WHITE PAPER

Protezione dei carichi di lavoro in AWS con una segmentazione completa: sicurezza più semplice e veloce

Introduzione

I problemi di sicurezza non devono impedire l'adozione del cloud. Un'unica soluzione è in grado di gestire la visibilità e prevenire il movimento laterale, nonché rilevare e rispondere alle violazioni di asset e risorse in AWS.

I vantaggi derivanti dall'utilizzo delle risorse PaaS (Platform-as-a-Service) in Amazon Web Services (AWS) e dalla migrazione dei carichi di lavoro critici off-premise sono evidenti: si eliminano i costi dell'infrastruttura e la manutenzione, la scalabilità e l'elasticità migliorano con una disponibilità di risorse e potenza quasi illimitate, mentre innovazioni come l'apprendimento automatico e l'intelligenza artificiale potenziano le performance e l'analisi. Tuttavia, i problemi in termini di sicurezza stanno trattenendo molte aziende, specialmente visto che le risorse cloud sono tra i principali bersagli degli attacchi informatici.

La sfida della sicurezza in AWS

Quando si prende in considerazione un ambiente completamente nuovo, non sorprende che sia necessario rivedere la sicurezza da zero. Potrebbe trattarsi di nuove adozioni del cloud o di migrazioni da un altro fornitore, dell'adozione di una nuova soluzione ibrida o dell'aggiunta di AWS all'ecosistema esistente. In ogni caso, il cloud richiede il proprio set di strumenti specifico per gestire le sfide uniche che presenta questa infrastruttura. Alcuni fattori sono comuni a tutti i fornitori di servizi cloud, mentre altri sono specifici per Microsoft Azure, Google Cloud Platform o AWS. Ecco alcuni dei principali problemi per le aziende che utilizzano il cloud (anche in modalità ibrida) con tecnologia AWS.

Comprensione della responsabilità condivisa: dopo lo spostamento dei carichi di lavoro su AWS o l'utilizzo delle sue risorse PaaS integrate, è necessario riconoscere di avere ancora molte responsabilità. Dovrete proteggere i dati, le applicazioni e le piattaforme dei clienti. La mancanza di comprensione del modello di responsabilità condivisa è il motivo per cui Gartner prevede che il 99% degli errori di sicurezza del cloud saranno dovuti ai clienti fino al 2025.

Mancanza di visibilità: è impossibile controllare ciò che non si vede. Nel cloud, la visibilità è molto più complicata, soprattutto quando si tratta di proteggere e visualizzare il traffico di rete che si sposta da est a ovest e da nord a sud. Controllare solo i flussi non è sufficiente. Le vostre risorse critiche possono essere distribuite su più account AWS, container o gruppi di sicurezza di rete e, senza contestualizzare tutto ciò, può essere impossibile ottenere un'idea precisa dei flussi e delle interdipendenze.

Controllo limitato per la creazione di policy: se la vostra azienda è abituata a disporre di informazioni di livello 7 on-premise, di certo non vorrete fare un passo indietro a una visibilità di livello 4, perdendo tale visibilità e controllo granulari ora che i vostri carichi di lavoro sono nel cloud. I gruppi di sicurezza Amazon (Amazon Security Groups) supportano il controllo del traffico verso di livello 4. Ma la visibilità e il controllo di livello 7, indipendentemente dall'infrastruttura sottostante, consentono molto di più che affidarsi unicamente alle porte e IP, ampiamente insufficienti per il rilevamento delle violazioni o la risoluzione dei problemi.

Sicurezza dei container: AWS utilizza i gruppi di sicurezza Amazon per applicare la policy per la sicurezza dei container, ma questo è limitato ai cluster piuttosto che ai singoli pod. Per una visibilità completa delle comunicazioni, è necessaria una soluzione in grado di riconoscere il contesto di una rete overlay in esecuzione a livello superiore e di eseguire un'analisi dettagliata in modo granulare a livello di pod. Ciò diventa più complesso se si desidera creare policy di rete che includano sia macchine virtuali (VM) che container, con il risultato che, spesso, le organizzazioni gestiscono due serie di controlli di sicurezza.

Adozione delle risorse PaaS: si osserva una significativa tendenza ad adottare le risorse PaaS insieme alla migrazione dei carichi di lavoro critici nel cloud, il che riflette le mutevoli esigenze delle organizzazioni incentrate sul cloud. Queste risorse PaaS, tuttavia, non supportano gli agenti, quindi la maggior parte delle soluzioni di sicurezza basate sugli agenti è troppo limitata per estendere una protezione completa sulle risorse PaaS. In tal modo, si possono creare policy di sicurezza nel cloud frammentate, che determinano costi aggiuntivi per i vostri team e lasciano potenzialmente lacune di sicurezza che possono essere sfruttate dai criminali.

Risoluzione dei problemi con una piattaforma di sicurezza completa

Amazon fornisce alcuni strumenti integrati, come i gruppi di sicurezza Amazon, impegnati a risolvere alcune delle sfide della migrazione al cloud della vostra infrastruttura. Incoraggiamo le organizzazioni a sfruttare al meglio la soluzione IAM (Identity and Access Management) di AWS, usando i gruppi per assegnare le autorizzazioni, ruotando regolarmente le credenziali e utilizzando i gruppi IAM per garantire la semplicità. Tuttavia, questi strumenti da soli rappresentano solo un punto di partenza nel cloud pubblico dinamico di oggi, soprattutto se si considera un ambiente ibrido che include tutto, dall'infrastruttura legacy alla tecnologia dei container fino alle risorse PaaS utilizzate nei diversi ambienti del cloud pubblico.

Una soluzione di sicurezza sofisticata vi consentirà di integrare le funzioni offerte da AWS con una tecnologia che rimuove i punti ciechi e funziona perfettamente con lo stack di sicurezza esistente, anche in un ambiente ibrido. Ecco cosa offre Akamai.

Visibilità completa delle istanze AWS

Più complessa diventa la vostra infrastruttura IT, più importante è avere una visibilità approfondita e automatizzata. Spostamenti, aggiunte, modifiche ed eliminazioni manuali non sono solo inaffidabili e soggetti a lacune ed errori, ma comportano anche un rallentamento e quindi ostacolano l'adozione del cloud. Al contrario, una visibilità migliorata e automatizzata rileverà tutte le applicazioni e i flussi, aggiungendo visibilità alle vostre istanze fino al livello del singolo processo.

Akamai Guardicore Segmentation, la soluzione principale della piattaforma Akamai Guardicore per la sicurezza Trust, include una potente API di AWS che inserisce i dati di coordinamento insieme ad un componente dedicato per raccogliere le informazioni su asset, flussi e tag in modo da offrirvi un contesto utile per l'etichettatura e la mappatura delle applicazioni. Nel porre la basi della vostra infrastruttura, potete disporre dei dettagli necessari per comprendere appieno come le vostre applicazioni comunicano tra loro, dove si trovano le interdipendenze e come dovrebbero essere create le policy per consentire elasticità e flessibilità. Invece di disporre di una soluzione di sicurezza separata per ogni fornitore o ambiente cloud, gli utenti possono visualizzare le informazioni del cloud nativo e i dati specifici di AWS nella stessa dashboard. La nostra soluzione funziona su piattaforme, infrastrutture e cloud, in modo da garantire l'assenza di punti ciechi.

Segmentazione e applicazione: una policy che segue il carico di lavoro

Una volta raggiunta questa visibilità "da un'unica posizione" in tutti i vostri ambienti, potete iniziare a progettare e implementare la policy di sicurezza. La policy dipendente da applicazioni offre molto di più rispetto ai gruppi di sicurezza Amazon, fornendo una granularità di livello 7 (anziché di livello 4). I firewall di nuova generazione, che alcune organizzazioni stanno tentando di utilizzare on-premise per limitare il movimento laterale, supportano solo la segmentazione grossolana del traffico est-ovest. È una soluzione dalla complessità proibitiva per i controlli di segmentazione granulare a causa della necessità di enormi modifiche all'infrastruttura e alla rete per reindirizzare il traffico attraverso il firewall. Anche se fosse un'opzione a livello locale, alle organizzazioni resta il problema di mantenere questo livello di controllo sul cloud.

La microsegmentazione di livello 7 è la risposta, con policy create per carichi di lavoro dinamici, senza la necessità di alcuna modifica all'infrastruttura di rete sottostante. Poiché la policy segue il carico di lavoro stesso abbiamo eliminato la necessità di modifiche manuali e migliorato la capacità della vostra organizzazione di adottare i processi DevOps flessibili e in rapida evoluzione. Una policy di microsegmentazione può semplificare un ambiente ibrido, applicando regole tra aree geografiche, VPC, container, VM e on-premise, il tutto con un'espressione di policy coerente. A partire dalla visibilità che forniamo, potete definire e applicare le policy di segmentazione in pochi minuti. Il processo di creazione delle policy è inoltre potenziato dalle raccomandazioni automatiche sulle policy che forniscono i migliori protocolli di sicurezza sul cloud pubblico.

Rilevamento delle violazioni e risposta agli incidenti sul cloud AWS

Con Akamai, potete portare la sicurezza di AWS oltre la semplice segmentazione o visibilità. Il rilevamento delle violazioni delle policy è una parte importante del rilevamento delle violazioni, poiché consente di rispondere a una potenziale minaccia informatica in tempo reale, con dettagli a livello di applicazione. Offriamo diversi metodi di rilevamento delle violazioni in grado di segnalare immediatamente intenti dannosi in un ambiente cloud ibrido.

- **Analisi della reputazione:** consente di rilevare automaticamente le informazioni sospette all'interno dei flussi, dai nomi di dominio e indirizzi IP agli hash dei file e alle righe di comando
- **Elusione dinamica:** contrastate i criminali a loro insaputa, indirizzandoli in un ambiente honeypot ad alta interazione che vi consente di apprendere in modo sicuro il loro comportamento
- **Strumenti per velocizzare la risposta agli incidenti:** l'integrazione con AWS vi consente di inviare in tempo reale ad AWS Security Hub eventuali segnalazioni di violazione delle policy o incidenti di sicurezza
- **Ricerca delle minacce personalizzata:** sfruttate l'infrastruttura e la notevole intelligence globale sulle minacce di Akamai per fermare le minacce più elusive nel vostro ambiente cloud ibrido con il nostro servizio Akamai Hunt

Utilizzo congiunto per una maggiore sicurezza su AWS e oltre

Raccogliere i vantaggi offerti dal cloud pubblico non deve significare accontentarsi di un livello di sicurezza, visibilità o controllo inferiori rispetto a quelli di cui gode la vostra organizzazione on-premise. Con Akamai, potete ottenere una visibilità completa degli asset e delle risorse di AWS, nonché dell'intera infrastruttura. L'utilizzo di questa mappa di base semplifica la creazione di policy e migliora le misure di sicurezza esistenti per fornire un controllo granulare senza la necessità di supporto manuale. Con l'integrazione delle funzioni di rilevamento delle violazioni e risposta agli incidenti, potrete disporre di un'unica soluzione per la sicurezza end-to-end che copre tutte le implementazioni nel cloud di AWS e oltre.

Per ulteriori informazioni, visitate il sito akamai.com/guardicore.

Informazioni sulle soluzioni per la sicurezza di Akamai

Le soluzioni per la sicurezza di Akamai proteggono le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo unire le nostre forze per prevenire, rilevare e mitigare le minacce affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 11/24.