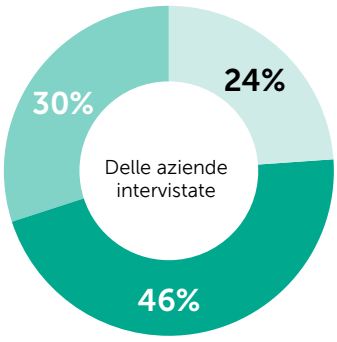
Kaspersky® Hybrid Cloud Security

Salvaguardia del cloud Amazon Web Services

Ora, i cloud privati e pubblici fanno parte del panorama IT aziendale. La novità è una crescente consapevolezza del fatto che i cloud pubblici come Amazon Web Services (AWS) o Microsoft Azure sono maturati al punto tale da essere pronti a gestire anche workload business-critical.

Queste funzionalità avranno un impatto sulla vision della security delle organizzazioni aziendali e sulla costruzione delle loro strategie IT. In che modo l'infrastruttura IT dell'azienda si amplierà e si evolverà nei prossimi tre/cinque anni? Come si possono sfruttare al meglio le funzionalità dei cloud pubblici e gestiti, garantendo al tempo stesso che l'infrastruttura ibrida risultante rimanga affidabile e, soprattutto, al sicuro?

Gli incidenti di cybersecurity continuano a essere una grande preoccupazione, con un numero crescente di organizzazioni di grandi dimensioni che subiscono le conseguenze finanziarie, alla reputazione e talvolta legali. La sicurezza del cloud aziendale deve essere sufficientemente agile e intelligente da combattere le minacce attuali e future e deve avere la scalabilità e la flessibilità necessarie per adattarsi ed evolversi insieme al proprio ambiente cloud ibrido, includendo entrambe le funzionalità cloud, sia pubblica sia privata.



- Utilizza il cloud, ma deve ancora eseguire una verifica o un controllo della conformità
- Utilizza il cloud, ma non dispone di un piano di mitigazione delle minacce definito
- È passato a tecnologie cloud con un piano di mitigazione delle minacce completamente testato

Fonte: rapporto Maintaining Control and Data Security in the Cloud, Kaspersky Lab, 2017

Cloud privati e pubblici: l'ambiente ibrido

La protezione del cloud privato è un'attività relativamente semplice. L'uso della virtualizzazione per creare un data center abilitato per il software è una pratica relativamente consolidata e Kaspersky Lab ha risposto con un software specializzato che offre il minimo ingombro sulla macchina virtuale (o, nel caso di VMware, nessun impatto) per ottimizzare l'efficienza e proteggere il risparmio di risorse e la flessibilità offerte dalla tecnologia di virtualizzazione.

Ma passare dal cloud privato al cloud pubblico, e in particolare trovarsi a cavallo tra i due, ha introdotto nuovi problemi. Dove inizia e termina la responsabilità della sicurezza dell'azienda e come organizza e protegge i carichi di lavoro mentre passano da on-premise a off-premise?

Minacce alla sicurezza e loro mitigazione

Esistono molteplici rischi per gli ambienti cloud elastici indipendentemente dalle dimensioni, dalle piattaforme di virtualizzazione utilizzate nel data center privato software defined o nella piattaforma cloud scelta per eseguire applicazioni business-critical. I fornitori di servizi cloud, come Amazon, si impegnano molto per assicurarsi che i cloud pubblici restino un porto sicuro per gli utenti di qualsiasi dimensione. AWS offre una gamma di strumenti di sicurezza nativi per il cloud altamente efficaci per la creazione di ambienti a livello aziendale senza confini. Tuttavia, il rischio rimarrà sempre.

In Kaspersky Lab, vediamo una serie di gravi minacce (e non solo in termini di cybersecurity) che potrebbero influire negativamente sulle strategie di adozione del cloud e rallentare il percorso di trasformazione digitale.

Violazioni o fuga di dati

La raccomandazione di Kaspersky Lab per la prevenzione delle violazioni dei dati consiste nel mantenere difese informatiche affidabili per ogni singolo workload nel proprio ambiente cloud ibrido. La visibilità e la trasparenza dei livelli sia IT sia di security sono essenziali anche qui, poiché garantiscono la visibilità su ogni workload da proteggere e forniscono funzionalità di cybersecurity automatizzate in ogni angolo dell'ambiente cloud elastico in rapida evoluzione.

La visibilità dell'infrastruttura è un problema negli odierni ambienti digitali elastici e anche la stessa cybersecurity potrebbe diventare meno trasparente, quindi non è sempre possibile individuare esattamente dove il punto in cui si è a rischio e neanche il momento. E senza saperlo, potrebbe essere troppo tardi. Questo approccio frammentato alla sicurezza rende i cloud ibridi aziendali un punto debole a favore dei cybercriminali, in particolare perché di solito gli stessi strumenti possono essere utilizzati per penetrare nelle infrastrutture tradizionali e cloud. Una grave violazione dei dati può rivelare informazioni riservate relative a clienti o partner commerciali, proprietà intellettuali e segreti commerciali, la cui divulgazione può portare a gravi conseguenze.

Perdita o assenza di integrità dei dati

Il modo più efficiente per mantenere l'integrità dei dati è implementare strumenti di cybersecurity che forniscono potenti funzionalità di protezione runtime con analisi del comportamento potenziato dal machine learning. Ciò consente l'identificazione delle minacce più avanzate o dei ransomware sofisticati.

Anche se le violazioni dei dati rimangono in genere il risultato di attività dannose, esistono diversi scenari in cui i dati potrebbero diventare inaccessibili o danneggiati anche a causa di azioni non intenzionali dei propri utenti finali, nonché di attività dannose. La maggior parte delle organizzazioni prevede strategie di recupero dati per garantire il minimo RTO (Recovery Time Objective) e il più breve RPO (Recovery Point Objective). Tuttavia, il backup o la replica dei tuoi dati non significa necessariamente che potrebbero essere presenti spiacevoli sorprese al successivo ripristino. Statistiche , in rapida crescita, di attacchi ransomware molto dannosi contro organizzazioni di tutti i tipi dimostrano che il mantenimento dell'integrità dei dati è una missione piuttosto difficile. Indipendentemente dall'età dei dati o dalla posizione in cui si trovano, workload fisico, virtuale o cloud, la perdita o l'integrità dei dati è a proprio rischio.

Applicazioni vulnerabili o indesiderate

Kaspersky Lab sa esattamente come affrontare questi pericoli. Le strategie di difesa informatica di maggior successo si basano su una combinazione application startup control (whitelisting, Default Deny) e funzionalità di exploit prevention.

Le aziende installano e lavorano con un'ampia gamma di sistemi e applicazioni per molte ragioni e non è sempre possibile controllare ciò che viene installato sui dispositivi degli utenti finali o persino su server business-critical. Più ampio è l'ambiente aziendale, più difficile è tenere tutto sotto controllo. Anche le applicazioni business-critical con cui si ha completa familiarità potrebbero non essere resistenti alle vulnerabilità e agli exploit zero-day, ma richiedono una remediation immediata contro potenziali rischi informatici.

Sicurezza a elevato consumo di risorse

È importante comprendere che è propria responsabilità avere un'immagine molto chiara di tutti gli aspetti del cloud ibrido e delle sue parti costitutive e implementare le funzionalità di cybersecurity che offriranno la combinazione più efficiente di protezione ed efficienza delle risorse.

La maggior parte dei cloud ibridi funziona come una combinazione di data center privati software defined e servizi elastici di cloud pubblico. Entrambi richiedono protezione, combinando tecnologie che offrono diverse funzionalità di integrazione. L'adozione di un approccio "antivirus tradizionale ovunque" per la sicurezza del cloud ibrido comporta un utilizzo estremamente inefficiente delle risorse cloud, che compromette l'efficacia dei sistemi business-critical e riduce notevolmente il ROI nella trasformazione digitale.

Sicurezza ed errato allineamento dell'infrastruttura

Kaspersky Hybrid Cloud Security offre integrazione nativa tramite API che consente di stabilire una connessione affidabile tra i livelli IT e di security a del patrimonio cloud, in modo che possano lavorare a stretto contatto, rafforzando le rispettive funzionalità. Ciò include l'abilitazione del rilevamento dell'infrastruttura automatizzato e il provisioning della sicurezza, indipendentemente dalla dimensione dell'ambiente cloud ibrido.

L'adozione del cloud ibrido promuove un nuovo dinamismo nonché il provisioning costante della cybersecurity in centinaia di workload cloud appena implementati contemporaneamente, cosa che può finire con il diventare un incubo costante della sicurezza IT. Come professionista della sicurezza, la visibilità delle macchine cloud è limitata o ritardata, quindi quelle macchine rimarranno vulnerabili fino alla prossima scansione della rete aziendale. Tuttavia, gli strumenti automatizzati utilizzati dal personale IT generalista per eseguire attività amministrative come segmentazione della rete, isolamento e riconfigurazione della topologia possono essere molto utili per rispondere rapidamente alle cyberminacce emergenti e per aiutare a svolgere pratiche di dovuta diligenza appropriate. Se i livelli IT e di sicurezza non interagiscono, i team di security non saranno mai in grado di salvaguardare ciò che non possono vedere e i generalisti IT non saranno in grado di aiutarli ad abilitare un ecosistema realmente sicuro e adattivo in tutto il cloud ibrido.

Perché Kaspersky Hybrid Cloud Security?

1. Progettata per workload cloud, virtuali e fisici
2. Sicurezza integrata multi-layered per data center privati
3. Sicurezza impeccabile, agile e automatizzata per cloud pubblici Azure e AWS
4. Soddisfazione dei requisiti di responsabilità condivisa con un set completo di strumenti di sicurezza
5. Orchestrazione della sicurezza di livello aziendale in tutto il cloud ibrido

Responsabilità condivisa nei cloud pubblici

I cloud pubblici dispongono della propria sicurezza integrata. Tuttavia, il modello di responsabilità condivisa stabilisce che la sicurezza dei workload, delle applicazioni e dei dati nei cloud pubblici rimanga di responsabilità dell'azienda. E quando questi carichi di lavoro sono business-critical, questa responsabilità diventa ancora più importante.

AWS è leader nella fornitura del cloud pubblico, offre l'ambiente più avanzato sul mercato, include una straordinaria affidabilità e scalabilità e fornisce una gamma di strumenti di sicurezza nativi per il cloud di ambienti di livello aziendale senza confini.

Tuttavia, la responsabilità condivisa della sicurezza impone la necessità di funzionalità aggiuntive, consentendo un livello di cybersecurity elastico che copra l'intero ambiente cloud, pubblico e privato, proteggendo completamente i dati presenti nel patrimonio AWS.

Sicurezza integrata per il cloud AWS

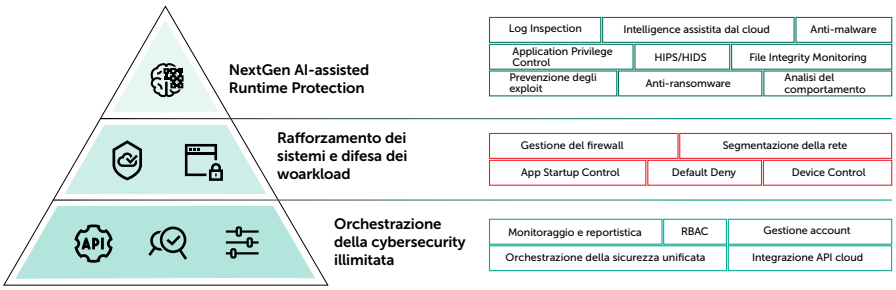
Protezione, visibilità e gestibilità leader del settore

La stretta integrazione delle nostre funzionalità di cybersecurity avanzate con quelle di AWS attraverso la loro API offre ulteriori vantaggi:

- **Efficienza dei sistemi**
  L'inventario dell'infrastruttura cloud diventa molto più semplice, così come il provisioning della sicurezza automatizzato delle istanze di AWS EC2 indipendentemente dalla loro posizione. Tali efficienze dei sistemi possono generare risparmi significativi in termini di tempo e risorse.
- **Piena visibilità**
  La visibilità può diventare uno dei problemi principali negli ambienti cloud ibridi e anche in questo caso una stretta integrazione porta grandi vantaggi in termini di profitti. L'integrazione tramite l'API AWS consente di vedere in ogni angolo, comprendere come è organizzato il cloud e avere la certezza di proteggere tutti i carichi di lavoro cloud.
- **Orchestrazione continua**
  L'integrazione API AWS consente la gestione unificata di tutte le risorse IT, in loco e sul cloud, attraverso un'unica console, offrendo piena trasparenza e permettendo un funzionamento continuo ed efficiente di orchestrazione e gestione.
- **Sicurezza "per il" e "dal" cloud**
  La nostra protezione leader del settore per le istanze di AWS EC2 è disponibile anche in AWS MarketPlace, contribuendo a rendere la migrazione verso il cloud fluida, semplice e sicura. Cosa c'è di meglio della migliore protezione per il cloud, disponibile dal cloud?
- **Licenze flessibili**
  Molteplici opzioni di licenza e di prezzo, tra cui BYOL (Bring Your Own License) e PPU (Pay Per Use) consentono di ottimizzare l'investimento nell'IT e nella trasformazione digitale e mantengono un elevato ROI nel progetto di cloudizzazione.

La filosofia di Kaspersky Lab è stata quella di creare una miscela perfettamente equilibrata di protezione di primo livello, cybersecurity a basso consumo di risorse e funzionalità di orchestrazione a livello aziendale per l'ambiente AWS. Grazie in parte all'integrazione tramite API AWS, possiamo farlo meglio di chiunque altro.

In collaborazione con AWS, iniziamo sfoderando le nostre funzionalità di "Next Generation" cybersecurity all'avanguardia, basate sul motore di protezione attualmente più testato, più premiato[1] e più apprezzato[2] del settore. La Next Generation cybersecurity consentirà agli individui e alle macchine di lavorare insieme per costruire un ambiente di sicurezza cloud adattivo ed elastico. Questo è ciò che offriamo, permettendo all'azienda di rilevare e rispondere alle cyberminacce più avanzate.



- **Pluripremiato motore anti-malware**, che garantisce protezione a livello di file automatica in tempo reale per tutti i carichi di lavoro, all'accesso e on-demand.
- **Intelligence basata su cloud**, che identifica rapidamente nuove minacce e fornisce aggiornamenti automatici.
- **Rilevamento del comportamento**, che monitora applicazioni e processi, protegge dalle minacce avanzate e anche dal malware ed esegue il rollback di eventuali modifiche nocive apportate all'interno dei workload cloud, se necessario.
- **Prevenzione degli exploit**, che controlla i processi operativi e il comportamento delle applicazioni e blocca le minacce avanzate, incluso il ransomware.
- **Anti-ransomware**, che protegge i workload cloud e le loro reti condivise dagli attacchi ed esegue il rollback di tutti i file interessati al loro stato precrittografato.
- **HIPS/HIDS**, che rileva e impedisce le intrusioni basate su rete nelle risorse basate su cloud.
- **Application Control**, che consentono di bloccare tutti i workload del cloud ibrido in modalità Default Deny per un rafforzamento del sistema ottimale e consente di limitare la gamma di applicazioni in esecuzione solo a quelle legittime e attendibili.

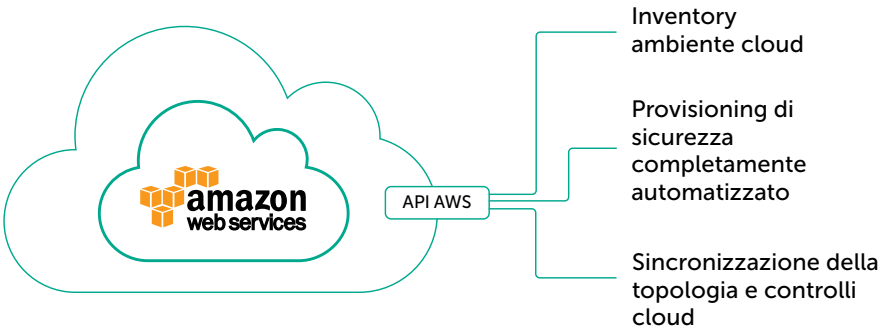
1 https://www.kaspersky.com/it/top3
2 Premi Gartner Peer Insights Customer Choice per le piattaforme di protezione degli endpoint

- **Device Control**, che specifica quali dispositivi virtualizzati possono accedere ai singoli workload cloud, mentre il controllo Web protegge contro cyberminacce basate su Internet.
- **Segmentazione della rete**, che fornisce visibilità e protezione automatizzata della rete dell'infrastruttura del cloud ibrido.
- **Schermatura di vulnerabilità**, che impedisce a malware avanzato e minacce zero-day di sfruttare vulnerabilità non corrette da patch.
- **Sicurezza della posta elettronica** incluso l'anti-spam, che protegge il traffico e-mail nei workload cloud.
- **Sicurezza del Web**, incluso l'anti-phishing, che protegge dalle minacce da script e siti Web potenzialmente pericolosi.
- **Monitoraggio dell'integrità dei file**, che protegge file di sistema e critici, mentre l'ispezione dei log esegue la scansione dei file log interni.

Tutte queste funzionalità, che coprono l'ambiente del server fisico e le risorse basate su cloud virtuali e AWS, sono fornite in un unico prodotto Kaspersky Lab, orchestrato attraverso un'unica console di sicurezza unificata.

Funzionalità di sicurezza complete

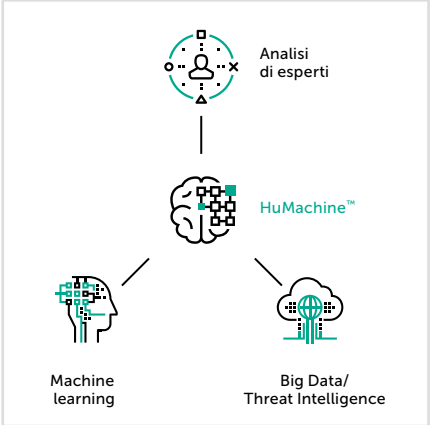
Implementando queste funzionalità e applicando questa qualità e questo ambito di sicurezza multi-layered nell'intera infrastruttura cloud pubblica e privata, viene garantita la certezza che tutti i dati, tutti i processi e tutte le applicazioni siano protetti da una sicurezza completa in tutti i punti.



Futuro assicurato dell'IT aziendale

Amazon Web Services sta cambiando il volto dell'IT aziendale. In Kaspersky Lab, contribuiamo a garantire la sicurezza, la visibilità e la gestibilità di ogni workload, sia nel patrimonio cloud AWS sia nell'ambiente cloud privato, ora e in futuro.

Kaspersky Hybrid Cloud Security offre tecnologie di sicurezza riconosciute dal settore per supportare e semplificare la trasformazione dell'ambiente IT, assicurando la migrazione da fisico a virtuale e al cloud, mentre visibilità e trasparenza garantiscono un'esperienza di 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