Kaspersky® Hybrid Cloud Security

Salvaguardia del patrimonio cloud Microsoft Azure

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 Microsoft Azure sono maturati al punto tale da essere pronti a gestire anche workload business-critical.

Queste funzionalità avranno un impatto sulla visione della sicurezza 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 privati, 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, causando ad un numero crescente di organizzazioni di grandi dimensioni conseguenze finanziarie, reputazionali 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.

51%

delle imprese ammette che la complessità dell'infrastruttura IT influisce direttamente sulla loro capacità di mantenere un adeguato livello di cybersecurity

Fino a

80%

delle perdite di dati in cloud ibridi è causato da soluzioni di sicurezza informatica obsoleta o reattiva

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 software-enabled è una pratica relativamente consolidata e Kaspersky Lab ha risposto con un software progettato per offrire 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 al cloud pubblico, e in particolare trovarsi a cavallo tra cloud privati e pubblici, ha introdotto nuovi problemi. Dove inizia e termina la responsabilità della sicurezza dell'azienda e come organizza e protegge i workload mentre passano da on-premise a off-premise?

Informarsi prima della migrazione

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 Microsoft Azure, si impegnano molto per assicurarsi che i cloud pubblici restino un porto sicuro per gli utenti di qualsiasi dimensione. Azure offre una gamma di strumenti di sicurezza nativi per il altamente efficaci per la creazione di ambienti a livello aziendale senza confini. Tuttavia, il rischio rimarrà sempre.

Kaspersky Lab riscontra 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 nostra raccomandazione 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 possibilità di vedere 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 il punto in cui si è a rischio e 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 forniscano potenti funzionalità di protezione del tempo di esecuzione 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 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 e dalla posizione in cui si trova il workload, fisico, virtuale o cloud, la perdita o l'integrità dei dati è a proprio rischio.

Applicazioni vulnerabili o indesiderate

Le strategie di difesa informatica di maggior successo si basano su una combinazione application startup control (whitelisting, Default Deny) e funzionalità di prevenzione degli exploit.

Gli utenti finali aziendali 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 totalmente resistenti alle vulnerabilità e agli exploit zero-day, ma richiedono una riparazione immediata contro potenziali rischi informatici.

Sicurezza a elevato consumo di risorse

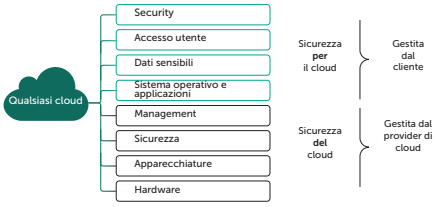
È importante comprendere che rientra nella propria responsabilità avere un'immagine molto chiara di tutti gli aspetti del cloud ibrido e delle sue parti costitutive e implementare le funzionalità di cybersecurity che offriranno la combinazione più efficiente di protezione ed efficienza delle risorse.

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 è 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

La collaborazione con le API e le estensioni del cloud pubblico consente di stabilire una connessione affidabile tra i livelli IT e di security, in modo che entrambi i livelli possano lavorare a stretto contatto, rafforzando le rispettive funzionalità e semplificando il provisioning della sicurezza, indipendentemente dalle dimensioni dell'ambiente cloud ibrido.

L'adozione del cloud ibrido promuove un nuovo dinamismo e un inventario efficace, 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 che i colleghi IT implementano 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 appropriate. Se i livelli IT e di security non interagiscono, i team di sicurezza 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.



Estensioni di cybersecurity per difendere il cloud Azure

L'approccio di Kaspersky Lab consiste nel lavorare con le estensioni di Microsoft Azure, non solo nell'applicare la protezione Next Generation AI-assisted per workload cloud, ma anche nel consentire il monitoraggio e il provisioning della sicurezza semplici e impeccabili. Questa facilità e semplicità di gestione significa che i workload in esecuzione nel patrimonio Azure possono essere sottoposti a protezione in pochi secondi, salvaguardando completamente le risorse basate su cloud e gli utenti.

Iniziamo sfoderando le nostre funzionalità di "prossima generazione" all'avanguardia, basate sul motore di protezione più testato, più premiato[1] e più apprezzato[2] del settore oggigiorno. 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 e alla sua sicurezza integrata basata sul cloud di rilevare e rispondere alle più avanzate cyberminacce.

Responsabilità condivisa nei cloud pubblici

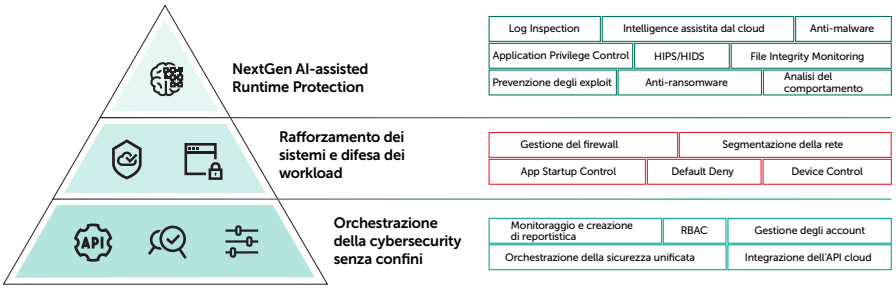
I cloud pubblici dispongono della propria sicurezza integrata. Tuttavia, il modello di responsabilità condivisa stabilisce che la sicurezza dei workload, delle applicazioni e dei dati nei cloud pubblici rimanga di responsabilità dell'azienda. E quando questi sono business-critical, questa responsabilità diventa ancora più importante. Microsoft Azure è un servizio cloud pubblico leader del settore, che offre un ambiente altamente avanzato in cui sono incorporate affidabilità e scalabilità eccezionali.

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 nei workload basati su Azure. È necessario essere pienamente consapevoli dei rischi e dei modi in cui rimediare a tali rischi in tutto l'ecosistema del cloud.

Reale protezione Next Generation

Integriamo gli strumenti nativi su cloud di Azure con protezione del tempo di esecuzione e sistemi assistiti dalla AI proattivi, tra cui:

- **Pluripremiato motore anti-malware**, che garantisce protezione a livello di file automatica in tempo reale per tutti i workload, all'accesso e on-demand.
- **Intelligence assistita da 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, 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.
- **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 di log interni.



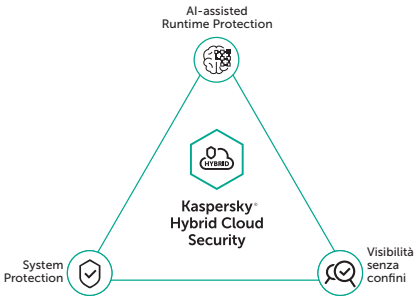
Tutte queste funzionalità, che coprono l'ambiente del server fisico e le risorse basate su cloud virtuali e Azure, sono fornite in un unico prodotto Kaspersky Lab, orchestrato attraverso un'unica console di sicurezza unificata.

1 https://www.kaspersky.com/it/top3

2 Premi Gartner Peer Insights Customer Choice per le piattaforme di protezione degli endpoint

Perché Kaspersky Hybrid Cloud Security?

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



Protezione, visibilità e orchestrazione integrate

Sicurezza completa

Implementando questa qualità e questo ambito di sicurezza multi-layered nell'intera infrastruttura cloud pubblica e privata, viene garantita la certezza che ogni workload, indipendentemente dalla posizione, operi in un ecosistema di cloud ibrido completamente sicuro in tutti i punti.

Provisioning basato su cloud

Grazie alle estensioni di Azure, è possibile eseguire il provisioning di tutte queste funzionalità di cybersecurity direttamente nei workload cloud, mantenendo le applicazioni aziendali sempre sicure e protette.

Conformità

Il nostro approccio alla sicurezza integrata consente di avere la certezza che la sicurezza di tutti gli elementi inseriti nel cloud Azure sia conforme agli standard aziendali e che le risorse e gli utenti siano sempre tutelati.

Orchestrazione unificata

La cybersecurity diventa una parte naturale dell'ecosistema cloud grazie all'integrazione nel Centro sicurezza di Azure.

Semplifica il provisioning della sicurezza

È possibile distribuire protezione multi-layered in tempo reale per workload del cloud Azure direttamente da Azure MarketPlace.

Licenze flessibili

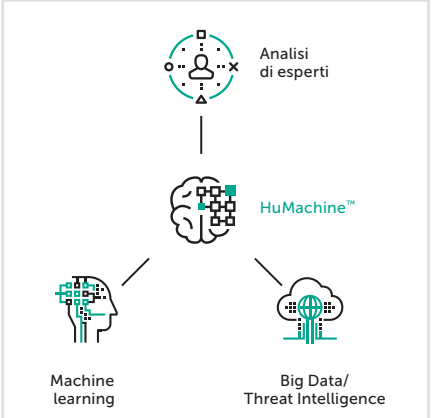
Molteplici opzioni di licenza e di prezzo, tra cui BYOL (Bring Your Own License) e PPU (Pay Per Use) consentono di ottimizzare l'investimento nell'IT e nella trasformazione digitale e mantengono un elevato ROI.

Una sicurezza del cloud che funziona

Il risultato complessivo è un ecosistema di cybersecurity perfettamente orchestrato e adattativo che offre esattamente le funzionalità richieste dai workload cloud ibridi e per cui l'efficienza delle risorse e l'orchestrazione continua rimangono fondamentali.

Futuro assicurato dell'IT aziendale

Microsoft Azure 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 Azure sia nell'ambiente cloud privato, ora e in futuro.



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