DESCRIZIONE DELLA SOLUZIONE AKAMAI

La segmentazione negli ambienti cloud ibridi

Contenere gli attacchi con la segmentazione dell'infrastruttura cloud

Con la crescita del numero di applicazioni e carichi di lavoro trasferiti nel cloud, i team addetti alla sicurezza e al cloud si trovano ad affrontare una serie di sfide sempre maggiore. Una di queste sfide è rappresentata dall'estensione della segmentazione e dei principi Zero Trust alle applicazioni e ai carichi di lavoro trasferiti negli ambienti cloud. Con Akamai Guardicore Segmentation, le organizzazioni possono ridurre le superfici di attacco e contenere gli attacchi sferrati contro le applicazioni e i carichi di lavoro nei loro ambienti sul cloud pubblico senza installare agenti. Questo obiettivo viene raggiunto tramite l'automazione del rilevamento delle applicazioni, una visione completa dei flussi nel cloud, accurate policy di segmentazione e avvisi sulla sicurezza della rete, il tutto da un unico pannello di controllo.

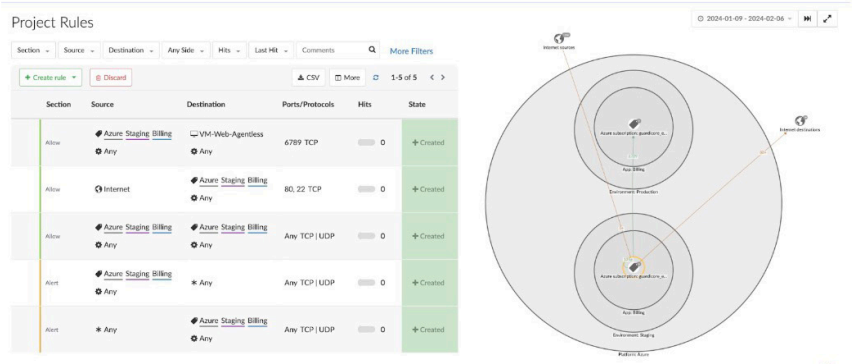
Nuove sfide per il cloud

Le organizzazioni moderne si affidano sempre più al cloud per gestire i sistemi di importanza critica e per archiviare i dati più importanti di cui dispongono.

Secondo un rapporto stilato dalla IBM nel 2023 sui costi di una violazione di dati, l'82% delle violazioni ha interessato i dati archiviati nel cloud (pubblico, privato o entrambi). Con i criminali che spesso sono riusciti ad ottenere l'accesso a più piattaforme cloud, il 39% delle violazioni si è esteso a più ambienti e ha implicato un costo superiore alla media pari a 4,75 milioni di dollari.

La natura unica e dinamica del cloud implica una maggiore esposizione alle minacce esterne dei carichi di lavoro nel cloud rispetto alle risorse on-premise. I team addetti alla sicurezza si trovano, pertanto, ad affrontare nuove sfide di vario tipo:

- **Scarsa visibilità**: la visibilità del provider di servizi cloud si basa sui registri non elaborati dei flussi presenti tra diversi carichi di lavoro. Senza una chiara comprensione delle relazioni esistenti tra i diversi carichi di lavoro e le diverse applicazioni presenti negli ambienti cloud, diventa praticamente impossibile creare policy di sicurezza efficaci.
- **Nessuna singola policy** : creare una policy coerente per gli ambienti cloud ibridi solo con strumenti nativi per la sicurezza nel cloud è estremamente complesso perché ogni istanza nel cloud presenta propri oggetti e proprie regole, quindi proprie policy, il che determina una serie frammentata di policy.
- **Mancanza di una governance unificata**: la sicurezza non è sempre una priorità nel cloud, pertanto, si possono creare problemi tra i team addetti alla sicurezza e i proprietari delle app che accelerano i carichi di lavoro senza prendere sempre in considerazione la sicurezza.



Isolamento di un'applicazione Azure con policy automatizzate

Vantaggi per la vostra azienda

Visione dei flussi nel cloud con una sola interfaccia
Una profonda comprensione del modo con cui i carichi di lavoro e le applicazioni nel cloud interagiscono tra loro grazie ad una mappa dinamica delle dipendenze di rete e una semplice applicazione dei controlli di sicurezza.

Applicazione di policy di segmentazione coerenti
Implementazione di una sola soluzione di segmentazione coerente per tutti gli ambienti cloud ibridi in modo da evitare soluzioni specifiche di un fornitore che creano sistemi di sicurezza compartizzati.

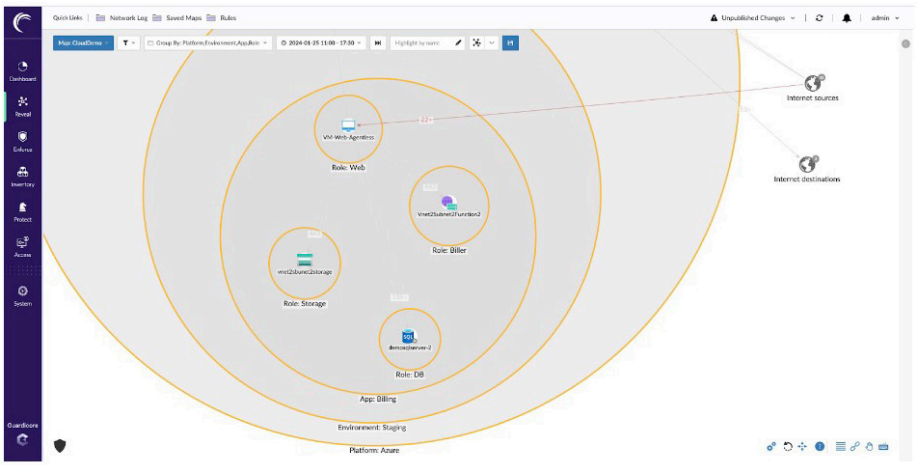
Blocco delle violazioni
Le policy di sicurezza vengono adattate a qualsiasi cambiamento dell'ambiente cloud per evitare al team l'onere di eseguire gli aggiornamenti manuali.

Prevenzione delle minacce alla sicurezza nel cloud

Akamai Guardicore Segmentation estende la sua segmentazione leader del settore alle applicazioni e ai carichi di lavoro nel cloud. Estendendo la segmentazione alle risorse nel cloud, qualsiasi connessione non autorizzata viene fermata automaticamente, limitando così il movimento laterale e i danni causati dalle violazioni o dagli attacchi ransomware.

Funzionalità principali

- **Un livello completo di applicazione e visibilità cloud-native senza agenti** consente agli amministratori di visualizzare i carichi di lavoro nel cloud tramite una mappa interattiva degli effettivi flussi di rete quasi in tempo reale, comprendendo le dipendenze delle applicazioni e riunendo i team DevOps e SecOps nella governance della sicurezza di rete nel cloud.
- **Un motore ibrido con più punti di applicazione** consente ad un'organizzazione di definire in modo semplice l'ambito delle policy di rete, lasciando fare il resto al motore delle policy di Akamai Guardicore Segmentation, decidendo in modo dinamico quali punti di applicazione basati su agenti e senza agenti verranno utilizzati nel data center.
- **Le funzionalità integrate del firewall di intelligence sulle minacce** e di analisi della reputazione sono progettate per ridurre il tempo necessario per il rilevamento e la risposta agli incidenti in caso di violazione.
- **Una soluzione scalabile e sicura** garantisce che i dati non escano dall'ambiente cloud e che l'architettura della soluzione al suo interno sia in grado di scalare automaticamente.



Una sola mappa per gli ambienti on-premise e cloud ibridi

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