DESCRIZIONE DELLA SOLUZIONE AKAMAI

Protezione dei carichi di lavoro in AWS con Akamai Guardicore Segmentation

L'impiego delle risorse PaaS in Amazon Web Services (AWS) è in costante crescita e molte aziende stanno migrando i propri carichi di lavoro critici nel cloud pubblico. I vantaggi legati a questa migrazione includono costi ridotti, performance e scalabilità migliorate e un'agilità aziendale molto maggiore. Tuttavia, il passaggio al cloud presuppone anche notevoli rischi per la sicurezza, tra cui:

Nuovo set di strumenti

L'utilizzo di un ambiente cloud richiede un set completamente nuovo di controlli di sicurezza, che devono essere in grado di supportare AWS nel cloud e on-premise (tramite AWS Outposts), nonché nei carichi di lavoro dei cloud ibridi. I gruppi di sicurezza cloud esistenti sono magari sufficienti per gli asset e le risorse disponibili nel cloud AWS, ma non proteggono gli asset e le risorse presenti in altri ambienti. Ne consegue quindi la necessità, da parte del vostro team, di gestire un numero maggiore di strumenti di protezione, che potrebbe generare potenziali lacune nella sicurezza.

Nuovo modello operativo di sicurezza

In linea con il modello di responsabilità condivisa di AWS, l'impiego di risorse AWS nel cloud oppure on-premise significa che Amazon si assume solo la responsabilità di proteggere l'infrastruttura che esegue tutti i servizi offerti nel cloud AWS. Qualsiasi software applicativo o utility installati su quelle istanze, nonché la configurazione dei gruppi di sicurezza, sono di esclusiva responsabilità degli utenti. Ciò include anche la protezione e il monitoraggio del traffico (sia da nord a sud che da est a ovest) e l'implementazione di controlli volti a rilevare, prevenire e rispondere a eventuali violazioni.

Riduzione della visibilità e del controllo dell'infrastruttura

Gli stessi vantaggi che rendono l'ambiente AWS così appetibile sono anche i fattori che possono ridurre il controllo e la visibilità degli asset distribuiti tra molteplici account AWS, cloud privati virtuali (VPC) e gruppi di sicurezza della rete, nonché all'interno del più ampio ecosistema ibrido di un'organizzazione.

Vantaggi principali

- Soluzione end-to-end in grado di proteggere i carichi di lavoro in AWS, incluse le risorse PaaS, consentendo ai team addetti alla sicurezza e DevOps di concentrarsi su attività prioritarie anziché sulla gestione della sicurezza del data center
- Gestione e applicazione delle rigorose policy di microsegmentazione, che si estendono oltre AWS per includere asset che risiedono on-premise e persino su cloud pubblici
- Rilevamento affidabile di violazioni delle policy e risposte in tempo reale
- Protezione degli ambienti da potenziali violazioni mediante diversi metodi di prevenzione e rilevamento delle intrusioni, tra cui l'analisi della reputazione e il rilevamento dinamico in tempo reale

Akamai Guardicore Segmentation per la protezione di AWS

Akamai Guardicore Segmentation fornisce una soluzione unificata che garantisce la massima visibilità e l'applicazione delle policy per i carichi di lavoro e le risorse PaaS in esecuzione nel cloud AWS, negli outpost e negli ambienti ibridi. Fornisce microsegmentazione e visibilità a livello delle applicazioni, nonché funzionalità di individuazione e risposta.

Rilevamento e visibilità automatici

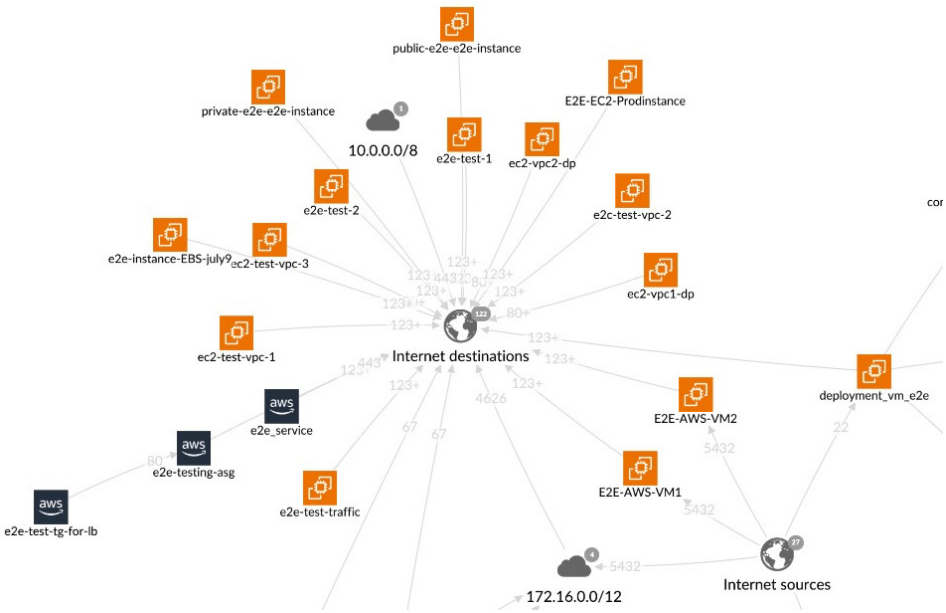
- Visualizzazione automatica di applicazioni, risorse e flussi di comunicazione
- Rapida comprensione e impostazione di uno standard di riferimento per decifrare il comportamento delle applicazioni
- Mappatura delle dipendenze delle applicazioni con visibilità granulare a livello dei processi (livello 7)

Efficacia nella segmentazione e nell'applicazione

- Definizione delle policy di segmentazione in pochi minuti
- Raccomandazioni automatiche sulle policy
- Etichettatura e raggruppamento intelligenti per una navigazione più semplice negli ambienti complessi

Rilevamento delle minacce e risposta agli incidenti

- Nessuna configurazione necessaria; vantaggi sin dal primo giorno
- Molteplici metodi di rilevamento per tutti i tipi di minacce
- Rilevamento dinamico in grado di coprire l'intera rete



Visualizzazione e protezione delle applicazioni e delle risorse in AWS con Akamai Guardicore Segmentation

> Selezionando Akamai Guardicore Segmentation, siamo riusciti a colmare le lacune critiche nella sicurezza in termini di microsegmentazione e visibilità a livello delle applicazioni, nonché di individuazione e risposta alle violazioni, sia per quanto riguarda i server AWS che on-premise.
>
> — **DevOps Team Leader**
> **Azienda di biotecnologia**

Proteggete in modo agevole e rapido i carichi di lavoro e le risorse PaaS in AWS Maggiori informazioni alla pagina akamai.com/guardicore.