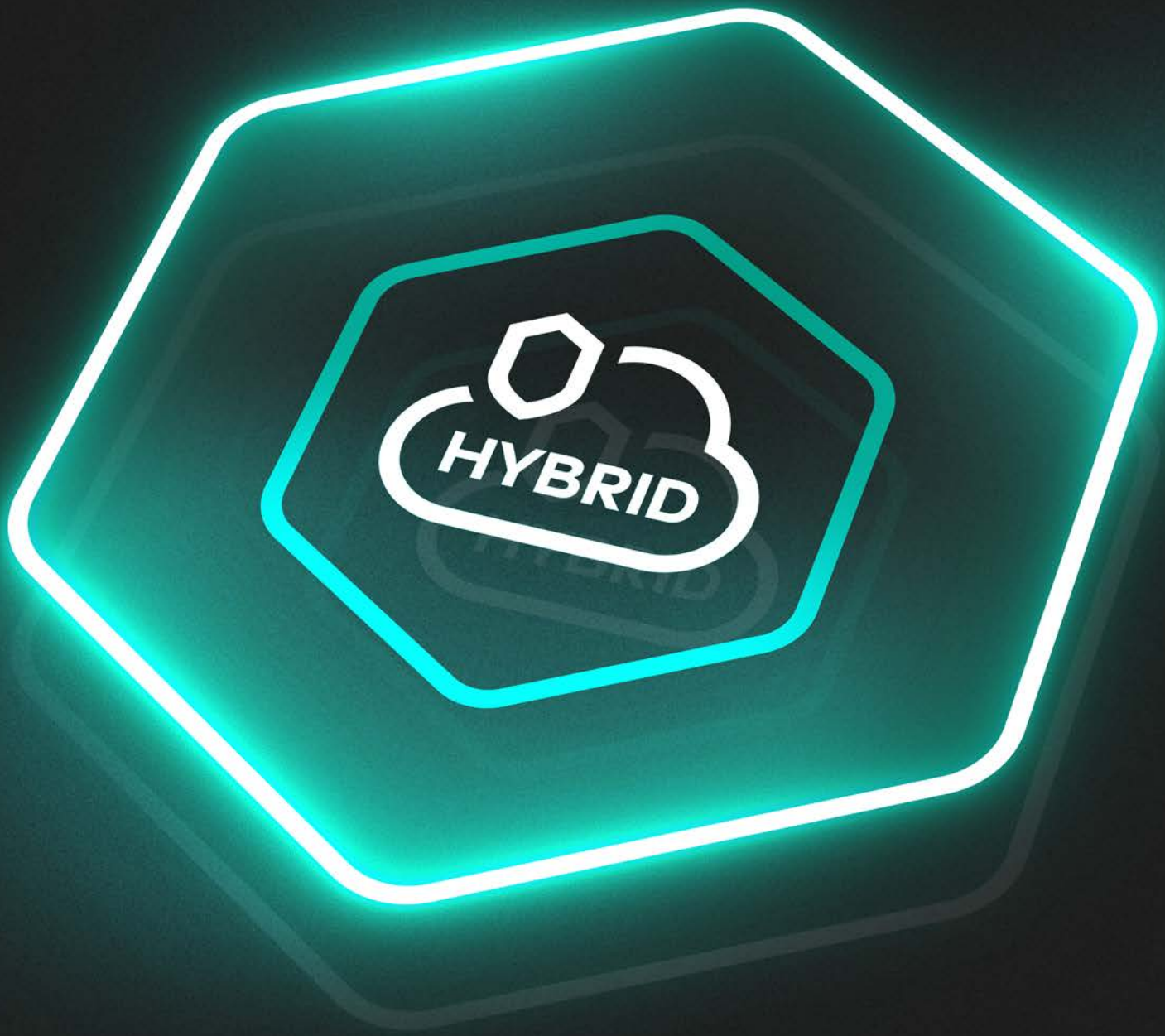


Kaspersky Hybrid Cloud Security

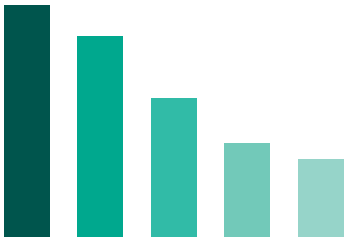
kaspersky BRING ON THE FUTURE

L'attuale focus delle aziende sulla trasformazione digitale sta spingendo la rapida adozione. Da una parte, tali iniziative offrono molti vantaggi alle aziende, tra cui un'efficienza ottimizzata. Dall'altra parte, le infrastrutture diventano più complesse, generando preoccupazioni in termini di rischi per la sicurezza, la governance, le risorse del personale, l'ottimizzazione delle prestazioni, le nuove normative e i costi. Kaspersky Hybrid Cloud Security risponde a tutte queste sfide.

Protezione cloud-native comprovata e prestazioni ottimali per i vostri ambienti ibridi

Kaspersky Hybrid Cloud Security rende globalmente più sicure ed efficienti l'adozione cloud, la trasformazione digitale e le attività aziendali. Questo singolo prodotto protegge l'intera infrastruttura ibrida, mitigando il rischio, riducendo il consumo di risorse di virtualizzazione e supportando la compliance alle normative. Kaspersky Hybrid Cloud Security garantisce una visibilità ottimizzata e una gestione semplificata, offrendo a voi e al vostro team un prezioso risparmio in termini di tempo e risorse di budget. Non dovrete più preoccuparvi della security e sarete liberi di concentrarvi su altri aspetti della trasformazione digitale.

Principali sfide associate al cloud



- Sicurezza **81%**
- Gestione della spesa cloud **79%**
- Governance e compliance **75%**
- Gestione multi-cloud **72%**
- Migrazione cloud **71%**

Secondo il rapporto Flexera State of the Cloud Report 2021

La migliore protezione progettata per gestire i rischi per la sicurezza degli ambienti ibridi

- La protezione multilivello contro le minacce contrasta in modo proattivo un'ampia gamma di attacchi informatici, tra cui malware, phishing e molto altro.
- Algoritmi di machine learning potenziati dall'esperienza umana per garantire i massimi livelli di detection con percentuali minime di falsi positivi.
- Dati di threat intelligence in tempo reale aiutano a difendersi dagli exploit più recenti.

Un approccio cloud-native per le migliori prestazioni di sicurezza delle infrastrutture ibride

- Il motore di cybersecurity protegge l'intera infrastruttura ibrida, indipendentemente dal workload, che può essere fisico o virtuale, basato su cloud ibridi, pubblici o privati.
- L'approccio indipendente dalla piattaforma, combinato all'integrazione nativa, rende i cloud pubblici capaci di supportare pienamente il DevOps.
- I light agent ottimizzati per ciascun sistema operativo consumano circa il 30% in meno di risorse di virtualizzazione rispetto alle tradizionali soluzioni di security, liberando l'hardware per impiegarlo in altre operazioni aziendali.

Sostenibilità e gestione immediata per un'esperienza cloud confortevole

- Un licensing flessibile vi consente di scegliere solo le funzionalità di cui avete bisogno, capitalizzando al meglio l'investimento nella sicurezza.
- Una console cloud unificata vi consente di semplificare la gestione della security dell'intera infrastruttura, risparmiando preziose risorse dello staff IT.
- L'inventario semplificato dell'infrastruttura cloud e il provisioning automatico della sicurezza indipendentemente dalla posizione degli agent contribuiscono alla massima visibilità.

Sicurezza orientata alla compliance per i settori soggetti a normative stringenti

- Adattivo e poliedrico, questo prodotto è progettato per abilitare e supportare in modo continuativo la piena compliance alle normative, attraverso tecnologie che vanno dalla protezione avanzata del sistema e dall'autodifesa degli agent alla valutazione delle vulnerabilità e al patch management automatizzato.
- L'ampia gamma di funzionalità è garanzia di compliance e adattamento al panorama dei rischi, per una security sempre al passo con le normative vigenti.

Funzionalità

Protezione dalle minacce multilivello

Global Threat Intelligence	Raccoglie i dati in tempo reale sullo stato del panorama delle minacce, anche quando questo subisce variazioni.
Machine learning	Sfrutta i Big Data della Threat Intelligence globale con algoritmi di machine learning associati all'esperienza umana.
Protezione dalle minacce e-mail e web	Protegge desktop virtuali e sessioni remote, difendendoli dalle minacce basate sulle e-mail e sul web.
Analisi log	Esegue la scansione dei file di log per la massima efficienza operativa.
Analisi del comportamento	Protegge dalle minacce avanzate, incluso il malware basato su script o bodiless, attraverso il monitoraggio di processi e applicazioni.
Motore di Remediation	Se necessario, esegue il rollback di qualsiasi modifica malevola apportata ai workload cloud.
Prevenzione dagli exploit	Garantisce una protezione efficace dalle minacce che penetrano nella rete, compatibilmente con le applicazioni protette e con un impatto minimo sulle prestazioni.
Funzionalità anti-ransomware	Protegge i dati aziendali importanti da qualsiasi tentativo di esfiltrazione con richiesta di riscatto, incluso il blocco della crittografia avviata da remoto e il rollback dei file allo stato che avevano prima della crittografia.
Protezione dalle minacce di rete	Rileva e blocca le intrusioni attraverso la rete nelle risorse cloud-based.
Protezione dei container	Impedisce alle infezioni di diffondersi nell'infrastruttura IT ibrida tramite container compromessi.

Maggiore resilienza grazie alla protezione avanzata del sistema

Controllo delle applicazioni	Il controllo delle applicazioni consente di bloccare tutti i workload nel cloud ibrido in modalità Default Deny per la protezione avanzata e ottimale del sistema, nonché di limitare la gamma di applicazioni in esecuzione solo a quelle legittime e attendibili.
Controllo dei dispositivi	Specifica quali dispositivi virtualizzati possono accedere ai singoli workload cloud.
Controllo web	Regola l'utilizzo delle risorse web dai desktop virtuali e tramite le sessioni remote, riducendo i rischi e incrementandone la produttività.
Host-based Intrusion Prevention System (HIPS)	Assegna categorie di attendibilità alle applicazioni avviate, limitandone l'accesso alle risorse critiche e diminuendone le funzionalità.
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 di 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 rollout delle applicazioni.

Visibilità senza confini

Gestione unificata della sicurezza	La protezione di server ed endpoint per l'intera infrastruttura può essere gestita tramite un'unica console in ufficio, nel data center o in cloud.
API cloud	La perfetta integrazione con gli ambienti pubblici consente la discovery dell'infrastruttura, la distribuzione automatizzata degli agent di sicurezza e la gestione basata su criteri, oltre a semplificare l'inventario e il provisioning di sicurezza.
Opzioni di gestione flessibili	Funzionalità multi-tenancy, gestione degli account basata su autorizzazioni e controllo degli accessi role-based offrono flessibilità consentendo al contempo di mantenere i vantaggi dell'orchestrazione unificata da un singolo server.
Integrazione SIEM	Consente l'integrazione dei prodotti con il sistema SIEM (Security Information and Management), unendo diversi aspetti della cybersecurity aziendale in tutta la rete IT ibrida.

Perché Kaspersky Hybrid Cloud Security?

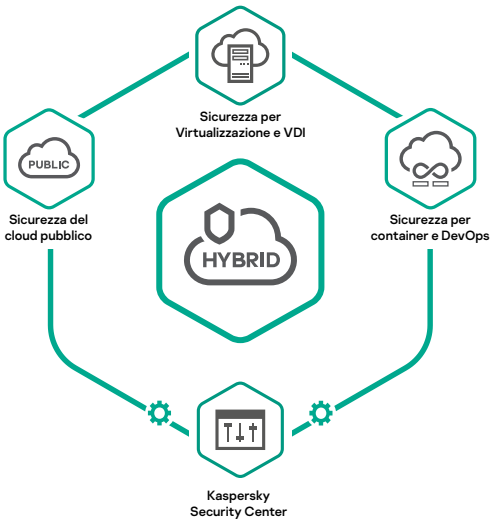
Il 30%

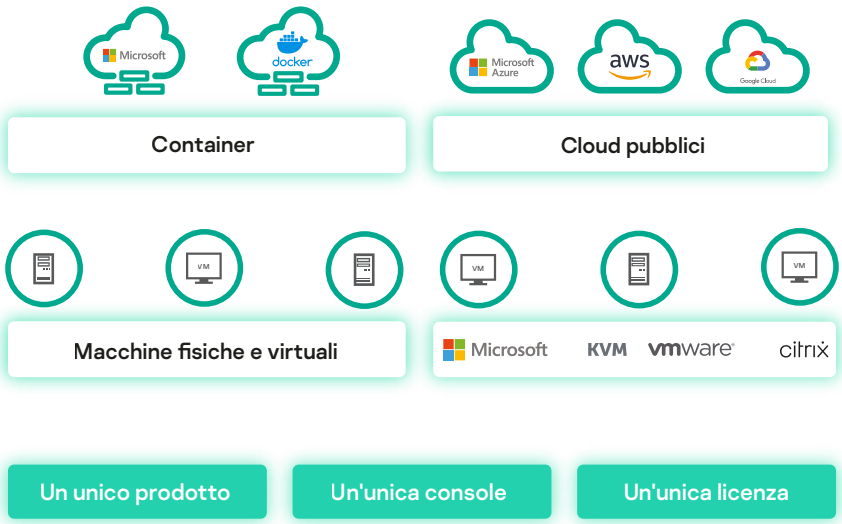
di potenziale risparmio sulle risorse hardware di virtualizzazione rispetto all'utilizzo di una soluzione tradizionale di sicurezza endpoint.

TOP3

Prestazioni sorprendenti e durature. Lo scorso anno i prodotti Kaspersky hanno nuovamente dimostrato prestazioni eccezionali in più test indipendenti, ottenendo 57 prime posizioni e classificandosi sul podio per ben 63 volte (scoprite di più all'indirizzo kaspersky.it/top3).

Un solo prodotto per tutte le esigenze di sicurezza cloud





Un unico prodotto | **Un'unica console** | **Un'unica licenza**

Recensioni dei clienti

"Questa soluzione aiuta a proteggere gli ambienti cloud e virtuali, senza compromettere le prestazioni del sistema o danneggiare la user experience."

"Un modo fantastico per unire tutte le soluzioni di sicurezza in un'unica licenza."

"Non serve installare un software antivirus aggiuntivo e altri agent."

"Soluzione cloud centralizzata per la protezione dei dati. Tutto in un'unica posizione."

"La protezione si applica all'istante a tutte le macchine virtuali, perché non è necessario scaricare nuovi aggiornamenti".

"La soluzione ottimale che non richiede una lunga formazione degli amministratori."

Opinioni tratte dalle recensioni Gartner e Amazon

Richiedete una demo

www.kaspersky.it