SOPHOS

Come proteggere il cloud pubblico: sette best practice

Whitepaper Sophos giugno 2019

Indice dei contenuti

Come proteggere il cloud pubblico: sette best practice

Qual è la dimostrazione pratica di una protezione efficace per le applicazioni nel cloud pubblico?

Forse potrebbe essere utile giungere a fine anno senza essere mai citati nei titoli dei notiziari per via di un caso di violazione dei dati. O magari è più utile capire l'impatto sulla propria organizzazione dell'infrastruttura cloud, per poterne garantire la sicurezza. Può darsi che l'obiettivo sia superare gli audit di conformità senza problemi, oppure migliorare la collaborazione sulle questioni di sicurezza e conformità tra i team (tradizionalmente isolati) che si occupano di compliance e sviluppo.

Qualsiasi sia il traguardo desiderato, questa guida rappresenta un valido aiuto. Esplora i sette passaggi più importanti per il processo di messa in sicurezza del cloud pubblico, fornendo consigli pratici che possono essere seguiti da qualsiasi organizzazione. Include i risultati delle ricerche sulle minacce svolte dai SophosLabs, che esaminano la frequenza con cui i cybercriminali colpiscono le istanze basate sul cloud. Questa guida descrive anche come Sophos Cloud Optix è in grado di aiutare le organizzazioni a risolvere le proprie sfide di sicurezza e visibilità.

Creare nuove istanze in Amazon Web Services (AWS), Microsoft Azure o Google Cloud Platform (GCP) è semplice. I compiti più difficili spettano ai team operativi, di sicurezza, sviluppo e conformità, che devono monitorare i dati, i workload e le modifiche dell'architettura in questi ambienti, per garantire la massima sicurezza dell'intera struttura.

Mentre i provider di servizi di cloud pubblico hanno la responsabilità di garantire la sicurezza del cloud (la struttura fisica dei data center e la compartimentalizzazione tra gli ambienti e i dati dei clienti), il compito di proteggere workload e dati spetta interamente a chi li carica sul cloud. Proprio come i dati memorizzati nelle reti on-premise, anche il vostro ambiente cloud deve essere protetto. Molti fraintendono questa suddivisione delle responsabilità, e il risultato è la presenza di lacune di sicurezza che hanno trasformato i workload in cloud in una vera e propria miniera d'oro per gli hacker più esperti attualmente in circolazione.

La sfida più difficile della protezione per il cloud

Il cloud pubblico offre massima semplicità e un ottimo rapporto qualità-prezzo, per cui non sorprende affatto che una quantità sempre maggiore di organizzazioni decida di passare ad Amazon Web Services, Microsoft Azure e Google Cloud Platform. Questi servizi consentono di creare una nuova istanza nel giro di pochi minuti, di incrementare o ridurre le risorse in qualsiasi momento e pagando solamente per il consumo effettivo, nonché di evitare di dover affrontare ingenti costi iniziali per l'hardware.

Se da un lato il cloud pubblico risolve molte delle sfide presentate dall'uso delle risorse informatiche tradizionali, dall'altro introduce anche nuove problematiche. Il segreto di una cybersecurity efficace nel cloud è migliorare lo stato di sicurezza generale: garantendo una protezione efficace e una configurazione corretta per l'architettura, si ottiene un livello adeguato di visibilità sull'intero sistema, e soprattutto su chi è in grado di accedervi.

Anche se sembra tutto molto semplice, in realtà non lo è per niente.

La rapida diffusione dell'utilizzo del cloud ha dato vita a una distribuzione frammentaria dei dati, con workload suddivisi su varie istanze o addirittura, per alcune organizzazioni, su piattaforme diverse. In media, le organizzazioni eseguono già applicazioni in due cloud pubblici, e nel frattempo provano nuove opzioni su altri 1,8 cloud pubblici [1]. Questo approccio multi-cloud è alla base del problema della visibilità per i responsabili IT, che devono passare rapidamente da una piattaforma a un'altra per ottenere il quadro completo della situazione dei propri ambienti basati sul cloud.

La mancanza di visibilità sui workload in cloud genera rischi di sicurezza e di conformità:

Maggiore esposizione ai rischi

Per le aziende, la maggiore flessibilità e la rapidità dei tempi di commercializzazione per prodotti e servizi sono ottimi incentivi per passare al cloud pubblico. Di solito il processo richiede l'agilità e la velocità di risposta di un approccio DevOps. Per molti, questo nuovo approccio allo sviluppo e al rilascio dei prodotti implica la collaborazione di vari sviluppatori su piattaforme diverse e a volte persino in fusi orari differenti.

Monitorare i workload non era un problema grave quando i cicli di sviluppo duravano mesi o anni, ma quei tempi sono ormai un ricordo lontano. Oggi come oggi occorre monitorare rilasci multipli, a volte nello stesso giorno. Tenere il passo con i ritmi frenetici con cui vengono effettuate le modifiche dell'architettura, gli aggiornamenti delle configurazioni e le impostazioni dei gruppi di sicurezza è praticamente impossibile. Il risultato di tutto questo è una maggiore esposizione alle minacce informatiche, che sfruttano rapidamente le vulnerabilità dei sistemi.

Minacce per dati, proprietà intellettuale e servizi

Il cloud pubblico offre alle organizzazioni molti vantaggi in termini di automazione, ma lo stesso vale anche per i cybercriminali. Al giorno d'oggi gli autori degli attacchi agiscono sempre più frequentemente creando ambienti cloud e sfruttando le API native dei provider di servizi cloud per automatizzare la distribuzione sulle nuove istanze, per attaccare database esposti, per modificare le impostazioni di sicurezza e per bloccare utenti legittimi.

Al fine di quantificare il problema, i SophosLabs hanno recentemente impostato ambienti virtuali in 10 dei data center di AWS più utilizzati nel mondo. Le ricerche hanno rivelato che:

- Nel giro di due ore, tutti e 10 sono stati vittima di tentativi di accesso non autorizzato[2]
- Ciascun dispositivo ha subito in media 13 tentativi di accesso al minuto, ovvero circa 757 ogni ora

Questi risultati a dir poco scioccanti mettono in luce la frequenza con cui i cybercriminali colpiscono le istanze basate sul cloud, sfruttando tecniche sofisticate e automatizzate. La sfida dei responsabili di sicurezza è identificare e proteggere le potenziali vulnerabilità prima che lo facciano gli autori degli attacchi, rilevando i comportamenti insoliti (tipici degli hacker) in tempo reale, per bloccare gli attacchi sul nascere.

Rispetto degli standard di conformità

Indipendentemente da dove siano situati infrastruttura e dati, esiste l'obbligo di dimostrare la conformità alle normative applicabili, incluse CIS, HIPPA, GDPR e PCI. In caso contrario, si rischia di violare gli standard di conformità alle normative.

Il problema del cloud è che gli ambienti cambiano ogni giorno, ogni ora e persino ogni minuto. Se in passato i controlli della conformità potevano essere svolti una volta alla settimana o una volta al mese per le reti on-premise, questo approccio non è idoneo per il cloud pubblico. Il dover effettuare continue analisi di conformità può rappresentare un peso enorme in termini di consumo delle risorse per i team che gestiscono gli ambienti cloud manualmente o con gli strumenti nativi. Inoltre, una volta identificato un problema di conformità, spesso è difficile risolvere la situazione con la dovuta tempestività, per via della natura frammentaria dei team operativi, di sicurezza, sviluppo e conformità che caratterizza la maggior parte delle organizzazioni.

Sette passi per proteggere il cloud pubblico

1: scoprire quali sono le proprie responsabilità

A prima vista, sembra ovvio, ma la sicurezza deve essere gestita in maniera diversa nel cloud. I provider di servizi di cloud pubblico, come Amazon Web Services, Microsoft Azure e Google Cloud Platform, applicano un modello di responsabilità condivisa: i provider garantiscono la sicurezza del cloud, mentre la responsabilità di proteggere qualsiasi elemento presente nel cloud ricade su chi lo carica.

Gli aspetti quali la protezione fisica a livello di data center, la separazione virtuale dei dati e degli ambienti dei clienti sono tutti gestiti dai provider di servizi cloud pubblico.

Potrebbero essere presenti alcune regole di base simili a quelle dei firewall per monitorare l'accesso al proprio ambiente. Tuttavia, se non vengono configurate in maniera adeguata (ad esempio se le porte rimangono accessibili a chiunque), le conseguenze ricadono su di voi. Di conseguenza, occorre scoprire quali sono le proprie responsabilità.

La Fig. 1 fornisce una panoramica di queste responsabilità condivise. Se preferite, potete anche guardare questo video.

Modello di responsabilità condivisa per la sicurezza	On-Premise	Cloud pubblico	Perché?
Utenti	■	■	Implementare l'autenticazione, definire limitazioni di accesso e monitorare l'utilizzo delle credenziali.
Dati	■	■	Bloccare la fuga dei dati, definire e implementare l'accesso a dati specifici da parte di utenti specifici, garantendo allo stesso tempo il rispetto degli standard di conformità.
Applicazioni	■	■	Prevenire la compromissione delle applicazioni grazie all'uso di policy, patch e sicurezza.
Controlli di rete	■	◪	Monitorare e implementare autorizzazioni di accesso alla rete.
Infrastruttura host	■	◪	Gestire e proteggere sistemi operativi, soluzioni di archiviazione e sistemi correlati, al fine di prevenire i rischi causati da bug per cui non sono presenti patch e da exploit di tipo privilege escalation.
Sicurezza fisica	■	■	Limitare l'accesso fisico ai sistemi e progettare ridondanza per prevenire singoli punti di errore.

■ Cliente ■ Provider della piattaforma

Fig. 1. Riepilogo Sophos del modello di responsabilità condivisa. Per le versioni specifiche per ciascun provider, visitare: sophos.it/public-cloud.

2: pianificare un approccio multi-cloud

Ormai il multi-cloud non è solamente una strategia opzionale. È diventato un must. I motivi per utilizzare cloud multipli possono essere diversi, ad esempio maggiore disponibilità e flessibilità o una migliore funzionalità. Quando si pianifica la propria strategia di sicurezza, bisogna partire dal presupposto che l'ambiente sarà multi-cloud, se non subito di sicuro in futuro. In questo modo si garantisce l'attuazione di un approccio pronto per le sfide del futuro.

Occorre pensare a come si gestiranno le attività di messa in sicurezza, monitoraggio e rispetto della conformità in provider di servizi cloud multipli, con sistemi e console diversi. A una maggiore semplicità per l'esperienza di gestione corrisponderà una più rapida risposta in caso di incidenti, un incremento nel numero delle minacce rilevate e una riduzione dei grattacapi dovuti agli audit di conformità. Per non parlare di come ciò contribuisce alla fidelizzazione dei dipendenti più importanti.

Consigliamo di optare per soluzioni agentless che consentano di monitorare ambienti di provider di servizi cloud multipli da un'unica console SaaS, riducendo così la quantità di strumenti, tempo e personale necessari per gestire la sicurezza per account cloud e regioni multipli.

3: ottenere una visibilità completa

Ciò che non è visibile non può essere protetto. Ed è per questo motivo che uno dei maggiori ostacoli al garantire un adeguato stato di sicurezza complessivo è proprio la mancanza di visibilità sulla propria infrastruttura.

Utilizzate strumenti che offrano una visualizzazione in tempo reale della topologia della rete e del flusso di traffico, fornendo un inventario completo e dettagliato di tutti gli host, le reti, gli account utente, i servizi di storage, i container e le funzionalità indipendenti dai server.

Per una maggiore visibilità, si consiglia di optare per strumenti in grado di identificare le potenziali vulnerabilità all'interno della propria architettura, per evitare che si creino potenziali punti di violazione. Gli ambiti potenzialmente a rischio includono:

- Database con porte aperte pubblicamente a internet, che potrebbero consentire l'accesso degli autori degli attacchi
- Amazon S3 (Simple Storage Service) pubblici
- Comportamenti di accesso sospetti e chiamate API non riconosciute. Alcuni esempi possono essere accessi multipli allo stesso account effettuati contemporaneamente, oppure l'accesso dello stesso utente in parti del mondo diverse nell'arco di 24 ore

4: integrare la conformità nei processi di ogni giorno

Il trasferimento verso il cloud dei workload introduce una nuova sfida: dover rispettare le normative di conformità in una rete maggiormente distribuita, che spesso richiede vari rilasci di sviluppo a intervalli regolari. Per garantire il rispetto della conformità, occorre generare report accurati sull'inventario e diagrammi di rete dell'impatto del proprio ambiente cloud, nonché garantire l'adempimento di tutti i requisiti di conformità in un ambiente dinamico.

Quando si trovano ad affrontare scadenze per gli audit, spesso le organizzazioni ricorrono a una soluzione a breve termine, utilizzando risorse che dovrebbero essere dedicate a progetti volti a incrementare il fatturato. Questo stratagemma non è sostenibile a lungo termine e, man mano che gli snapshot di analisi quotidiana diventano obsoleti, non garantisce il monitoraggio continuo della conformità richiesto da standard quali ISO 27001, HIPAA e GDPR.

Optate per soluzioni che consentano di elevare gli standard di sicurezza senza dover aumentare il numero di dipendenti, grazie a snapshot di analisi in tempo reale della topologia della rete e al rilevamento automatico con segnalazione immediata delle modifiche agli ambienti cloud. Un'altra opzione desiderabile è la possibilità di personalizzare le policy per soddisfare le esigenze specifiche del proprio settore o mercato verticale.

Ovviamente la reportistica è solamente uno degli aspetti della conformità. È anche essenziale poter risolvere i problemi derivati dal mancato rispetto della conformità. La sfida più difficile è garantire la collaborazione tra personale operativo, di sviluppo e di conformità, a causa della mancanza di adeguati canali di collaborazione.

Per agevolare il processo di risoluzione dei problemi di conformità, consigliamo di optare per soluzioni che siano in grado di integrarsi con le attuali soluzioni di segnalazione dei problemi, e che includano un sistema di segnalazione con informazioni utili per creare, assegnare e monitorare i problemi fino alla loro risoluzione. In questo modo, nessuna attività importante viene dimenticata, anche durante un rilascio.

5: automatizzare i controlli di sicurezza

La capacità di automatizzare i processi è uno dei vantaggi di DevOps. I team possono usufruire dell'automatizzazione dei processi di distribuzione di modelli e script per le infrastrutture, risparmiando così diverse ore di tempo prezioso che altrimenti sarebbero state destinate alle operazioni di sviluppo. Analogamente, occorre anche considerare quali sono i controlli di sicurezza che possono essere automatizzati.

Nel quadro collaborativo di DevOps, la sicurezza è una responsabilità da condividere e da integrare end-to-end. Questa corrente di pensiero ha dato origine al termine "DevSecOps", che enfatizza la necessità di impostare solide fondamenta di sicurezza per tutte le iniziative di DevOps.

Il bisogno di automatizzare la sicurezza è evidente quanto la maggiore tendenza dei cybercriminali ad approfittare loro stessi delle opzioni di automatizzazione per sferrare i propri attacchi, utilizzando ad esempio credenziali rubate per automatizzare il provisioning di istanze destinate ad attività quali cryptojacking, modifica delle impostazioni dell'account o rimozione di utenti legittimi per evitare il rilevamento. Infatti, ormai non è insolito imbattersi nella creazione di ambienti cloud volti a sfruttare le vulnerabilità delle password, delle impostazioni dei gruppi di sicurezza e del codice.

I due motivi principali per cui gli attacchi sferrati contro gli ambienti del cloud pubblico vanno a segno sono la mancanza di protezione della configurazione dell'architettura e un inadeguato sistema di risposta alle minacce. Automatizzare i controlli di sicurezza è fondamentale per risolvere questi problemi.

Per garantire la protezione degli ambienti del cloud pubblico, occorre cercare una soluzione in grado di:

- **Correggere automaticamente le vulnerabilità relative all'accesso degli utenti e alle risorse**, per proteggere i sistemi contro il traffico in ingresso proveniente da qualsiasi origine e destinato a qualsiasi porta
- **Identificare gli eventi che corrispondono ai tentativi di accesso sospetti alla console e alle chiamate API non autorizzate**, visto che indicano la probabilità che l'autore di un attacco stia utilizzando le credenziali condivise o rubate di un utente
- **Segnalare le anomalie nel traffico in uscita** per mettere in guardia l'organizzazione in caso di attività quali il cryptojacking o l'esfiltrazione dei dati
- **Rivelare i workload delle applicazioni nascoste** in base al comportamento dell'istanza del computer host per mettere in evidenza i punti deboli nascosti (ad es. i database)

6: proteggere TUTTI gli ambienti (inclusi sviluppo e controllo qualità)

Sebbene i casi di violazione dei dati nel cloud pubblico che vengono citati nei notiziari tendono a essere quelli che colpiscono l'ambiente di produzione nel cloud di un'azienda (ovvero quello utilizzato dai clienti), è altrettanto probabile che gli autori degli attacchi puntino anche a sfruttare la potenza di elaborazione delle organizzazioni (negli ambienti di sviluppo e controllo qualità), per svolgere attività quali il cryptojacking.

Occorre una soluzione che sia in grado di proteggere tutti gli ambienti (produzione, sviluppo e controllo qualità), sia in maniera reattiva che proattiva. Questa soluzione deve integrare i log delle attività (ad es. i log sui flussi del VPC e i log di CloudTrail) per identificare i problemi che si sono già verificati, ad esempio l'apertura indesiderata di una porta nel firewall. Allo stesso tempo, la soluzione deve essere in grado di effettuare una scansione proattiva dei modelli Infrastructure-as-Code (IaC) da archivi come GitHub, e di integrarsi con gli strumenti di pipeline per CI/CD quali Jenkins. In questo modo, si può avere la certezza che le vulnerabilità introdotte nel codice vengano rilevate molto prima che possano raggiungere i server, impedendo così che l'azienda finisca nei notiziari per i motivi sbagliati.

7: mettere in pratica tutto quello che si è appreso dalla sicurezza on-premise

Questo concetto può sembrare insolito per una guida per il cloud pubblico, ma la sicurezza on-premise è il risultato di vari decenni di ricerca ed esperienza. Quando si tratta di proteggere i server in cloud contro infezioni e perdita dei dati, consigliamo di cominciare prendendo in considerazione i principi già applicati alla propria infrastruttura tradizionale, adattandoli al cloud:

- Next-Gen Firewall: consigliamo in primo luogo di impedire alle minacce di infiltrarsi nei server in cloud, collocando un Web Application Firewall (WAF) a livello di gateway cloud. Inoltre, è bene includere funzionalità IPS (per favorire il rispetto della conformità) e il controllo dei contenuti in uscita, per proteggere server/VDI.
- Protezione per i server: occorre eseguire una soluzione efficace di cybersecurity sui server in cloud, proprio come quella che si applicherebbe ai server fisici.
- Protezione endpoint: anche se la rete può essere nel cloud, i laptop e gli altri dispositivi hanno i piedi ben piantati per terra e basta una semplice e-mail di phishing o uno spyware per prelevare illecitamente le credenziali utilizzate dagli utenti per gli account cloud. Accertatevi di aggiornare la sicurezza per endpoint ed e-mail sui dispositivi, per impedire l'accesso non autorizzato agli account cloud.

La nuova Sophos Cloud Optix

See everything, secure everything

La visibilità rappresenta le fondamenta su cui devono essere impostate tutte le policy e le attività di sicurezza. Sophos Cloud Optix semplifica il monitoraggio di ambienti di provider di servizi cloud multipli, inclusi gli account Amazon Web Services (AWS), le subscription Microsoft Azure, i progetti Google Cloud Platform (GCP), i cluster Kubernetes e gli archivi di codice. Questo livello superiore di visibilità, a cui si aggiungono controlli e avvisi su livelli multipli grazie ai criteri di conformità e di DevSecOps, consente ai team di assumerne il controllo della situazione e procedere con la propria strategia di protezione per il cloud in assoluta tranquillità.

Cloud Optix è un servizio agentless e basato su SaaS che si integra con le API del provider di servizi cloud. Compone automaticamente un quadro a 360° e in tempo reale dell'architettura, inclusa la visualizzazione dell'inventario completo e della topologia della rete, compresi host, reti, account degli utenti, dispositivi di memorizzazione, container e funzionalità indipendenti dai server.

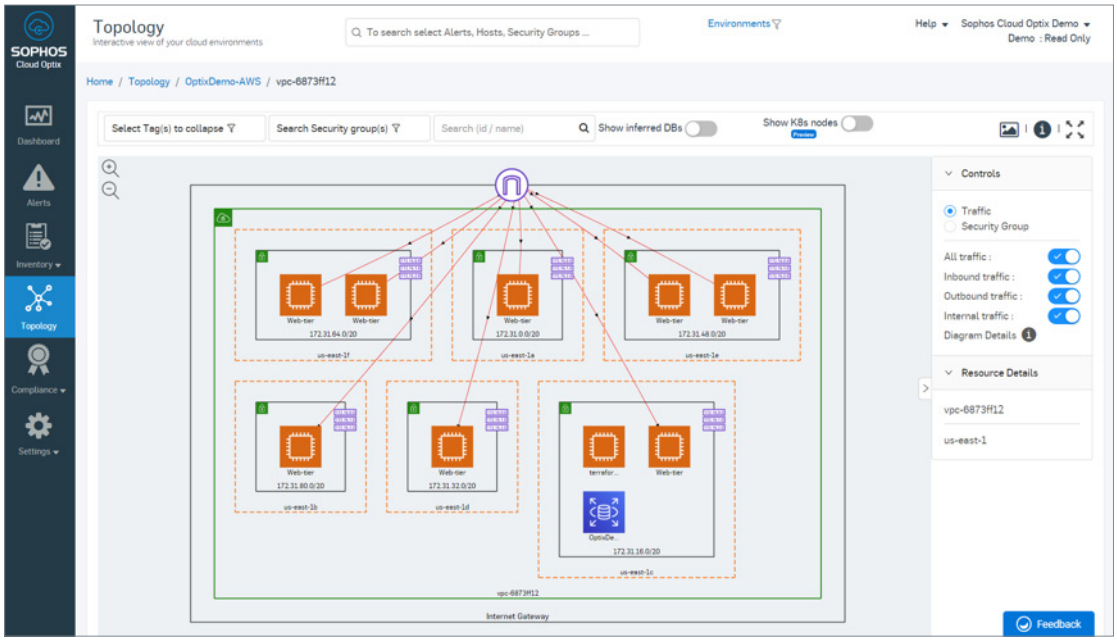

Fig. 2. La visualizzazione della topologia della rete di Sophos Cloud Optix mostra il traffico in entrata, in uscita e interno in un ambiente AWS.

Molto di più di una semplice verifica delle configurazioni

Cloud Optix sfrutta l'intelligenza artificiale del Machine Learning per verificare la presenza di anomalie e vulnerabilità di sicurezza nella vostra piattaforma, monitorando il traffico di rete, le configurazioni delle risorse, gli eventi di accesso degli utenti e le chiamate API, oltre allo stato di conformità, agli archivi infrastructure-as-code (IaaC) e molto altro ancora, con barriere protettive che attivano automaticamente la correzione automatica delle modifiche intenzionali o non intenzionali al traffico della rete.

Nel frattempo, gli avvisi contestuali aiutano a identificare la causa originaria dei problemi di sicurezza e di conformità, permettendovi di concentrare la vostra attenzione sugli aspetti più critici del sistema che richiedono aggiornamenti di sicurezza. Infatti, forniscono una descrizione del problema, indicando le procedure di risoluzione consigliate e le risorse che sono state colpite.

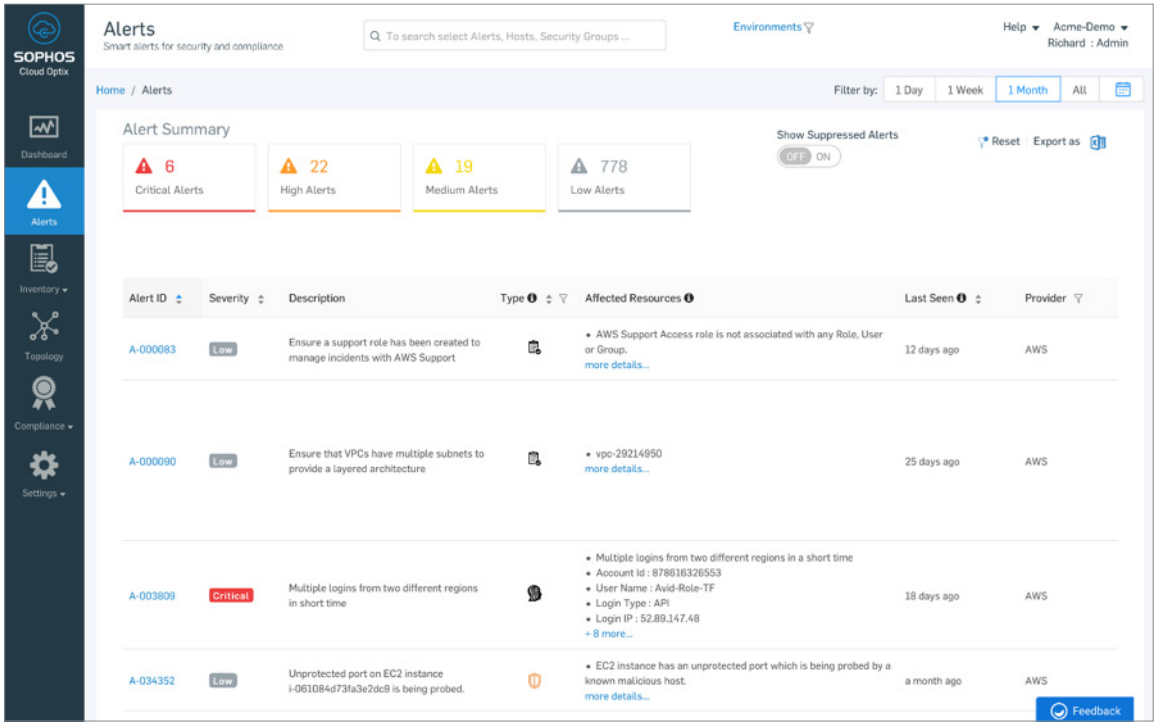

Fig. 3. Il riepilogo degli avvisi di Sophos Cloud Optix mostra un avviso critico relativo ad accessi multipli e simultanei allo stesso account da regioni diverse.

Monitoraggio e risposta personalizzati

Cloud Optix offre una REST API e l'integrazione con Splunk, PagerDuty e Amazon GuardDuty, per garantire informazioni in tempo reale sugli avvisi da qualsiasi piattaforma. Allo stesso tempo, grazie all'integrazione con Jira e ServiceNow, le informazioni sugli avvisi possono anche essere utilizzate per creare ticket rintracciabili fino alla loro risoluzione, per garantire che non venga dimenticata nessuna attività importante, anche durante un rilascio.

A corredare il tutto, vi sono dashboard a visualizzazione immediata per i report su richiesta, che vi permettono di risparmiare ore o persino giorni di tempo prezioso che altrimenti avreste trascorso a gestire lo stato di sicurezza generale nel cloud. Tutto questo vi aiuta a mettere in pratica le sette best practice per proteggere il cloud pubblico.

Maggiori informazioni

Sophos Cloud Optix è la soluzione ideale per le organizzazioni che utilizzano o che hanno intenzione di utilizzare il cloud pubblico. Grazie alla combinazione vincente tra intelligenza artificiale e automazione, questa soluzione offre alle organizzazioni la visibilità ininterrotta necessaria per rilevare, rispondere e prevenire le vulnerabilità di sicurezza e di conformità che potrebbero esporre i sistemi a rischi.

Per maggiori informazioni su Sophos Cloud Optix e per cominciare una prova gratuita di 30 giorni senza obbligo di acquisto nei vostri ambienti cloud, oppure per una demo on-line immediata, visitate www.sophos.it/cloud-optix.

Conclusione

Il passaggio dai workload tradizionali ai workload in cloud offre opportunità straordinarie per le organizzazioni di tutte le dimensioni. Tuttavia, proteggere il cloud pubblico è indispensabile per garantire la sicurezza dell'infrastruttura e per difendere l'organizzazione dagli attacchi informatici. Seguendo i sette passi descritti in questa guida, potete ottimizzare la sicurezza dei vostri cloud pubblici, semplificando allo stesso tempo la gestione e la reportistica sullo stato di conformità.

Modello di responsabilità condivisa: Sophos vi può aiutare, ecco come

	On-Premise	Cloud pubblico	Perché?	L'aiuto che offre Sophos
Utenti	■	■	Implementare l'autenticazione, definire limitazioni di accesso e monitorare l'utilizzo delle credenziali.	XG Firewall e Sophos UTM implementano l'autenticazione in entrata e in uscita con single sign-on (SSO) e l'autenticazione a due fattori (2FA). Inoltre, offrono report di accesso dettagliati. Sophos Cloud Optix monitora l'utilizzo condiviso o non autorizzato delle credenziali degli account.
Dati	■	■	Bloccare la fuga dei dati; definire e implementare l'accesso a dati specifici da parte di utenti specifici, garantendo allo stesso tempo il rispetto degli standard di conformità.	Sophos Cloud Optix offre l'automazione dei processi di conformità, governance e monitoraggio della sicurezza nel cloud, mentre Sophos SafeGuard, DLP e Sophos Mobile aiutano a proteggere i dati e a determinare le autorizzazioni di accesso.
Applicazioni	■	■	Prevenire la compromissione delle applicazioni grazie all'uso di policy, patch e sicurezza.	L'IPS di XG Firewall e Sophos UTM e le funzionalità HIPS e Lockdown di Sophos Server Protection difendono i sistemi contro gli attacchi alle applicazioni e l'esposizione non intenzionale a rischi da parte delle app.
Controlli di rete	■	◪	Monitorare e implementare autorizzazioni di accesso alla rete.	La semplicissima interfaccia di XG Firewall e Sophos UTM, unita all'efficace sistema di ispezione dei pacchetti e alla Synchronized Security (solo con XG), aiutano a proteggere e gestire l'accesso alla rete e a implementare privilegi di rete.
Infrastruttura host	■	◪	Gestire e proteggere sistemi operativi, soluzioni di archiviazione e sistemi correlati, al fine di prevenire i rischi causati da bug per cui non sono presenti patch e da exploit di tipo privilege escalation.	Sophos Intercept X protegge i sistemi dalle minacce del giorno zero, analizzando le tecniche di exploit. Il Lockdown di Sophos Server Protection implementa limitazioni di runtime e Sophos XG Sandstorm blocca la proliferazione di codice sconosciuto.
Sicurezza fisica	■	■	Limitare l'accesso fisico ai sistemi e progettare ridondanza per prevenire singoli punti di errore.	Sia XG Firewall che Sophos UTM offrono opzioni di distribuzione con disponibilità elevata, sia per appliance fisiche che per piattaforme cloud.

■ Cliente ■ Provider della piattaforma

Fig. 4. Le soluzioni Sophos per il modello di responsabilità condivisa del cloud pubblico

"Sophos Cloud Optix garantisce al nostro team una visibilità intelligente e disponibile in tempo reale sui nostri ambienti AWS: tutto quello di cui abbiamo bisogno, a portata di mano. Questo ci consente di raggiungere un livello di monitoraggio e segnalazione dei problemi precedentemente impossibile da ottenere in un'unica vista. Sophos Cloud Optix offre una visualizzazione olistica sull'attività dell'infrastruttura e ci consente di concentrare l'attenzione su sistemi di protezione completi."

Ryan Stinson
Manager of Security Engineering
HubSpot Inc.

1 Report RightScale 2019 State of the Cloud a cura di Flexera

2 Automated attack data source: Exposed: Cyberattacks on Cloud Honeypots, Matt Boddy, Sophos, aprile 2019

Provate gratuitamente Sophos Cloud Optix

www.sophos.it/cloud-optix

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

19/06/19 WP-IT (RP)

SOPHOS