2020

Protezione comprovata e orchestrazione senza confini per il cloud ibrido

kaspersky

Maggiori informazioni su kaspersky.it
#truecybersecurity

Kaspersky Hybrid Cloud Security

La virtualizzazione è diventata un approccio fondamentale per ogni azienda che cerchi di essere flessibile ed efficiente. Il cloud computing è il successivo passo naturale. Consente di superare le complessità infrastrutturali e assicura livelli di efficienza precedentemente irraggiungibili. Ma il passaggio al cloud comporta complicazioni e difficoltà, alcuni delle quali nuove e altre derivanti dal mondo "fisico".

Kaspersky Hybrid Cloud Security offre sicurezza unificata per ogni fase o scenario del passaggio verso il cloud. Adatta sia per la migrazione verso il cloud sia per gli scenari di cloud nativo, protegge i workload fisici e virtualizzati in esecuzione on-premise, in un data center o in un cloud pubblico. Poiché le sue applicazioni sono state create tenendo presenti le specifiche del funzionamento della virtualizzazione e dei server, offre una protezione perfettamente bilanciata contro le minacce attuali e future più avanzate senza compromettere le prestazioni del sistema.

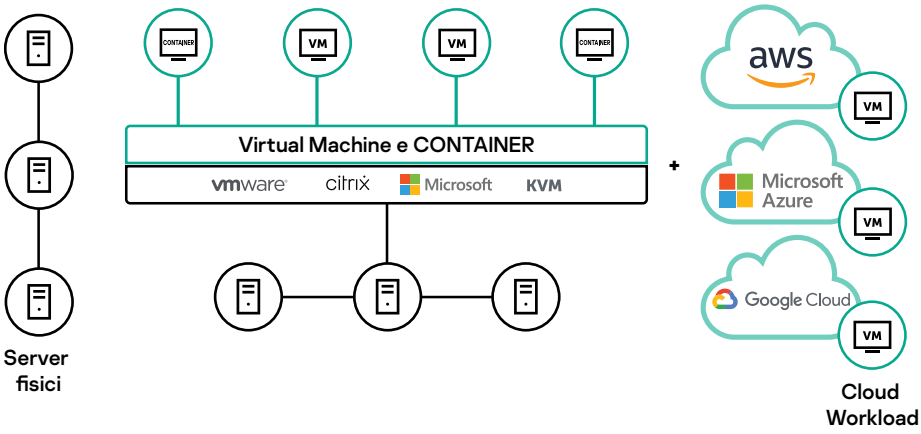
Principali sfide per gli utenti cloud:

- La crescente complessità dell'infrastruttura può causare difficoltà di gestione
- Un approccio multi-layer, fondamentale per una protezione affidabile, raramente si trova in un unico prodotto
- La sicurezza tradizionale consuma importanti risorse di sistema
- Un approccio "isolato" e controlli diversi possono comportare sfide aggiuntive per la sicurezza e la gestione
- I malware e i ransomware attaccano endpoint sia virtuali che fisici
- La mancata attuazione di adeguate misure di cybersecurity per la protezione dei dati personali può comportare problemi legali

Perché Kaspersky Hybrid Cloud Security?

- Progettata per carichi di workload cloud, virtuali e fisici
- Sicurezza multi-layer integrata per tutti i tipi di workload
- Sicurezza conforme, flessibile e automatizzata per cloud pubblici AWS Azure e Google
- Soddisfazione dei requisiti di responsabilità condivisa con un set completo di strumenti di sicurezza
- Orchestrazione della sicurezza continua in tutto il cloud ibrido
- La protezione più testata e più sicura, secondo numerosi premi e test indipendenti[1]

Key benefit



Consente una transizione al cloud sicura, senza compromettere i livelli di protezione

- Le nostre funzionalità pluripremiate per garantire il massimo livello di cybersecurity proteggono tutti i workload: fisici, virtuali o in cloud.
- La protezione multi-layer in tempo reale, supportata dal machine learning, protegge i dati, i processi e le applicazioni dalle minacce emergenti.
- Un approccio olistico alla sicurezza dei dati aiuta a ridurre i rischi legali e per la reputazione correlati alle normativa sulla protezione dei dati.

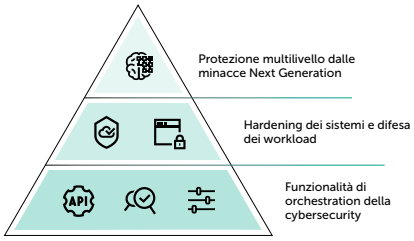
Consente di ottenere il massimo dalle risorse e dagli investimenti

- La sicurezza agentless e light agent protegge le risorse virtualizzate in reti fisiche e definite da software, senza alcun impatto sulle performance.
- L'integrazione con la sicurezza cloud gestita e con il cloud pubblico nativo consente di proteggere le applicazioni, i sistemi operativi, i flussi di dati e le aree di lavoro dell'utente con minimo impatto sulle risorse.
- La gestione centralizzata delle risorse fisiche e virtuali consente di risparmiare ore-uomo nel processo di adozione e manutenzione.

1 I test indicati coprono una vasta gamma di prodotti Kaspersky basati sulle stesse tecnologie di protezione dalle minacce utilizzate in Kaspersky Hybrid Cloud Security. Ulteriori informazioni all'indirizzo kaspersky.com/top3

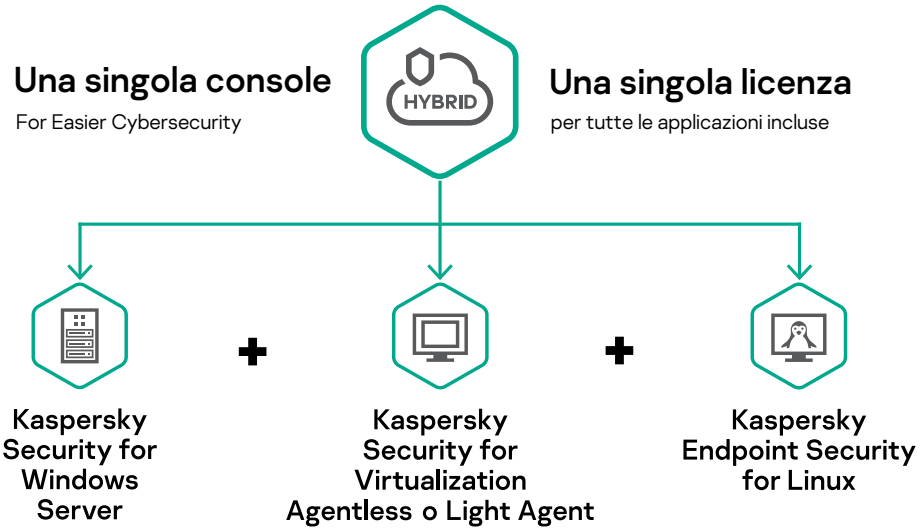
Caratteristiche principali

Caratteristiche principali	Descrizione
Protezione dalle minacce multilivello La protezione Next Generation anti-malware di Kaspersky incorpora diversi livelli di sicurezza proattiva in grado di bloccare la più ampia gamma di cyberattacchi che minaccia i workload business-critical.	
Threat intelligence globale	Fornisce dati in tempo reale sullo stato del panorama delle minacce, garantendo una protezione costante.
Machine learning	I grandi volumi di dati della threat intelligence globale vengono elaborati dalla potenza combinata degli algoritmi di machine learning e delle competenze umane, per livelli di rilevamento elevati e collaudati con falsi positivi minimi.
Protezione dalle minacce su Web e posta elettronica	Consente il funzionamento sicuro di desktop virtuali e sessioni remote, proteggendoli dalle minacce basate sulle e-mail e sul Web.
Log Inspection	Esegue la scansione degli eventi per rilevare eventuali tentativi di attacco.
Behavior Analysis	Monitora le applicazioni e i processi, proteggendo dalle minacce avanzate, incluse quelle "fileless" e gli script malevoli.
Remediation engine	Se necessario, esegue il rollback di qualsiasi modifica malevola apportata ai workload cloud.
Exploit prevention	Assicura protezione efficace contro gli attacchi, pur garantendo una perfetta compatibilità con le applicazioni protette, il tutto con un impatto minimo sulle prestazioni.
Funzionalità anti-ransomware	Protegge i workload virtualizzati da eventuali tentativi di crittografare i dati business-critical rendendoli inutilizzabili, eseguendo il rollback dei file al loro stato precrittografato e bloccando i tentativi di cifratura avviati da remoto.
Network Threat Protection	Rileva e blocca le intrusioni attraverso la rete nelle risorse cloud-based.
Protezione dei container	Assicura che il malware non venga trasferito nell'infrastruttura IT ibrida attraverso container Docker o Windows compromessi.
Maggiore resilienza grazie all'hardening dei sistemi	
Application Control	Consente di bloccare tutti i workload del cloud ibrido in modalità Default Deny per l'hardening del sistema e consente di limitare la gamma di applicazioni in esecuzione solo a quelle legittime e attendibili.
Device Control	Specifica quali dispositivi virtualizzati possono accedere ai singoli workload cloud.
Web Control	Regola l'uso delle risorse Web da desktop virtuali e tramite le sessioni remote per ridurre i rischi e incrementare la produttività.
Host-based Intrusion Prevention System (HIPS)	Assegna categorie di attendibilità alle applicazioni avviate, limitandone l'accesso alle risorse critiche e diminuendone le capacità.
File Integrity Monitoring	Consente di garantire l'integrità dei componenti critici del sistema e di altri file importanti.
Vulnerability Assessment e Patch Management	Centralizza e automatizza le funzionalità di sicurezza base, la configurazione dei sistemi e le attività di gestione, come la valutazione delle vulnerabilità, la distribuzione di patch e aggiornamenti, la gestione dell'inventario e il deployment delle applicazioni.
Visibilità senza confini	
Gestione unificata della sicurezza	Kaspersky Security Center consente la gestione della sicurezza centralizzata in tutta l'infrastruttura, dagli endpoint ai server, dai workload nel data center on-premise a quelli ospitati nel cloud.
API cloud	L'efficace integrazione con gli ambienti pubblici AWS e Azure consente il rilevamento dell'infrastruttura, la distribuzione automatizzata degli agenti di sicurezza e la gestione basata su criteri, oltre a inventario e provisioning di sicurezza più semplici.
Console di gestione flessibile	Offre funzionalità tenancy multiple, gestione degli account basata su autorizzazioni e controllo degli accessi role-based, fornendo flessibilità e mantenendo i vantaggi dell'orchestrazione unificata da un singolo server.
Integrazione SIEM	In infrastrutture con un IT più complesso, le informazioni sulla sicurezza e i sistemi di gestione possono essere utilizzati come una finestra unificata per i diversi aspetti della cybersecurity di un'azienda, attraverso l'intera rete IT ibrida.



Offre controllo e visibilità conformi, indipendentemente dalla configurazione dell'infrastruttura ibrida

- Le operazioni basate su policy e il provisioning dei servizi di sicurezza più semplici sono abilitati direttamente nel cloud ibrido.
- L'orchestrazione delle sicurezza e la gestibilità operano in modo efficiente attraverso più cloud.
- La piena visibilità, il controllo e la protezione olistica contro le minacce avanzate per ogni workload sia on-premise che su qualsiasi cloud.



Kaspersky Hybrid Cloud Security offre tecnologie di sicurezza pluripremiate e riconosciute dal settore per supportare e semplificare la trasformazione dell'ambiente IT. Protegge la migrazione da fisico a virtuale e al cloud, mentre la visibilità e la trasparenza garantiscono un'orchestrazione della sicurezza a 360 gradi.

Sicurezza unificata per qualsiasi cloud:

Cloud pubblici
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Private data centers
- VMware NSX
- Microsoft Hyper-V
- Citrix Hypervisor
- KVM
- Proxmox

Ambienti VDI
- Vmware Horizon
- Citrix Virtual Apps and Desktops

Server fisici
- Windows
- Linux

Desktop fisici:
- Windows
- Linux

aws

Microsoft Azure

vmware

citrix

Google Cloud

KVM

Novità sulle minacce informatiche: www.securelist.it
IT Security News: business.kaspersky.com
Cybersecurity per PMI: kaspersky.it/business
Cybersecurity per aziende Enterprise: kaspersky.it/enterprise

www.kaspersky.it

We are proven. We are independent. We are transparent. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia possa migliorare le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Soluzioni di Cybersecurity Kaspersky, per un futuro più sicuro.

Per saperne di più: kaspersky.it/transparency

Proven. Transparent. Independent.