Kaspersky® Hybrid Cloud Security

Protezione comprovata e orchestrazione senza confini per il cloud ibrido

Principali sfide degli utenti cloud:

- La crescente complessità dell'infrastruttura può significare una ridotta trasparenza
- Un approccio multi-layered, fondamentale per una protezione affidabile, raramente si trova in un unico prodotto
- La sicurezza tradizionale si integra con le risorse di sistemi di valore
- I malware e i ransomware attaccano endpoint sia virtuali sia fisici
- La mancata attuazione di adeguate misure di cybersecurity per la protezione dei dati personali può comportare problemi legali.

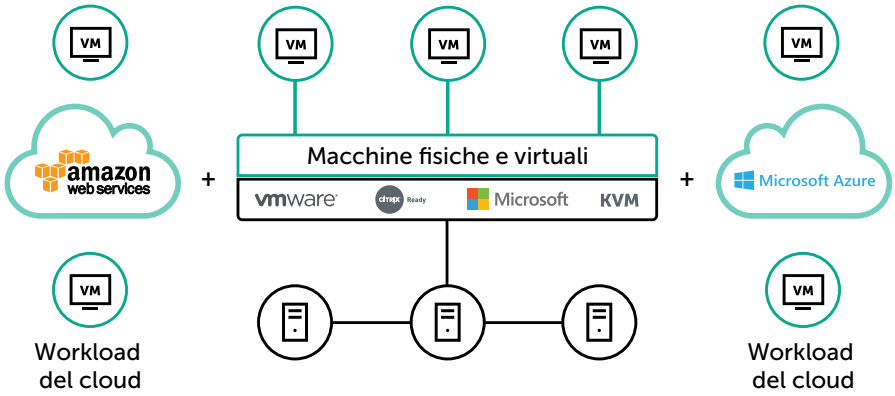
Perché Kaspersky Hybrid Cloud Security?

- Progettata per workload cloud, virtuali e fisici
- Sicurezza multi-layered integrata per tutti i tipi di carichi di lavoro
- Sicurezza impeccabile, agile e automatizzata per cloud pubblici Azure e AWS
- 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]
- Basata su tecnologie che hanno guadagnato la fiducia e il riconoscimento dei clienti incluso il premio Platinum Customer di Gartner Peer Insights.

1 I test indicati coprono una vasta gamma di prodotti Kaspersky Lab basati sulle stesse tecnologie di protezione dalle minacce utilizzate in 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. Offre sollievo dai vincoli di un complesso supporto infrastrutturale e assicura livelli di efficienza precedentemente irraggiungibili. Ma il viaggio verso il cloud comporta complicazioni e pericoli, alcuni dei quali nuovi e altri derivanti dal mondo fisico.

Kaspersky Hybrid Cloud Security offre sicurezza unificata adatta sia per la migrazione verso il cloud sia per gli scenari di cloud nativo. Protegge 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.



Vantaggi chiave

Consente un viaggio verso il cloud sicuro, senza compromettere i livelli di protezione

- Le tecnologie brevettate e il nostro pluripremiato motore di cybersecurity proteggono tutti i workload: fisici, virtuali o in cloud.
- La protezione multi-layered 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.

Approccio HuMachine™ di Kaspersky

Alimentata da una perfetta fusione tra threat intelligence basata su grandi volumi di dati, funzionalità di machine learning ed esperienza umana, HuMachine™ di Kaspersky offre numerosi vantaggi e una protezione più efficiente. Combinando questi elementi, i singoli componenti vengono migliorati per un risultato complessivo ancora più efficiente ed efficace.

Consente di ottenere il massimo dalle risorse e dagli investimenti

- La sicurezza agentless e light agent protegge le risorse virtualizzate in reti fisiche e software defined senza alcun impatto sulle prestazioni.
- L'integrazione con la sicurezza cloud gestita e del 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.

Offre controllo e visibilità trasparenti indipendentemente dalla configurazione dell'infrastruttura ibrida

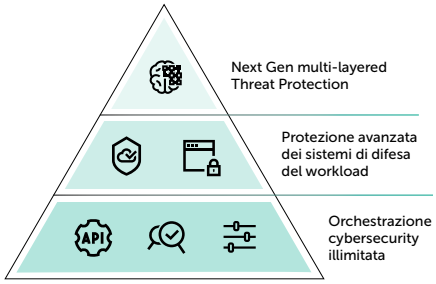
- L'orchestrazione delle sicurezza e la gestibilità operano in modo efficiente attraverso più cloud.
- La piena visibilità, il controllo e la protezione olistica contro le minacce avanzate per ogni workload in qualsiasi posizione.
- Le operazioni basate su policy e il provisioning dei servizi di sicurezza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

Funzionalità

Protezione multi-layered, supportata da HuMachine

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 la 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.
- **File Integrity Monitoring:** consente di garantire l'integrità dei componenti critici del sistema e di altri file importanti.
- **Log Inspection:** esegue la scansione degli eventi per rilevare eventuali tentativi di attacco.
- **Analisi dei comportamenti:** monitora le applicazioni e i processi, proteggendo dalle minacce avanzate, incluso il malware basato su script.
- **Motore di correzione:** esegue il rollback di qualsiasi modifica nociva apportata ai workload cloud, se necessario.
- **Prevenzione degli exploit:** 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 workload virtualizzati da eventuali tentativi di tenere i dati business-critical "in ostaggio", eseguendo il rollback dei file al loro stato precrittografato e bloccando la crittografia avviata da remoto.
- **Protezione contro le minacce di rete:** rileva e impedisce le intrusioni basate su rete nelle risorse in cloud.



Sicurezza unificata per qualsiasi cloud

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

Centri dati privati
- VMware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM
- Proxmox

Ambienti VDI
- Vmware Horizon
- Citrix XenDesktop

Server fisici
- Windows
- Linux

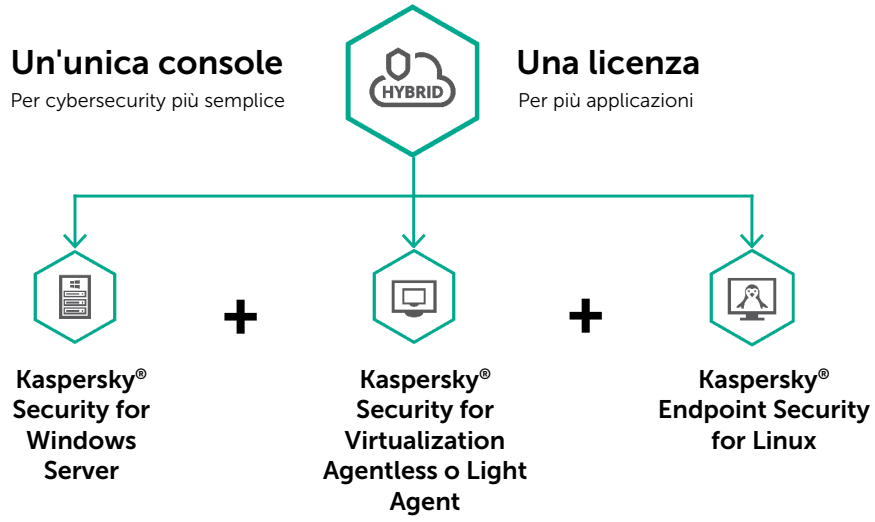
Maggiore resilienza grazie al rafforzamento del sistema

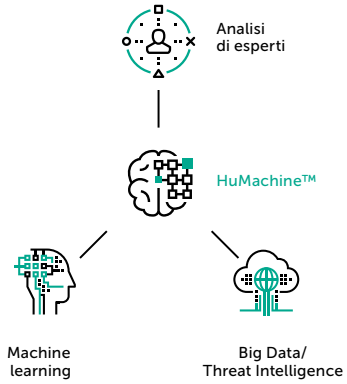
- **Application Control:** consente di bloccare tutti i workload del cloud ibrido in modalità Default Deny per l'hardening del sistema e consente di limitare la gamma di applicazioni in esecuzione solo a quelle legittime e attendibili.
- **Device Control:** specifica quali dispositivi virtualizzati possono 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.

Visibilità senza confini

- **Gestione della sicurezza unificata di Kaspersky Security Center:** consente la gestione della sicurezza centralizzata in tutta l'infrastruttura, gli endpoint e i server, in ufficio, nel data center e nel cloud.
- **API cloud:** la perfetta 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.
- **Opzioni di gestione flessibili:** offrono funzionalità multi-tenancy, gestione degli account permission-based e controllo degli accessi role-based, fornendo flessibilità e mantenendo i vantaggi dell'orchestrazione unificata da un singolo server.
- **Integrazione SIEM:** in infrastrutture con IT più maturo, 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.

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 impeccabile.





Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Novità sulle minacce informatiche: **www.securelist.com**
Novità sulla sicurezza IT: **business.kaspersky.com/it**
Il nostro approccio unico: **www.kaspersky.com/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.it