ENTERPRISE DEFENDER

Sicurezza Zero Trust a livello di edge

Il perimetro della rete difendibile non esiste più, almeno non in una forma riconoscibile. L'utilizzo di un approccio alla sicurezza e all'accesso che aveva senso 20 anni fa, nell'ambiente odierno è, nella migliore delle ipotesi, fuori posto e, nella peggiore, pericoloso. E non si tratta solo di una teoria. Ciò risulta evidente dalla quantità e dalla portata delle violazioni di dati a cui abbiamo assistito negli ultimi cinque anni, la maggior parte delle quali si è verificata in seguito ad un abuso di fiducia all'interno del perimetro di rete. È il momento di adottare una sicurezza Zero Trust, in cui la fiducia nella rete aziendale non è più intrinseca e le decisioni relative alla sicurezza e all'accesso vengono applicate dinamicamente in base alle identità, ai dispositivi e al contesto dell'utente.

ENTERPRISE DEFENDER

Basato sull'Akamai Intelligent Edge Platform, Enterprise Defender affianca a un sistema di prevenzione dei malware un modello di accesso alle applicazioni adattivo e funzioni di sicurezza e accelerazione, il tutto integrato in un servizio dedicato e facile da utilizzare sull'edge. Enterprise Defender consente alle organizzazioni di passare a un sistema di sicurezza Zero Trust senza ricorrere a dispositivi hardware o apparecchiature. È sufficiente effettuare la sottoscrizione a Enterprise Defender per ridurre i rischi e la complessità, migliorando, nel contempo, la user experience.

COME FUNZIONA

Enterprise Defender sfrutta l'Akamai Intelligent Edge Platform per proteggere tutte le applicazioni e gli utenti aziendali, offrendo una sicurezza ottimale e riducendo la complessità senza influire sulle performance. Vi consente di proteggere l'accesso alle applicazioni da voi controllate, mitigando i rischi associati all'accesso degli utenti alle applicazioni che esulano dal vostro controllo.

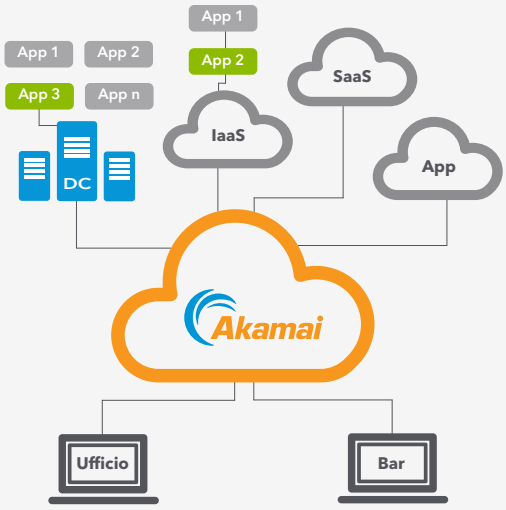
Enterprise Defender include le seguenti funzionalità in un servizio di sottoscrizione mensile, per singolo utente, di facile utilizzo:

Prevenzione dei malware: Akamai consente di identificare, bloccare e mitigare in maniera proattiva minacce mirate come malware, ransomware, phishing ed esfiltrazione di dati che sfruttano il DNS e attacchi zero-day avanzati. Akamai offre un SIG (Secure Internet Gateway) che permette ai team addetti alla sicurezza di offrire a utenti e dispositivi una connessione sicura a Internet e alle applicazioni non controllate ovunque, senza la complessità associata ai sistemi tradizionali.

Accesso alle applicazioni: Akamai assicura che solo gli utenti e i dispositivi autorizzati possano accedere alle applicazioni interne di cui necessitano e non all'intera rete aziendale. Nessuno può accedere direttamente alle applicazioni poiché queste non sono esposte né in Internet né pubblicamente. Enterprise Defender integra funzioni di protezione del percorso dati, SSO (Single Sign-On), identità, accesso alle applicazioni, nonché visibilità e controllo della gestione, il tutto in un solo servizio.

WAF (Web Application Firewall): Akamai offre un'ampia protezione per le applicazioni web di importanza critica dagli attacchi DDoS e web più vasti e sofisticati. Il nostro WAF include solide protezioni di sicurezza per i siti web, aggiornate dal miglior team di ricerca delle minacce del settore, per aiutare le organizzazioni a restare al passo con la costante evoluzione delle minacce alla sicurezza.

Accelerazione delle applicazioni: Akamai consente alle aziende di fornire applicazioni rapide, affidabili e sicure in modo conveniente. Ciò consente alle aziende di superare le sfide correlate alla fornitura di applicazioni aziendali tramite Internet, collocando le funzionalità di delivery delle applicazioni all'interno dell'Akamai Intelligent Edge Platform, molto vicino agli utenti, al cloud e ai carichi di lavoro in sede, ovunque nel mondo.



Accesso alle applicazioni, accelerazione e controlli di sicurezza sull'edge

Chiusura della rete aziendale agli utenti

Accesso SSO (Single Sign-On) e autenticazione multifattore per le applicazioni aziendali

Blocco dell'accesso a domini, URL e contenuti dannosi, ovunque

ENTERPRISE DEFENDER

VANTAGGI PER IL BUSINESS

- **Arresto della propagazione dei malware e del movimento laterale**
  Nelle tradizionali reti perimetrali, in genere i malware penetrano in profondità a causa della mancanza di segmentazione e di una scarsa visibilità della rete. Con Enterprise Defender, la combinazione di controlli degli accessi più granulari per specifiche applicazioni unita alla prevenzione proattiva delle minacce rende più complicata la propagazione per i malware o l'accesso ad altri carichi di lavoro per gli utenti malintenzionati.

- **Riduzione della complessità e ottimizzazione delle operazioni**
  Le soluzioni per la sicurezza sul cloud, come Enterprise Defender, consentono ai team di sostituire le apparecchiature virtuali o hardware costose in termini di gestione e manutenzione con un semplice servizio di sicurezza sull'edge.

- **Riduzione di CapEx e OpEx per la sicurezza**
  Il miglioramento della sicurezza è inevitabilmente associato a un aumento dei costi. Con Enterprise Defender, non è generalmente così; al contrario, una migliore sicurezza combinata con la semplicità basata sul cloud consente ai CISO e ai team addetti alla sicurezza di consolidare più controlli di sicurezza diversificati e ridurre i costi di gestione.

- **Aumento della visibilità e riduzione dei tempi di rilevamento delle violazioni**
  A proposito delle violazioni, spesso, viene riferito che "gli utenti malintenzionati non sono stati rilevati per *tot* mesi" e che "una volta superato il perimetro, gli utenti malintenzionati sono stati in grado di muoversi liberamente all'interno della rete". Con Enterprise Defender, la combinazione di una registrazione degli accessi alle applicazioni più granulare con controlli di sicurezza basati sul DNS offre una maggiore visibilità e accelera i tempi di rilevamento delle violazioni.

- **Interruzione dell'esfiltrazione dei dati interni**
  Consentire che i dati finiscano nelle mani di utenti malintenzionati può avere gravi conseguenze per un'azienda, come sanzioni per non aver garantito una protezione sufficiente dei dati personali oppure la perdita di ricavi causata dal furto di proprietà intellettuale o piani strategici. Enterprise Defender consente di interrompere l'esfiltrazione dei dati interni con controlli degli accessi adattivi basati sul principio del "privilegio minimo" e sistemi di visibilità e sicurezza basati sul DNS.

- **Promuovere la trasformazione aziendale digitale**
  I team addetti all'IT e alla sicurezza possono collaborare nel processo di trasformazione digitale. Con la sicurezza basata sul perimetro, questi team si sono guadagnati la reputazione di custodi "paranoici", poiché, una volta consentito l'accesso al perimetro aziendale a supporto di un nuovo modello di servizio cloud, partner o clienti, aprivano una porta o un collegamento all'intera rete aziendale. Con Enterprise Defender, non è più così, poiché l'accesso viene concesso solo a un numero limitato di applicazioni, in base all'identità e al contesto di sicurezza, senza mai consentire l'accesso all'intera rete. Inoltre, questa soluzione consente di promuovere una moderna cultura aziendale basata sulla possibilità di lavorare ovunque, bloccando l'accesso a domini, URL e contenuti dannosi, sia che gli utenti si trovino in ufficio o al bar.