DESCRIZIONE DEL PRODOTTO AKAMAI

Akamai Guardicore Access

Funzionalità di microsegmentazione e ZTNA in una soluzione unificata

Un'unica console per la visibilità e il controllo semplifica e accelera l'adozione del modello Zero Trust

Le organizzazioni stanno rapidamente adottando la sicurezza Zero Trust per bloccare i ransomware, soddisfare gli obblighi di conformità e proteggere la loro forza lavoro ibrida insieme all'infrastruttura cloud. Le funzionalità di microsegmentazione e ZTNA (Zero Trust Network Access) sono due delle soluzioni più importanti per le aziende che stanno passando ad un'architettura Zero Trust perché, insieme, possono aiutare a ridurre la superficie di attacco, contenere le violazioni e fornire un maggior controllo degli accessi con user experience migliorate.

La potenza dell'unificazione

Akamai Guardicore Access combina le funzionalità di segmentazione e ZTNA implementate con un unico agente e gestite con un'unica console. Questo approccio innovativo garantisce una visibilità completa dall'utente al carico di lavoro (nord-sud) e da un endpoint o da un carico di lavoro (est-ovest) all'altro per offrire il controllo degli accessi alle applicazioni in base alle identità e la segmentazione degli endpoint in una soluzione unificata. Combinando queste tecnologie, le aziende possono trarre vantaggio da una solida struttura di sicurezza in grado di rafforzare i sistemi di difesa della rete, mitigare i rischi e promuovere un ambiente sicuro e conforme.

Akamai Guardicore è la prima piattaforma di sicurezza che combina l'innovativa soluzione ZTNA (Zero Trust Network Access) con la microsegmentazione per aiutare i team addetti alla sicurezza a prevenire i ransomware, a garantire i requisiti di conformità e a proteggere l'infrastruttura cloud e la forza lavoro ibrida.

Ora, per la prima volta, le organizzazioni possono implementare la segmentazione per minimizzare la propria superficie di attacco gestendo, al contempo e facilmente, l'accesso alla propria forza lavoro ibrida da qualsiasi posizione con un unico agente e un'unica console su tutti i tipi di risorse e infrastrutture.

Funzionalità principali

Visibilità end-to-end
Potete comprendere pienamente la vostra rete con una visibilità end-to-end, che include sia la visualizzazione sulla mappa che nei registri, e fornire preziose informazioni sui modelli di accesso degli utenti finali. Tutto ciò è reso possibile solo combinando le funzionalità di segmentazione e ZTNA in un unico prodotto. Potete visualizzare i percorsi delle connessioni, dagli endpoint ai carichi di lavoro, fino al livello dei processi. La visibilità quasi in tempo reale e storica facilita l'analisi forense e velocizza la mitigazione.

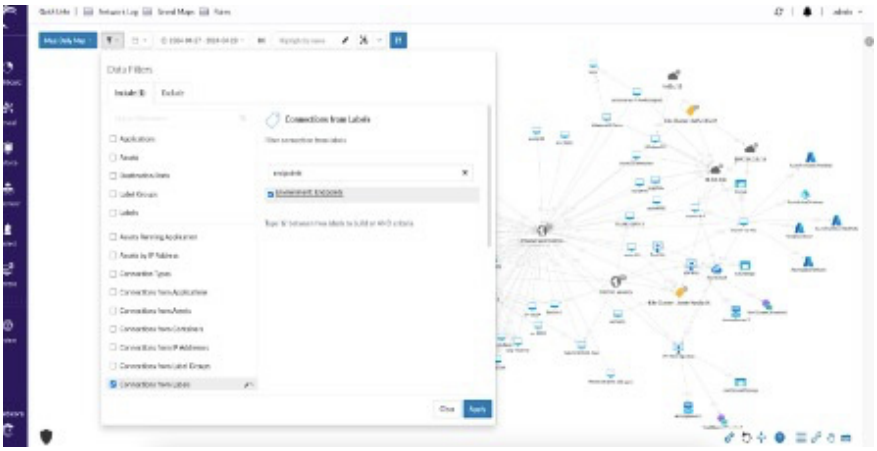
Vantaggi per le aziende

Un'unica console e un unico agente
Implementate la segmentazione per minimizzare la superficie di attacco, gestendo, al contempo e facilmente, l'accesso ad una forza lavoro ibrida da qualsiasi posizione con un unico agente e un'unica console

Ampia copertura
Applicate i controlli degli accessi ovunque e proteggete i dipendenti che lavorano da remoto e in ufficio

Motore di policy unificato
Rafforzate le policy per il traffico est-ovest e l'accesso nord-sud senza cambiare sintassi o console utilizzando la piattaforma Zero Trust nel modo più semplice ed efficace

Individuazione delle applicazioni
Potete ridurre il tempo di implementazione delle policy identificando rapidamente le applicazioni che richiedono le autorizzazioni di accesso. Scoprite facilmente le applicazioni private e ottenete informazioni preziose sui loro modelli di utilizzo, inclusi gli accessi e la frequenza degli utenti.



Facile individuazione delle applicazioni per cui è richiesto l'accesso

Sincronizzazione delle policy di accesso e segmentazione
Sincronizzate automaticamente i controlli degli accessi e le regole di segmentazione per ridurre le dipendenze tra i vari team e per eliminare la possibilità di commettere errori.

Casi di utilizzo principali

Protezione completa dai ransomware: potete ridurre la probabilità e l'impatto dei ransomware e di altri attacchi malware con le policy basate sulle identità e le policy tra computer. Assicuratevi che l'accesso alle risorse da parte degli endpoint sia basato sul principio del privilegio minimo e che vengano applicati, al contempo, i controlli granulari degli accessi.

- Protezione delle risorse più importanti: consentite agli utenti di accedere alle risorse critiche con controlli degli accessi sicuri e bloccate il traffico VPN diretto
- Limitate il numero di utenti con privilegi: bloccate il traffico VPN sulle porte di amministrazione vulnerabili per fornire un accesso sicuro agli amministratori

Distribuzione della forza lavoro: supportate il lavoro eseguito da qualsiasi posizione applicando rigorosi controlli degli accessi per garantire che ciascun dispositivo possa connettersi solo alle risorse necessarie. In tal modo, sarà possibile minimizzare la superficie di attacco e ridurre il movimento laterale all'interno della rete.

Compliance: implementate la segmentazione degli endpoint per consentire alle aziende di garantire che i loro endpoint siano conformi alle normative e agli standard di settore pertinenti allo scopo di ridurre il rischio di sanzioni per mancata conformità e di rafforzare il sistema di sicurezza complessivo.

Accesso di terze parti: consentite a collaboratori e partner di connettersi a specifiche applicazioni senza installare un agente instradando e autenticando il loro accesso tramite un portale dedicato di Akamai.

Per ulteriori informazioni, visitate la pagina dedicata alla sicurezza Zero Trust di Akamai