DESCRIZIONE DELLA SOLUZIONE AKAMAI

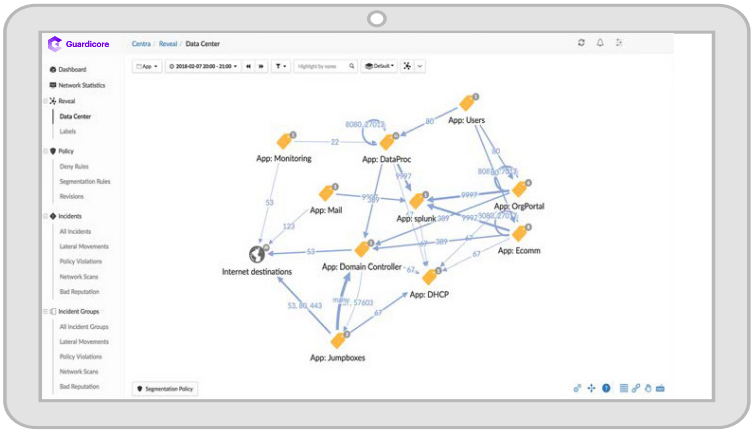
Microsegmentazione rapida in ambienti ibridi con Akamai Guardicore Segmentation

Il percorso per implementare la microsegmentazione non è lineare; il rilevamento, la comprensione e il controllo dei flussi delle applicazioni nel vostro ambiente IT ha numerosi risvolti. Ma senza il giusto approccio a tale percorso, potreste imbattervi in diverse sfide. I punti ciechi della rete spesso impediscono un rilevamento e una mappatura delle comunicazioni sufficienti di applicazioni, carichi di lavoro e processi sottostanti. Motori di policy rigidi possono forzare decisioni radicali, che comportano il rischio di interrompere le applicazioni. Un'espressione di policy incoerente tra i sistemi operativi può causare pericolose lacune di sicurezza. Infine, le integrazioni complesse, e spesso manuali, dei dati sulle violazioni delle policy con gli strumenti di rilevamento delle violazioni possono rallentare l'indagine e la risposta agli incidenti. Akamai Guardicore Segmentation vi aiuta a percorrere con successo il percorso verso la microsegmentazione in tre passaggi.

Fase 1. Rilevamento

Rilevate automaticamente le applicazioni e visualizzate i flussi

Akamai Guardicore Segmentation offre la migliore visibilità del settore che rileva e visualizza automaticamente tutte le applicazioni, i carichi di lavoro e i flussi di comunicazione con contesto a livello di processo, indipendentemente da dove risiedono. Avrete la stessa visibilità per le risorse on-premise, nel cloud, su più cloud e altro ancora. Questa visibilità, unita all'importazione automatica dei metadati di orchestrazione, consente ai team di sicurezza di etichettare e raggruppare rapidamente e facilmente tutte le risorse e le applicazioni, semplificando lo sviluppo delle policy.



Protezione delle applicazioni critiche ovunque

Indipendenza dalla piattaforma

Akamai Guardicore Segmentation è in grado di visualizzare le risorse e applicare policy di sicurezza in tutte le infrastrutture: on-premise, nel cloud e su più cloud

Rapido time-to-policy

Suggerimenti di regole automatizzati, un motore di policy flessibile e un'interfaccia utente intuitiva rendono la creazione e l'applicazione delle policy meno dispendiose in termini di tempo

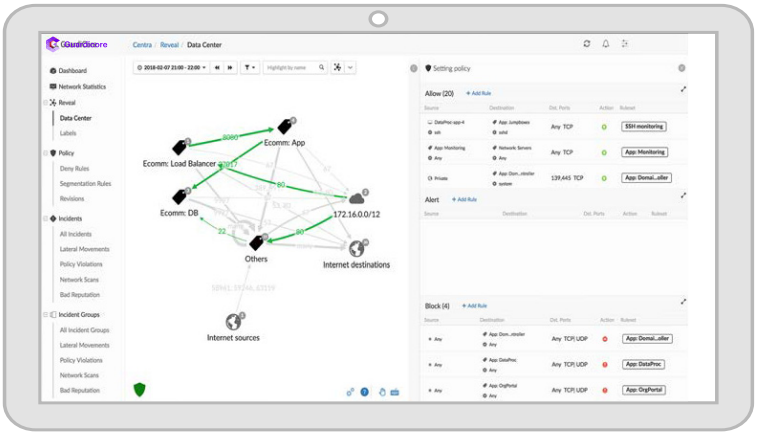
Risposta e rilevamento delle violazioni integrati

Visualizzate le violazioni delle policy e rispondete rapidamente alle minacce attive, proteggendo le vostre risorse più critiche ovunque risiedano

Fase 2. Creazione

Progettate, testate e applicate rapidamente le policy

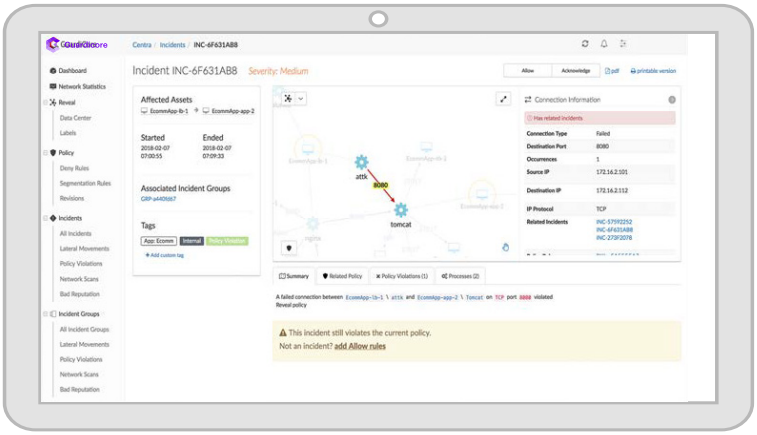
Akamai Guardicore Segmentation semplifica lo sviluppo e la gestione delle policy di microsegmentazione. Un singolo clic su un flusso di comunicazione nella mappa di rilevamento genera suggerimenti di regole automatizzati basati su osservazioni storiche, consentendovi di creare rapidamente una policy efficace. Un workflow intuitivo e un motore di policy flessibile supportano il perfezionamento continuo delle policy e riducono errori costosi.



Fase 3. Applicazione

Garantite una solida sicurezza in qualsiasi ambiente

Grazie alla capacità di applicare policy di comunicazione a livello di rete e di processo su tutti i sistemi, Akamai Guardicore Segmentation mantiene la sicurezza indipendentemente dai limiti di applicazione del sistema operativo. Inoltre, le funzionalità integrate di rilevamento e risposta alle violazioni consentono di visualizzare le violazioni delle policy nel contesto di una violazione attiva, consentendo di identificare rapidamente il metodo di attacco e porvi rimedio.



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

 | Supporto | | Data di pubblicazione: 06/23