della rete.

## Flow View orientata al business

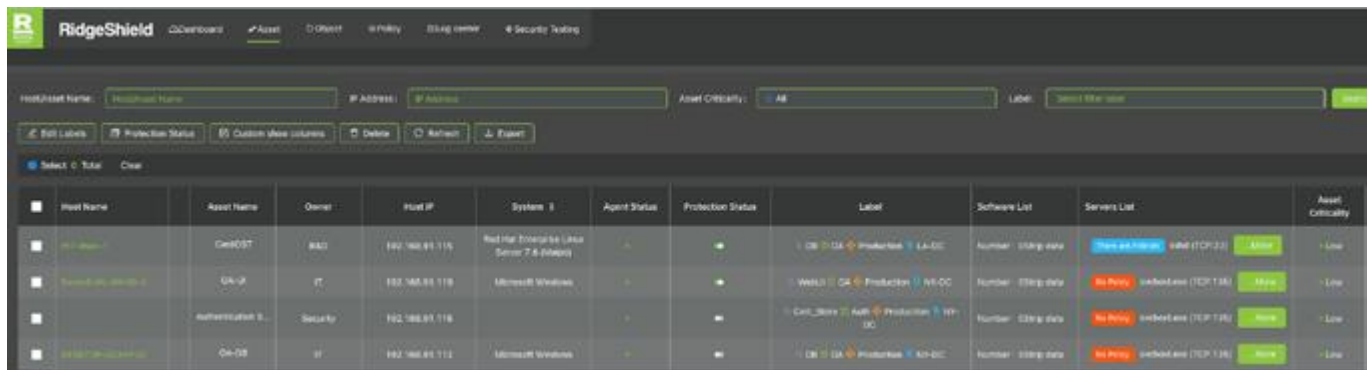
Gli ambienti IT odierni sono complessi e tipicamente ibridi in modalità di distribuzione. Garantire la sicurezza zero-trust infatti è una grande sfida se un'organizzazione IT non ha visibilità sui processi aziendali. Una visualizzazione del flusso orientata al business però, fornisce un gran livello di sicurezza, visibilità di come risorse e servizi siano collegati all'interno di una rete e come interagiscono tra loro. Questo può essere di grande aiuto per identificare potenziali vettori di attacco, potenziali vulnerabilità e per dare priorità ai controlli di sicurezza.

La Flo View orientata al business di RidgeShield consente alle organizzazioni di visualizzare le comunicazioni tra i Workload e di monitorare e applicare le policy di sicurezza in tempo reale. Fornisce una visione semplificata e incentrata sul business dell'architettura di rete, evidenziando risorse e servizi critici nonché le loro dipendenze e relazioni. Le informazioni rilasciate possono poi essere utilizzate per identificare potenziali rischi per la sicurezza, come accessi non autorizzati, violazioni dei dati o interruzioni di servizio. Non solo, aiutano anche le organizzazioni a risolvere questi problemi in modo proattivo prima che possano essere sfruttati dagli hacker



**Solo RidgeShield combina test di sicurezza automatizzati con la protezione dei Workload in cloud**

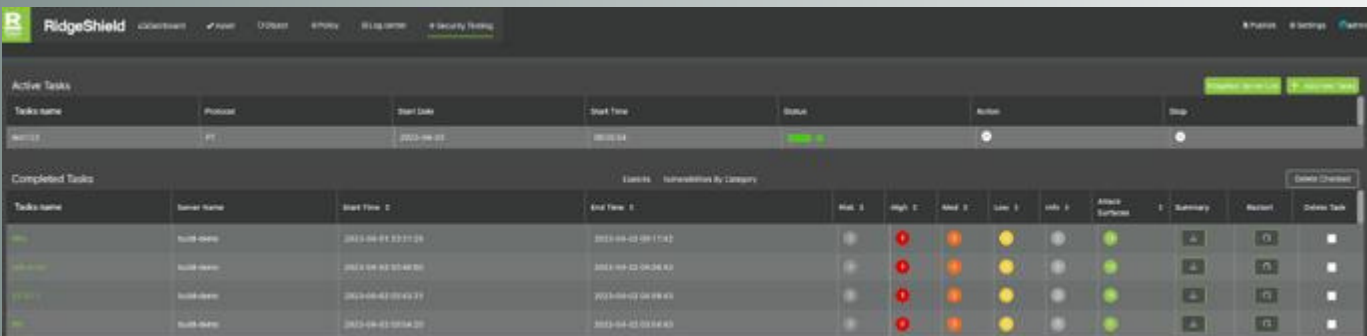




## Gestione delle risorse

La gestione delle risorse è una componente critica di qualsiasi soluzione di penetration test. Essa infatti, aiuta a garantire che tutte le risorse siano correttamente inventariate, tracciate e protette, per ridurre al minimo potenziali vulnerabilità e rischi in ogni rete. RidgeShield offre funzionalità di gestione delle risorse in grado di aiutare le organizzazioni a identificare e gestire i propri assets e workload in tutti gli ambienti.

Vengono utilizzate diverse tecniche e diversi strumenti per identificare ed inventariare tali risorse perché, in questo modo, si possono aiutare le varie organizzazioni a garantire che i propri Workload siano adeguatamente protetti e conformi ai vari requisiti normativi.



## Completa il ciclo DevSecOps con i test di sicurezza integrati

RidgeShield integra le principali funzionalità dei test di sicurezza di RidgeBot, consentendo alle organizzazioni di eseguire i Dynamic Application Security Testing (DAST) e gli Interactive Application Security Testing (IAST) sui propri Workload. Inoltre, grazie a questa integrazione, per le organizzazioni è possibile testare anche il proprio livello di sicurezza complessivo su cloud, server, applicazioni e reti da un'unica piattaforma. Grazie a questa funzionalità è possibile quindi identificare potenziali falle nella sicurezza e correggerle in modo proattivo, prima che possano essere sfruttate.

RidgeShield è una soluzione di sicurezza completa che fornisce una micro-segmentazione zero-trust e protegge i vari Workload in diversi ambienti, offrendo vantaggi aziendali come:

- Efficienza delle operazioni di sicurezza in tutti gli ambienti;
- Risparmi sui costi con l'automazione e l'integrazione;
- Visibilità multidimensionale in tempo reale delle risorse di rete;
- Aumento della posizione di sicurezza e tempi di inattività dell'infrastruttura ridotti.

## Controllo del sistema operativo del Workload, per ridurre al minimo i rischi

Il controllo del sistema operativo del Workload offerto da RidgeShield è fondamentale per ridurre al minimo i rischi di sicurezza informatica di Windows e Linux. Eseguendo un controllo di sicurezza di base infatti, RidgeShield identifica le discrepanze di configurazione tra il sistema in esecuzione e le best practice consigliate dal fornitore. Tutte le impostazioni configurate in modo errato o non sicure verranno contrassegnate come avvisi, consentendo

così ai clienti di affrontare rapidamente qualsiasi potenziale vulnerabilità e rafforzare il proprio livello di sicurezza generale. Identificando e risolvendo in modo proattivo questi problemi di configurazione, RidgeShield aiuta a mitigare i potenziali rischi per la sicurezza e garantisce che i Workload funzionino in modo sicuro.

The image displays the RidgeShield dashboard interface. The top navigation bar includes the RidgeShield logo, a search icon, and menu items for Dashboard, Asset, Object, Policy, and Location. The main content area is titled "Query Criteria" and features several filters: Perspective (Application), Unmanaged (unchecked), Internet (checked), and Unknown (unchecked). Below these are tabs for Location, Environment, Application, and Role. A "Last Day" filter and a "Select Action" button are also visible. At the bottom, there are filters for "online" status and "Select direction" (Two way).

An inset window titled "Hostname centos7-1" shows a "Best Practice Check" report. The report includes a "GET DATA" button and a list of 49 items. The results are summarized as follows:

Item ID	Description	Status
[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 openssl security configuration.	FAIL
[47]	Other configuration-21: Check system coreutils 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

- **Maggiore sicurezza:** RidgeShield fornisce una soluzione di sicurezza completa che protegge i Workload contro le moderne minacce di sicurezza. Grazie alla micro-segmentazione basata su Label, alla Flow View orientata al business, e al controllo di sicurezza di base del sistema operativo, le organizzazioni avranno Workload sicuri.
- **Rischio ridotto:** RidgeShield riduce la superficie di attacco creando zone sicure intorno alle applicazioni e ai Workload. Questo approccio impedisce il movimento laterale all'interno della rete e riduce il rischio di violazioni dei dati e altri incidenti di sicurezza.
- **Operazioni di sicurezza semplificate:** RidgeShield utilizza l'automazione per semplificare le operazioni di sicurezza e ridurre il carico sui team IT. Grazie ai miglioramenti della policy automatici e a controlli di sicurezza istantanei, le organizzazioni possono ridurre il tempo e le risorse necessarie a mantenere la loro posizione di sicurezza.
- **Migliore conformità:** RidgeShield fornisce una soluzione di sicurezza completa che aiuta le organizzazioni a soddisfare i requisiti normativi e gli standard del settore. Con RidgeShield, le organizzazioni possono mantenere la conformità in tutti gli ambienti, evitando così multe e sanzioni costose.



### Leggi cosa dicono i clienti su Ridge Security

Il logo GARTNER PEER INSIGHTS è un marchio commerciale di servizio di Gartner, Inc. e/o dei suoi affiliati, utilizzato qui con il permesso del brand. Tutti i diritti sono riservati. Le recensioni di Gartner Peer Insights costituiscono le opinioni soggettive dei singoli utenti finali basate sulle proprie esperienze; non rappresentano le opinioni di Gartner o dei suoi affiliati.

Contatta Ridge Security per saperne di più:

[Sales@RidgeSecurity.ai](mailto:Sales@RidgeSecurity.ai)

[RidgeSecurity.ai/contact-us](https://www.RidgeSecurity.ai/contact-us)



Ridge Security Technology Inc.

[www.ridgesecurity.ai](https://www.ridgesecurity.ai)



[@RidgeSecurityAI](https://twitter.com/RidgeSecurityAI)



[www.linkedin.com/company/ridge-security](https://www.linkedin.com/company/ridge-security)