E-book

I principali casi d'uso della protezione dei dati con il Security Service Edge

Come bloccare le violazioni dei dati nel mondo aziendale moderno con il servizio SSE di Zscaler

Contenuti

E-book

L'ascesa del modello SSE

Un tempo, gli utenti e le applicazioni delle organizzazioni erano tutti on-premise, e per questo veniva adottato un approccio alla sicurezza "a castello e fossato", in cui apparecchi costosi creavano perimetri di rete per proteggere i dati al loro interno.

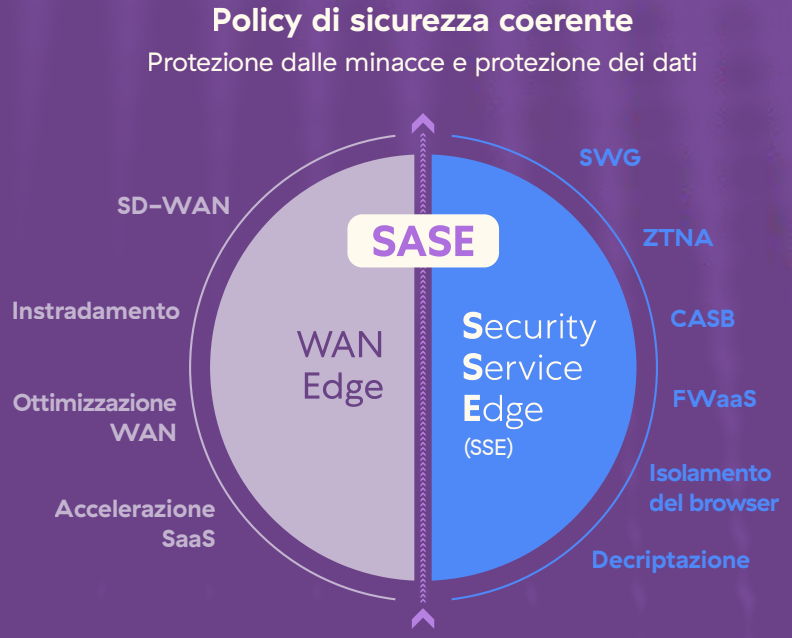
Con il cloud, il web e il lavoro da remoto, il castello è scomparso, ma molti continuano comunque ad affidarsi ad architetture di questo tipo. Purtroppo, le esigenze di protezione dei dati non possono essere soddisfatte con complessi set di dispositivi; inoltre, il backhauling del traffico riduce le prestazioni, limita la scalabilità e ostacola la produttività degli utenti.

Tuttavia, anche molti strumenti moderni di protezione dei dati risultano inefficaci, in particolare quelli che si concentrano sulle minacce interne e trascurano le minacce provenienti dall'esterno. Per una sicurezza dei dati efficace, è dunque fondamentale disporre di un sistema di sicurezza solido.

Il **Security Service Edge (SSE)** è la soluzione a queste sfide. Si tratta di piattaforme complete che riducono la complessità e colmano le lacune nella protezione dati integrando CASB, SWG, ZTNA e altre soluzioni. Con la sicurezza cloud fornita all'edge, il Security Service Edge offre prestazioni, scalabilità ed esperienza utente ottimali.

Zero Trust Exchange™ di Zscaler è il security cloud più grande del mondo, ed è una soluzione che è stata progettata per difendere qualsiasi transazione molto prima dell'introduzione dell'SSE, e che protegge i dati da tutti i rischi interni ed esterni.

Continua a leggere per scoprire i casi d'uso della protezione dei dati che i nostri clienti affrontano con la nostra soluzione SSE.



Ottenere la sicurezza zero trust

Gli strumenti di sicurezza legacy estendono l'accesso senza restrizioni all'intera rete (e a tutti i dati e le app al suo interno). In questo modo si favorisce il movimento laterale delle minacce tra le risorse, che può aumentare esponenzialmente gli effetti di una violazione dei dati. Viola inoltre il principio dei privilegi minimi dello zero trust, secondo cui gli utenti autorizzati ottengono solo l'accesso alla risorsa di cui hanno bisogno, nel momento in cui ne hanno bisogno.

Zero Trust Exchange

Zero Trust Exchange adotta un approccio radicalmente diverso e offre una protezione dati moderna e zero trust. Agendo da centralino intelligente tra utenti, app SaaS, app private, IoT/OT e altro ancora, Zscaler estende l'accesso sicuro solo alle singole risorse e applica contemporaneamente misure di prevenzione della perdita di dati (DLP), per offrire maggiore granularità.

Il vantaggio di Zscaler

- Nasconde tutte le risorse IT dietro a Zero Trust Exchange per eliminare la superficie di attacco
- Previene il movimento laterale delle minacce, collegando gli utenti direttamente alle app, non alla rete
- Blocca la compromissione proteggendo tutte le transazioni da utente ad applicazione, da applicazione ad applicazione e da computer a computer

Prevenire la perdita di dati attraverso il traffico criptato

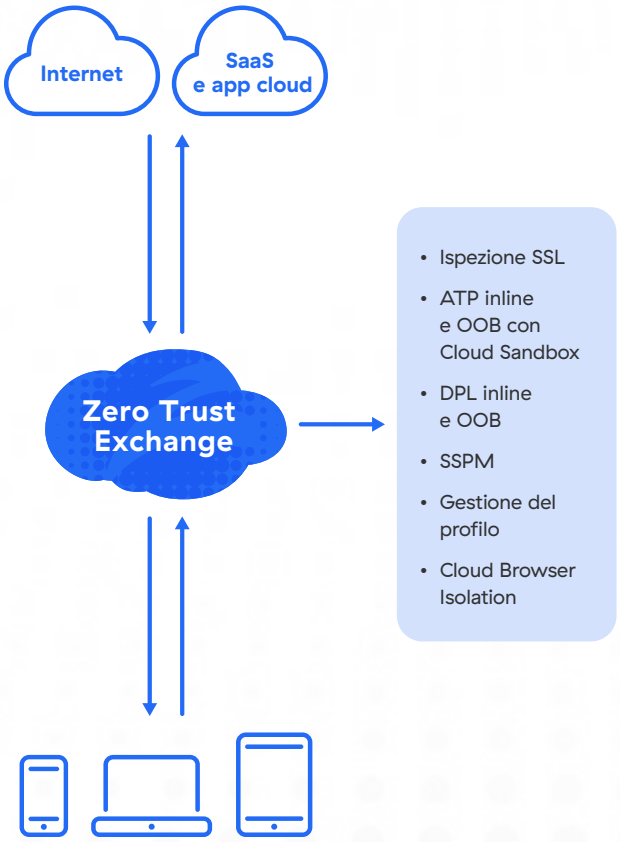
Spesso, per ispezionare il traffico web e prevenire la perdita di dati, vengono impiegati apparecchi di sicurezza legacy (sia hardware che virtuali). Tuttavia, tali apparecchi hanno capacità fisse, non sono in grado di gestire il traffico criptato su larga scala e, di conseguenza, forniscono una funzione di ispezione SSL minima o del tutto inesistente. La percentuale di traffico web criptato ormai è pari al 95%, e questa mancanza può rivelarsi molto pericolosa.

Una vera architettura cloud

Costruito sul security cloud più grande del mondo, il servizio SSE di Zscaler offre le prestazioni necessarie per ispezionare tutto il traffico criptato e soddisfare le esigenze delle aziende globali con centinaia di migliaia di utenti. Questo assicura che qualsiasi potenziale perdita di dati nascosta nel traffico SSL venga rilevata e risolta in tempo reale.

Il vantaggio di Zscaler

- Un servizio SSE con scalabilità e prestazioni senza eguali, che elabora oltre 200 miliardi di transazioni al giorno
- Una piattaforma costruita su un'architettura inline collaudata, utilizzata da oltre il 25% delle aziende Forbes Global 2000
- Un'impronta globale di oltre 150 data center, che applicano la sicurezza all'edge per un'esperienza utente d'eccellenza



Bloccare i ransomware a doppia estorsione

Oltre a criptare il dispositivo, i ransomware a doppia estorsione rubano i dati e ne minacciano la divulgazione, a meno che non venga pagato un riscatto. Queste minacce colpiscono obiettivi deboli (come i dati inattivi non protetti e le app non configurate in modo corretto) per duplicare ed esfiltrare i dati. Purtroppo, nel mondo cloud first in cui viviamo, gli apparecchi di sicurezza legacy non sono in grado di prevenire questo problema.

Protezione completa dalle minacce e protezione dei dati

Zscaler fornisce una protezione completa contro le minacce, per bloccare i ransomware in caricamento e inattivi in tutto l'ecosistema IT. Inoltre, DLP e CASB esaminano tutti i canali dei dati nel cloud per bloccare l'esfiltrazione, mentre la funzione di gestione del profilo e l'SSPM individuano gli errori di configurazione delle app cloud che espongono i dati.

Il vantaggio di Zscaler

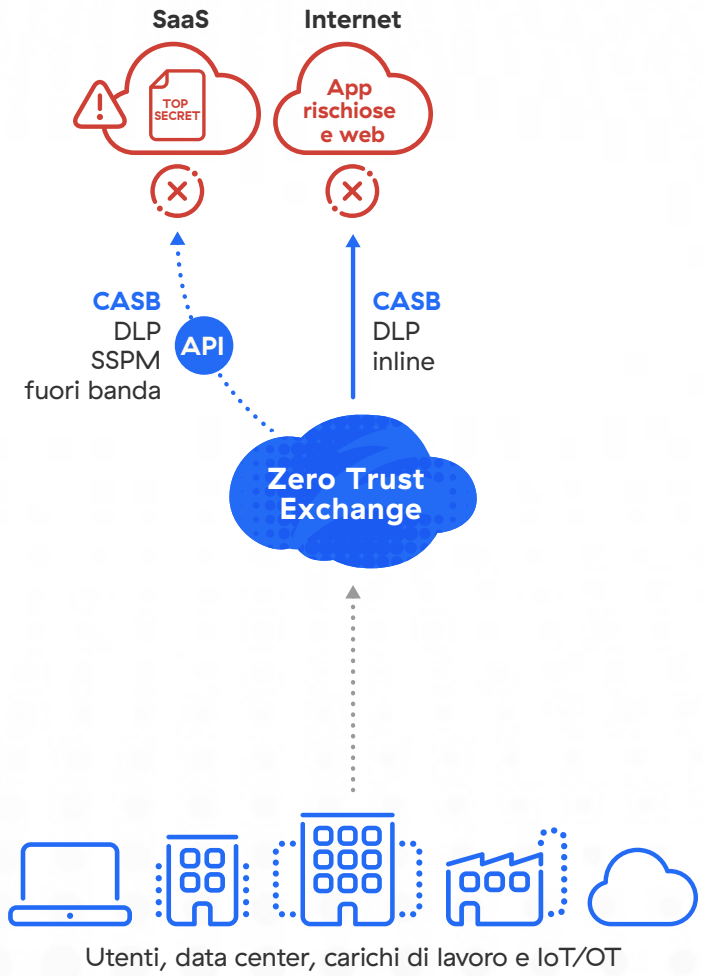
- Ispezione SSL completa e scalabile per identificare in tempo reale l'esfiltrazione dei dati e i ransomware in transito
- Tecnologia di sandboxing sul cloud per fermare i ransomware O-day sia inline che fuori banda
- La potenza del security cloud più grande del mondo: le minacce individuate vengono bloccate ovunque

Proteggere le applicazioni SaaS

Le app SaaS offrono una produttività e flessibilità senza precedenti, ma possono facilmente portare alla perdita di dati se non vengono protette adeguatamente. Ciò è dovuto al fatto che gli utenti caricano continuamente dati su app non autorizzate, i file inattivi possono essere facilmente condivisi con parti non autorizzate e gli errori di configurazione possono compromettere il profilo di sicurezza delle app ed esporre i dati.

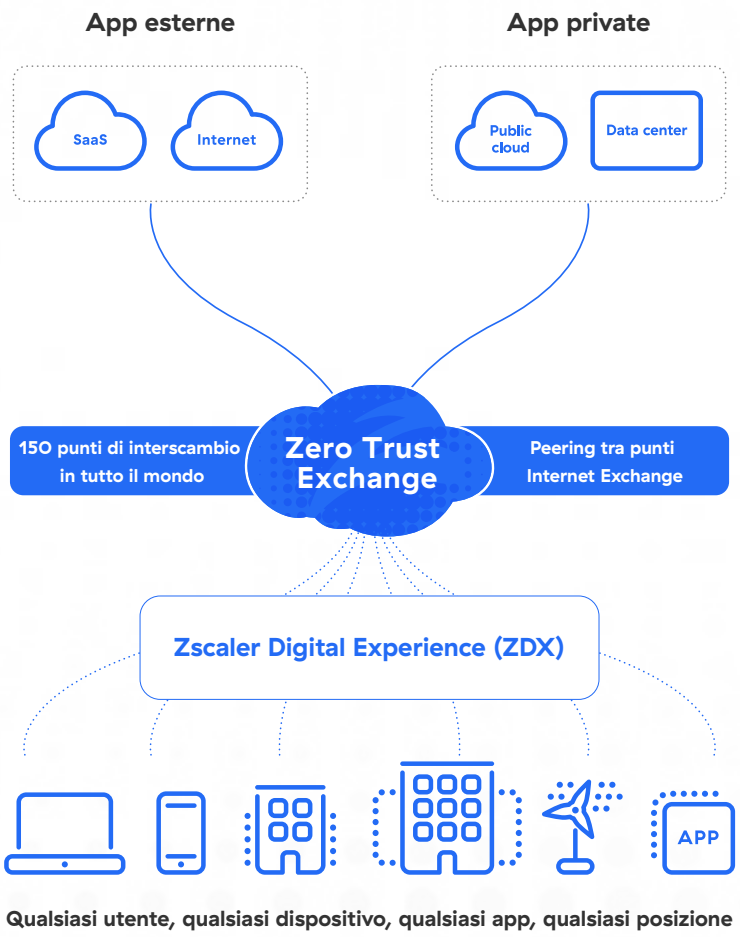
CASB con DLP

Zscaler mette in sicurezza le app SaaS individuando automaticamente lo shadow IT, monitorando il caricamento dei dati nelle app cloud non autorizzate e proteggendo i dati inattivi nelle app cloud autorizzate. Inoltre, la gestione del profilo di sicurezza SaaS esegue la scansione delle app alla ricerca di errori di configurazione che potrebbero esporre i dati o compromettere la conformità.



Il vantaggio di Zscaler

- Una protezione unificata dei dati, che protegge in modo uniforme tutti i canali di dati su SaaS e sul cloud con un'unica policy
- Funzionalità CASB ad alte prestazioni offerte con il servizio SSE più collaudato e integrato
- Soluzione Cloud DLP completa, con funzionalità avanzate come Exact Data Match (EDM) e Optical Character Recognition (OCR), per proteggere valori specifici e immagini



Difendere i dati degli utenti in remoto

Il lavoro da remoto ormai fa parte delle nostre vite, ma la sicurezza legacy non è stata progettata per questo nuovo modo di lavorare. Utilizzando le VPN ed effettuando il backhauling del traffico verso gli apparecchi di sicurezza, si ottiene una scalabilità insufficiente, la produttività degli utenti viene danneggiata e non si risolvono le moderne sfide di protezione dei dati che le aziende cloud first si trovano ad affrontare.

La sicurezza cloud fornita all'edge

Con il security cloud più grande e collaudato del mondo, Zscaler offre la scalabilità e le competenze necessarie per tutelare i dati e supportare il lavoro da remoto in tutto il mondo. Zscaler è in grado di mettere in sicurezza SaaS, IaaS, PaaS, e le app web e private senza effettuare il backhauling del traffico verso appliance e garantendo al contempo una protezione globale dei dati con il massimo delle prestazioni.

Il vantaggio di Zscaler

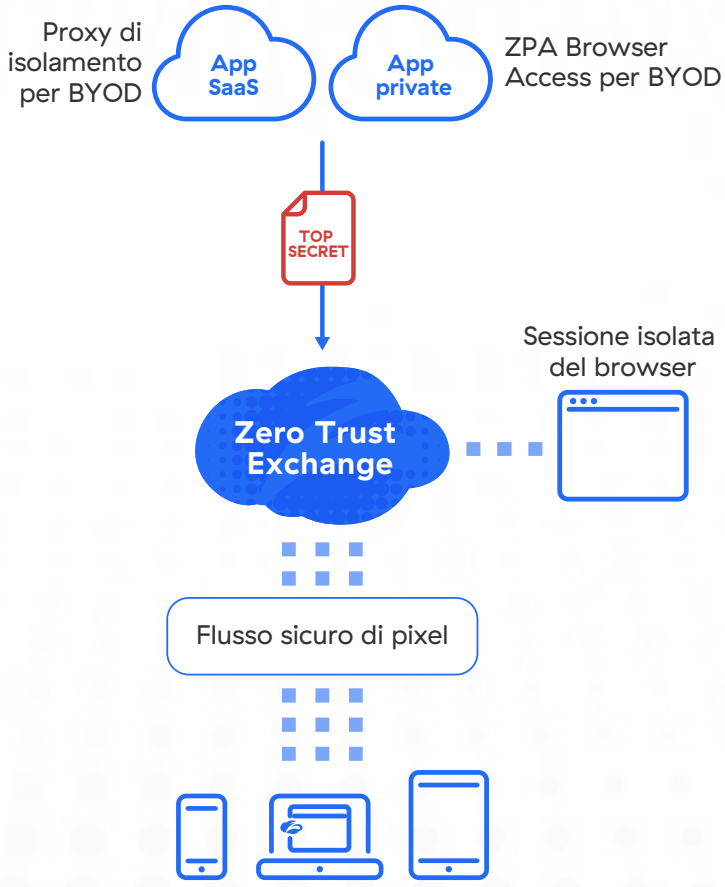
- Un security cloud globale con oltre 150 data center per una protezione dei dati con prestazioni elevate all'edge
- Una soluzione di sicurezza come servizio elimina la necessità di eseguire il backhauling su hardware e apparecchi virtuali
- Un'architettura single-pass, con CASB, SWG, ZTNA e molto altro, offre una protezione efficiente e completa, in ogni luogo

Proteggere i dispositivi personali e altri dispositivi non gestiti

Spesso endpoint non aziendali o non gestiti, come i dispositivi personali (anche detti BYOD, Bring Your Own Device) e B2B, hanno bisogno di accedere alle app aziendali. Tuttavia, una volta che i dati vengono scaricati al loro interno, l'IT ne perde il controllo. Bloccare questi dispositivi significa interrompere la produttività, le installazioni di agenti software sono spesso impossibili e i proxy inversi si guastano frequentemente. Alla luce di tutto questo, cosa dovrebbe fare l'IT?

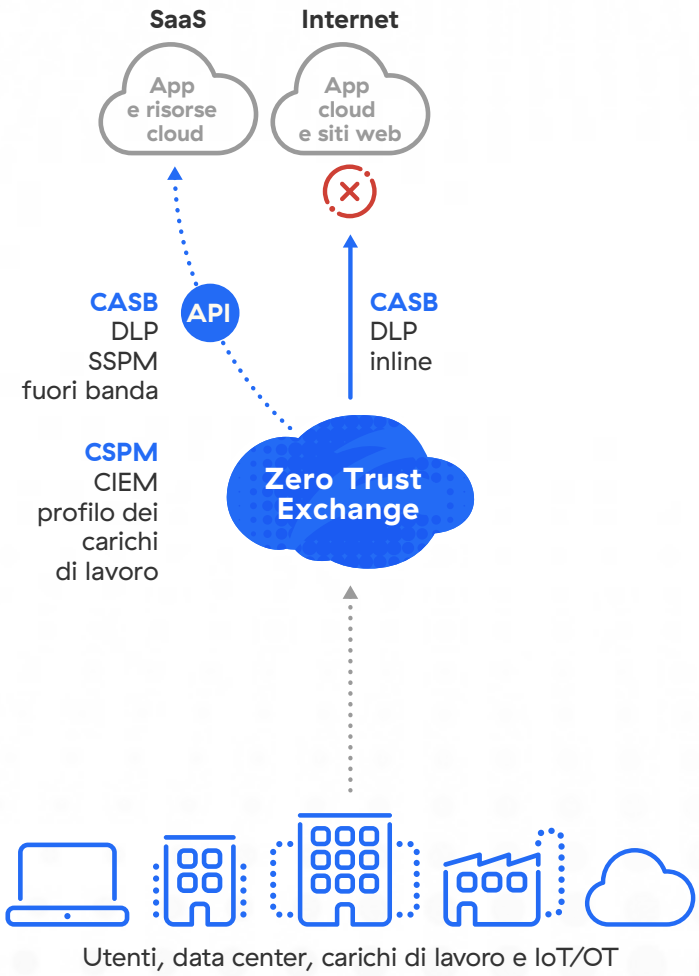
Isolamento del browser su cloud

Grazie all'isolamento del browser senza agente, Zscaler virtualizza una sessione dell'app di un utente in un ambiente isolato e trasmette all'endpoint solo i pixel, impedendo così il download, il copia e incolla e la stampa dei dati. Questo significa che l'IT può abilitare l'accesso ai dispositivi non gestiti mantenendo al contempo i dati al sicuro e aggirando le problematiche relative ad agenti e proxy inversi. Impedisce inoltre il caricamento di file infetti da endpoint a rischio.



Il vantaggio di Zscaler

- Cloud Browser Isolation, basato sul security cloud più grande del mondo e con le prestazioni più elevate
- Isolation Proxy per la sicurezza senza agente sui dispositivi che accedono alle app SaaS
- ZPA Browser Access per un accesso sicuro alle app private senza l'installazione di software lato client



Garantire la conformità alle normative

I dati regolamentati da RGPD, HIPAA e altre normative, insieme al resto delle informazioni sensibili, si stanno spostando al di fuori delle sedi aziendali, ma gli strumenti legacy non sono in grado di proteggerli e preservare la conformità sul cloud. Questo aspetto è cruciale, dato che il mancato rispetto delle leggi sulla privacy, come il CCPA, e di framework come il PCI DSS, può portare a sanzioni, alla perdita di fiducia da parte dei consumatori e alla perdita di fatturato.

Massima garanzia di conformità

Abbiamo creato il Security Service Edge di Zscaler tenendo in considerazione la necessità di garantire la conformità alle normative. Questa soluzione offre visibilità e controllo completi in tutto l'ecosistema IT, per garantire che i dati regolamentati rimangano al sicuro, che le applicazioni non contengano vulnerabilità pericolose per la conformità e che i principi dello zero trust siano applicati ovunque.

Il vantaggio di Zscaler

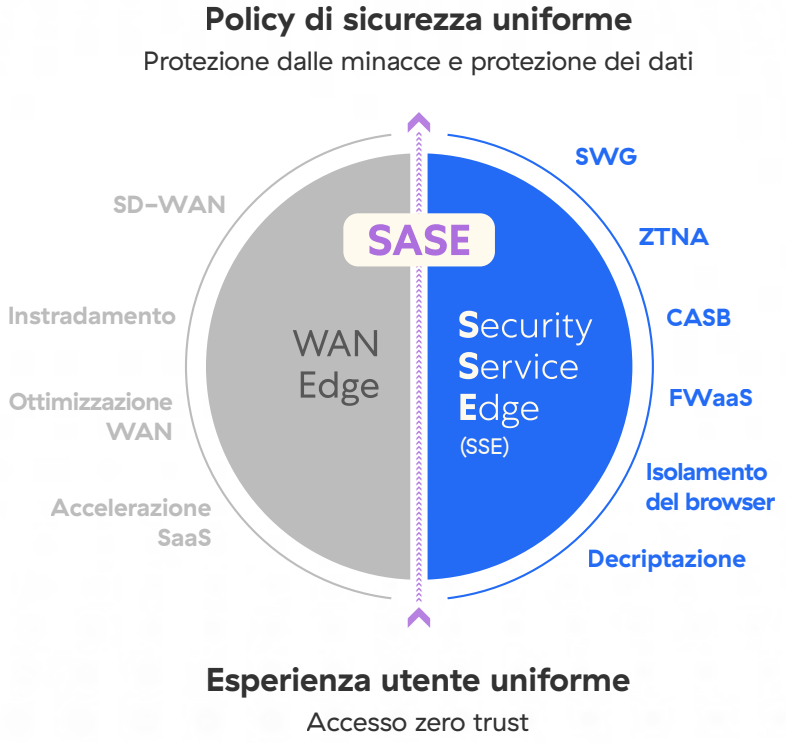
- Cloud DLP con funzionalità CASB multimodale che protegge i dati regolamentati in movimento e quelli inattivi
- La conformità è garantita: Zscaler non scarica i dati per l'ispezione, neanche per misure come l'EDM
- Zscaler SSPM e la funzionalità di gestione del profilo, per individuare e correggere gli errori di configurazione e le autorizzazioni che portano alla mancanza di conformità

Ottenere una protezione dati uniforme e gestibile

Affidarsi a un insieme di prodotti diversi, in cui ognuno ha diverse funzioni, porta a varie difficoltà. In particolare, si genera una protezione dei dati incoerente su un ecosistema IT sempre più complesso. Inoltre, per gli amministratori, gestire questa miriade di soluzioni isolate si rivela un compito gravoso.

Una piattaforma unificata

La soluzione SSE di Zscaler integra tecnologie all'avanguardia che consentono di proteggere qualsiasi transazione e difendere tutti i dati ovunque e in modo uniforme. Grazie a una soluzione cloud completa, con un'architettura unificata, l'azienda è inoltre in grado di ridurre la complessità IT e alleggerire il carico di gestione per gli amministratori.



Il vantaggio di Zscaler

- Misure di protezione dati uniformi per tutte le applicazioni SaaS, cloud, web e private
- Semplificazione dell'architettura che riduce il numero di prodotti e di appliance
- Facilità di gestione consolidata, che evita la duplicazione delle policy e consente agli amministratori di risparmiare tempo

Il cloud e la mobilità offrono innumerevoli vantaggi per la produttività e la flessibilità, ma per approfittare di questi benefici senza compromettere la sicurezza dei dati, è necessario adottare un nuovo approccio alla sicurezza informatica. Il servizio SSE di Zscaler permette all'azienda di intraprendere il percorso di trasformazione digitale e di proteggere i dati, ovunque essi siano.

- **Scopri cosa dicono i clienti del Security Service Edge do Zscaler**
- **Leggi il Magic Quadrant per il Security Service Edge**

zscaler™ | **Experience your world, secured.™**

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zero Trust Exchange di Zscaler protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata sul SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it