DESCRIZIONE DELLA SOLUZIONE AKAMAI

Akamai Enterprise Application Access con Secure Enterprise Browser

Le soluzioni SSE (Secure Service Edge) tradizionali promettono una sicurezza completa, ma, spesso, determinano una protezione frammentata, una complessità operativa e problemi che ostacolano la produttività degli utenti. Le organizzazioni si trovano a gestire grandi sistemi di policy e colli di bottiglia nelle performance del proxy, mentre, nel contempo, devono cercare di garantire un'efficace protezione dalle sofisticate minacce basate sul web.

Akamai Enterprise Application Access con Secure Enterprise Browser

La combinazione di Akamai Enterprise Application Access e Secure Enterprise Browser con tecnologia Seraphic consente l'utilizzo della soluzione SSE nei casi di utilizzo più importanti (accesso sicuro alle applicazioni, sicurezza web e protezione dei dati) con un approccio mirato e performante. Questa combinazione fornisce il modello ZTNA (Zero Trust Network Access) per le applicazioni aziendali private insieme ad un'avanzata sicurezza del browser per le applicazioni SaaS e l'accesso a Internet, offrendo una solida protezione senza le lacune difensive delle piattaforme tradizionali.

Focalizzandosi sui requisiti di sicurezza fondamentali anziché tentare di soddisfare tutte le esigenze di tutti gli utenti, questa soluzione fornisce performance eccellenti, ridotte complessità e un minor costo totale di proprietà.

Caratteristiche e funzionalità principali

Accesso sicuro (ZTNA per le applicazioni private)

- **Controllo degli accessi alle applicazioni private**, che sostituisce l'ampio accesso alla rete con autorizzazioni granulari e basate sulle identità per le applicazioni aziendali.
- **Applicazione dinamica delle policy** basata sulle identità degli utenti, sul comportamento dei dispositivi e sulla valutazione dei rischi in tempo reale.
- **Integrazione con il provider dei servizi di identità** per supportare i sistemi delle identità aziendali esistenti per un semplice accesso alle applicazioni private.
- **Prevenzione della perdita di dati** con analisi dei contenuti in tempo reale e applicazione delle policy per le applicazioni private.
- **Supporto delle applicazioni private multicloud** per un accesso sicuro alle applicazioni interne presenti negli ambienti ibridi e cloud native.

Vantaggi per le aziende

Migliori risultati con soluzioni SSE mirate che risultano eccellenti in applicazioni specifiche anziché scendere a compromessi in più domini di sicurezza, fornendo performance di livello superiore per l'accesso alle applicazioni, la sicurezza del browser e le moderne sfide legate alla protezione dei dati per i dispositivi gestiti o meno.

Controllo della condivisione dei dati tramite gli strumenti dell'AI generativa con una visibilità in tempo reale e un'applicazione delle policy dei dati per ChatGPT, Copilot e piattaforme simili per favorire la produttività degli utenti, proteggendo, al contempo, la proprietà intellettuale nel rispetto dei requisiti di conformità.

Accelerazione del time-to-value con semplici operazioni di implementazione e gestione rispetto alle implementazioni complete delle soluzioni SSE, focalizzandosi, nel contempo, sui principali casi di utilizzo che favoriscono la maggior parte dei progetti SSE, tra cui i nuovi requisiti di governance.

Minimizzazione dei problemi per gli utenti tramite l'utilizzo di un browser esistente anziché forzarli ad adattarsi a nuove interfacce, browser specializzati o performance delle applicazioni peggiorate che sono comuni con le piattaforme SSE tradizionali.

Riduzione della complessità e dei costi delle soluzioni SSE fornendo funzionalità di accesso sicuro e sicurezza web tramite un'architettura semplificata che elimina la necessità di una licenza completa per la piattaforma SSE o un'ampia gamma di servizi professionali e la complessità di una gestione continua.

- **Accesso senza client e con client** per supportare diversi casi degli utenti senza la complessità della VPN.
- **Delivery ottimizzata in base alle performance** tramite l'infrastruttura sull'edge globale di Akamai.

Sicurezza web e protezione dei dati (accesso alle soluzioni SaaS e Internet)

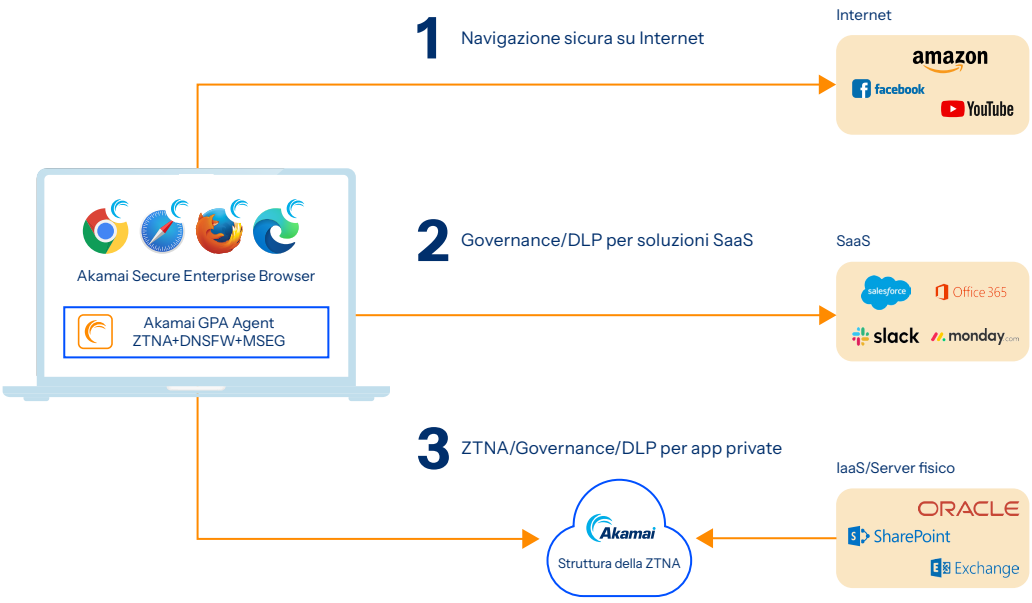
- **Controllo degli accessi alle applicazioni SaaS** con applicazione delle policy basata sul comportamento dei dispositivi per le applicazioni cloud.
- **Prevenzione avanzata delle minacce** per fermare gli exploit zero-day e i sofisticati attacchi basati sul web e incentrati sulle identità con un rilevamento tempestivo.
- **Prevenzione completa della perdita di dati** con analisi dei contenuti in tempo reale, mascheramento dei dati sensibili e applicazione delle policy nelle applicazioni SaaS, nella navigazione web e nei modelli LLM basati sull'AI.
- **Sicurezza indipendente dal browser**, che trasforma qualsiasi browser in un browser sicuro di livello aziendale per l'accesso a Internet e alle soluzioni SaaS.
- **Protezione a livello di sessione**, inclusa la sicurezza delle identità e la gestione delle sessioni crittografate.
- **Sicurezza delle applicazioni SaaS** per estendere la protezione ai moderni strumenti di collaborazione come Slack, Teams e altre applicazioni cloud.

Funzionalità di sostituzione delle soluzioni SSE

- **Protezione SaaS e web diretta**, che elimina la necessità di soluzioni CASB separate.
- **Prevenzione integrata delle minacce**, che sostituisce la funzionalità SWG (Secure Web Gateway).
- **Sicurezza nativa del browser**, che offre i vantaggi derivanti dall'isolamento del browser remoto senza aumentare i costi legati alle performance.

Architettura SSE semplificata

Anziché implementare una piattaforma SSE rigida, questa soluzione offre i risultati garantiti dalle soluzioni SSE tramite due componenti ottimizzati che interagiscono perfettamente tra loro.



Sicurezza della rete fornita sull'edge: l'accesso Zero Trust alle applicazioni aziendali private, che viene fornito dall'Akamai Connected Cloud, elimina le falle nella sicurezza della rete che vengono gestite dalle soluzioni SSE, fornendo, nel contempo, eccellenti performance tramite i PoP (Point-of-Presence) distribuiti a livello globale. In tal modo, vengono sostituiti i componenti SWG (Secure Web Gateway) e ZTNA delle soluzioni SSE tradizionali per l'accesso alle applicazioni interne.

Protezione dei dati a livello del browser: l'avanzata sicurezza del browser fornisce una protezione completa per le applicazioni SaaS e l'accesso a Internet, offrendo un'eccellente prevenzione della perdita di dati e una sicurezza web direttamente nel punto di interazione degli utenti. Proteggendo il browser, in cui gli utenti accedono sia alle applicazioni SaaS autorizzate che ai contenuti generici su Internet, questo approccio elimina la necessità delle soluzioni CASB, SWG e RBI tradizionali, fornendo, nel contempo, un miglior livello di performance e user experience.

Questa architettura fornisce i componenti fondamentali delle soluzioni SSE (accesso sicuro, protezione web e sicurezza dei dati), eliminando, al contempo, le comuni sfide legate a queste soluzioni, come il backhaul del traffico, il peggioramento delle performance e la complessa gestione delle policy.

Per ulteriori informazioni su Akamai Enterprise Application Access e Secure Enterprise Browser con tecnologia Seraphic, potete contattare il vostro rappresentante Akamai o inviare un'e-mail all'indirizzo sales@akamai.com.