KASPERSKY lab

Sicurezza senza confini progettata per il cloud ibrido

Kaspersky Hybrid Cloud Security

www.kaspersky.it
#truecybersecurity

Sicurezza senza confini progettata per l'ambiente cloud ibrido

I dati sono diventati sempre più fluidi, viaggiando costantemente oltre il perimetro IT aziendale su dispositivi mobili oltre a essere elaborati su macchine virtuali e fisiche. Inoltre, con l'adozione di cloud pubblici e infrastrutture gestite, i dati fluiscono off-premise e on-premise come mai prima d'ora.

La crescente adozione di un modello di servizi cloud elastico, in cui le risorse dei data center privati si espandono istantaneamente su richiesta e secondo esigenze in cloud esterni, offre flessibilità, agilità e chiari vantaggi economici senza precedenti. Non esistono investimenti iniziali in infrastrutture, nessuno spreco e nessun ritardo nel soddisfare i requisiti di risorse immediati, mantenendo al tempo stesso la gestibilità.

I cloud pubblici offrono un altro grande vantaggio: la continuità aziendale. Se il data center subisce interruzioni o danni, le risorse off-premise possono continuare a lavorare finché il problema non viene risolto. Gli stessi fornitori di cloud pubblici hanno investito molto nella continuità aziendale e nella cybersecurity, creando ambienti sicuri e resilienti per i workload aziendali. Ma questa non è la fine...

Principali sfide per la sicurezza per gli utenti cloud

- Malware e ransomware che attaccano workload fisici, virtuali e basati su cloud
- Violazioni dei dati a seguito di un approccio alla sicurezza reattivo e non coordinato
- Diminuzione della trasparenza dovuta alla crescente complessità dell'infrastruttura
- Sfide amministrative a causa di controlli e strumenti disparati
- Risorse di sistema sprecate da soluzioni tradizionali pesanti
- Protezione insufficiente per i dati archiviati nei data center privati
- Attacchi DoS che interrompono la continuità operativa o impediscono lo scambio di dati

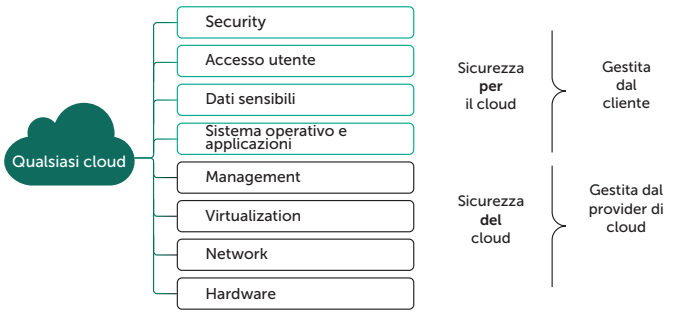
Quanto sono protetti i dati nei cloud pubblici?

La risposta a questa domanda non è così semplice come potrebbe sembrare.

I cloud pubblici, così come sono attualmente, sono luoghi molto sicuri. Si presta molta attenzione ad assicurare costantemente che i dati rimangano assolutamente contenuti nell'ambiente ospitato e che non vi siano pericoli di fughe, all'interno o all'esterno del cloud esterno.

Ma il fatto che i dati siano contenuti in modo sicuro non significa necessariamente che sia al sicuro. La fuga di dati è solo uno degli aspetti della sicurezza. I dati esposti a ransomware potrebbero, ad esempio, rimanere contenuti in modo completo e sicuro, ma potrebbero anche essere danneggiati e quindi essere assolutamente inutili. E tutti i dati che interagiscono con le persone, che in definitiva rappresentano la funzione principale come risorsa organizzativa, sono esposti agli effetti dell'errore umano e potenzialmente dei criminali umani.

Modello di responsabilità della sicurezza condivisa

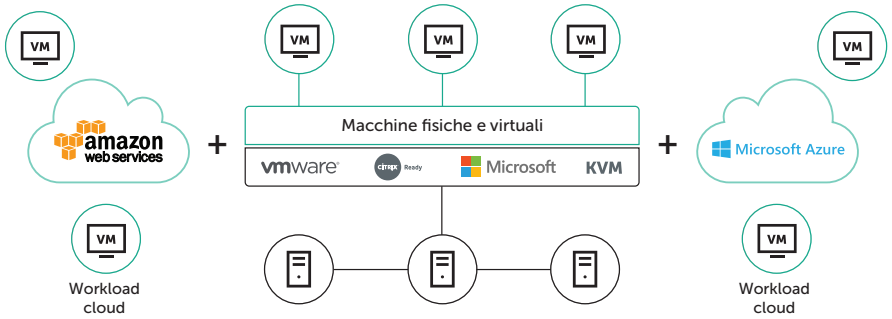


I fornitori di servizi cloud ospitati sono responsabili della sicurezza dell'ambiente che forniscono, ma la responsabilità per la sicurezza interna di ciascun workload, ovunque si trovi, rimane dell'azienda. Questo è il cosiddetto modello di "Responsabilità Condivisa della Sicurezza", in cui l'azienda e il fornitore di servizi sono equamente responsabili per i diversi ambiti di sicurezza del rapporto di lavoro e delle risorse di dati.

Quindi la risposta alla domanda su quanto sono protetti i dati nei cloud pubblici, nella migliore delle ipotesi, è che sono più al sicuro che altrove. Le stesse considerazioni sulla sicurezza si applicano ai dati ovunque si spostino. Non è possibile proteggere i dati semplicemente proteggendo il luogo in cui si trovano in qualsiasi momento. Riconoscere questa evidenza sta diventando sempre più importante in quanto sempre più dati business-critical si spostano oltre l'ambiente controllato del perimetro IT aziendale.

Protezione dei dati, non solo dell'ambiente circostante

Ogni pacchetto di dati deve essere protetto dall'interno, ovunque si trovi, in qualsiasi momento e mentre è in transito. Questa è la responsabilità aziendale, che non può essere esternalizzata o delegata.



Per proteggere il flusso di lavoro, è necessario essere in grado di orchestrarlo

Quindi, prima domanda, l'azienda sa esattamente dove ogni singolo pacchetto di dati si trova o dove si sta spostando, in qualsiasi momento e chi sta interagendo con esso?

Il monitoraggio e il controllo degli accessi rappresentano un costante problema di sicurezza. Più grande e complessa è l'infrastruttura IT, maggiori sono le soluzioni necessarie per ottimizzare l'efficienza e le prestazioni dei sistemi e più difficile è tenere traccia di ogni workload e ogni applicazione. L'espansione delle infrastrutture del data center per incorporare risorse esterne aggiunge un'ulteriore dimensione a questo problema. È fondamentale assicurarsi poter individuare con precisione cosa viene letto ed elaborato, on-premise e off-premise.

Per proteggere i workload, è necessario essere in grado di rafforzarli

Cosa succede? Quali applicazioni sono in esecuzione in una determinata posizione e si comportano come dovrebbero? Le vulnerabilità nelle applicazioni rimangono il principale mezzo di penetrazione e infezione utilizzato dai cybercriminali. L'hardering dei sistemi si ottiene fornendo livelli di tecnologia per impedire che ciò accada. Dalla messa al bando o dalla limitazione di alcune applicazioni al monitoraggio del comportamento costante di ogni applicazione in esecuzione nella propria organizzazione e alla schermatura di vulnerabilità dallo sfruttamento: tutti questi controlli e interventi critici di prevenzione e rilevamento delle minacce sono di responsabilità dell'azienda.

Per proteggere l'organizzazione, è necessario essere in grado di proteggere i dati

Per proteggere i dati runtime, è necessario essere in grado di riconoscere quando sono sotto attacco potenziale o effettivo e il tipo di minaccia.
Da APT (Advanced Persistent Threat) che prendono di mira in modo specifico l'azienda al ransomware, dal furto di dati e dalle frodi finanziarie a errori umani casuali, le minacce ai dati arrivano in varie forme e dimensioni. E poiché il cybercrimine è un settore altamente lucrativo e sofisticato, i nuovi metodi di attacco vengono sviluppati e applicati costantemente.

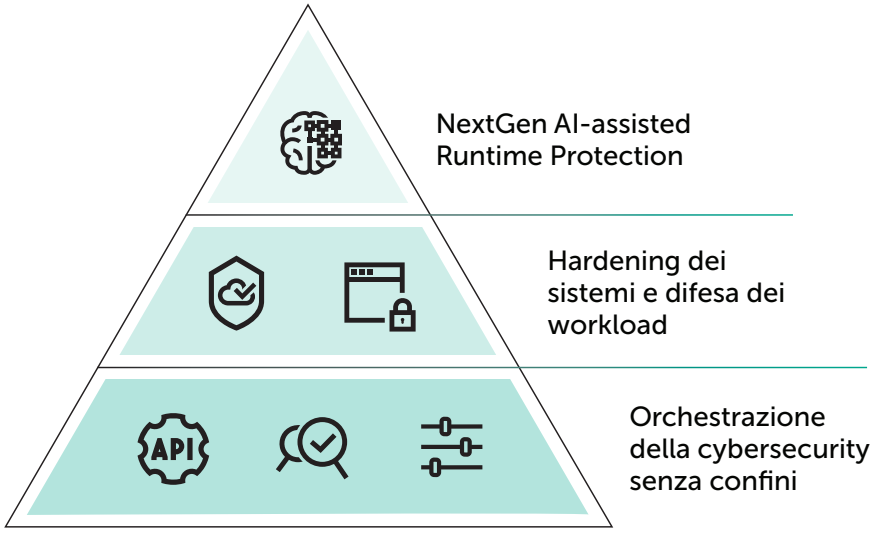
Ciò che è vero per i dati nei cloud rimane vero per tutti i dati: la qualità della threat intelligence su cui si basa il sistema di sicurezza, la tempestività e l'accuratezza della sua applicazione determineranno l'efficacia della protezione. Il sistema di sicurezza IT deve essere in grado di individuare, bloccare e correggere una potenziale minaccia prima che raggiunga i dati e abbia impatto sulle operazioni. E deve farlo senza compromettere le prestazioni del sistema e, soprattutto, senza generare "falsi positivi", causando interruzioni e spreco di risorse con falsi allarmi.

Ancora una volta, tutto questo è una responsabilità dell'azienda. Il fornitore di servizi cloud può proteggere i dati solo fino a un certo punto: il resto spetta all'azienda.

Cosa cercare quando si protegge il data center cloud ibrido

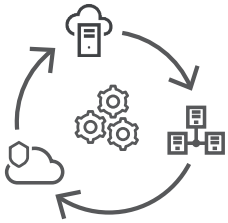
In sintesi, è possibile guardare a fornitori di software di hosting di dati esterni per offrire un ambiente sicuro e completamente contenuto in cui far funzionare i workload. Tuttavia, è responsabilità dell'azienda monitorare, controllare e proteggere tutti i dati, ovunque si trovino.

In Kaspersky Lab chiamiamo questi tre aspetti della responsabilità della sicurezza orchestrazione della cybersecurity, hardening dei sistemi e protezione runtime. Implementiamo ciascuno di questi livelli di sicurezza tramite una serie di tecnologie complementari e interdipendenti, come mostrato di seguito.



Quando si implementa una soluzione per proteggere il proprio ambiente cloud ibrido, è consigliato includere un requisito, in particolare:

Orchestrazione senza confini



API cloud: l'integrazione con cloud pubblici (come Amazon AWS e Microsoft Azure) tramite API native. Ciò consente il rilevamento dell'infrastruttura, la distribuzione di agenti di sicurezza automatizzati e la gestione basata su criteri.

Gestione account: il blocco delle macchine in cloud garantisce che gli operatori e gli amministratori della sicurezza dispongano delle autorizzazioni corrette per accedere a specifiche aree della console di cybersecurity.

Controllo dell'accesso in base al ruolo: i team di sicurezza e l'infrastruttura possono avere diversi livelli di accesso e controllo sulla cybersecurity dell'ambiente cloud ibrido, in base ai ruoli operativi che vengono assegnati.

Hardening dei sistemi

Controllo delle applicazioni e whitelisting: la messa al bando o il controllo di quali possono essere eseguite, dove e quando, riduce la superficie di attacco. (Kaspersky Lab rimane l'unico a gestire il proprio Whitelisting Lab, specificando quali applicazioni possono essere eseguite in sicurezza dai nostri clienti in qualsiasi momento, consentendo l'implementazione di un criterio di Default Deny altamente sicuro, se necessario)

Scudo delle vulnerabilità: le tecniche come la prevenzione degli exploit, la valutazione delle vulnerabilità e la gestione automatizzata delle patch (ovviamente incluse in Kaspersky Hybrid Cloud Security), che impediscono ai criminali di penetrare nei sistemi attraverso vulnerabilità nelle popolari applicazioni su cui fanno affidamento gli utenti.

Protezione runtime

Anti-ransomware: la prevenzione della penetrazione dei ransomware, inclusi anti-malware di posta elettronica e Web. Kaspersky Hybrid Cloud Security include anche il "rollback automatico", in modo che tutti i file danneggiati vengano automaticamente ripristinati al precedente stato non crittografato.

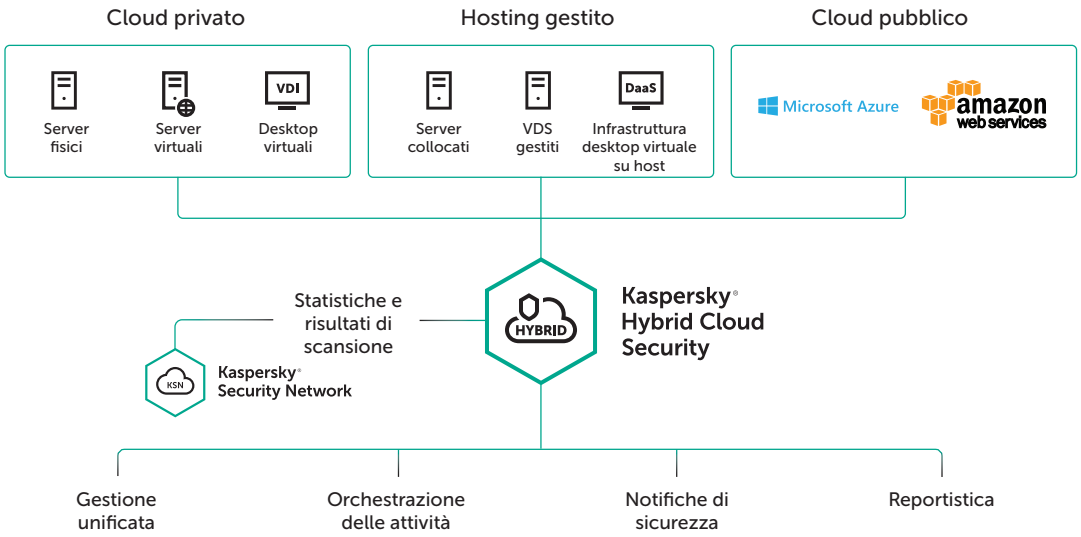
Threat intelligence avanzata: l'accesso e la capacità di applicare la threat intelligence in tempo reale ai sistemi e ai meccanismi di protezione dei dati.

Quest'ultima funzione è la più critica. Parliamo di intelligenza artificiale: la capacità di un sistema di individuare software o anomalie comportamentali e quindi riconoscere e identificare le minacce mai rilevate prima.

Questa capacità di identificare e difendere da minacce sconosciute è assolutamente fondamentale per la sicurezza dei dati. Senza questo livello di quella che chiamiamo "intelligence HuMachine®", i dati saranno vulnerabili agli attacchi futuri, indipendentemente dal numero di altre tecnologie di sicurezza applicate. Le soluzioni Kaspersky Lab si basano su questa combinazione di machine intelligence (stiamo implementando il machine learning nelle nostre tecnologie da oltre un decennio) e competenze impareggiabili, che ci consente di individuare, identificare e bloccare le minacce di attuali e future.

Sicurezza cloud efficace ed elegante

La soluzione Hybrid Cloud Security di Kaspersky Lab offre tutto quanto è stato sopra illustrato, e molto altro ancora, fornendo un panorama di sicurezza adattivo per proteggere l'intero cloud ibrido dalle minacce più sofisticate.



Cloud sicuri ed elastici

Gli ambienti ibridi sono altamente dinamici, per questo la sicurezza deve adattarsi rapidamente al panorama operativo in continuo cambiamento mentre si evolve e si adatta.

- Accelera la visibilità attraverso gli ambienti cloud per una protezione superiore in tutti i punti.
- Rileva e risponde alle cyberminacce avanzate sfruttando la potenza combinata di persone e macchine.
- Protegge qualsiasi workload cloud, sistema, network o dati con controlli multipli.

Un unico prodotto, qualsiasi cloud

Una soluzione progettata per offrire la Next Generation cybersecurity per ambienti cloud ibridi di livello aziendale.

- Sicurezza comprovata per server fisici e virtuali, VDI, archiviazione e persino canali di dati nel cloud privato.
- Controlli di sicurezza avanzati per workload in cloud pubblici, inclusi AWS e Azure.
- Soddisfazione degli SLO (service-level objective) aziendali attuali riducendo al minimo il rischio informatico.

Una perfetta esperienza di sicurezza

La trasparenza e l'integrazione trasversale dei livelli IT e di sicurezza impongono uno stato di sicurezza contro minacce note, sconosciute ed emergenti.

- Integrazione tra tecnologie core del cloud e i relativi livelli di sicurezza tramite API native
- Provisioning della sicurezza automatizzato, per la migrazione del cloud sicura e senza compromessi
- Perfetta esperienza di orchestrazione della sicurezza a livello aziendale per qualsiasi cloud

Grazie alle funzionalità all'avanguardia implementate nella nostra soluzione Hybrid Cloud Security, i livelli di infrastruttura e sicurezza si integrano e interagiscono, combinando punti di forza per creare un ambiente sicuro ed efficiente, consentendo la migrazione senza confini dei workload tra cloud pubblici e privati. Il risultato è una sicurezza continua, elastica, trasparente e gestibile, in modo che sia possibile scegliere l'ibrido in base alle esigenze aziendali.

In breve...

I servizi di hosting basati su cloud gestiti esternamente assicurano notevoli vantaggi aziendali e offrono ambienti protetti in cui i dati aziendali possono essere archiviati ed elaborati in modo sicuro. Ma la responsabilità per la sicurezza dei pacchetti di lavoro rimane dell'azienda. Garantendo in ogni momento la piena visibilità e il controllo dei dati, dei processi e delle applicazioni e applicando la threat intelligence avanzata basata sull'intelligence HuMachine® per la protezione dei dati, è possibile garantire la sicurezza di tutti gli aspetti del data center ibrido.

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