

Akamai Guardicore DNS Firewall

Il massimo livello di controllo e visibilità sul traffico DNS dei carichi di lavoro

Il DNS (Domain Name System) è essenziale per i servizi Internet, tuttavia non riesce a distinguere le richieste legittime da quelle dannose. Di conseguenza, le aziende hanno implementato soluzioni di firewall DNS per esaminare le query DNS, bloccare i domini dannosi e risolvere le richieste sicure. Tuttavia, poiché l'utilizzo del DNS si estende per includere carichi di lavoro, server e altri dispositivi connessi, la mancanza di visibilità e controllo su questo traffico DNS introduce ulteriori rischi per la sicurezza.

Segmentazione unificata e firewall DNS





Insieme, le soluzioni Akamai Guardicore Segmentation e Akamai Guardicore DNS Firewall forniscono una solida difesa per la vostra rete. Bloccando le richieste DNS dannose e isolando i segmenti di rete più importanti, questa integrazione riduce notevolmente la vostra superficie di attacco e impedisce la diffusione delle minacce. Questo duplice approccio migliora la sicurezza, garantisce la conformità e mantiene elevata l'efficienza operativa, rendendolo la scelta ideale per garantire una solida protezione della rete.

Come funziona Akamai Guardicore DNS Firewall

Potete attivare la soluzione di sicurezza Akamai Guardicore DNS Firewall in pochi minuti in modo semplice e sicuro senza influire sulle performance. Poiché ogni dominio richiesto viene verificato a fronte dell'intelligence sulle minacce in tempo reale di Akamai, le richieste a domini dannosi vengono automaticamente bloccate. L'utilizzo del DNS come livello di sicurezza iniziale blocca in modo proattivo le minacce nelle fasi iniziali della kill chain prima di stabilire qualsiasi connessione IP. Inoltre, il DNS è progettato in modo da agire praticamente su tutte le porte e su tutti i protocolli, garantendo persino la protezione dal malware che non utilizza i protocolli e le porte web standard.

Quando una richiesta DNS viene bloccata, si crea un incidente che fornisce ai team addetti alla sicurezza e alla ricerca delle minacce informazioni approfondite sul motivo per cui la minaccia è stata bloccata, sull'origine e sulla destinazione della richiesta da poter visualizzare su una mappa, nonché dettagli accurati sugli indicatori di compromissione.

Vantaggi per la vostra azienda

-  **Protezione completa dalle minacce**
Filtrando il traffico DNS al perimetro della rete e rafforzando la microsegmentazione all'interno della rete, le aziende possono difendersi in modo efficace da malware, phishing, attacchi C2 (Command and Control) e tentativi di esfiltrazione dei dati.
-  **Maggiore efficacia nella ricerca delle minacce**
Gli incidenti aiutano i team addetti alla sicurezza a rilevare, analizzare e rispondere meglio alle minacce emergenti, minimizzando l'impatto delle violazioni e rafforzando i sistemi di cybersicurezza nel complesso.
-  **Miglior livello di visibilità e controllo**
Una soluzione combinata di firewall DNS e funzionalità di microsegmentazione offre una maggiore visibilità sui modelli del traffico DNS per identificare potenziali minacce e violazioni delle policy.
-  **Gestione semplificata**
L'integrazione di un firewall DNS con le funzionalità di microsegmentazione semplifica la gestione della sicurezza fornendo un sistema unificato per la creazione, l'applicazione e il monitoraggio delle policy. In tal modo, si riducono la complessità e i costi operativi, consentendo alle aziende di gestire in modo efficiente la propria infrastruttura di sicurezza.

Akamai Cloud Security Intelligence

Akamai Guardicore DNS Firewall si basa sulla soluzione Akamai Cloud Security Intelligence, che offre un'intelligence in tempo reale sulle minacce e sui rischi che tali minacce comportano. L'intelligence sulle minacce di Akamai è progettata per proteggere dai pericoli attuali e pertinenti, che potrebbero influenzare negativamente l'azienda, ma anche per ridurre al minimo il numero di avvisi di falsi positivi da far approfondire ai propri team addetti alla sicurezza. Questa intelligence si basa sui dati raccolti ogni giorno dall'Akamai Connected Cloud, che gestisce fino al 30% del traffico web globale e distribuisce ogni giorno fino a 14 trilioni di query DNS. L'intelligence di Akamai è migliorata grazie a centinaia di feed delle minacce esterne e i dataset, così combinati, vengono continuamente analizzati e trattati con avanzate tecniche di analisi comportamentale, funzioni di intelligenza artificiale e algoritmi proprietari. Non appena identificate, le nuove minacce vengono immediatamente aggiunte al dataset dell'intelligence sulle minacce per fornire una protezione in tempo reale.

Akamai Connected Cloud

Il servizio Akamai Guardicore DNS Firewall si basa sull'Akamai Connected Cloud, la piattaforma più distribuita al mondo per il cloud computing, la sicurezza e la delivery dei contenuti. La piattaforma Akamai Connected Cloud offre un accordo sul livello di servizio che prevede una disponibilità del 100% e garantisce un'affidabilità ottimale per la sicurezza del DNS dell'azienda.

Per ulteriori informazioni, visitate la pagina dedicata alla [sicurezza Zero Trust di Akamai](#).