DESCRIZIONE DELLA SOLUZIONE AKAMAI

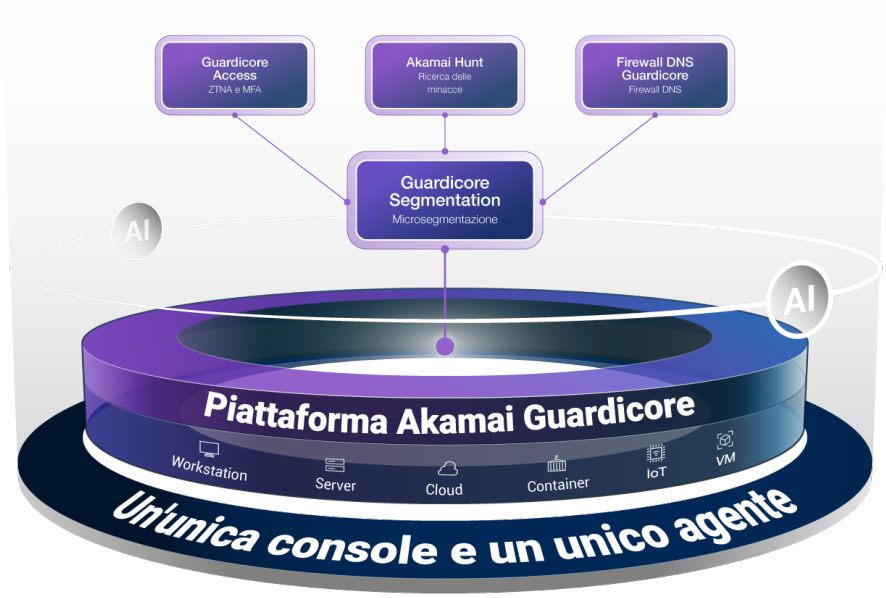
La piattaforma Akamai Guardicore per la sicurezza Zero Trust

L'implementazione del modello Zero Trust è complessa e costosa in modo proibitivo per la maggior parte delle aziende, specialmente se i sistemi di protezione devono coprire le risorse on-premise e nel cloud e se i dipendenti lavorano da remoto o in ufficio. Ecco perché la piattaforma Akamai Guardicore è progettata per soddisfare in modo efficiente tutti gli aspetti del modello Zero Trust con un'unica console e un unico agente.

Poiché le minacce informatiche diventano sempre più sofisticate e i requisiti normativi continuano ad inasprirsi, le organizzazioni si trovano ad affrontare un'enorme pressione per proteggere le loro reti, mantenendo, al contempo, l'efficienza operativa. La piattaforma Akamai Guardicore offre una soluzione Zero Trust completa nell'intento di affrontare queste sfide fornendo alle organizzazioni le funzionalità e gli strumenti necessari per implementare un affidabile modello di sicurezza Zero Trust in modo efficace.

La piattaforma Akamai Guardicore è progettata per supportare i progetti Zero Trust combinando le migliori soluzioni di microsegmentazione, ZTNA (Zero Trust Network Access), firewall DNS e ricerca delle minacce in un unico prodotto. Insieme, questi componenti semplificano le iniziative Zero Trust per ridurre notevolmente la superficie di attacco e rafforzare il sistema di sicurezza in tutta l'azienda.

La piattaforma Akamai Guardicore



Microsegmentazione

Uno dei componenti principali della piattaforma Akamai Guardicore è rappresentato dalla microsegmentazione. Tradizionalmente, la sicurezza della rete si è affidata a sistemi di difesa basati sul perimetro che si sono focalizzati sulla protezione dei confini esterni della rete stessa. Tuttavia, con l'evoluzione delle minacce informatiche, è diventato sempre più chiaro che i sistemi di difesa basati sul perimetro non sono più sufficienti per proteggere la rete da attacchi sofisticati.

Vantaggi

Infrastruttura consolidata
Rapida implementazione e semplice scalabilità con un impatto minimo sulle performance.

Visibilità ampia e completa
Informazioni complete sulle risorse di rete e sulle comunicazioni.

Motore di policy unificato
Semplificate l'applicazione delle policy nei vari ambienti utilizzando una sola interfaccia utente.

Flessibilità modulare
Utilizzate i componenti modulari personalizzati in base alle vostre alle esigenze aziendali.

Copertura completa
Proteggete tutte le vostre risorse on-premise e nel cloud e gli utenti che lavorano da casa e in ufficio.

Soluzioni innovative
Combinate le funzionalità di microsegmentazione e ZTNA leader del settore per migliorare il sistema di sicurezza.

Akamai

La microsegmentazione adotta un approccio diverso dividendo la rete in segmenti più piccoli e facilmente gestibili e applicando policy di sicurezza a ciascun segmento in base al principio del privilegio minimo. Questo approccio granulare alla sicurezza garantisce che, anche se un segmento viene compromesso, il resto della rete rimane protetto. Con Akamai Guardicore Segmentation, ogni risorsa è protetta, inclusi data center on-premise, istanze cloud, sistemi operativi legacy, dispositivi IoT, cluster Kubernetes e molto altro, senza dover neanche cambiare le console.

Zero Trust Network Access

Oltre alla microsegmentazione, la piattaforma Akamai Guardicore offre anche funzionalità ZTNA (Zero Trust Network Access). Il sistema ZTNA è un modello di sicurezza basato sul principio Zero Trust, secondo cui nessun utente o dispositivo deve essere considerato automaticamente attendibile, anche se si trova all'interno della rete aziendale. Al contrario, l'accesso alle risorse viene concesso in base ad una rigorosa verifica delle identità, del comportamento dei dispositivi e di altri fattori contestuali. Questo approccio riduce al minimo il rischio di accessi non autorizzati e aiuta le organizzazioni a prevenire violazioni di dati e minacce interne.

Firewall DNS

Un altro componente essenziale della piattaforma Akamai Guardicore è rappresentato dal firewall DNS. Il DNS (Domain Name System) è un componente fondamentale di Internet, che traduce nomi di dominio leggibili in indirizzi IP, ma è anche un bersaglio comune per gli attacchi informatici, poiché molte varianti di malware si basano sul DNS per comunicare con i server C2 (Command and Control) o per esfiltrare i dati. Implementando un firewall DNS, le organizzazioni possono bloccare le query DNS dannose e impedire ai malware di comunicare con domini dannosi, riducendo così il rischio di violazioni di dati e altre minacce informatiche.

Ricerca delle minacce

Infine, la piattaforma Akamai Guardicore include un servizio di segmentazione adattiva che consente alle organizzazioni di identificare e mitigare in modo proattivo le minacce alla sicurezza prima che si trasformino in incidenti conclamati. La ricerca delle minacce implica la ricerca attiva di segnali di violazione all'interno della rete, come comportamenti anomali o indicatori di compromissione (IoC). Sfruttando strumenti e tecniche di ricerca delle minacce, le organizzazioni possono stare un passo avanti rispetto ai criminali informatici e proteggere le loro preziose risorse da eventuali danni.

Oltre alle sue funzionalità principali, la piattaforma Akamai Guardicore offre anche numerosi vantaggi chiave che la distinguono dalle altre soluzioni per la sicurezza disponibili sul mercato. La piattaforma fornisce un'infrastruttura agile e consolidata che riduce al minimo lo stress degli agenti e il sovraccarico della console, consentendo alle organizzazioni di implementare e gestire il proprio sistema di sicurezza in modo più efficiente. Inoltre, la piattaforma offre una visibilità ampia e completa sulle risorse di rete e sulle comunicazioni, consentendo agli addetti alla sicurezza di ottenere informazioni complete sul proprio ambiente di rete e di rispondere alle minacce in modo rapido ed efficace.

> Nel rapporto Gartner®, Quick Answer: What Is Zero Trust Networking? di Andrew Lerner e John Watts del 13 settembre 2023, Gartner suggerisce di implementare le funzionalità di microsegmentazione e/o ZTNA per passare ad un sistema ZTN (Zero Trust Networking).*

*GARTNER è un marchio commerciale e un marchio di servizio di Gartner, Inc. e/o delle sue società affiliate, registrato negli Stati Uniti e a livello internazionale e usato previa autorizzazione. Tutti i diritti riservati.

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