



3 passaggi per un SSE vincente

Una semplice guida per proteggere la forza
lavoro ovunque

Sommario

4 Il punto di partenza: perché scegliere l'SSE?

5 Gli elementi dell'SSE

5 Best practice per il successo con l'SSE

6 Fase 1: pianificazione

6 Fase 2: esecuzione

7 Fase 3: revisione

8 Sfruttare il successo dell'SSE

9 Ulteriori informazioni alla pagina



In un mondo IT in cui le risorse aziendali sono suddivise tra più provider cloud e sistemi interni distribuiti (e gli utenti possono connettersi da qualsiasi luogo), gli approcci tradizionali alla sicurezza non sono più un'opzione percorribile come un tempo a causa della scalabilità limitata, delle nuove lacune nella sicurezza, delle prestazioni ridotte e di altre carenze.

Forse la parola più agghiacciante per i CISO di oggi è "ovunque".

Considerata singolarmente, potrebbe sembrare abbastanza innocua. Ma è un grande segnale d'allarme quando si tratta di garantire la sicurezza IT dell'azienda. Infatti, un'indagine recente ha rilevato che il 94% delle organizzazioni opera attualmente con un modello remoto o ibrido.¹

A differenza dell'ambiente IT aziendale ben definito di pochi anni fa, che disponeva principalmente di risorse autonome e access point distinti, oggi i CISO devono proteggere asset aziendali che possono risiedere ovunque, consentendo al contempo l'accesso da qualsiasi luogo.

Inoltre, la crescente complessità dell'IT aziendale ha introdotto nuovi rischi per la sicurezza, mentre i cambiamenti derivanti dall'adozione di servizi cloud, dall'aumento dei lavoratori remoti e mobili distribuiti e dalla dipendenza da soluzioni basate su SaaS, hanno reso la sicurezza IT più difficile, costosa e dispendiosa in termini di tempo.

Di conseguenza, molte organizzazioni stanno adottando un approccio Security Service Edge (SSE). L'SSE, un sottoinsieme del SASE (Secure Access Service Edge), è una combinazione di servizi di sicurezza basati su cloud che consentono alle organizzazioni di fornire accesso illimitato alle risorse e ai servizi aziendali per gli utenti distribuiti ovunque, in modo sicuro e protetto. Con un approccio SSE, i team di sicurezza possono fornire una protezione avanzata per supportare i moderni ambienti mobili e orientati al cloud, con maggiore scalabilità e flessibilità, complessità ridotta, migliori prestazioni, efficienza dei costi e altro ancora.

Per quanto tutto ciò sia positivo, questi vantaggi iniziano a maturare solo dopo che le aziende hanno mosso i primi passi verso l'SSE. Ecco perché abbiamo stilato questa roadmap per le organizzazioni che intendono iniziare in modo sicuro e graduale il loro percorso verso l'SSE. Con il giusto approccio, i CISO e le organizzazioni possono trasformare la sicurezza aziendale tradizionale per affrontare le complesse problematiche IT di oggi, ovunque e in qualsiasi momento, fornendo al contempo una base sicura ed economicamente vantaggiosa per la crescita e l'agilità future.

Questo documento fornisce una guida alla distribuzione accelerata dell'SSE e un modello per il successo a lungo termine.

¹SSE Adoption Report, Cybersecurity Insiders, 2024



Il punto di partenza: perché scegliere l'SSE?



Panoramica dell'SSE

Le soluzioni SSE sono in genere costituite da una combinazione di servizi essenziali, tra cui Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) e Digital Experience Monitoring (DEM) integrato. I servizi funzionano in combinazione, ma possono essere implementati separatamente per un approccio incrementale all'SSE.

Il notevole interesse per l'SSE tra i CISO e i responsabili della sicurezza IT è dovuto a due fattori principali: i cambiamenti nel panorama IT aziendale e i vantaggi di questo framework.

— **Cambiamenti nell'IT aziendale.** Per anni, gli approcci tradizionali alla sicurezza incentrati sulla rete, come le reti private virtuali (VPN), si sono dimostrati sufficientemente efficaci negli ambienti IT aziendali convenzionali, in cui la maggior parte delle applicazioni, dei servizi, dei dati e persino degli utenti risiedeva fisicamente all'interno delle strutture aziendali.

Tuttavia, tali approcci si sono rivelati molto meno opportuni con l'evoluzione del panorama aziendale negli ultimi cinque anni. Il rapido passaggio al cloud computing e alle risorse multi-cloud richiede alle organizzazioni di garantire una sicurezza integrata all'interno e all'esterno delle proprie sedi fisiche. La tendenza verso connessioni più mobili e l'aumento del lavoro da remoto richiedono sicurezza ovunque e una maggiore protezione degli asset aziendali. Con l'aumento della complessità degli ambienti aziendali e dei rischi per la sicurezza, trovare il modo di applicare policy di sicurezza coerenti nell'intera organizzazione è diventato sempre più importante. Contribuiscono a questo cambiamento anche altre tendenze generali, tra cui l'aumento delle minacce alla cybersicurezza, il passaggio a modelli di sicurezza zero trust, una maggiore compliance normativa e la necessità di efficienza dei costi e di migliori esperienze utente.

— **I vantaggi dell'SSE.** Un approccio SSE offre una serie di vantaggi significativi. L'SSE migliora la sicurezza complessiva tramite l'accesso zero trust a tutte le applicazioni aziendali, che siano private, pubbliche, basate su cloud o distribuite nel data center. L'SSE migliora la compliance e la gestione dei rischi attraverso il controllo e l'applicazione automatici e continui delle policy di sicurezza. Rende il lavoro da remoto sicuro, pratico, gestibile ed efficiente da qualsiasi luogo. Semplifica la gestione e l'amministrazione della sicurezza, facilitando il monitoraggio e centralizzando visibilità e controllo. L'SSE migliora inoltre l'esperienza utente semplificando i processi di accesso e sicurezza, ottimizzando le connessioni e favorendo la produttività degli utenti.

Sebbene esistano numerose potenziali applicazioni dell'SSE, alcuni casi d'uso tipici che inizialmente spingono le organizzazioni a distribuirlo includono quanto segue.

- Supportare in modo sicuro i lavoratori remoti e mobili ovunque
- Proteggere e mettere in sicurezza dati e servizi in qualsiasi luogo
- Proteggere tutti gli accessi al cloud e al web
- Migliorare l'approccio complessivo alla cybersicurezza, riducendo al contempo l'esposizione alle minacce



Gli elementi dell'SSE

Zero Trust Network Access (ZTNA). ZTNA rappresenta un notevole miglioramento rispetto all'accesso alle applicazioni private attraverso una tradizionale VPN: estende agli utenti remoti l'accesso alle applicazioni e consente l'accesso solo alle risorse autorizzate, previa autenticazione. ZTNA garantisce sostanzialmente che nessun utente o dispositivo sia considerato attendibile per impostazione predefinita. Tutti gli utenti e i dispositivi devono invece superare rigorosi processi di verifica dell'identità per poter accedere alle risorse appropriate. Inoltre, viene applicato l'accesso con privilegi minimi, dato che gli utenti possono accedere solo alle applicazioni e ai dati specificati, autorizzati dagli amministratori.

Secure Web Gateway (SWG). L'SWG è un servizio SSE fondamentale che gestisce l'accesso a Internet applicando le policy aziendali e impedendo al traffico Internet indesiderato e sconosciuto di accedere alla rete interna di un'organizzazione. L'SWG protegge gli utenti dall'accesso a siti Web dannosi, virus generati da Internet e malware, consentendo loro di accedere comunque alle risorse necessarie per svolgere il proprio lavoro.

Cloud Access Security Broker (CASB). Il CASB ottimizza la funzione di sicurezza SSE. Applica policy di sicurezza per la prevenzione della perdita di dati quando utenti e servizi accedono a varie risorse aziendali (che siano basate su cloud, applicazioni private, ecc.), contribuendo al rispetto delle policy di sicurezza aziendali e di settore.

Digital Experience Monitoring (DEM). Il DEM consente alle organizzazioni di offrire un'esperienza utente che rende i dipendenti produttivi e sicuri. Il DEM monitora l'esperienza digitale degli utenti per garantire che il sistema sia in grado di gestire i picchi nell'utilizzo delle CPU, le interruzioni di rete e i problemi di prestazioni delle applicazioni, offrendo al contempo visibilità e metriche IT su ogni passaggio di Internet e di rete.

Best practice per il successo con l'SSE

Indipendentemente dalle dimensioni o dal settore della tua organizzazione, prendi in considerazione le best practice quando intraprendi il tuo percorso verso l'SSE.

- **Adotta un approccio incrementale.** Sebbene l'SSE possa offrire vantaggi interessanti, ciò che solitamente incoraggia i CISO e le organizzazioni a compiere i primi passi verso l'SSE è l'adozione graduale di questo framework. Per molte organizzazioni, un approccio incrementale all'implementazione dell'SSE risulta spesso la soluzione più sensata. Ecco perché questa è una delle best practice per il successo dell'SSE.
- **Sfrutta team di piccole dimensioni e concentrati su problemi specifici.** Le organizzazioni interessate all'SSE dovrebbero avvalersi di team di piccole dimensioni e concentrarsi su problemi critici in aree specifiche. Questo creerà le condizioni per ottenere rapidamente dei risultati e consentirà all'organizzazione di utilizzare tali risultati come base per un'ulteriore espansione.
- **Non dimenticare l'esperienza utente.** Una parte importante di qualsiasi distribuzione SSE di successo è facilitare il lavoro agli utenti. L'approccio migliore per raggiungere tale obiettivo è considerare sicurezza ed esperienza insieme, senza trascurare un aspetto a favore dell'altro. I team SSE dovrebbero adottare il punto di vista dei dipendenti quando valutano i componenti e i processi della soluzione.
- **Focalizzati inizialmente su un unico servizio SSE.** Evitare di fare il passo più lungo della gamba è un'altra best practice fondamentale dell'SSE per ottenere risultati positivi. Il primo progetto dovrebbe probabilmente utilizzare solo alcuni componenti di una piattaforma SSE. La parte critica è avviare il passaggio a SSE e quindi aggiungere ulteriori funzionalità o servizi in futuro, se necessario, basandosi sul successo iniziale.

ZTNA è una scelta eccellente come primo servizio SSE, perché in genere risolve diversi problemi IT e aziendali urgenti, fornendo al contempo una solida base per ulteriori casi d'uso futuri.

- **Considera ZTNA come un primo passo.** Per molte organizzazioni, Zero Trust Network Access (ZTNA) può rappresentare un punto di partenza ideale per risultati ottimali con l'SSE. ZTNA sostituisce una tecnologia inizialmente non progettata per le attuali esigenze di lavoro da remoto e di accesso da parte di terzi. Può essere implementato in modo indipendente e spesso fornisce un upgrade immediato rispetto all'esperienza utente delle VPN tradizionali, aumentando al contempo le prestazioni e riducendo notevolmente i rischi per la sicurezza.

Per implementare queste best practice per l'SSE, è bene adottare un approccio in tre fasi per il primo progetto in questo ambito: 1. pianificazione, 2. esecuzione e 3. revisione.

Sebbene questo documento utilizzi una distribuzione del servizio ZTNA come fase iniziale dell'SSE a fini illustrativi, la tua organizzazione può iniziare con un componente SSE diverso, come i Secure Web Gateway (SWG), nel caso sia più adatto alle tue esigenze aziendali. I passaggi generali per raggiungere i migliori risultati saranno simili.

Fase 1: pianificazione

Il primo passo per un rapido successo con l'SSE è la pianificazione. Sebbene sia una buona idea studiare l'impatto strategico che una distribuzione completa dell'SSE potrebbe avere sul tuo ambiente IT, è perfettamente legittimo adottare un approccio tattico alla pianificazione basato sul servizio SSE distribuito inizialmente e sul problema aziendale che si intende risolvere.

I passaggi di base per pianificare una distribuzione SSE iniziale includono quanto segue.

- **Valutazione e pianificazione.** Inizia valutando l'infrastruttura e l'approccio alla sicurezza della tua organizzazione per individuare possibili carenze e potenziali esigenze. Seleziona quindi un ambito di progetto iniziale che corrisponda a specifiche esigenze aziendali o IT. Per molte aziende, un buon punto di partenza è la distribuzione di ZTNA per un gruppo, un set di applicazioni, risorse o utenti specifici. Sebbene questa pianificazione iniziale si concentri su obiettivi tattici, dovrebbe includere una visione più a lungo termine delle esigenze aziendali e di sicurezza. Questo contribuirà a orientare le fasi future e la scelta del fornitore di SSE.
- **Scelta del fornitore.** La scelta di un fornitore di SSE è un passaggio fondamentale nel tuo percorso e avrà un impatto diretto sia sui progetti iniziali che su quelli successivi. Dopo la valutazione e la pianificazione iniziali, la tua organizzazione deve valutare i potenziali fornitori di SSE in base alle loro capacità e caratteristiche specifiche e al modo in cui soddisfano le tue particolari esigenze IT e aziendali. La scelta del fornitore di SSE dovrebbe essere basata sulla valutazione e sulla pianificazione effettuate nella fase precedente. I fattori da considerare possono includere capacità funzionali, reputazione, costi, scalabilità, tempistiche, capacità di integrazione, ecc.
- **Definizione della strategia di distribuzione.** Come accennato in precedenza, spesso è ideale per un'organizzazione iniziare la distribuzione dell'SSE con un singolo componente SSE principale, come ZTNA, SWG o CASB. Quando si definisce una strategia di distribuzione per il progetto iniziale, è necessario comprendere il progetto e definire la strategia ottimale attraverso risultati misurabili in termini di sicurezza, produttività e operazioni.

Fase 2: esecuzione

Una volta completati i componenti della fase 1 (valutazione, selezione di un fornitore e definizione di una strategia di distribuzione), è il momento di concentrarsi sull'esecuzione del processo di distribuzione.

ZTNA è una scelta eccellente come primo servizio SSE, perché in genere risolve diversi problemi IT e aziendali urgenti, fornendo al contempo una solida base per ulteriori casi d'uso futuri.

ZTNA è progettato per supportare la moderna forza lavoro con applicazioni ormai esterne alla rete aziendale e per soddisfare i crescenti requisiti di accesso remoto e persino di terze parti, a differenza delle tecnologie di accesso tradizionali. L'approccio VPN all'accesso remoto si basava su una strategia di sicurezza "a castello e fossato" rigida e difficile da scalare, che spesso implicava che, una volta ottenuto l'accesso alla VPN, l'utente disponesse dell'accesso laterale a tutto quello che si trovava sulla rete, un grave rischio nel mondo attuale. Inoltre, le VPN spesso utilizzano solo l'autenticazione tramite nome utente e password, trasformandole in un bersaglio sempre più facile per diverse minacce e violazioni della sicurezza.

Inoltre, un approccio ZTNA mantiene sia la sicurezza che i suoi utenti "in primo piano", offrendo un'esperienza utente di gran lunga migliore rispetto alle soluzioni esistenti come le VPN, eliminando lo stress delle autenticazioni continue o la necessità per gli utenti di superare costantemente ostacoli nell'autenticazione per accedere a risorse e sistemi IT diversi. ZTNA offre agli utenti un'esperienza molto più efficiente.

ZTNA supera gli approcci VPN legacy, offrendo ai team una serie di vantaggi immediati e vitali, tra cui:

- **Scalabilità, flessibilità e agilità.** ZTNA eccelle a livello di scalabilità e flessibilità grazie alla sua natura distribuita tramite cloud. Con l'aumento della domanda aumenterà anche la scala dell'infrastruttura. La piattaforma SSE complessiva è progettata per adattarsi ai requisiti aziendali in continua evoluzione, semplificando il supporto rapido di nuove applicazioni, risorse o utenti.
- **Sicurezza con accesso granulare.** Sebbene l'esperienza utente sia un aspetto essenziale, per i CISO la sicurezza è fondamentale. ZTNA migliora significativamente la sicurezza dell'accesso remoto e ibrido con una granularità estrema, garantendo l'autenticazione completa di utenti e dispositivi remoti prima di accedere alle risorse, consentendo agli utenti di ottenere l'accesso alle applicazioni senza estendere l'accesso alla rete e mantenendo l'ambiente aziendale invisibile agli autori delle minacce.
- **Integrazione tra ambienti cloud.** ZTNA integra e supporta facilmente i servizi basati su cloud e ambienti ibridi, garantendo al contempo la sicurezza avanzata. In questo modo, le organizzazioni possono utilizzare un'unica soluzione di accesso sicuro per integrare rapidamente nuove aggiunte all'ambiente aziendale, senza compromettere la sicurezza o aumentare la complessità.
- **Onboarding e offboarding degli utenti notevolmente semplificati.** Un approccio alla sicurezza basato su ZTNA semplifica notevolmente l'aggiunta (o la rimozione) di utenti su sistemi e risorse distribuiti. Questo approccio zero trust garantisce che gli utenti ricevano l'accesso con privilegi minimi alle applicazioni autorizzate, mentre le funzionalità SCIM (System for Cross-domain Identity Management) standard di settore consentono l'interruzione immediata della procedura di accesso, anche a metà sessione.

L'implementazione del primo servizio SSE può essere realizzata con risorse interne, sebbene anche i fornitori e molte società di consulenza possano fornire risorse, indicazioni e personale aggiuntivi.

Mentre la maggior parte delle organizzazioni sceglierà un approccio graduale all'SSE, basandosi sugli ottimi risultati della distribuzione, il successo a lungo termine dell'SSE richiede una combinazione continua di decisioni strategiche, soluzioni tecniche, coinvolgimento e formazione degli utenti, nonché gestione e perfezionamento costanti.

Passaggio 3: revisione

Il successo a lungo termine dell'SSE non si ferma una volta implementato tale servizio. L'organizzazione deve invece compiere il terzo e ultimo passo per il successo dell'SSE: la revisione. Questa fase include anche l'ottimizzazione delle distribuzioni dei servizi SSE, in linea con l'evoluzione dell'ambiente IT.

Poiché le distribuzioni di SSE sono spesso iterative e possono avere un impatto significativo sugli utenti, nonché sulle funzionalità IT e aziendali, i CISO e le loro organizzazioni devono prendersi del tempo per riesaminare tutti i progetti SSE e metterli a punto per il futuro, identificando le aree di miglioramento per le distribuzioni successive.

169%

dei team prevede di adottare l'SSE nei prossimi 2 anni²

Tra le aree che i team di cybersicurezza dovrebbero valutare figurano:

- Formazione degli utenti
- Test e ottimizzazione
- Processi di revisione e feedback

Infine, una volta completate le revisioni e gli aggiornamenti della distribuzione iniziale di SSE, le organizzazioni dovrebbero riavviare il processo pianificando i successivi passaggi di implementazione dei componenti SSE. Un ottimo punto di partenza per valutare gli obiettivi della seconda fase di SSE è l'individuazione di altre tecnologie e casi d'uso SSE che possono essere aggiunti, concentrandosi sulla scalabilità aggiuntiva per la distribuzione iniziale o scoprendo nuovi modi per ampliarla. Ecco un esempio di un comune percorso SSE.

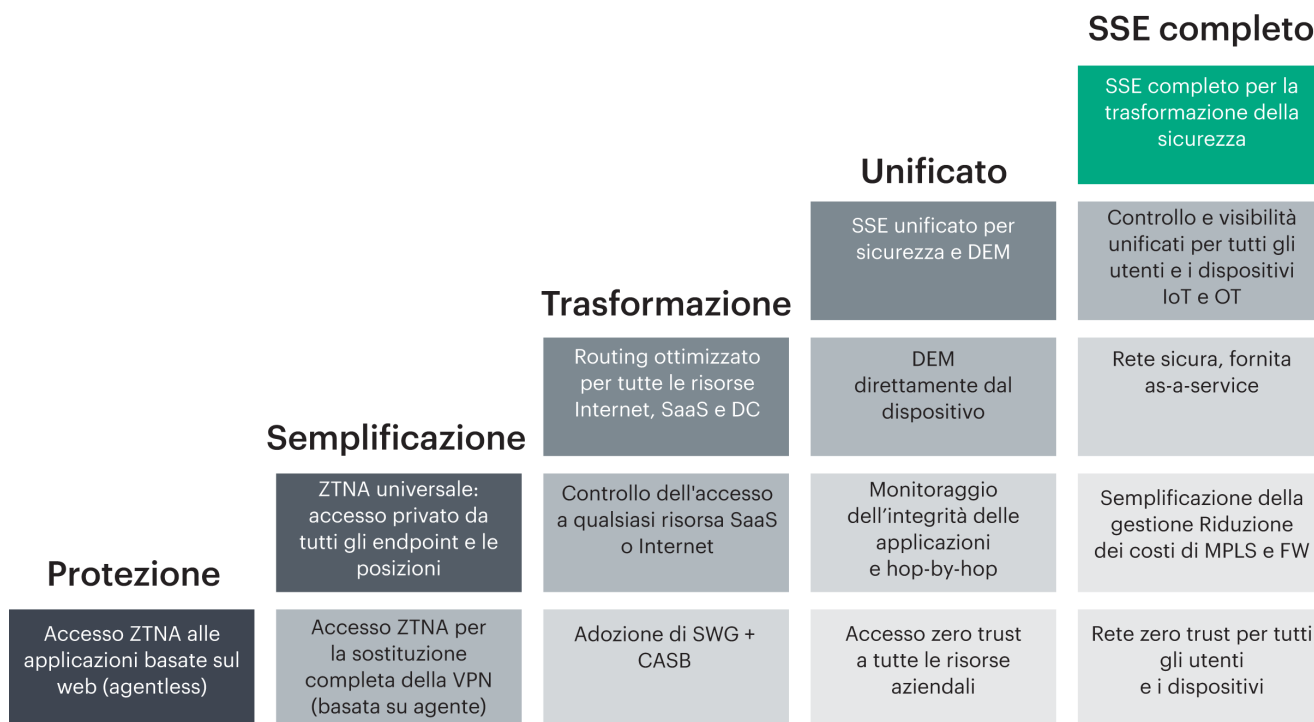


Figura 1. Approccio graduale all'adozione dell'SSE

Sfruttare il successo dell'SSE

Con l'SSE, i CISO e i team di sicurezza non devono più preoccuparsi del termine "ovunque". I servizi SSE come ZTNA, SWG e CASB consentono alle organizzazioni di sostituire gradualmente le tecnologie e i processi di sicurezza obsoleti con altri più efficienti e moderni. I metodi moderni non solo consentono di affrontare tempestivamente i requisiti più urgenti di sicurezza e degli utenti, ma offrono anche una piattaforma flessibile per soddisfare le esigenze future.

Mentre la maggior parte delle organizzazioni sceglierà un approccio graduale all'SSE, basandosi sul successo della distribuzione, il successo a lungo termine dell'SSE richiede una combinazione continua di decisioni strategiche, soluzioni tecniche, coinvolgimento e formazione degli utenti, nonché gestione e perfezionamento costanti.

In altre parole, il successo dell'SSE è un processo che può iniziare e terminare rapidamente, a seconda del fornitore di SSE con cui si sceglie di collaborare. Prendi in considerazione HPE Aruba Networking SSE per il tuo progetto SSE e ti accompagneremo in ogni fase della distribuzione.

² SSE Adoption Report, Cybersecurity Insiders, 2024

Ulteriori informazioni alla pagina

[HPE Aruba Networking SSE](#)

[Effettua un test drive gratuito di 24 ore di SSE](#)



[Visita HPE.com](#)

[Chatta ora \(commerciale\)](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i servizi e i prodotti Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

Tutti i marchi di terzi sono di proprietà dei rispettivi titolari.

a00138655ITE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

