

DESCRIZIONE DEL PRODOTTO AKAMAI

Secure Internet Access Enterprise: il firewall DNS basato sul cloud

Poiché le organizzazioni si servono di Direct Internet Access, applicazioni SaaS (Software-as-a-Service), servizi cloud, policy per il telelavoro e l'IoT (Internet of Things), la loro superficie di attacco aumenta notevolmente, portandole a dover affrontare una serie di nuove sfide per la sicurezza. Pertanto, diventa sempre più difficile proteggere aziende e utenti da minacce mirate e avanzate, come i malware, i ransomware, il phishing e l'esfiltrazione dei dati. È necessario gestire le complicazioni e le complessità relative ai punti di controllo per la sicurezza, ma anche le lacune nella sicurezza delle soluzioni tradizionali già esistenti in sede.

Akamai Secure Internet Access Enterprise è un firewall DNS (Domain Name System) basato sul cloud che permette ai team addetti alla sicurezza di offrire a utenti e dispositivi una connessione sicura a Internet ovunque, senza la complessità e i costi di gestione associati alle altre soluzioni di sicurezza tradizionali. Secure Internet Access Enterprise è una soluzione che si avvale dell'intelligence sulle minacce in tempo reale aggiornata grazie alle preziose informazioni globali raccolte da Akamai sul traffico DNS e Internet.

Secure Internet Access Enterprise

Basato sulla soluzione globale Akamai Connected Cloud e sul servizio DNS ricorsivo carrier-grade di Akamai, Secure Internet Access Enterprise è un firewall DNS basato sul cloud, semplice da distribuire e rapido da configurare, che non richiede hardware da installare e mantenere.

Secure Internet Access Enterprise sfrutta l'Akamai Cloud Security Intelligence in tempo reale per identificare e bloccare in modo proattivo minacce mirate come malware, ransomware, phishing ed esfiltrazione di dati basata sul DNS a bassa velocità.

Il portale Akamai consente ai team addetti alla sicurezza di creare, distribuire e applicare, in modo centralizzato e in pochi minuti, sia le policy di sicurezza unificate che le policy di utilizzo (AUP) per tutti gli utenti, da qualunque punto siano connessi a Internet.

VANTAGGI PER LA VOSTRA AZIENDA



Spostamento della sicurezza web sul cloud con un firewall DNS basato sul cloud che può essere configurato e distribuito globalmente in pochi minuti (senza interruzioni per gli utenti) e scalato rapidamente



Potenziamento delle difese di sicurezza bloccando in modo proattivo le richieste indirizzate a siti che diffondono malware e ransomware, siti di phishing, server C2 (Command and Control) relativi al malware ed esfiltrazione dei dati DNS a bassa velocità, che si basano su un'intelligence delle minacce esclusiva e aggiornata



Controllo dell'utilizzo di applicazioni IT nascoste e non autorizzate tramite l'identificazione e il blocco delle applicazioni in base alle categorie o ai punteggi di rischio



Minimizzazione dei tempi e della complessità di gestione della sicurezza riducendo gli avvisi di sicurezza di falsi positivi, diminuendo quelli provenienti da altri prodotti di sicurezza e gestendo le policy e gli aggiornamenti di sicurezza da qualunque luogo e in pochi secondi, al fine di proteggere tutte le sedi



Come funziona

Secure Internet Access Enterprise è un servizio di sicurezza basato sul cloud che può essere attivato in pochi minuti per offrire sicurezza e ridurre la complessità, senza influire sulle performance. È possibile fornire questo sistema di protezione indirizzando il traffico DNS ricorsivo alla soluzione Secure Internet Access Enterprise mediante una vasta gamma di diversi metodi, inclusi i tunnel IPsec, un client agile, il server d'inoltro DNS gestito da Akamai o una modifica del resolver DNS esistente.

Poiché ogni dominio richiesto viene verificato a fronte dell'intelligence sulle minacce in tempo reale di Akamai, le richieste a domini identificati come 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 e prima di stabilire qualsiasi connessione Internet. Inoltre, il DNS è progettato in modo da agire su tutte le porte e su tutti i protocolli, garantendo la protezione dal malware che non utilizza protocolli e porte web standard. È possibile verificare i domini anche per stabilire il tipo di contenuti a cui tenta di accedere un utente ed eventualmente bloccare i domini se i contenuti rappresentano una violazione dell'AUP dell'organizzazione.

Per un'ulteriore protezione, è possibile inoltrare i domini rischiosi ad un proxy basato su cloud per consentire di esaminare gli URL: gli URL HTTP/S richiesti vengono verificati a fronte dell'intelligence sulle minacce in tempo reale di Akamai e gli URL dannosi vengono automaticamente bloccati.

Secure Internet Access Enterprise si integra senza problemi con altri prodotti di sicurezza e strumenti per la creazione di rapporti, tra cui firewall e soluzioni SIEM (Security Information and Event Management), nonché feed di intelligence delle minacce esterne, per consentirvi di ottimizzare gli investimenti in tutti i livelli dello stack di sicurezza dell'azienda.

Inoltre, l'implementazione dell'agile client Secure Internet Access Enterprise sui dispositivi consente alle organizzazioni di proteggere in modo rapido e semplice i laptop o i dispositivi mobili utilizzati al di fuori della rete.

Akamai Cloud Security Intelligence

Secure Internet Access Enterprise si basa sull'Akamai Cloud Security Intelligence, una soluzione che offre intelligence in tempo reale sulle minacce e sui rischi che tali minacce comportano.

L'intelligence sulle minacce di Akamai è progettata per fornire protezione dalle minacce 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 11 trilioni di query DNS. L'intelligence di Akamai è migliorata grazie a centinaia di feed delle minacce esterne e i set di dati, così combinati, vengono continuamente analizzati e trattati con avanzate tecniche di analisi comportamentale, funzioni di apprendimento automatico e algoritmi proprietari. A mano a mano che vengono identificate nuove minacce, queste vengono immediatamente aggiunte al servizio Secure Internet Access Enterprise, garantendo protezione in tempo reale.

Akamai Connected Cloud

Il servizio Secure Internet Access Enterprise si basa sull'Akamai Connected Cloud, la piattaforma più distribuita al mondo per il cloud computing, la sicurezza e la delivery dei contenuti. Akamai Connected Cloud offre una disponibilità totale coperta da SLA (accordo sul livello di servizio) e un'affidabilità ottimale per la sicurezza web dell'azienda.

VANTAGGI PER LA VOSTRA AZIENDA



Riduzione dei rischi e maggiore sicurezza per i dispositivi al di fuori della rete senza utilizzo di VPN grazie all'agile client Secure Internet Access Enterprise, che applica le policy di sicurezza e utilizzo



Applicazione rapida e uniforme della conformità e delle policy di utilizzo bloccando l'accesso a categorie di contenuti e domini inappropriati o discutibili



Incremento della resilienza e dell'affidabilità con Akamai Connected Cloud e la piattaforma DNS carrier-grade di Akamai

Portale di gestione basato sul cloud

Le attività di configurazione e gestione continua di Secure Internet Access Enterprise vengono eseguite tramite il portale Akamai Control Center basato su cloud, rendendo possibile la gestione in qualsiasi luogo e momento.

La gestione delle policy è semplice e veloce e le modifiche possono essere inoltrate a livello globale in pochi minuti per garantire la protezione di tutte le sedi e di tutti gli utenti. Gli avvisi in tempo reale tramite e-mail e i rapporti programmati possono essere configurati per avvisare i team addetti alla sicurezza degli eventi critici relativi alle policy, affinché sia possibile intervenire per identificare e risolvere le potenziali minacce. Un dashboard in tempo reale fornisce una panoramica del traffico, delle minacce e degli eventi correlati alle policy di utilizzo. Le informazioni dettagliate sulle attività possono essere visualizzate tramite un'analisi approfondita dei singoli elementi del dashboard. Queste informazioni dettagliate costituiscono un'importante risorsa per l'analisi e la correzione degli incidenti relativi alla sicurezza.

Tutte le funzionalità del portale sono accessibili tramite API e i registri di dati possono essere esportati in un SIEM, consentendo così a Secure Internet Access Enterprise di integrarsi in modo semplice ed efficace con gli altri strumenti per la creazione di rapporti e con altre soluzioni di sicurezza.

Funzioni

Sicurezza
Blocco di malware, ransomware e URL/domini di delivery di phishing
Blocco delle richieste C2 relative ai malware
Identificazione dell'esfiltrazione dei dati basata sul DNS
Domini per proxy dannosi per l'ispezione degli URL HTTP e HTTPS richiesti
Creazione di un elenco personalizzato di domini per l'ispezione di URL HTTP e HTTPS
Esecuzione di analisi look-back dei registri del traffico di clienti per identificare e avvisare in caso vengano rilevate nuove minacce
Creazione di elenchi personalizzati di tipo Consenti/Rifiuta
Integrazione di altri feed di intelligence sulle minacce
Personalizzazione delle pagine di errore
Interrogazione del database di minacce di Akamai per accedere all'intelligence sui domini e sugli URL dannosi
Applicazione della sicurezza per dispositivi al di fuori della rete (Windows, macOS, iOS, Android, Chrome)
Policy di utilizzo (AUP, Acceptable Use Policy)
Creazione di policy di utilizzo basate su gruppi
Monitoraggio o blocco delle violazioni AUP per utenti all'interno e all'esterno della rete
Applicazione della SafeSearch su Google, Bing e YouTube

Cloud Access Security Broker (online)
Identificazione e blocco delle applicazioni IT nascoste
Blocco delle applicazioni sui punteggi di rischio o sul gruppo di applicazioni
Applicazione del tenant SaaS
Generazione di rapporti, monitoraggio e amministrazione
Integrazione IDP e Active Directory
Visualizzazione a livello aziendale di tutte le attività con dashboard personalizzabili
Analisi dettagliata di tutte le minacce ed eventi AUP
Log completi e visibilità per tutte le richieste di traffico pubblicato, nonché per gli eventi di minacce e AUP
Delivery di tutti i registri; i registri vengono conservati per 30 giorni ed è possibile esportarli tramite un'API
Configurazione, elenchi di sicurezza personalizzati ed eventi disponibili tramite un'API
Integrazione con altri sistemi di sicurezza, come SIEM, tramite un'API
Avvisi di sicurezza in tempo reale basati su e-mail
Pianificazione di rapporti giornalieri o settimanali ricevuti tramite e-mail
Amministrazione delegata
Piattaforma Akamai Connected Cloud
VIP IPv4 e IPv6 dedicati per ogni cliente per DNS ricorsivo
SLA per il 100% di disponibilità
Routing DNS Anycast per performance ottimali
DNSSEC, DoH e DoT applicati per una maggiore sicurezza
Attribuzione dei dispositivi aziendali
Attribuzione online tramite il server d'inoltro DNS
Attribuzione offline tramite Security Connector
Attribuzione basata su client per laptop e dispositivi mobili (Windows, macOS, iOS, Android, Chrome)

Per maggiori informazioni su Secure Internet Access Enterprise e per accedere a una prova gratuita, [visitare il sito akamai.com/it](https://akamai.com/it).