DESCRIZIONE DEL PRODOTTO AKAMAI

Segmentazione per IoT e OT

Estendete le funzionalità di segmentazione Zero Trust a tutti i dispositivi connessi

Molte aziende stanno incrementando l'uso dei dispositivi IoT (Internet of Things) e della tecnologia operativa (OT) per promuovere la crescita, migliorare l'efficienza e ottimizzare il servizio offerto ai clienti. Se da un lato queste tecnologie possono offrire molti vantaggi per l'azienda, dall'altro rappresentano un nuovo vettore di attacco critico che i team addetti alla sicurezza devono monitorare. I dispositivi IoT sono particolarmente soggetti a vulnerabilità hardware e software e molti sistemi OT tradizionali non sono stati progettati tenendo conto dei requisiti di sicurezza del mondo connesso. Akamai Guardicore Segmentation estende la sicurezza Zero Trust a questi dispositivi, riducendo il rischio che possano essere utilizzati da utenti malintenzionati per accedere all'infrastruttura IT dell'azienda.

Vantaggi per l'azienda

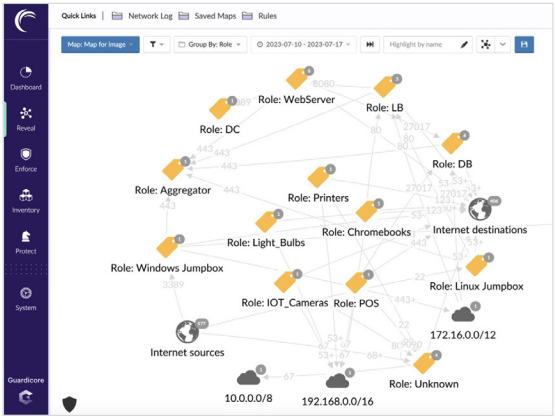
- Individuazione, fingerprinting e classificazione di tutti i dispositivi connessi
- Implementazione di policy di segmentazione Zero Trust da un'unica interfaccia, anche per sistemi IoT e OT specializzati
- Applicazione di policy basate su agenti e senza agenti per garantire una copertura completa

Monitoraggio continuo dei nuovi dispositivi connessi

L'implementazione dei dispositivi IoT e OT è molto diversa rispetto agli endpoint e ad altri dispositivi aziendali tradizionali. In particolare, i dispositivi IoT e OT vengono implementati in quantità molto più elevate e il loro impatto cambia in modo dinamico in base all'evoluzione delle esigenze operative. Akamai Guardicore Segmentation monitora e rileva continuamente tutti i dispositivi IoT e OT connessi. Ciò impedisce ai dispositivi non autorizzati di comunicare e permette di catalogare e proteggere quelli autorizzati.

Identificazione e classificazione di tutti i dispositivi connessi

Akamai Guardicore Segmentation include il fingerprinting integrato dei dispositivi. Il nostro approccio sofisticato va oltre gli identificatori dei dispositivi facilmente falsificabili e analizza il comportamento della rete e altri segnali per sviluppare un'impronta digitale affidabile per ogni dispositivo connesso alla rete. Man mano che vengono identificati, i dispositivi vengono suddivisi in categorie che possono essere utilizzate per creare policy di sicurezza astratte e scalabili.



Visualizzazione centralizzata di tutte le risorse aziendali

I dispositivi IoT e OT individuati e classificati tramite Akamai Guardicore Segmentation vengono visualizzati, insieme agli endpoint aziendali e ai carichi di lavoro delle applicazioni più tradizionali, nella mappa Guardicore Reveal di Akamai, un'interfaccia visiva altamente interattiva. Ciò consente ai team addetti alla sicurezza di comprendere come interagiscono tra loro i vari dispositivi connessi e di sviluppare strategie di segmentazione Zero Trust efficaci che si avvalgono di tecniche di applicazione basate su host e senza agenti.

Applicazione di policy di segmentazione granulare per tutti i dispositivi

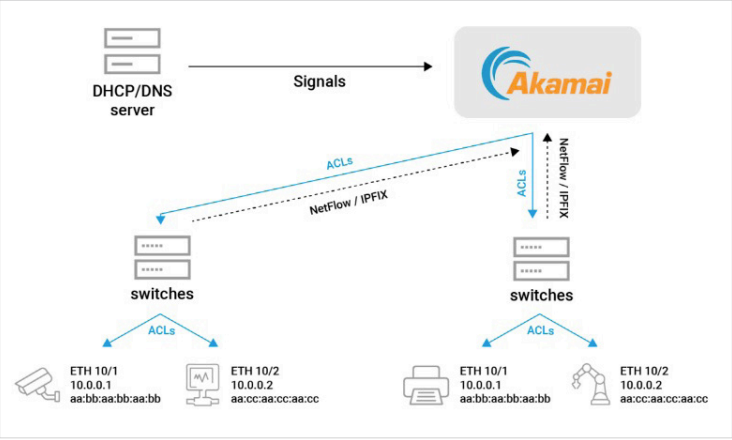
Akamai Guardicore Segmentation estende l'applicazione delle policy Zero Trust offrendo una segmentazione basata sulla rete appositamente progettata per i dispositivi IoT e i sistemi OT che non possono eseguire software di sicurezza basati su host. Ciò permette di controllare e limitare la comunicazione tra dispositivi OT e IoT e con altre risorse di rete e di definire confini sicuri pur mantenendo le connessioni necessarie con i sistemi di gestione IT, i server di aggiornamento dedicati e i server di registrazione.

Visibilità e controllo dei dispositivi ovunque si trovino

L'architettura di Akamai Guardicore Segmentation offre controllo e visibilità costanti, anche in caso di spostamento dei dispositivi all'interno della rete. Ciò garantisce l'applicazione di policy di segmentazione Zero Trust, inclusi eventuali adattamenti in base alla posizione, sempre appropriate.

Come funziona

Il traffico generato dai dispositivi di rete fornisce dei segnali (ad esempio, DHCP, DNS, Netflow, TCP, ecc.) che vengono utilizzati da Akamai Guardicore Segmentation per identificare e classificare tutti i dispositivi. Successivamente, è possibile creare policy di segmentazione tramite un'interfaccia unificata. Per i dispositivi IoT e OT, e per altri dispositivi che non possono eseguire agenti basati su host, le policy di segmentazione vengono applicate attraverso l'implementazione automatizzata delle regole di controllo degli accessi a livello di rete.



Visitate il nostro sito web per ulteriori informazioni sull'estensione di Zero Trust a IoT e OT