Una guida per la protezione delle piattaforme cloud

Indice

Punti salienti

1. Idealmente, un cloud provider dovrebbe essere in grado di integrare il sistema di gestione delle identità di un' azienda nella propria piattaforma – e, in ogni caso, fornire una soluzione affidabile per la gestione delle identità, da utilizzare in caso di necessità.

2. Come parte del consolidamento della fiducia, verificare che una piattaforma cloud offra firewall correttamente integrati, gruppi di sicurezza e opzioni per la micro-segmentazione basate sul carico di lavoro e host di calcolo attendibili.

3. I cloud provider devono poter prevedibilmente offrire soluzioni BYOK che consentano all' organizzazione di gestire in modo esclusivo chiavi in tutti i servizi e lo storage di dati.

4. La best practice di sicurezza per i container consiste nella scansione dei contenitori medesimi, per individuare vulnerabilità, sia prima dell' implementazione che in fase di esecuzione.

5. La sicurezza della piattaforma cloud deve garantire un controllo efficace degli accessi, operare a livello dei carichi di lavoro, tenere una traccia dettagliata dell' attività e integrarsi nei sistemi on-premise.

Riprogettare la sicurezza per le applicazioni cloud-based

Dal momento che un numero sempre maggiore di organizzazioni passa ad un modello cloud-native per lo sviluppo di app e la gestione dei carichi di lavoro, le piattaforme di cloud computing stanno rapidamente limitando l' efficacia del modello di sicurezza tradizionale, basato sul perimetro. Sebbene sia ancora necessaria, la sicurezza del perimetro è, di per se stessa, insufficiente. Poiché i dati e le applicazioni nel cloud risiedono all' esterno dei vecchi confini dell' azienda, devono essere protetti in modi nuovi.

La transizione delle organizzazioni a un modello cloud-native o la pianificazione di implementazioni di app per cloud ibrido deve fare da supplemento alla sicurezza tradizionale della rete basata sul perimetro, con tecnologie che proteggono i carichi di lavoro basati su cloud. Le aziende devono avere fiducia nel modo in cui il cloud provider di servizi protegge il loro stack, a partire dall' infrastruttura. Consolidare l' affidabilità della sicurezza della piattaforma è diventato un aspetto fondamentale nella scelta di un provider.

Fattori chiave della sicurezza cloud

La protezione dei dati e la conformità alla normativa sono tra i principali fattori chiave della sicurezza cloud – e sono anche fattori che ostacolano l' adozione del cloud. Per fare fronte a queste preoccupazioni, si devono prendere in considerazione tutti gli aspetti dello sviluppo e delle operazioni. Con applicazioni cloud-native, i dati possono essere diffusi in archivi oggetti, servizi dati e cloud, che creano più fronti per attacchi potenziali. E gli autori degli attacchi non sono soltanto bande di criminali informatici molto esperti e fonti esterne; secondo un recente sondaggio, il 53 percento degli intervistati ha confermato di aver subito attacchi dall' interno nei 12 mesi precedenti.[1]

Cinque principi fondamentali della sicurezza cloud

Quando le organizzazioni affrontano le esigenze specifiche di sicurezza generate dall' utilizzo di piattaforme cloud, hanno bisogno e si aspettano che i loro provider diventino partner di tecnologia affidabili. Infatti, un' organizzazione dovrebbe valutare i cloud provider sulla base di questi cinque aspetti della sicurezza, per come sono correlati ai requisiti specifici propri di un' organizzazione:

1. **IAM (Identity and access management-Gestione di identità e accessi):** Autenticazione, controlli di identità e accessi
2. **Sicurezza della rete** Protezione, isolamento e segmentazione
3. **Protezione dei dati** Crittografia dei dati e gestione delle chiavi
4. **Sicurezza delle applicazioni e DevSecOps:** Include test della sicurezza e sicurezza dei container
5. **Visibilità e intelligence:** Monitoraggio e analisi di log, flussi ed eventi per individuare schemi

Verificare l’ identità e gestire l’ accesso su una piattaforma cloud

Qualsiasi interazione con una piattaforma cloud inizia dalla verifica dell’ identità, che stabilisce chi o cosa sta effettuando l’ interazione – un amministratore, un utente o addirittura un servizio. Nell’ economia delle API, i servizi assumono la propria identità, così la capacità di effettuare in modo accurato e sicuro una chiamata API a un servizio, in base a questa identità, è essenziale per un’ esecuzione corretta di app cloud-native.

Cercare provider che offrano una modalità coerente per autenticare un’ identità per l’ accesso di API e le chiamate di servizio. È anche necessaria una modalità per identificare e autenticare utenti finali che accedono ad applicazioni in hosting nel cloud. A titolo di esempio, IBM Cloud utilizza ID dell’ app come modo per gli sviluppatori di integrare l’ autenticazione nelle loro app web e mobile.

Un’ autenticazione avanzata evita che utenti non autorizzati accedano a sistemi cloud. Dal momento che l’ IAM (identity and access management) della piattaforma è così fondamentale, le organizzazioni con un sistema esistente dovrebbero aspettarsi che i cloud provider integrino il sistema di gestione dell’ identità della loro azienda. Questo approccio spesso è supportato dalla tecnologia di federazione dell’ identità, che collega l’ ID e gli attributi di un individuo attraverso molteplici sistemi.

Perché autenticare le chiamate di servizio?

Nelle architetture basate sui microservizi, le API consentono alle applicazioni di comunicare e condividere dati. Durante l’ esecuzione di un’ applicazione, questa utilizza API per effettuare chiamate ai servizi, come necessario per portare a termine varie operazioni. Ad esempio, l’ applicazione potrebbe effettuare una chiamata ad un object storage service per ottenere dati. Come parte dell’ evasione della richiesta, l’ object storage service stesso potrebbe quindi effettuare una chiamata a un servizio di gestione chiavi per ottenere le chiavi di crittografia necessarie per decodificare i dati. E, come parte dell’ erogazione della propria user experience, un’ app potrebbe utilizzare API per accedere a informazioni sull’ identità utente, pubblicare contenuto tra app (ad esempio, pubblicare contenuto da un’ app a Twitter) e determinare l’ ubicazione di un utente per fornire informazioni specifiche in base all’ ubicazione. **Tutti questi punti di integrazione pongono delle sfide per la sicurezza.**

I cloud provider dovrebbero adottare una modalità coerente per autenticare l’ identità di un utente o di un servizio che deve accedere a un’ API o a un servizio. Naturalmente, come parte dell’ autenticazione, tutte le sessioni e transazioni di richiesta di accesso dovrebbero essere registrate ai fini di una verifica. **API e servizi è estremamente probabile che detengano una proprietà intellettuale di valore; non si può consentire a chiunque di farne uso.**

Chiedere ai potenziali cloud provider di dimostrare che l' architettura e i sistemi IAM che mettono a disposizione coprano tutte le basi. In IBM Cloud, ad esempio, la gestione di identità e accessi si basa su varie funzioni chiave (Figura 1):

Identità

- Ad ogni utente è assegnato un identificativo univoco
- Servizi e applicazioni vengono identificati mediante i relativi ID
- Risorse vengono identificate e indicate tramite CRN (cloud resource name)
- Gli utenti e i servizi vengono autenticati e si emettono token con le loro identità

Gestione accessi

- Mentre utenti e servizi tentano di accedere a risorse, un sistema IAM determina se sono consentiti o negati accesso e azioni
- I servizi definiscono azioni, risorse e ruoli
- Gli amministratori definiscono policies, che assegnano ruoli utente e autorizzazioni
- su varie risorse
- La protezione si estende ad API, funzioni cloud e risorse di backend in hosting sul cloud

Quando si valuta la sicurezza di un cloud provider, ricercare gli ACL (access control list) insieme ai nomi comuni di risorsa, che consentono di limitare gli utenti non solo a determinate risorse, ma anche a determinate operazioni su quelle risorse. Queste funzionalità aiutano a garantire che i propri dati siano protetti da accesso non autorizzato, sia interno che esterno.

Estendere il proprio Enterprise Identity Provider (Enterprise IdP) al cloud è particolarmente utile quando si crea un' app cloud-native usando come base un' applicazione aziendale esistente, che si avvale dell' Enterprise IdP. Gli utenti possono accedere senza difficoltà all' applicazione cloud-native e a quella sottostante, senza dover utilizzare più sistemi o ID. Ridurre la complessità è sempre un obiettivo che vale la pena di raggiungere.

Punto saliente

Idealmente, un cloud provider dovrebbe essere in grado di integrare il sistema di gestione delle identità di un' azienda nella propria piattaforma – e, in ogni caso, fornire una soluzione affidabile per la gestione delle identità, da utilizzare in caso di necessità.

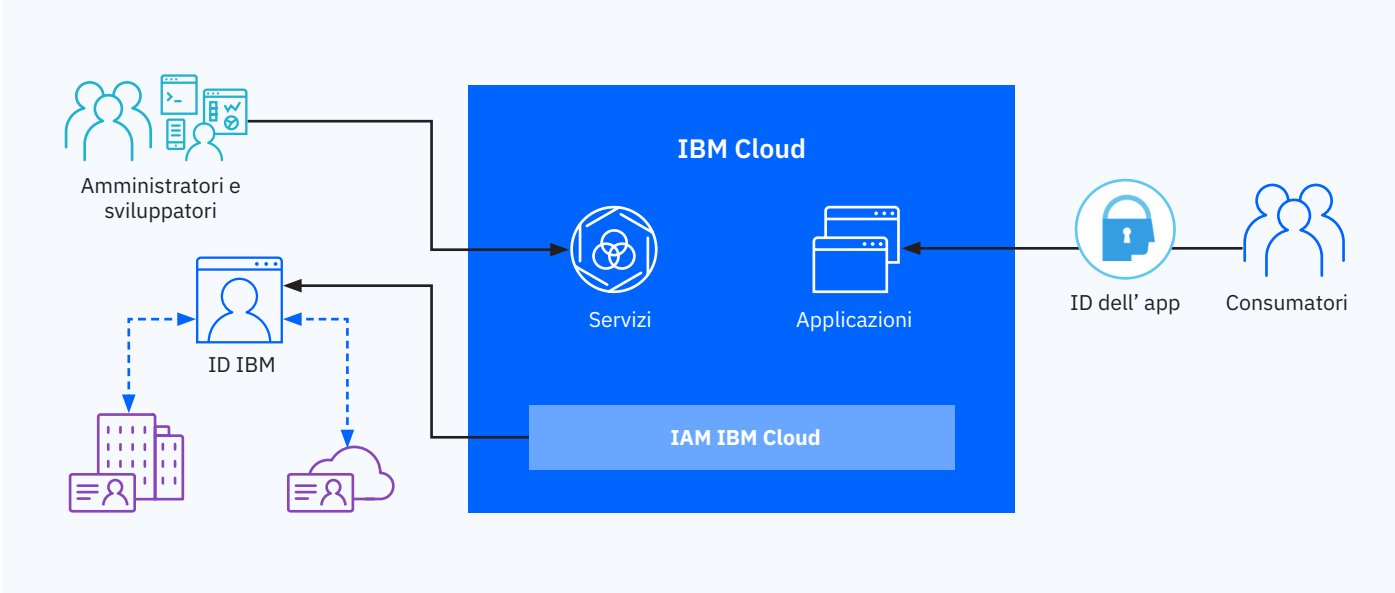


Figura 1. Separazione di elementi del cluster gestiti dal provider e gestiti dal cliente.

Ridefinire l’ isolamento e la protezione della rete

Molti cloud provider utilizzano la segmentazione della rete per limitare l’ accesso a dispositivi e server nella stessa rete. Inoltre, i provider creano reti virtuali isolate usando come base l’ infrastruttura fisica e limitano automaticamente utenti o servizi a una specifica rete isolata. Queste e altre tecnologie di sicurezza della rete di base sono la posta in gioco per consolidare la fiducia in una piattaforma cloud.

I cloud provider offrono tecnologie di protezione – da firewall per applicazioni Web a VPN (virtual private network) e attenuazione del denial-of-service – come servizi per la sicurezza SDN (software-defined network) e applicano una tariffa per l’ utilizzo. Considerare le seguenti tecnologie come una sicurezza di rete cruciale nell’ era del cloud computing.

Gruppi di sicurezza e firewall

I clienti cloud spesso inseriscono firewall di rete per la protezione del perimetro (accesso alla rete a livello di sottorete/cloud privato virtuale) e creano gruppi di sicurezza di rete per l’ accesso a livello di istanza. I gruppi di sicurezza rappresentano una valida prima linea di difesa per assegnare l’ accesso a risorse cloud. Si possono utilizzare questi gruppi per aggiungere facilmente sicurezza di rete a livello di istanza, per gestire il traffico in entrata e in uscita su reti pubbliche e private.

Molti clienti richiedono controllo del perimetro per proteggere la rete e le sottoreti del perimetro e firewall virtuali si possono implementare facilmente per soddisfare questa esigenza. I firewall sono progettati per evitare che traffico indesiderato colpisca i server e ridurre la superficie di attacco. I cloud provider devono prevedibilmente offrire firewall sia virtuali che hardware, per consentire di configurare regole basate su autorizzazione per l’ intera rete o le sottoreti.

Le VPN, naturalmente, forniscono connessioni sicure dal cloud nuovamente alle risorse on-premise. Sono indispensabili, se si sta gestendo un ambiente cloud ibrido.

Micro-segmentazione

Lo sviluppo di applicazioni in modalità cloud-native, come serie di servizi di piccole dimensioni, fornisce il vantaggio in termini di sicurezza di essere in grado di isolarli, utilizzando segmenti di rete. Ricercare una piattaforma cloud che implementi la micro-segmentazione attraverso l’ automazione della configurazione e del provisioning della rete. **Applicazioni in contenitori, progettate sul modello dei microservizi, stanno rapidamente diventando la norma per supportare l’ isolamento dei carichi di lavoro che si espande.**

Punto saliente

Prima cosa, verificare che una piattaforma cloud offra firewall correttamente integrati, gruppi di sicurezza e opzioni per la micro-segmentazione basate sul carico di lavoro e host di calcolo attendibili.

Proteggere i dati con la crittografia e la gestione delle chiavi

Proteggere i dati in modo affidabile è un fondamento della sicurezza per qualsiasi business digitale – specialmente per quelli che operano in settori d' industria estremamente regolamentati, ad esempio i servizi finanziari e l' assistenza sanitaria.

I dati associati ad applicazioni cloud-native possono essere distribuiti attraverso servizi object, data service e cloud. Le applicazioni tradizionali possono disporre di un proprio database, di una propria VM e di dati sensibili ubicati in file. In questi casi, la crittografia di dati sensibili, sia inattivi che in movimento, diventa di cruciale importanza.

Le aziende si preoccupano giustamente che operatori cloud o altri utenti non autorizzati accedano ai loro dati, senza che ne siano informate e si aspettano una totale visibilità dell' accesso ai dati.**Controllare l' accesso ai dati con la crittografia e controllare anche l' accesso alle chiavi di crittografia stanno diventando misure di sicurezza previste.** Come risultato, un modello BYOK (bring-your-own-keys) ora è un requisito di sicurezza del cloud. Consente di gestire chiavi di crittografia in un sito centrale, fornisce la garanzia che le chiavi principali non lascino mai i confini del sistema di gestione delle chiavi e permette di verificare tutte le attività del ciclo di vita di gestione delle chiavi (Figura 2).

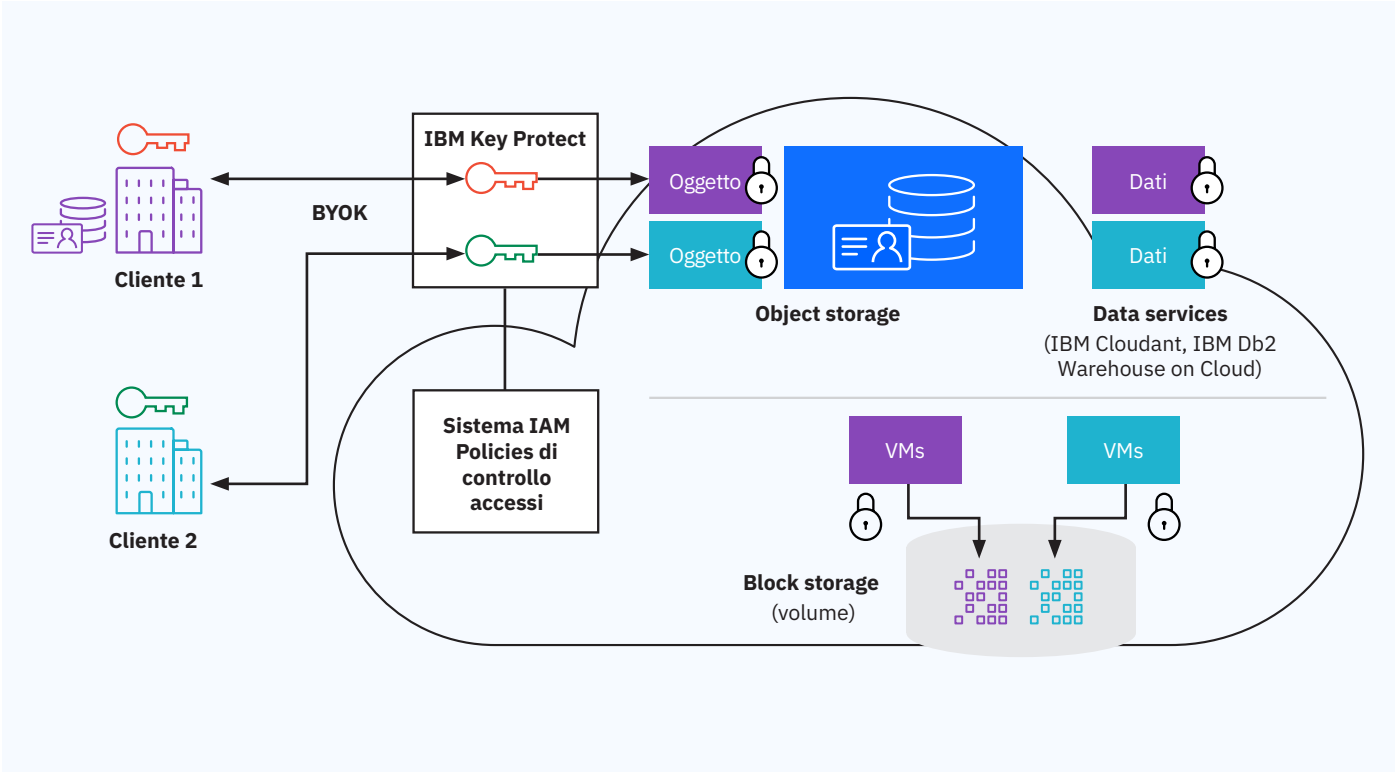
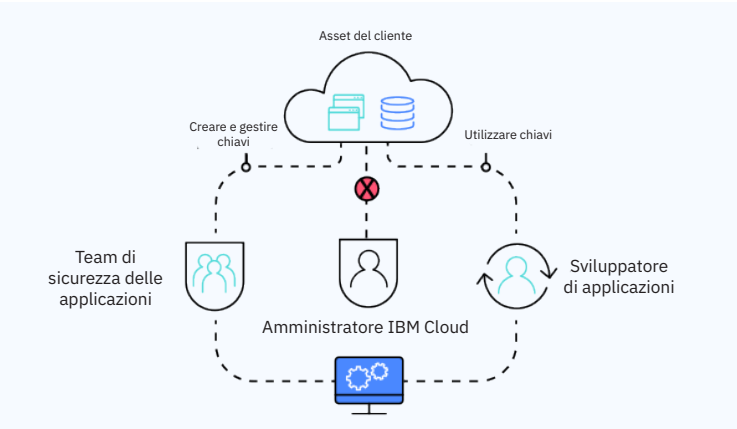


Figura 2. Architettura di una soluzione BYOK.

KYOK (Keep your own key)

Per implementare una sicurezza dei dati che rimanga privata al 100% in un cloud pubblico, IBM offre in esclusiva una soluzione che consente all' utente di essere il solo custode della propria chiave di crittografia. Come unico servizio nel settore d' industria basato su hardware con certificazione FIPS 140-2 Livello 4, IBM Cloud Hyper Protect Crypto Services fornisce una gestione chiavi e un HSM (hardware security module) cloud.



Host di calcolo attendibile

Si tratta semplicemente di hardware: nessuno vuole implementare dati e applicazioni di valore su un host non attendibile. I provider di piattaforme cloud che offrono hardware con protocolli di misurazione-verifica-lancio forniscono host estremamente sicuri per applicazioni implementate all' interno del sistema di orchestrazione dei contenitori.

Intel TXT (Intel Trusted Execution Technology) e TPM (Trusted Platform Module) sono esempi di tecnologie a livello di host che consentono di avere fiducia nelle piattaforme cloud. Intel TXT difende da attacchi basati su software, con l' intento di appropriarsi di informazioni sensibili corrompendo il sistema o il codice BIOS o modificando la configurazione della piattaforma. Intel TPM è un dispositivo di sicurezza basato sull' hardware che aiuta a proteggere il processo di avvio del sistema, garantendo che sia scevro da manomissioni, prima di rilasciare il controllo del sistema al sistema operativo.

Protezione dei dati inattivi e in transito

La crittografia integrata nel modello BYOK consente di mantenere il controllo dei propri dati, sia on premise o nel cloud. È un modo eccellente per controllare gli accessi ai dati in implementazioni di applicazioni cloud-native. In questo approccio, il sistema di gestione chiavi del cliente genera una chiave on premise e la passa al servizio di gestione chiavi del provider. Questo approccio comprende crittografia dei dati inattivi attraverso vari tipi di storage, ad esempio a blocchi, di oggetti e servizi dati.

Per i dati in transito, la comunicazione e il trasferimento sicuri avvengono su TLS/SSL (Transport Layer Security/ Secure Sockets Layer). La crittografia TLS/SSL consente anche di dimostrare conformità, sicurezza e governance, senza richiedere controllo amministrativo sul sistema di crittografia o sull' infrastruttura. La capacità di gestire certificati SSL è un requisito per l' affidabilità di una piattaforma cloud.

Come soddisfare esigenze di verifica e conformità

Fornire le proprie chiavi di crittografia e conservarle nel cloud – senza che i provider di servizi possano accedervi – consente la visibilità e il controllo delle informazioni che sono necessari per le verifiche di conformità CISO.

Punto saliente

I cloud provider devono poter prevedibilmente offrire soluzioni BYOK che consentano all' organizzazione di gestire chiavi in tutti i servizi e lo storage di dati.

Automatizzare la sicurezza per DevOps

Quando i team DevOps creano servizi cloud-native e operano con tecnologie di container, hanno bisogno di un modo per integrare i controlli di sicurezza in una pipeline sempre più automatizzata. Poiché siti quali Docker Hub promuovono lo scambio aperto, gli sviluppatori possono facilmente risparmiare il tempo di preparazione dell' immagine scaricando semplicemente il materiale di cui hanno bisogno. Ma, una tale flessibilità, porta con sé l' esigenza di ispezionare regolarmente tutte le immagini di contenitori collocate in un registro, prima che vengano implementate.

Un sistema di scansione automatizzata aiuta a garantire l' attendibilità, ricercando potenziali vulnerabilità nelle proprie immagini, prima di iniziare a eseguirle. Chiedere ai vendor delle piattaforme se consentono a un' organizzazione di creare politiche (ad esempio "non implementare immagini che contengano vulnerabilità" o "avvertimi prima di implementare queste immagini in produzione") come parte della sicurezza della pipeline DevOps.

IBM Cloud Container Service, ad esempio, offre un sistema VA (Vulnerability Advisor) per fornire la scansione di container statici e operativi. VA ispeziona ogni livello di ogni immagine in un registro privato di un cliente del cloud, per rilevare vulnerabilità o malware prima dell' implementazione dell' immagine. Poiché con la semplice scansione delle immagini del registro si possono non rilevare problemi quali ad esempio una deviazione dall' immagine statica per i contenitori implementati, VA effettua anche una scansione dei contenitori in esecuzione per rilevare anomalie. Fornisce inoltre suggerimenti sotto forma di avvisi su più livelli.

Punto saliente

La best practice di sicurezza per i container consiste nella scansione dei container medesimi, per individuare vulnerabilità, sia prima dell' implementazione che in fase di esecuzione.

Altre funzioni del VA che consentono di automatizzare la sicurezza nella pipeline DevOps includono:

- **Impostazioni di violazioni della politica:** Con VA, gli amministratori possono impostare politiche di implementazione delle immagini sulla base di tre tipi di situazioni di errore dell' immagine: installati pacchetti con vulnerabilità note; accessi da remoto abilitati; e accessi da remoto abilitati con utenti che hanno facilmente scoperto le password.
- **Best practice:** VA attualmente verifica 26 regole, in base all' ISO 27000, che includono impostazioni quali la durata minima e la lunghezza minima della password.
- **Rilevamento di errori di configurazione della sicurezza:** VA segnala ogni problema dovuto ad errore di configurazione, ne fornisce una descrizione e suggerisce una linea d' azione per porvi rimedio.
- **Integrazione con IBM X-Force:** VA riceve security intelligence da cinque fonti di terze parti e utilizza criteri quali ad esempio il vettore dell' attacco, la complessità e la disponibilità di una correzione nota, per classificare ogni vulnerabilità. Il sistema di classificazione (critica, elevata, moderata o bassa) consente agli amministratori di comprendere facilmente la gravità delle vulnerabilità e determinare la priorità della correzione.

Quando arriva il momento della correzione, VA non interrompe l' esecuzione delle immagini per applicare la patch. Piuttosto, IBM corregge la "golden" image nel registro e implementa una nuova immagine nel container. Questo approccio aiuta a garantire che a tutte le future istanze di tale immagine sarà applicata la stessa correzione. Le VM possono ancora essere gestite in modo tradizionale, utilizzando un servizio di sicurezza dell' endpoint per applicare patch alle VM e correggere vulnerabilità della sicurezza di Linux.

Panoramica su Kubernetes

Se il team DevOps utilizza il popolare software di orchestrazione dei container Kubernetes, questo garantisce che possano continuare a utilizzare i loro strumenti preferiti. Inoltre, valutare con quanta facilità una piattaforma fornisce nuovi cluster Kubernetes e gestisce quelli esistenti.

Chiedere se un provider di piattaforma cloud supporta Calico e Istio con il suo sistema Kubernetes. Calico e Istio sono due componenti importanti di Kubernetes che contribuiscono alla sicurezza delle applicazioni e dei carichi di lavoro. Calico aiuta a semplificare la gestione di indirizzi IP assegnati ai carichi di lavoro in un nodo di calcolo e programma ACL (access control list) in ogni nodo di calcolo per applicare politiche di sicurezza. Utilizzando definizioni di politica impostate e applicate tramite etichette di configurazione, Istio fornisce controllo basato su certificato della comunicazione tra microservizi in un pod o cluster Kubernetes.

Creare un security immune system attraverso il monitoraggio intelligente

Quando si passa al cloud, i CISO spesso si preoccupano della scarsa visibilità e della perdita di controllo. Dal momento che l' intero cloud dell' organizzazione può disattivarsi se una determinata chiave viene eliminata o una modifica alla configurazione inavvertitamente interrompe una connessione a risorse on-premise o a un SOC (security operations center - centro operazioni di sicurezza) aziendale, perché gli ingegneri delle operazioni non dovrebbero aspettarsi una visibilità completa dei carichi di lavoro, delle API e dei microservizi basati su cloud – di ogni componente?

Tracce dell' accesso e log di verifica

Tutto l' accesso di utenti e amministrazione, sia da parte del cloud provider o dell' organizzazione, dovrebbe essere registrato automaticamente. Un programma di traccia dell' attività cloud integrato può creare una traccia di tutti gli accessi alla piattaforma e ai servizi, che includono accesso a dispositivi mobili, al Web e alle API. L' organizzazione dovrebbe essere in grado di utilizzare questi log e integrarli nel SOC aziendale.

Security intelligence aziendale

Assicurarsi di avere l' opzione di integrare tutti i log e gli eventi nel sistema SIEM (security information and event management) on-premise (Figura 3). Alcuni provider di servizi cloud offrono anche monitoraggio della sicurezza con gestione degli incidenti e produzione di report, analisi in tempo reale degli avvisi di sicurezza e una vista integrata delle implementazioni ibride.

IBM QRadar, ad esempio, è una soluzione SIEM completa, che offre una serie di soluzioni di security intelligence che possono crescere in base alle esigenze di un' organizzazione. Le sue funzionalità di machine learning si addestrano su schemi di minaccia in un modo che crea un security immune system predittivo.

Sicurezza gestita con competenza

Se la propria organizzazione non dispone di competenze sulla sicurezza significative, prendere in considerazione provider a cui delegare la gestione della sicurezza. Alcuni provider sono in grado di monitorare gli incidenti di sicurezza, applicare la threat intelligence messa a disposizione da vari settori d' industria e correlare queste informazioni per intraprendere un' azione. Chiedere se i provider possano anche fornire una singola console che integri servizi di sicurezza interni e gestiti.

Punto saliente

La sicurezza della piattaforma cloud deve garantire un controllo efficace degli accessi, operare a livello dei carichi di lavoro, tenere una traccia dettagliata dell' attività e integrarsi nei sistemi on-premise.

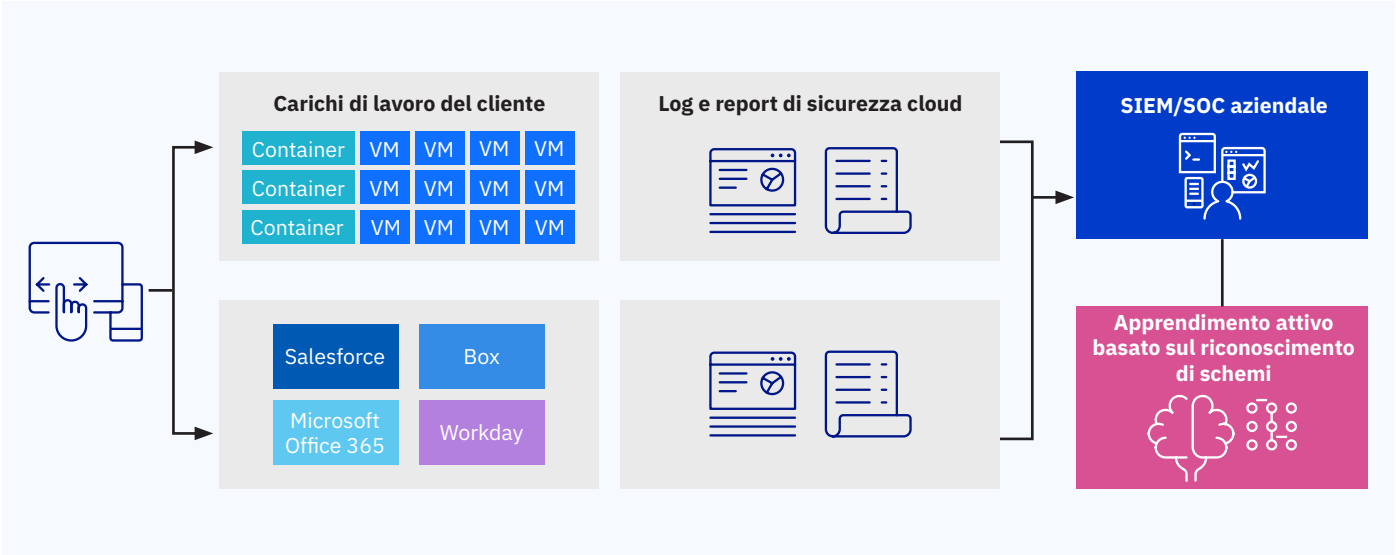


Figura 3. Integrazione della visibilità del cloud in un SIEM/SOC aziendale.

Sicurezza che promuove il successo di business

Con la tecnologia cloud che diventa una parte più ampia ed importante della conduzione di un business digitale, vale letteralmente la pena di cercare un cloud provider che offra una serie adeguata di funzionalità e controlli per proteggere dati, applicazioni e l' infrastruttura cloud da cui dipendono applicazioni rivolte ai clienti. La soluzione di sicurezza della piattaforma deve prevedibilmente contemplare le cinque aree di focalizzazione chiave della sicurezza del cloud: identità e accesso; sicurezza di rete; protezione dei dati; sicurezza delle applicazioni; visibilità e intelligence. L' obiettivo è quello di preoccuparsi meno della tecnologia e focalizzarsi maggiormente sul business di base.

Un cloud con protezione adeguata offre notevoli vantaggi in termini di business e IT, che includono:

- **Riduzione del time to value:** Dal momento che la sicurezza è già installata e configurata, i team possono facilmente eseguire il provisioning di risorse e creare rapidamente prototipi di esperienze utente, valutare risultati e iterare in base alle necessità.
- **Riduzione della spesa in conto capitale:** Utilizzando servizi di sicurezza nel cloud si possono eliminare molti costi iniziali, che includono server, licenze software e appliance.
- **Riduzione del sovraccarico amministrativo:** Stabilendo e consolidando correttamente l' attendibilità della piattaforma cloud, il provider con valide offerte di sicurezza si assume il maggior carico amministrativo, riducendo i costi della produzione di report e della manutenzione di risorse.

Consulta il Gartner Peer Insights per scoprire perché IBM Cloud:

Ha ricevuto le massime valutazioni per l' integrazione aziendale (4,6 su 5 stelle)

E ha ottenuto la massima valutazione complessiva tra i principali cloud provider (4,7 su 5 stelle)

...in base a **90 recensioni negli ultimi 12 mesi, a partire dal 1 giugno 2020.**

https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/ibm/product/ibm-cloud

Le recensioni di Gartner Peer Insights costituiscono opinioni soggettive di singoli utenti finali, basate sulle loro esperienze e non rappresentano punti di vista di Gartner o di sue affiliate.

Per ulteriori informazioni

Per saperne di più sulle cinque aree chiave della sicurezza cloud e sulle tecnologie e servizi correlati, messi a disposizione da IBM, visitare il sito all' indirizzo: ibm.com/cloud/security

Resta connesso

Blog su IBM Cloud

Seguici

@IBMcloud
Facebook

Connettiti con noi

LinkedIn
YouTube

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page di IBM Italia si trova all' indirizzo:
ibm.com

[1] Report Insider Threat 2018, pubblicato a novembre 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report