I 7 ERRORI DA EVITARE DURANTE LA SCELTA DI UNA SOLUZIONE SSE

Costruire il Security Service Edge (SSE) sulle fondamenta dello Zero Trust

Di:

Sanjit Ganguli
VP Strategia di trasformazione/Field CTO di Zscaler

Nathan Howe
VP Tecnologie emergenti e 5G di Zscaler

Con il patrocinio di:

zscaler

I 7 errori da evitare durante la scelta di una soluzione SSE

Indice

SSE. Che cos'è e perché dovrebbe interessarti?

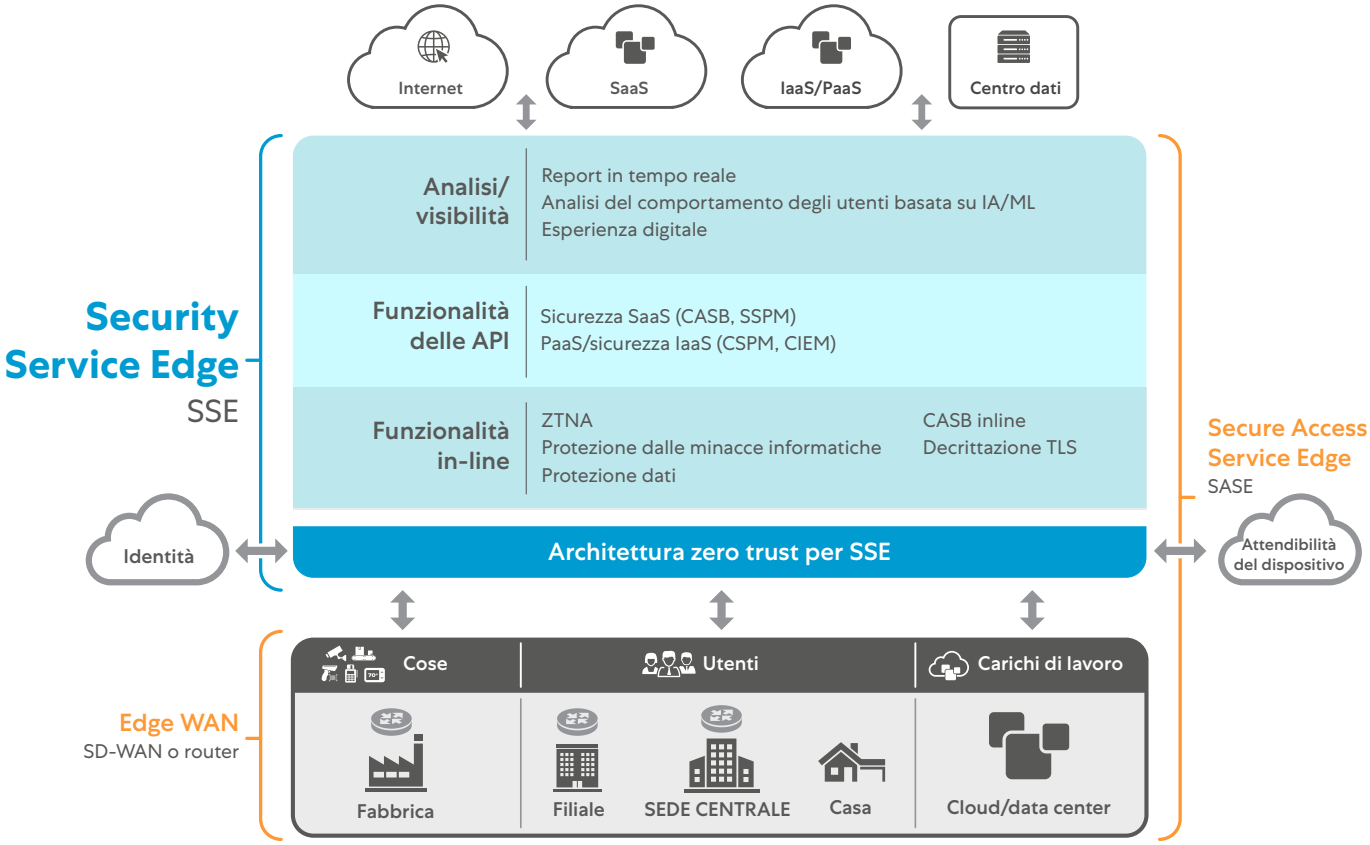

Figura 1: l'architettura SASE (Secure Access Service Edge) include il traffico SSE per la decisione e l'applicazione delle policy. Il SASE richiede l'uso di soluzioni di connettività dedicate per l'entità richiedente e il security edge in cui viene applicata la policy.

Il Security Service Edge (SSE) è la specifica di Gartner per la decisione e l'applicazione delle policy come componenti dell'architettura SASE (Secure Access Service Edge). Il modello SSE promette sicurezza e connettività consolidate, semplificate e fornite sul cloud.

La semplicità architetturale rappresenta sempre un vantaggio per le aziende, soprattutto se questa semplicità riduce al minimo il debito tecnico e accelera il business. Tuttavia, in molte organizzazioni, la sicurezza informatica è vista come un inconveniente, un ostacolo che crea colli di bottiglia, limita l'agilità o frena il successo aziendale. Il Security Service Edge abbatte questi stereotipi. All'interno di un ambiente SSE, la sicurezza offre protezione e controllo, che diventano fattori abilitanti del progresso aziendale.

Alcune informazioni: introdotta nel 2019, l'architettura SASE punta a guidare le imprese nel loro percorso di digitalizzazione, un percorso che ha avuto inizio principalmente con l'adozione del cloud e la mobilità. Il SASE fa convergere l'accesso alla rete e la sicurezza, fornendoli entrambi all'edge del cloud (che è altamente distribuito) **(Figura 1)**. In questo modo, il SASE garantisce che la sicurezza non sia più centralizzata e che possano essere stabilite connessioni sicure da e verso qualsiasi luogo.

Pensa al modo in cui un telefono cellulare si connette a varie reti wireless e cellulari. Non esiste una soluzione dedicata di routing di rete, ma l'utente richiede comunque dei controlli di sicurezza per il traffico tra l'origine e la destinazione. Analogamente, l'edge, la rete o la posizione da cui l'utente si connette non dovrebbero avere importanza per la protezione del traffico aziendale. Questo è ciò che offre il Security Service Edge.

Le società di sicurezza informatica si sono rapidamente adeguate alla tendenza del SASE. Alcuni professionisti del marketing si sono appropriati piuttosto cinicamente del termine per incrementare la redditività del proprio marchio, lasciando intendere che la parte di "Access" dell'acronimo li rendesse conformi al SASE (o che, al contrario, rendesse non conforme la concorrenza), e sostenendo in modo semplicistico che se si dispone di una funzione di rete si è SASE, mentre se non si stanno costruendo dei percorsi di rete, allora non lo si è.

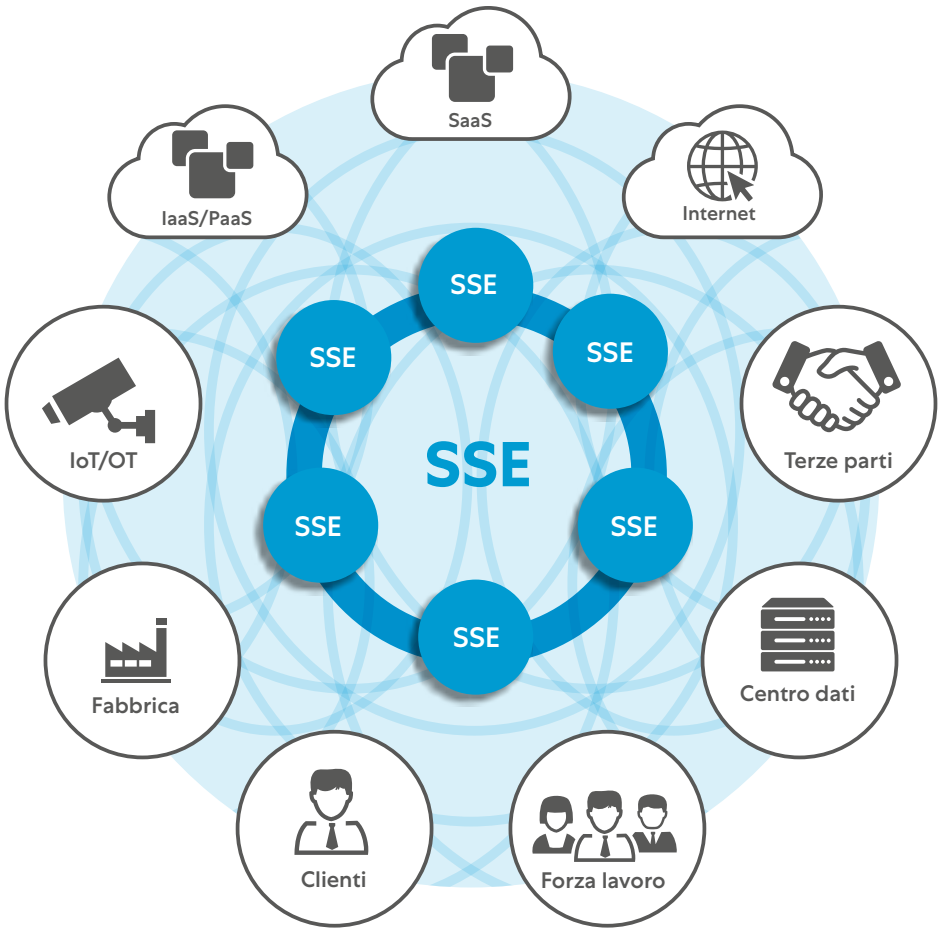

Figura 2: accesso tra entità convalidato e basato su policy fornito all'edge per un mondo mobile e cloud. Il Security Service Edge consente di portare la sicurezza all'utente, senza scendere a compromessi sulle prestazioni ed eliminando al contempo tutti i firewall e le VPN

Il Security Service Edge è costituito dalla suite di servizi SASE utilizzata per proteggere il traffico aziendale. Il modello SSE garantisce che l'utente (o il carico di lavoro) corretto ottenga l'accesso, in modo sicuro e sotto il controllo dell'IT aziendale, alle applicazioni e ai servizi richiesti. Questi servizi potrebbero essere carichi di lavoro su IaaS o PaaS, applicazioni SaaS o servizi Internet, come LinkedIn o YouTube. L'accesso al servizio deve essere concesso seguendo i controlli ZTA (Zero Trust Access, o accesso zero trust), che vengono delineati in modo più approfondito nella sezione dedicata al **secondo errore da evitare**.

Per raggiungere questi obiettivi ambiziosi, il provider di soluzioni SSE deve fornire una soluzione globale, altamente disponibile, scalabile e indipendente dalla rete, che offra policy coerenti, accesso zero trust e un'esperienza digitale veloce.

Senza tali funzionalità, le soluzioni SSE non sono in grado di offrire protezione e disponibilità diffuse **(Figura 2).** A differenza del SASE, il Security Service Edge non prescrive alcun metodo di connessione o di accesso; funzionerà su qualsiasi rete e fornirà controlli per qualsiasi servizio autorizzato, ovunque esso sia.

Il concetto alla base del SASE consiste nell'unire connettività e protezione. Tuttavia, in un ecosistema aziendale, questa combinazione funzionerà solo se trasparente per i dipendenti degli utenti finali. La connettività è diretta, indipendentemente dal fatto che si tratti di una connessione tra utente e applicazione, tra due applicazioni, tra due carichi di lavoro o tra entità di qualsiasi altro tipo. Gli utenti non dovrebbero mai chiedersi se, per poter lavorare, debbano prima connettersi alla rete. Al contrario, la loro attenzione dovrebbe essere rivolta solo al lavoro da svolgere.

Questa integrazione non può essere ottenuta negli ambienti aziendali che dipendono dalla rete e da un'infrastruttura di sicurezza legacy. In questo modello obsoleto, la sicurezza è centralizzata e il traffico dati, indipendentemente dalla posizione (ad esempio, da remoto o dalle filiali), dall'origine (ad esempio, utente, app o carico di lavoro) e dalla destinazione (ad esempio, Internet, cloud, data center), deve prima essere connesso e instradato tramite la rete aziendale verso (e attraverso) la posizione fisica dei controlli di sicurezza basati su hardware.

Il valore reale della trasformazione SSE per l'azienda

L'adozione del modello SSE può comportare una trasformazione digitale significativa per l'azienda, e il cambiamento può generare un impatto concreto:

Controllo:

Il Security Service Edge parte da zero. I servizi SSE convalidano ogni persona, computer, carico di lavoro, rete ed edge. Senza una corretta identificazione, che è associata a sua volta al contesto fornito dall'analisi comportamentale, non vi è alcun accesso; così le aziende hanno il controllo completo su cosa o chi accede ai servizi all'interno dell'impresa.

Connettività diretta:

L'applicazione delle policy SSE risiede inline, tra l'entità di origine e il servizio di destinazione. Le decisioni in merito all'accesso vengono prese in base all'applicazione e non a livello della rete.

Sicurezza specifica per l'azienda

Le policy sulle entità che possono connettersi ai servizi sono definite utilizzando privilegi minimi. Gli utenti, i computer, i carichi di lavoro e altre entità possono connettersi solo a ciò per cui dispongono dell'autorizzazione, e a nient'altro. Non vengono stabilite ulteriori connessioni, e tutti gli altri accessi vengono bloccati.

Applicazione globale:

Il Security Service Edge deve avere un'applicazione globale, in modo che il percorso di accesso di qualsiasi entità possa essere controllato in base al contesto fornito da policy, insight engine e informazioni utili acquisite dall'esterno (monitoraggio delle minacce, deception technology, e altro). Questa applicazione globale deve adattarsi ai requisiti dell'azienda.

Completezza:

Il Security Service Edge fornisce una valutazione completa e inline, per ispezionare il traffico in modo approfondito e con la portata richiesta. Offre protezione dalle minacce avanzate, tutela le risorse aziendali (cloud e non), previene la perdita dei dati e assicura il controllo inline. Se necessario, la soluzione deve fornire il controllo dei contenuti archiviati all'interno dei servizi cloud.

Oscuramento:

Il Security Service Edge previene l'accesso indesiderato e l'esposizione delle risorse aziendali, e consente quindi di eliminare la superficie di attacco. Non è possibile attaccare ciò che non è accessibile.

Da qualsiasi luogo:

Il Security Service Edge offre questa connettività in ogni parte dell'azienda, da qualsiasi luogo. Protegge e connette una base flessibile di utenti, garantendo al contempo che carichi di lavoro, entità e computer possano muoversi, riposizionarsi e trasformarsi senza perderne il controllo.

Può fare da catalizzatore per il cambiamento di un'azienda semplicemente offrendo una protezione completa. Ma non tutte le soluzioni sono create allo stesso modo. I leader IT che desiderano adottare il Security Service Edge devono valutare e scegliere una soluzione che consenta alla loro organizzazione di semplificare la sicurezza.

Ci sono 7 errori da non fare nel percorso di trasformazione digitale aziendale verso il modello SSE. Evitare questi passi falsi consentirà ai responsabili IT di selezionare i servizi, l'architettura e le funzioni più adatte per concretizzare la promessa di valore del Security Service Edge. Questa trasformazione deve essere un percorso di allontanamento dai "vecchi modi di lavorare" ancorati alle reti o all'accesso incondizionato ai servizi, che limitano la possibilità di innovare e di soddisfare le esigenze aziendali.

1° errore:
Scegliere una soluzione SSE senza una comprovata esperienza con una piattaforma cloud globale, scalabile per prestazioni e disponibilità

2° errore:
Scegliere una soluzione SSE non fondata su un'architettura zero trust

3° errore:
Scegliere una soluzione SSE non in grado di ispezionare il traffico criptato su larga scala, pur promettendo protezione dalle minacce avanzate e DLP avanzata

4° errore:
Scegliere una soluzione SSE non personalizzabile e che non supporti opzioni flessibili, scalabili e diversificate di distribuzione e gestione

Errore N. 5:
Scegliere una soluzione SSE che fornisce un'esperienza utente mediocre, in quanto non ottimizza la connettività delle applicazioni o non diagnostica le degradazioni dell'UX

Errore n. 6:
Scegliere una soluzione SSE che ha integrazioni e orchestrazioni limitate con gli ecosistemi di fornitori terzi

7° errore:
Scegliere una soluzione SSE non in grado di rivelare rapidamente il proprio valore con un'esecuzione pilota in un ambiente di produzione

A chi è indirizzato questo e-book?

Il passaggio a una soluzione SSE non consiste solo nella trasformazione della sicurezza e non riguarda solamente **gli architetti della sicurezza informatica**. Le best practice descritte in questo e-book sono pensate per **architetti della sicurezza**, **architetti di rete**, **architetti aziendali**, **architetti del cloud** e **architetti delle applicazionis**.

N° 1
Errore

Cegliere una soluzione SSE senza una comprovata esperienza con una piattaforma cloud globale, scalabile per prestazioni e disponibilità

Considera invece soluzioni SSE che:

- Offrano un set globale e diversificato di service edge pubblici di applicazione delle policy, con prestazioni, disponibilità, throughput e funzionalità supportate da accordi sul livello del servizio. L'applicazione delle policy avviene a livello locale in base alle posizioni dei clienti.
- Siano native del cloud e offrano un'ottima resilienza, infrastruttura, diversità geografica e le migliori funzionalità del settore, e siano in grado di fornire un'esperienza utente ottimale. Forniscano servizi SSE inline in data center neutrali e non come servizio sulla base di un cloud gestito o di un provider di DC di destinazione.
- Abbiano una scalabilità, una capacità di crescita e una distribuzione convalidate da referenze dei clienti, report, certificazioni di terze parti e archivi di dati open source esterni (https://www.peeringdb.com/org/12297).

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

Costruire e gestire una piattaforma SSE multitenant, che supporta miliardi di transazioni, va al di là dell'aspetto computazionale e non è una cosa semplice. **Alla soluzione SSE verranno affidate la protezione, la connettività e la capacità di operare dell'azienda e**, quindi, il set di servizi SSE deve essere fornito in modo uniforme e puntuale in ogni parte dell'organizzazione.

La soluzione SSE giusta fornirà le sue funzionalità attraverso un servizio distribuito a livello globale. Dal punto di vista architetturale, la modalità di distribuzione più efficace consiste in un servizio con base proxy. In quanto non ancorato allo stato della rete, un servizio proxy si concentra sulla fornitura del Security Service Edge all'accesso alle applicazioni, e consente così di ottenere una comprensione più completa, senza che via sia la necessità di utilizzare delle piattaforme aggiuntive per ulteriori analisi, come l'ispezione su larga scala **(vedi il 3° errore)**.

Ricorda inoltre che. per soddisfare i requisiti di scalabilità dell'azienda moderna, una vera architettura proxy richiede attività intense di ricerca e sviluppo e molti anni di perfezionamento. La soluzione SSE giusta avrà al suo attivo un elevato numero di esempi di distribuzioni di grandi dimensioni, in cui l'architettura proxy è stata in grado di offrire scalabilità.

Questo servizio deve essere fornito tramite un set uniforme di edge policy, in cui tutte le funzioni di trasmissione dei dati dell'azienda sono protette e non è solo una questione del numero dei nodi, ma del numero di siti garantiti da accordi del servizio che offrono i servizi richiesti dal cliente. Il provider SSE non dovrebbe fornire punti di presenza pubblici se non è in grado di garantire un accordo sul livello del servizio in una regione a causa di problemi di peering o altre motivazioni.

Adottare il modello SSE significa consolidare, rafforzare e condividere la responsabilità della sicurezza, della connettività e del controllo dell'azienda con un provider affidabile di servizi di sicurezza. Questo modello condiviso semplificherà i mezzi con cui potrai fornire protezione e connettività a utenti, carichi di lavoro, servizi, filiali e altre entità. Il provider SSE deve soddisfare una serie di accordi definiti sul livello del servizio per assicurare l'operatività dell'azienda e garantirne al contempo la protezione.

Quando il servizio aziendale si connette, ha bisogno di un percorso efficace per poter utilizzare la funzione della destinazione. Questo si può ottenere solo tramite una soluzione SSE con un peering altamente efficace all'interno dei data center neutrali. I controlli devono quindi essere applicati inline, tra l'origine e la destinazione, indipendentemente dalla rispettiva posizione.

Le soluzioni che ospitano il servizio di sicurezza all'interno di cloud di elaborazione centrali, spesso all'interno di hyperscaler (strumenti di iperscalabilità) e con gateway di ingresso, come mostrato nella Figura 3 (spesso indicati come servizi on-ramp), si basano su edge di ingresso distribuiti, ma eseguono il controllo e l'applicazione delle policy a livello centralizzato, introducendo così latenza e dando vita a esperienze utenti scadenti.

I provider di soluzioni SSE devono disporre di una piattaforma cloud completa, massiccia e scalabile. Oltre agli accordi sul livello del servizio, la piattaforma SSE deve inoltre fornire prove di scalabilità, stabilità, disponibilità, distribuzione geografica ecc. Per verificare queste informazioni, è possibile consultare i dati disponibili pubblicamente e parlare con i clienti esistenti per conoscere le loro esperienze.

Applicazione di policy uniformi all'edge

L'insieme di service edge di un provider SSE deve fornire l'applicazione di policy. Questi non devono essere edge di connettività a una rete con base cloud più ampia esclusivamente per instradare il traffico verso un'infrastruttura centrale. Schemi di questo tipo non permettono di fornire servizi altamente efficaci e a bassa latenza

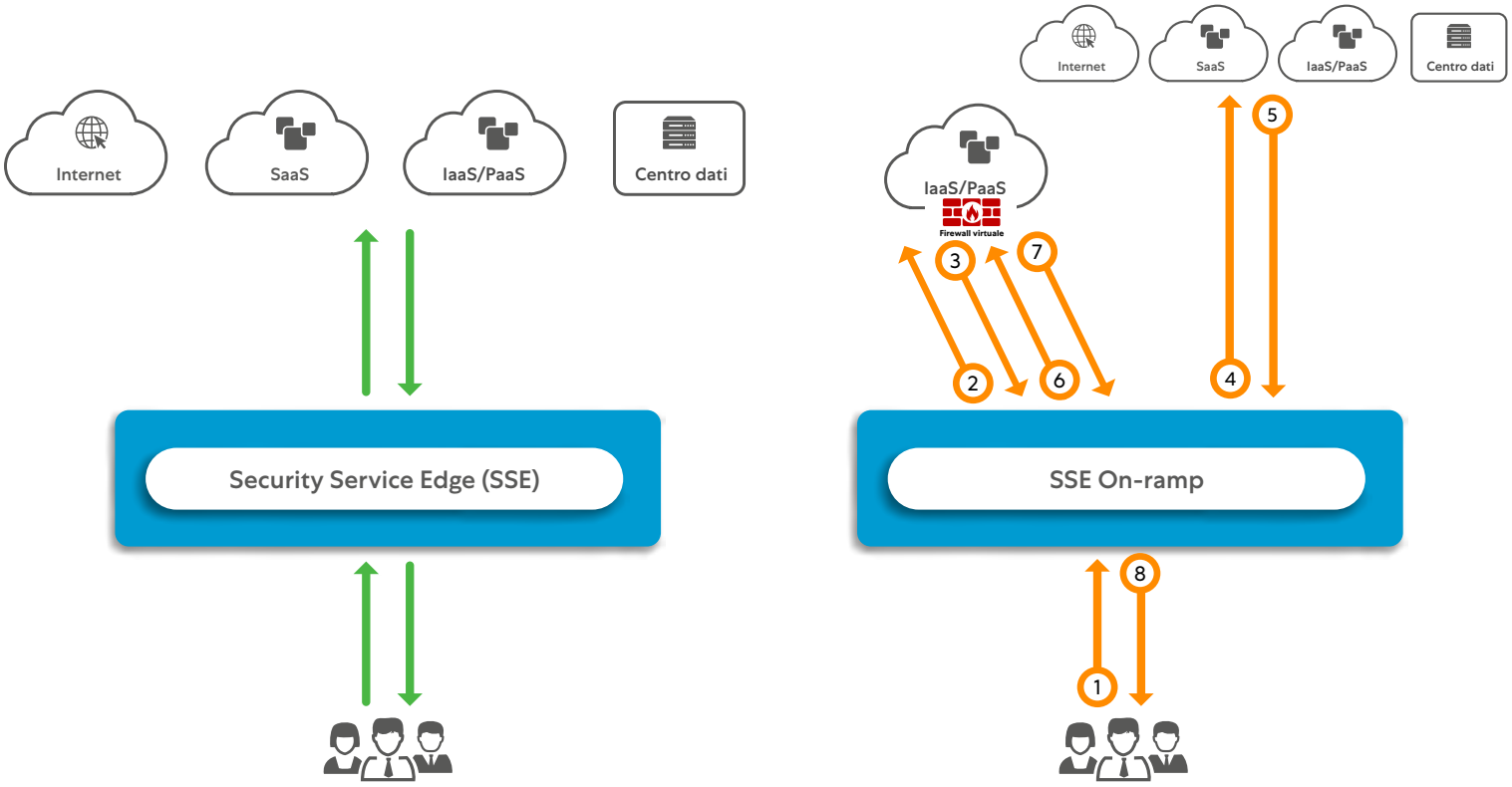

Figura 3: i servizi SSE inline (a sinistra) applicano i controlli di sicurezza al traffico inline. I controlli di sicurezza on-ramp (a destra) offrono gateway di ingresso all'edge, solo per poi procedere all'inoltro verso un controllo centralizzato e ospitato nel cloud, aggiungendo così latenza, inefficienza e dando vita a un'esperienza utente scadente.

Il provider deve rispondere alle seguenti considerazioni progettuali e assicurarsi che gli edge:

- Siano ospitati in posizioni importanti per il peering all'interno di data center neutrali, garantendo così una latenza minima tra l'origine e la destinazione. Quando si valuta un provider SSE, è bene rivedere le statistiche delle risorse disponibili pubblicamente, come PeeringDB e distribuzioni di partner **(vedi il 6° errore per i dettagli sull'integrazione dei partner)**.
- Siano supportati da un accordo sul servizio valido. Questo assicurerà la stabilità delle funzioni aziendali e testimonierà l'impegno del provider SSE nelle regioni per il rispetto degli accordi sul servizio.
- Siano distribuiti privatamente in base alle esigenze del cliente nei luoghi in cui le condizioni locali richiedono distribuzioni particolari, ad esempio on-premise o all'interno di un nodo di calcolo all'edge **(il 4° errore fornisce ulteriori dettagli)**.
- Dimostrino una crescita del throughput nel corso del tempo.
- Forniscano tolleranza ai guasti distribuita in modalità attivo-attivo, per garantire disponibilità e ridondanza (il provider monitora ed effettua la manutenzione dei service edge pubblici per garantire la disponibilità continua).
- Promuovano la privacy dei dati per garantire che il traffico dei clienti non venga trasferito ad altri componenti all'interno dell'infrastruttura e che nessun dato venga mai archiviato su disco.
- Forniscano controlli uniformi per le risorse aziendali a ogni edge e non instradino o effettuino l'inoltro "on-ramp" del traffico dagli edge in remoto alle posizioni centrali.
- Applichino la protezione su scala globale, per proteggere tutti i servizi aziendali quando viene rilevata una minaccia

⚠ A cosa fare attenzione:

- Edge pubblici che non forniscono l'applicazione delle policy e instradano il traffico verso data center più grandi che dispongono di risorse di elaborazione.
- Provider che affermano di avere centinaia di edge pubblici senza condividere la capacità e la funzione di ciascuno di essi.
- Edge senza accordi sul servizio per la disponibilità, la produttività e la resilienza.
- Servizi edge senza un approccio multitenancy e che forzano il traffico su percorsi on-ramp o lo instradano verso altre posizioni.
- Servizi SSE senza una comprovata esperienza di distribuzione con clienti di grandi dimensioni.
- Servizi per cui non esistono informazioni reperibili pubblicamente su stabilità e disponibilità

Esiti:

Scegliere una soluzione SSE che garantisca scalabilità per le esigenze aziendali attuali e per raggiungere gli obiettivi futuri è un investimento cruciale. La scalabilità non è solo un meccanismo per far crescere l'azienda, ma una proprietà fondamentale che permette di soddisfare le esigenze aziendali senza sacrificarne l'operabilità, la stabilità e la protezione. Puoi ottenere tutto questo con una soluzione che:

- Fornisca prove e sia trasparente sulla sua distribuzione globale e diversificata.
- Disponga di accordi sul servizio documentati e verificati per la perdita o la riduzione dei servizi SSE.
- Sia stata distribuita da un gran numero di clienti con dimensioni e complessità analoghe a quelle della tua azienda.
- Fornisca informazioni pubbliche e consultabili per ogni punto di presenza utilizzando strumenti pubblici (ad esempio PeeringDB).
- Fornisca tutte le funzioni critiche in tutti i siti, senza l'hairpinning del traffico.
- Offra protezione inline tra l'origine e la destinazione.
- Sia progettata per l'infrastruttura e la resilienza operativa e funzionale.
- Sia utilizzabile in più forme e su più siti.

N° 2
Errore

Scegliere una soluzione SSE non fondata su un'architettura zero trust

Considera invece soluzioni SSE che:

- Consentano l'accesso solo alle identità convalidate contestualmente, indipendentemente dalla posizione/rete, e in cui questo percorso a privilegi minimi sia destinato a tutti i servizi, non solo agli utenti. Collegando le origini, che vengono autorizzate tramite adeguati controlli SSE, esclusivamente a destinazioni valide, le aziende eliminano il movimento laterale, che spesso viene sfruttato dagli attori delle minacce.
- Si concentrino esclusivamente sulla connessione dell'accesso dinamico in base alla sessione, e in cui lo zero trust non sia fornito tramite firewall, SD-WAN e altri servizi di rete. Deve trattarsi un overlay indipendente dalla rete.
- Non espongano mai le risorse aziendali a un'origine non autorizzata, riducendo così la superficie di attacco e garantendo l'applicazione di controlli adeguati a tutti i servizi.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

Un approccio zero trust applicato a tutte le comunicazioni aziendali significa che, senza un'autorizzazione e un'approvazione esplicita, non viene concesso alcun tipo di accesso, indipendentemente dall'origine (utenti, terze parti, reti e così via), ad alcuna destinazione.

In passato, la distribuzione dello zero trust all'interno di un'azienda era un'operazione complessa, perché il contesto condiviso della connessione tra origine e destinazione faceva affidamento su un percorso di rete fisico o logico. La Figura 4 evidenzia questi problemi di condivisione. Non è possibile costruire o sviluppare un approccio zero trust con SD-WAN o firewall.

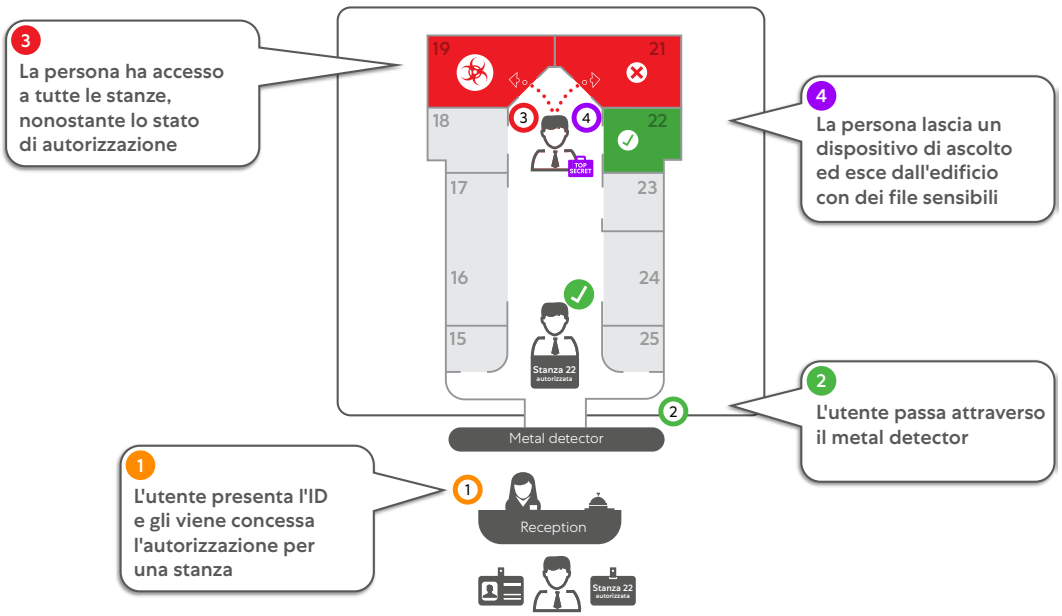

Figura 4: come non abilitare l'accesso: il vecchio mondo dell'analogia della sicurezza della rete. Connettere gli utenti alla rete aziendale è come permettere a dei visitatori non accompagnati di vagare all'interno della sede centrale dell'azienda: questo offrirebbe loro la possibilità di rubare dati sensibili.

La sicurezza SSE può aiutarti ad applicare regolamenti per l'accesso degli utenti e restrizioni per i carichi di lavoro in tutta l'azienda. Ampliando questi controlli ed estendendoli al di là dei dipendenti, è possibile proteggere l'azienda dai rischi associati alle superfici di attacco esposte o al movimento laterale delle minacce.

Tra le sue svariate funzionalità, l'architettura zero trust consente inoltre di applicare controlli granulari, assicurando che ogni richiedente comunichi con la destinazione corretta in ogni sessione, come illustrato nella Figura 5. Queste regole richiedono la conoscenza delle entità di origine e di destinazione e sono il motivo per cui la maggior parte delle aziende decide di avviare un percorso zero trust (ed SSE) con la propria base di utenti. Agli utenti viene spesso assegnata un'identità, che consente loro di differenziarsi dai vari servizi. Tuttavia, poiché le reti sono flat, esposte e aperte, il rischio che un utente abbia accesso a più informazioni solo perché condivide una rete, è una delle principali problematiche per la stabilità delle imprese.

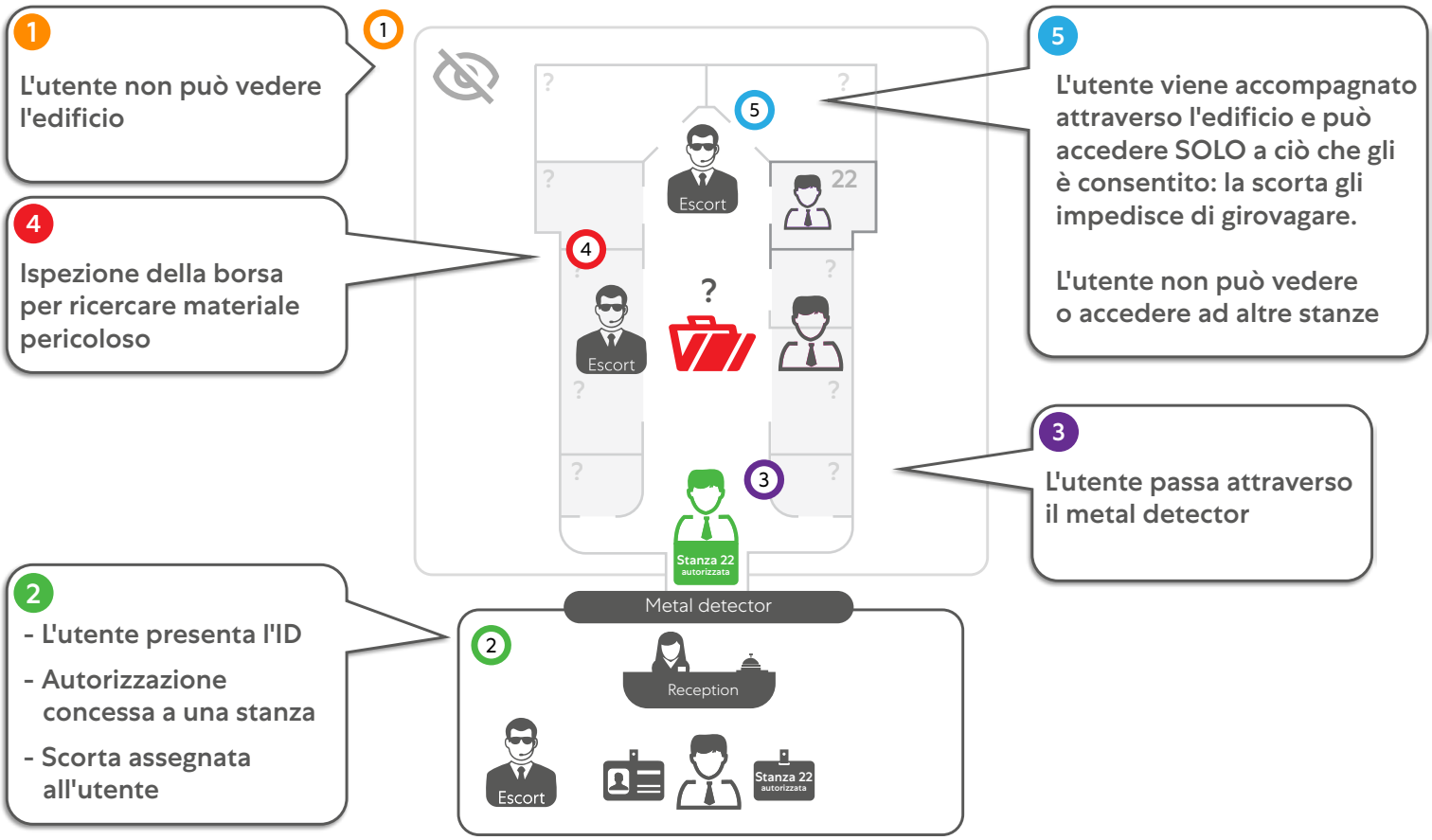

Figura 5: il modo corretto di fornire l'accesso è attraverso il controllo end-to-end. L'accesso zero trust può essere visto come l'accompagnamento di un visitatore bendato a una riunione nella sede centrale dell'azienda, per poi riaccompagnarlo all'uscita, impedendogli così di girovagare o di curiosare qua e là.

Vanno presi in considerazione tutti i casi d'uso aziendali, come la protezione degli utenti e delle risorse aziendali principali, e tutto il traffico SSE deve essere ispezionato. Le connessioni devono essere stabilite solo dopo aver esaminato dinamicamente e contestualmente il rischio dei seguenti quattro valori di connessione (si veda la Figura 6):

Iniziatore della connessione

Quali sono l'identità e l'attendibilità di utente/dispositivo/rete? In che modo questa identità contraddistingue l'accesso a questa origine e in quali condizioni?

Esempio: Sara delle Risorse umane ha bisogno di accedere al sistema HR ospitato sul cloud e al sistema di spesa ospitato internamente. L'accesso viene concesso mediante la piattaforma SSE, a condizione che la sua identità e l'attendibilità del dispositivo abbiano i diritti prestabiliti per ottenerlo.

Controllo delle policy

Dove, come e quali controlli verranno applicati? I criteri per il controllo includono l'efficacia del percorso, il rischio e l'attendibilità dell'iniziatore della connessione, la funzione della destinazione richiesta e la policy dell'azienda.

Esempio: Piero ha un'identità valida per accedere a Salesforce, ma la sua azienda vuole consentirgli solo la visualizzazione, senza dargli la possibilità di scaricare o manipolare i dati. La soluzione SSE consente quindi a Piero di accedere solo per visualizzare i contenuti dell'applicazione, e non gli consente di fare altro.

Destinazione della connessione

A quale servizio accede il richiedente? È un SaaS pubblico o un carico di lavoro interno? Quali controlli devono essere applicati? L'accesso può cambiare in base al contesto dell'identità e alla policy di controllo.

Esempio: un iniziatore valido può ottenere l'approvazione per accedere a uno specifico servizio cloud PaaS e, se si tratta di un servizio cloud, la piattaforma SSE ispezionerà il carico di lavoro per assicurarsi che non vi sia la divulgazione di segreti aziendali. Lo stesso iniziatore potrebbe quindi interfacciarsi con un servizio interno con un'attendibilità analoga, stabilendo quindi un iniziatore per la connessione al servizio, senza la necessità di ulteriori controlli.

Instaurazione della connessione

Infine, prendendo in considerazione gli input precedenti, le informazioni condizionali sui carichi di lavoro, le capacità della rete o dell'edge, la policy definita dall'azienda, ecc., si stabilisce l'accesso. La soluzione SSE deve essere in grado di identificare le variazioni, ad esempio cambiamenti di posizione, e adattare l'accesso con il migliore percorso applicabile.

Esempio: una volta convalidata l'origine, il controllo e le destinazioni, la connessione viene instaurata, ma solamente per quella singola sessione. Il flusso end-to-end per ogni sessione è descritto nella Figura 6.

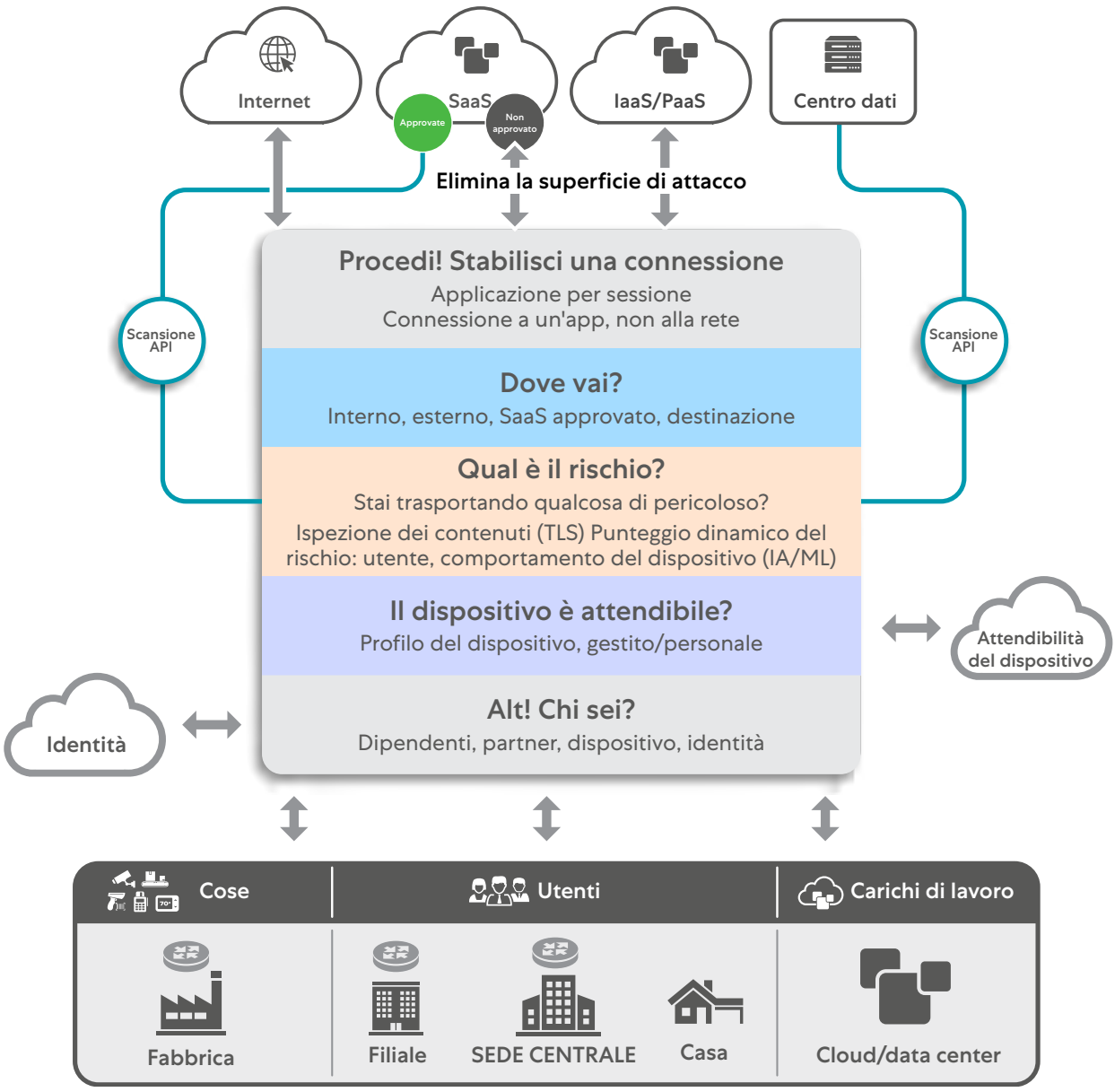

Figura 6: passaggi di un'architettura zero trust, che mostrano il controllo e l'applicazione delle policy a ogni passaggio

Definendo i controlli delle connessioni all'interno di una soluzione SSE **si fa in modo che solo una determinata origine possa usufruire di una determinata destinazione**. Il principio dei privilegi minimi applicato al modello SSE offre molteplici vantaggi per un'azienda, tra cui i seguenti:

- I controlli SSE corretti vengono applicati all'origine corretta
- I servizi protetti con SSE non vengono esposti alle origini non autorizzate, e questo riduce i rischi per la sicurezza informatica.
- Si riducono le connessioni inutili, perché non si consente a un server Linux di connettersi a un sistema di patch di Windows.
- Si ottiene visibilità granulare e si acquisiscono informazioni sui flussi in base alla richiesta di accesso, non da IP di rete a IP
- Si consolida l'accesso in base all'identità e non alla rete, e questo consente la razionalizzazione delle funzioni (e dell'infrastruttura) di rete

Percorso a fasi verso il modello SSE con lo zero trust:

Scegliendo una soluzione SSE che fornisca il controllo basato sull'utente in tutti i seguenti casi d'uso, è possibile estendere la protezione a tutte le funzioni aziendali (vedi la Figura 7):

Da utente a carico di lavoro

Permettendo agli utenti di accedere ai carichi di lavoro, è possibile rimuovere il contesto della rete dall'accesso degli utenti e ottenere contemporaneamente la visibilità sui carichi di lavoro a cui essi accedono. Questa combinazione è solitamente quella che genera valore più rapidamente.

Immagina di poter ottenere un controllo granulare per gli utenti nell'intera infrastruttura di applicazioni. Ad esempio, potresti limitare l'utilizzo di servizi Internet come YouTube al team di PR di un'azienda.

In questo modo, è possibile consentire uno sviluppo più ampio della gamma di servizi aziendali e applicare regole più granulari, come l'accesso a piattaforme OT e R&S isolate, senza mai esporre l'intero ecosistema alla base di utenti.

Accesso di terze parti

L'implementazione dell'accesso zero trust per i partner terzi elimina il rischio associato alla connettività della rete e alla superficie di attacco esposta derivante dalle soluzioni legacy con cui si concede l'accesso ai partner. Il controllo a privilegi minimi dello zero trust consente di controllare l'accesso dei partner da dispositivi non attendibili o personali e di concedere l'accesso esclusivamente a determinate app; in questo modo, si ottiene anche maggiore visibilità sulle risorse a cui si accede.

I controlli su terzi forniti dalla soluzione SSE dovrebbero offrire meccanismi diversificati per il controllo degli accessi. Le possibili opzioni includono l'accesso client autorizzato da più provider di identità per raggiungere applicazioni specifiche, l'accesso isolato solo da browser o l'isolamento completo dell'accesso attraverso un'immagine renderizzata che viene presentata all'entità terza (attraverso lo streaming di pixel sul dispositivo dell'utente, come per i dispositivi BYOD).

Da carichi di lavoro a carichi di lavoro

I controlli tra carichi di lavoro sono richieste di accesso ad applicazioni e servizi. In genere, un computer Windows richiederà le patch per Windows, non per Linux. Quindi, per un'azienda è fondamentale stabilire quali sistemi possono accedere a quali risorse.

Come nel caso degli utenti, i controlli dei carichi di lavoro devono fornire un'identità valida per poter utilizzare un servizio. Se il carico di lavoro utilizza risorse pubbliche, come i servizi IoT/OT con base PaaS, il security edge deve convalidare e comprendere il relativo contesto, quindi bloccare qualsiasi tentativo di utilizzo improprio.

Al contrario, se il carico di lavoro dovesse accedere a un servizio locale privato, ciò può avvenire solo tramite controlli SSE inline dopo l'approvazione dell'identità, come previsto dalla convalida zero trust.

Da posizione a posizione

Con l'evoluzione di accesso e controllo in tutta l'azienda, per la connettività tra siti dovrebbe essere preso in considerazione lo zero trust. Bisogna isolare un insieme di servizi rispetto a una rete, un sito, un VPC, ecc. La connessione tra la posizione e il sito noto non deve avvenire su una rete condivisa. Lo zero trust permette a una posizione valida di connettersi a un set valido di carichi di lavoro all'interno di un'altra posizione. Questo approccio non utilizza l'accesso alla rete a livello di collegamento; richiede una connettività da app ad app uniforme su qualsiasi sito, VPC, VLAN, ecc.

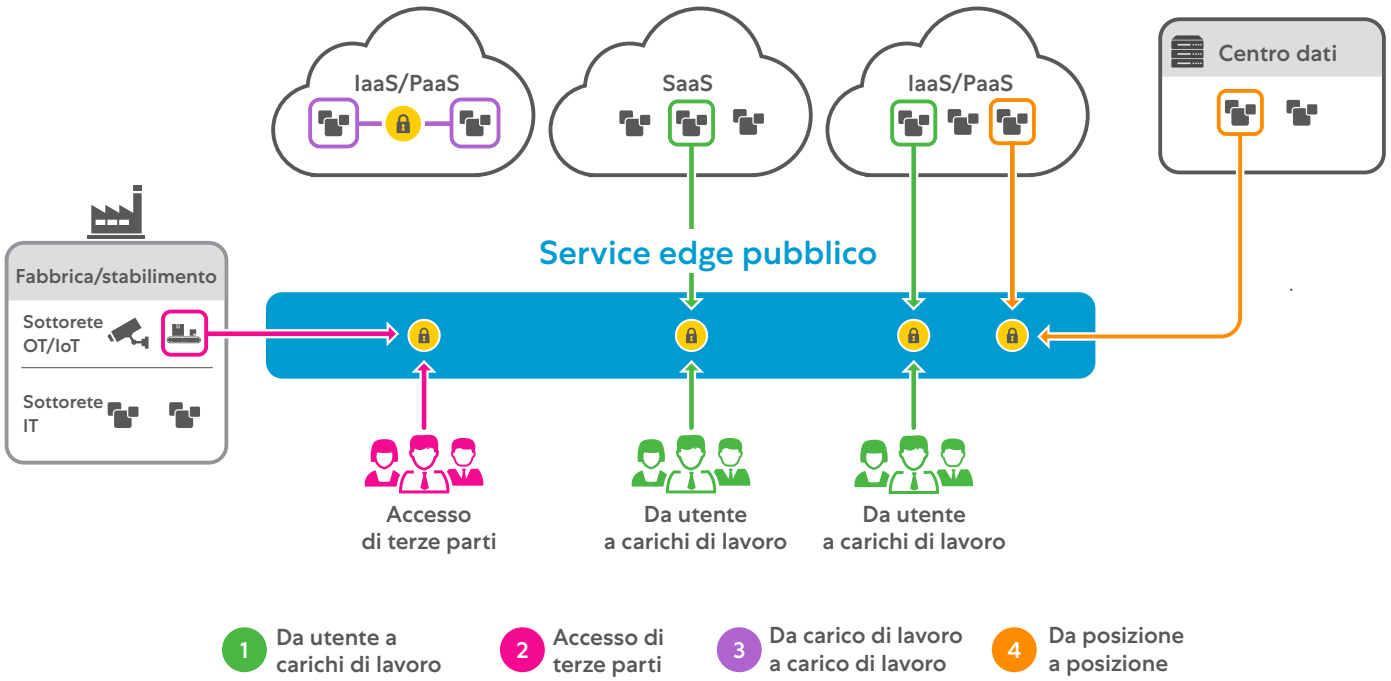

Figura 7: un approccio suggerito per la segmentazione aziendale. Consentire un approccio a fasi al controllo, all'apprendimento, alla segmentazione e all'isolamento, come parte della distribuzione dello zero trust

Ad esempio,quando è stata scoperta la vulnerabilità 0-day Log4j, ogni cliente che utilizzava la utility di logging vulnerabile basata su Apache Java era soggetto al rischio di esecuzione di codice da remoto. Nonostante questo, le app interne delle aziende che avevano già adottato un'architettura zero trust erano completamente invisibili a Internet, e di conseguenza né individuabili, né attaccabili dagli aggressori. In questo modo, le aziende sono state in grado di proteggere anche le versioni suscettibili di Apache Log4j da questa e da altre vulnerabilità. Tutto ciò sarebbe stato impossibile con dei servizi legacy esposti, come VPN e firewall. **L'approccio zero trust assicura che solo gli utenti autorizzati possano accedere alle app, evita il movimento laterale attraverso la microsegmentazione da utente ad app e da app ad app, e consente di ispezionare sia il traffico in entrata, sia quello in uscita**.

Lo stesso è valso per l'attacco a Colonial Pipeline, in cui gli hacker hanno ottenuto l'accesso grazie a credenziali VPN rubate (per cui non era abilitata l'autenticazione a più fattori). In questo modo, sono stati in grado di muoversi lateralmente attraverso la rete e di accedere ai dati sensibili. Un'architettura zero trust che collega solo gli utenti autorizzati alle applicazioni (e non alle reti), impedisce il movimento laterale segmentando le comunicazioni da utente ad app e da applicazione ad applicazione.

⚠ A cosa fare attenzione:

- Servizi SSE non in linea con i principi dell'architettura zero trust, come la Pubblicazione speciale 800-207 del NIST.
- Assicurati che il servizio SSE offra controlli zero trust a tutte le risorse aziendali, non solo agli utenti.
- Lo zero trust non è una funzione applicabile a firewall o SD-WAN. È indipendente rispetto alla rete. Una soluzione SSE di un provider dipendente dalla rete può esporre l'azienda a lacune nell'architettura zero trust.
- Assicurati che i controlli partano da un accesso zero trust: nessuna risorsa aziendale deve essere accessibile prima della convalida dell'accesso.
- Considera tutte le esigenze dell'azienda e non limitare i controlli zero trust solo a una sua parte.

Esiti:

La protezione di un'azienda e dei suoi utenti deve fornire l'accesso in base al principio dei privilegi minimi, e concederlo solo a ciò che è effettivamente necessario. **Nella scelta di una soluzione SSE, lo zero trust deve essere il fondamento**, in modo che:

- Il provider della soluzione SSE protegga tutti i servizi aziendali e, prima di concedere l'accesso, convalidi l'identità delle entità; tutto il resto deve essere bloccato.
- Le soluzioni che forzano la connettività della rete siano evitate e l'accesso sia indipendente dalla rete, in qualsiasi luogo.
- Il servizio SSE azzeri la superficie di attacco per i servizi aziendali privati.

N° 3
Errore

Scegliere una soluzione SSE non in grado di ispezionare il traffico criptato su larga scala, pur promettendo protezione dalle minacce avanzate e DLP avanzata

Considera invece soluzioni SSE che:

- Forniscano l'ispezione SSL/TLS di tutto il traffico, con un impatto minimo sulle prestazioni. Questo richiede un'architettura proxy scalabile.
- Acquisiscano e analizzino le informazioni approfondite ottenute tramite l'ispezione per applicare protezione dalle minacce avanzate e policy avanzate di classificazione dei dati per prevenirne la perdita.
- Ispezionino tutto il traffico proveniente da utenti, entità, carichi di lavoro, e altre entità, incluso quello criptato.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

Se non offrono la possibilità di ispezionare tutto il traffico, incluso quello criptato, i provider di soluzioni SSE non possono affermare di fornire i migliori servizi di protezione dalle minacce avanzate e di prevenzione della perdita di dati.

Diffida dei provider che lo fanno, poiché molto dipende dall'architettura su cui si fonda la soluzione. I provider che hanno sviluppato il proprio proxy come una soluzione interamente nativa del cloud, hanno un netto vantaggio.

Si stima che l'85% di tutto il traffico Internet sia criptato. Per questo motivo, è necessario che venga ispezionato su larga scala e in profondità, in modo che il provider SSE possa garantire un'adeguata protezione dalle minacce e prevenire la perdita di dati per far fronte alla crescita esponenziale dei rischi associati ai canali criptati. Perché la decrittazione SSL/TLS su larga scala è così importante (vedi la Figura 8)?

- La crittografia SSL/TLS può nascondere contenuti dannosi, come virus, spyware e altri tipi di malware.
- Gli aggressori sviluppano i propri siti web con la crittografia TLS e SSL o iniettano contenuti dannosi in siti conosciuti e attendibili che utilizzano i protocolli SSL e TLS.
- I protocolli SSL/TLS possono celare la perdita di dati, come la trasmissione di documenti finanziari sensibili di un'organizzazione.
- I protocolli SSL/TLS possono nascondere la navigazione su siti web appartenenti a classi oggetto di responsabilità legale.
- La capacità di controllare e ispezionare il traffico da e verso i servizi online HTTPS è diventata un elemento cruciale per la sicurezza di un'azienda.

Figura 8: l'architettura passthrough impiegata da alcuni provider non fornisce l'ispezione del traffico criptato su larga scala. Si può paragonare a un posto di blocco che permette alle auto di passare senza controllare il bagagliaio, che potrebbe contenere qualcosa di illecito.

Alla luce di questi rischi, l'architettura di un provider SSE deve essere in grado di garantire scalabilità per operare come un intermediario per il traffico SSL/TSL, fornendo un'analisi completa dei contenuti in entrata e in uscita e bloccando immediatamente qualsiasi minaccia rilevata nel cloud.

Gli aggressori continuano a innovare gli strumenti, le tecniche e le procedure che utilizzano per colpire le aziende. Fra questi, vi è l'uso improprio di provider di servizi di archiviazione legittimi, come Dropbox, Box, OneDrive e GDrive, per l'hosting di carichi utili dannosi. Queste connessioni utilizzano certificati SSL/TLS con caratteri jolly di questi noti fornitori quando distribuiscono i carichi utili dannosi che, se non ispezionati, consentono all'attacco di andare a buon fine. I carichi utili dannosi (file eseguibili, documenti d'ufficio, ecc.) sono inoltre di natura polimorfa, poiché l'obiettivo è quello di eludere i controlli di rilevamento di base delle impronte digitali (fingerprint). L'architettura dei provider SSE deve consentire l'estrazione completa del carico utile da queste connessioni criptate con SSL/TLS e, per consentire un rilevamento accurato, deve essere in grado di decomprimere e rivelare questi file. (vedi la Figura 9).

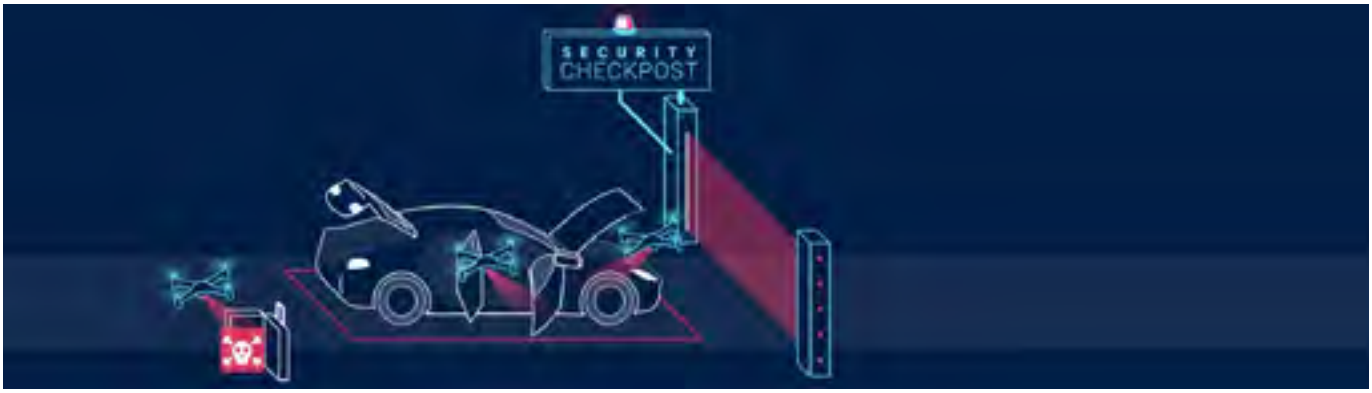

Figura 9: il provider SSE giusto fornisce un'ispezione SSL/TLS completa di tutto il traffico utilizzando un'architettura proxy. Questa modalità di ispezione si può paragonare a un posto di blocco in cui le auto vengono fermate e controllate a fondo prima che possano procedere

Questa protezione dovrebbe sfruttare i molti dati sulle minacce del settore provenienti da fonti open source, commerciali e private, e deve svolgere aggiornamenti di sicurezza frequenti.

Oltre a bloccare le minacce, l'ispezione su larga scala consente di implementare una prevenzione avanzata della perdita di dati. **I provider di soluzioni SSE devono essere valutati in base alle loro capacità di classificare i dati**, che dovrebbe includere le espressioni regolari (regex) come meccanismo di base; inoltre, rilevare e classificare rapidamente i dati sensibili su tutti i canali di dati cloud, è un requisito fondamentale per proteggere dati personali, sanitari e riservati e prevenirne la perdita. Tale classificazione richiede l'ispezione SSL/TLS e consente di mettere in atto funzionalità avanzate come:

- **Corrispondenza esatta dei dati (Exact Data Matching, o EDM)**. Le soluzioni SSE utilizzano modelli di indicizzazione per identificare un record da un'origine dati strutturata che corrisponda a criteri predefiniti.
- **Creazione di impronte digitali (fingerprint) per i documenti**. Le soluzioni SSE utilizzano un archivio di documenti per identificare quelli completamente o parzialmente corrispondenti durante la valutazione del traffico in uscita.
- **OCR (Riconoscimento ottico dei caratteri)**. La soluzione SSE rileva i dati sensibili all'interno di file immagine, immagini integrate, screenshot e testi scritti a mano, e chiude tutti i canali di esfiltrazione dei dati con base cloud.
- **Machine Learning.** Le decisioni in merito al livello di sensibilità dei dati vengono prese da algoritmi pre-istruiti.

Figura 10: allo stesso modo in cui un motore a combustione interna non può essere usato su un veicolo elettrico, è necessario prestare attenzione ai provider che utilizzano funzionalità come l'ispezione SSL/TLS con architetture legacy

Il Security Service Edge include la funzionalità CASB (Cloud Access Security Broker) per il monitoraggio e l'applicazione di policy agli utenti dei servizi cloud e delle app, ed essere in grado di ispezionare il traffico criptato inline presenta una serie di vantaggi in questo ambito. L'ispezione può essere "fuori banda", che prevede la scansione delle API dei provider SaaS per proteggere i dati inattivi, o "inline", e cioè la scansione dei dati in movimento. Ti consigliamo di prestare particolare attenzione a quest'ultima funzionalità, poiché l'ispezione inline impedisce che i dati vengano caricati su app non autorizzate, che vengano scaricati su dispositivi non autorizzati e che vengano scaricati o caricati contenuti dannosi. Il provider della soluzione SSE dovrebbe inoltre consentire il controllo granulare degli accessi in base a un set di definizioni di app cloud, controlli sui tipi di file e attributi di rischio.

Con l'adozione di centinaia e migliaia di applicazioni cloud, i dati sensibili delle aziende oggi sono ampiamente distribuiti. I due principali canali di esfiltrazione dei dati sono il desktop cloud e le applicazioni delle e-mail personali. Una buona soluzione SSE dovrebbe fornire visibilità e applicazione delle policy in modo contestuale e completo se gli utenti malintenzionati caricano dati sensibili su Box, Dropbox e altri desktop cloud personali. Dovrebbe inoltre bloccare l'esfiltrazione dei dati su servizi di webmail personali e non autorizzati, come Gmail e Hotmail.

I provider di soluzioni SSE si contraddistinguono principalmente in base all'efficienza con cui decriptano e ispezionano tutto il traffico SSL/TLS in modo scalabile ed elastico senza influire negativamente sulle prestazioni. Tutto ciò può essere realizzato solo con una soluzione SSE basata su proxy, sviluppata sin dal principio con l'obiettivo di garantire scalabilità (si veda la Figura 10).

È importante approfondire il modo in cui il provider SSE riesce a raggiungere questo obiettivo. Per mantenere una latenza minima a ogni ispezione di pacchetti, il provider deve utilizzare un'architettura a passaggio singolo (single pass), in cui il pacchetto viene collocato nella memoria una sola volta e i servizi di ispezione, ciascuno con risorse CPU dedicate, sono in grado di eseguire le scansioni contemporaneamente. I provider che effettuano queste ispezioni con applicazioni fisiche e virtuali serializzate, vengono penalizzati ad ogni hop durante l'elaborazione, e corrono il rischio che a ogni pacchetto sia applicata eccessiva latenza.

Questi vantaggi architetturali devono essere applicati agli standard più recenti, come il protocollo TLS 1.3, dove una vera architettura proxy ha il vantaggio di essere inline, con due connessioni separate al client e al server. Poiché ciò consente di riassemblare e scansionare l'intero oggetto, è possibile applicare la protezione dalle minacce avanzate, la prevenzione della perdita di dati e impiegare sandbox. Assicurati che le versioni TLS e gli aggiornamenti di cifratura siano gestiti dal provider direttamente all'interno del cloud; alcuni provider con base hardware potrebbero effettuare aggiornamenti forzati delle appliance per gestire il carico aggiuntivo e continuare a offrire supporto alla cifratura.

Data la potenziale complessità che potrebbe essere introdotta, è necessario prendere in considerazione anche la gestione dei certificati. I provider di soluzioni SSE devono consentire ai clienti di utilizzare i loro certificati o di portare i propri, e dovrebbero permettere la rotazione tra i due tramite l'API. I certificati devono quindi essere replicati automaticamente tra i vari service edge.

Ti consigliamo di diffidare dei provider di soluzioni SSE che associano la loro capacità di ispezione SSL/TLS a firewall di nuova generazione esistenti, perché questi ultimi hanno problemi intrinseci di scalabilità. Questo vale anche per i provider che trasferiscono i firewall di nuova generazione con funzionalità di ispezione di istanze virtuali su nodi di calcolo CSP

⚠ A cosa fare attenzione:

Quando valuti la capacità dei provider di soluzioni SSE di ispezionare il traffico SSL e TLS, assicurati di verificare che la latenza sia accettabile. Purtroppo, con le architetture non native del cloud, si può andare incontro a cali significativi delle prestazioni, specialmente quando si utilizza il protocollo TLS 1.2 o le versioni precedenti. **Anche la privacy dei dati può rappresentare un problema, ed è quindi importante comprendere i vincoli normativi e il modo in cui il provider li gestisce**. Una soluzione SSE dovrebbe consentire di escludere facilmente determinati tipi di dati in modo da poter assicurare il rispetto delle norme. Inoltre, non dovrebbe mai archiviare i dati degli utenti sul cloud.

Ti consigliamo di diffidare dei provider di soluzioni SSE che associano la loro capacità di ispezione SSL/TLS a firewall di nuova generazione esistenti, perché questi ultimi hanno problemi intrinseci di scalabilità. Questo vale anche per i provider che trasferiscono i firewall di nuova generazione con funzionalità di ispezione di istanze virtuali su nodi di calcolo CSP Inoltre, presta attenzione ai provider che combinano le funzionalità CASB fuori banda con un'ispezione del traffico inline limitata. La protezione dei dati inattivi e dei dati in movimento è fondamentale.

Valuta il modo in cui il provider gestisce i certificati e tieni presente che l'associazione dei certificati potrebbe rappresentare un problema.

L'implementazione dell'ispezione SSL/TLS è sempre stata difficoltosa per le aziende, per svariati motivi. **Il provider della soluzione SSE deve mostrare esperienza e affidabilità, e fornire assistenza e supporto durante l'implementazione di queste funzioni. L'ispezione SSL/TLS** non è negoziabile nel mondo del Security Service Edge, perché non deve esserci alcun compromesso sulla sicurezza.

Esiti:

L'ispezione SSL/TLS su larga scala con latenza minima incrementa significativamente la capacità di bloccare le minacce, e sfrutta la potenza del cloud per identificare e proteggere i dati sensibili. Solo le soluzioni SSE con la giusta architettura nativa del cloud ti permettono di ottenere:

- Un'ispezione SSL/TLS di tutto il traffico con un impatto minimo sulle prestazioni, per una protezione maggiore a tutela dei dati e contro le minacce.
- Un'architettura a passaggio singolo per ottenere vantaggi unici di scalabilità e per garantire la decriptazione su larga scala.
- L'esperienza per supportare i clienti e aiutarli ad affrontare le sfide che li porteranno a ottenere l'ispezione completa del traffico SSL/TSL.

N° 4
Errore

Scegliere una soluzione SSE non personalizzabile e che non supporti opzioni flessibili, scalabili e diversificate di distribuzione e gestione

Considera invece soluzioni SSE che:

- Offrano modelli di distribuzione flessibili per proteggere utenti e applicazioni, indipendentemente dalla posizione di queste ultime, siano esse in data center, cloud pubblico, nodo di calcolo all'edge e siti on-premise.
- Offrano protezione agli utenti finali che accedono alle applicazioni tramite dispositivi o strumenti gestiti e non gestiti.
- Estendano la stessa protezione impiegata per proteggere i dati e contro le minacce informatiche per tutelare tutte le altre comunicazioni tra carichi di lavoro all'interno dello stesso cloud o su più cloud.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

Durante la scelta di una soluzione SSE è necessario valutare la disponibilità del proprio ambiente per capire come applicare al meglio la protezione. Per supportare vari scenari di distribuzione, i provider di soluzioni SSE devono consentire l'utilizzo di service edge pubblici e privati.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

Durante la scelta di una soluzione SSE è necessario valutare la disponibilità del proprio ambiente per capire come applicare al meglio la protezione. Per supportare vari scenari di distribuzione, i provider di soluzioni SSE devono consentire l'utilizzo di service edge pubblici e privati.

La maggior parte degli utenti si connetterà alla soluzione SSE tramite il service edge pubblico di un fornitore. Si tratta di Gateway Internet sicuri con funzioni complete e broker di applicazioni private che forniscono una sicurezza integrata. Ispezionano tutto il traffico in modo bidirezionale alla ricerca di malware, e applicano sicurezza, conformità e policy dei firewall; inoltre, gestiscono centinaia di migliaia di utenti simultaneamente, con milioni di sessioni in contemporanea. Per questo motivo, indipendentemente da dove si trovino, gli utenti possono accedere da qualsiasi dispositivo:

- Internet, con service edge pubblici che proteggono il traffico e applicano le policy aziendali.
- Applicazioni interne, con policy di accesso e riautenticazione applicate in base a best practice aziendali.

Figura 11: una soluzione SSE deve offrire opzioni con service edge pubblici e privati. Questi devono funzionare in armonia tra loro, con una gestione centralizzata

È importante assicurarsi che questi service edge pubblici abbiano considerevoli capacità di tolleranza ai guasti e siano distribuiti in modalità attivo-attivo per garantire disponibilità e ridondanza. Per offrire disponibilità continua, il provider deve effettuare il monitoraggio e la manutenzione dei service edge pubblici. Inoltre, per garantire la privacy dei dati, il traffico dei clienti non deve essere trasferito su altri componenti all'interno dell'infrastruttura, e non deve mai essere memorizzato su disco.

Tuttavia, in alcune situazioni il service edge pubblico potrebbe non soddisfare i requisiti richiesti, ed è per questo motivo che il provider deve offrire anche opzioni di service edge privati (vedi la Figura 11). In questo modo, si estendono l'architettura e le capacità del service edge pubblico alle sedi di un'azienda o in una posizione privata, e si sfrutta la stessa policy controllata centralmente dei service edge pubblici.

Per consentire un accesso sicuro a Internet, i service edge privati possono essere installati nel data center di un'azienda. Questi sono dedicati al traffico aziendale, ma è il provider della soluzione SSE a doversi curare della loro gestione e manutenzione, in modo che l'azienda se ne debba occupare il meno possibile Questa modalità di distribuzione, in genere, va a vantaggio delle organizzazioni che presentano determinati requisiti geopolitici o che utilizzano applicazioni che richiedono che l'indirizzo IP sorgente sia quello dell'organizzazione.

Per l'accesso alle applicazioni interne, il service edge privato fornisce una gestione analoga delle connessioni tra l'utente e l'applicazione. Applica le stesse policy del service edge pubblico, e il servizio è ospitato in sede o nel cloud pubblico, ma viene comunque gestito dal provider della soluzione SSE. Questo modello di distribuzione consente di applicare lo zero trust all'interno dell'ambiente, perché è utile per ridurre la latenza delle applicazioni quando queste ultime e gli utenti si trovano nella stessa posizione (mentre raggiungere il service edge pubblico comporterebbe ulteriore latenza). Inoltre, è un'opzione che fornisce resilienza in caso di interruzione della connessione Internet. La soluzione deve distribuire immagini per l'utilizzo in data center aziendali e in ambienti cloud privati locali.

Per fornire una protezione zero trust alle applicazioni interne, i provider di soluzioni SSE devono permettere di creare un'interfaccia sicura e autenticata tra i server delle applicazioni e i service edge pubblici e privati, affinché queste applicazioni siano protette. **Questo meccanismo dovrebbe essere disponibile in diversi formati**: un'immagine standard di macchina virtuale (VM) o una distribuzione in container in data center aziendali, in ambienti cloud privati locali, come VMware, o in ambienti cloud pubblici, come Amazon Web Services (AWS) EC2, e pacchetti da installare sulle distribuzioni Linux supportate.

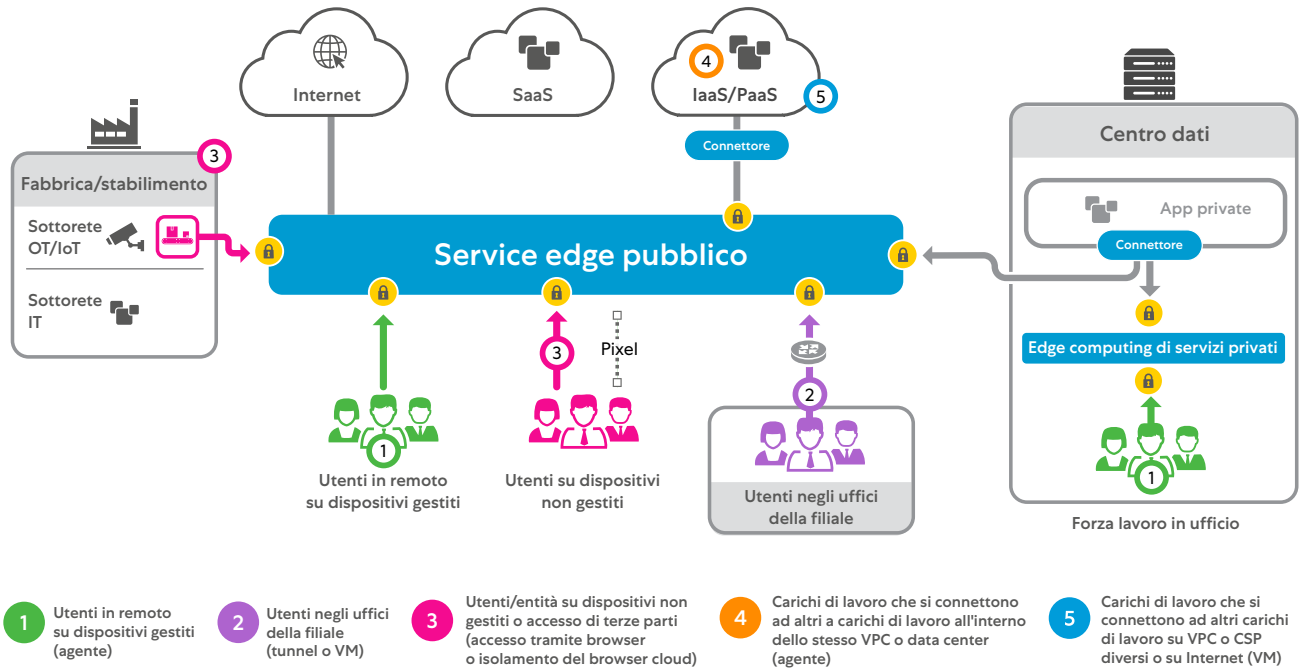

Figura 12: il provider della soluzione SSE dovrebbe supportare diverse modalità di distribuzione e gestione, tenendo conto degli utenti in remoto, di quelli nelle filiali e nella sede centrale, dei carichi di lavoro che comunicano con altri carichi di lavoro, ecc., tramite agenti e VM.

Una volta stabilito da dove verranno amministrate e applicate le policy, considera anche il modo in cui questa protezione verrà fornita agli utenti e ai carichi di lavoro. È importante prendere in considerazione diversi scenari (vedi la Figura 12):

Per gli utenti in remoto su dispositivi gestiti, il provider della soluzione SSE deve offrire un singolo agente unificato che inoltri il traffico al service edge per garantire un accesso sicuro a Internet. L'agente dovrebbe inoltre fornire un accesso granulare e basato su policy alle risorse interne. Tutto questo dovrebbe essere automatico e fare uso dell'intelligence integrata nell'agente. Dovrebbe inoltre proteggere il traffico mobile degli utenti su reti Wi-Fi o mobili. L'agente inoltra il traffico al servizio SSE, che applica le policy di sicurezza e di accesso dell'azienda indipendentemente dalla posizione degli utenti e stabilisce un trasferimento sicuro per l'accesso alle app e ai servizi aziendali. Assicurati che l'agente sia in grado di rilevare le reti attendibili e, in questo caso, se, in base alle policy aziendali, debba disattivare il suo servizio. Assicurati anche che gli agenti supportino vari sistemi operativi, inclusi Windows, macOS, Linux, iOS e Android.

Per gli utenti delle filiali, un metodo comune di inoltro del traffico verso il service edge è tramite tunnel GRE o IPSec. Tuttavia, la soluzione SSE dovrebbe offrire un approccio alternativo. Una macchina virtuale installata nella filiale può semplificare la complessità e l'amministrazione continua di questi tunnel ed eliminare il movimento laterale delle minacce, rimuovendo la rete instradabile gestita dal cliente. La distribuzione deve essere automatizzata e includere policy flessibili di indirizzamento del traffico verso il service edge, con monitoraggio degli accordi sul servizio e failover integrati. Questa opzione è ideale per le filiali di medie e grandi dimensioni e per quelle che offrono servizi in sede.

L'opzione precedente, in cui ogni utente viene trattato come un utente in remoto, dovrebbe essere presa in considerazione per le filiali più piccole, in cui non vengono offerti servizi in sede (pensa, ad esempio, al modello di una caffetteria). L'importanza delle filiali è cambiata con gli eventi recenti, e questa opzione è ideale perché non consente a nessuno di entrare sulla rete aziendale e previene il rischio del movimento laterale.

Per gli utenti/entità su dispositivi non gestiti o per l'accesso di terzi alle applicazioni web interne, i provider di soluzioni SSE devono fornire una protezione SSE analoga, senza la necessità di installare agenti. Questi utenti devono autenticarsi su un browser web che applichi la protezione zero trust pubblicando un record CNAME specifico per l'applicazione nella relativa zona DNS, in modo che il browser possa reindirizzare automaticamente le richieste. In alternativa, il provider deve disporre di una funzionalità integrata di isolamento del browser cloud (Cloud Browser Isolation, o CBI), per una sicurezza senza agente che agisca su qualsiasi dispositivo non gestito e in qualsiasi luogo. In questo modo, si elimina completamente la necessità di un fragile proxy inverso.

Con l'isolamento del browser cloud (Cloud Browser Isolation, o CBI), gli amministratori configurano il Single Sign-On di una risorsa cloud autorizzata per il reindirizzamento al provider della soluzione SSE. Dopodiché, quando gli utenti tentano di accedere a questa risorsa cloud da un endpoint personale o di terze parti, il loro traffico viene inviato automaticamente al CBI, senza che sia necessario installare software. I contenuti vengono forniti sotto forma di pixel che vengono inviati ai dispositivi degli utenti, e non è possibile effettuarne il download, il copia e incolla e la stampa. In questo modo, gli utenti possono svolgere le proprie mansioni lavorative dagli endpoint non gestiti senza il rischio di fuoriuscite dei dati e di upload di malware, il tutto rispettando i requisiti di conformità.

Per i carichi di lavoro che si connettono ad altri carichi di lavoro all'interno dello stesso VPC o data center, in passato si procedeva alla segmentazione tradizionale della rete. Sebbene ciò avesse senso in linea teorica, ottenere la segmentazione della rete nella pratica era un'operazione complessa. Ed è per questo che i provider di soluzioni SSE devono estendere la protezione anche alle comunicazioni tra carichi di lavoro. Con l'installazione di un agente sul carico di lavoro stesso, il provider SSE deve determinare il rischio e applicare una protezione basata sull'identità, senza alcuna modifica alla rete, e deve disporre di policy che si adattino automaticamente ai cambiamenti nell'ambiente.

I provider devono estendere la stessa protezione anche ai carichi di lavoro che si connettono ad altri carichi di lavoro su VPC, CSP o su Internet e offrire un meccanismo, che generalmente è tramite macchina virtuale (disponibile in cloud pubblici o hypervisor on-premise), che semplifichi l'inoltro del traffico al service edge. Il risultato è l'applicazione della protezione dalle minacce informatiche e dei dati anche ai carichi di lavoro diretti a Internet, nonché la protezione zero trust applicata ai carichi di lavoro su un cloud che accedono ai carichi di lavoro su un altro cloud. Con questo approccio, i provider SSE sono in grado di consolidare più prodotti (ad es. proxy web, firewall, gateway NAT, filtri URL, ecc.) in un'unica soluzione.

Per proteggere i dati inattivi negli ambienti IaaS e SaaS, il provider deve inoltre fornire soluzioni CASB, CIEM (Cloud Infrastructure Entitlements Management) e CSPM (Cloud Security Posture Management). In questo modo, è possibile effettuare la scansione API per le applicazioni SaaS e IaaS più diffuse e identificare e correggere gli errori di configurazione e le autorizzazioni improprie negli ambienti cloud. Inoltre, queste funzionalità sono abbinate a verifiche e scansioni di piattaforme SaaS e IaaS per una maggiore tutela dei dati e protezione contro le minacce. Un provider SSE deve offrire tali funzionalità fuori banda in perfetta sintonia con le proprie funzioni inline, per applicare policy coerenti ai dati inattivi e a quelli in movimento.

Il vantaggio di ottenere tutto questo con un unico provider SSE è che può essere gestito da un piano di controllo centralizzato, con policy aziendali applicate in modo uniforme e dinamico a tutti gli utenti e a tutte le comunicazioni tra entità e applicazione e tra carichi di lavoro

⚠ A cosa fare attenzione:

La distribuzione della tecnologia SSE dipende in larga misura dalla complessità dell'ambiente dell'azienda. **È quindi molto importante comprendere la posizione, il comportamento, i requisiti di accesso dell'utente e i requisiti delle applicazioni**. Inoltre, alcuni Paesi, come ad esempio la Cina, presentano difficoltà uniche in termini di prestazioni, dovute a controlli Internet che nemmeno i modelli di distribuzione flessibili sono in grado di superare. Il provider della soluzione SSE dovrebbe offrire soluzioni innovative per rispondere a queste sfide.

Esiti:

Se implementate correttamente, queste opzioni flessibili, diversificate e scalabili offriranno all'azienda tutti i vantaggi del Security Service Edge, indipendentemente dalla posizione dell'utente, dell'entità, o dal luogo in cui è ospitata l'applicazione, ed estenderanno la protezione all'interno dell'applicazione stessa:

- Il vantaggio di avere un unico provider SSE che fornisca una protezione ad ampia copertura, è che può essere gestito da un piano di controllo centralizzato, con policy aziendali applicate in modo uniforme e dinamico a tutti gli utenti e a tutte le comunicazioni tra entità e applicazioni e tra carichi di lavoro.
- Estendendo la stessa protezione dei dispositivi gestiti ai dispositivi personali non gestiti e all'accesso di terzi, è possibile ottenere una maggiore flessibilità per collaboratori e dipendenti.
- La sicurezza delle comunicazioni tra carichi di lavoro consente ai tecnici DevOps e CloudOps di usufruire delle stesse protezioni zero trust, che vengono estese alle loro applicazioni che accedono ad altri carichi di lavoro, ad altri cloud o a Internet.

N. 5
Errore

Scegliere una soluzione SSE che non ottimizzi la connettività delle applicazioni e non diagnostichi il peggioramento delle prestazioni, e che quindi non sia in grado di offrire un'esperienza utente fluida

Considera invece provider di soluzioni SSE che:

- Siano trasparenti, forniscano un'autenticazione semplice e siano sempre attive, garantendo che gli utenti finali sulla piattaforma SSE godano di un'esperienza ottimale, impiegando misure oggettive.
- Siano in grado di associare un'esperienza utente scadente alle giuste cause, sia che si tratti di endpoint, rete, applicazione o del set di servizi per la sicurezza.
- Abbiano partnership con i principali provider SaaS, come Microsoft 365, per ridurre al minimo la latenza tra il service edge pubblico e la rete del provider delle applicazioni.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

I punti di presenza in tutto il mondo del provider SSE e le relazioni di peering su Internet con provider e fornitori di applicazioni sono una potente alternativa al backhauling e all'hairpinning richiesti dai set di servizi di sicurezza legacy.

Oltre a questi vantaggi architetturali, i provider di soluzioni SSE si trovano in una posizione favorevole per misurare e diagnosticare l'esperienza degli utenti finali grazie alla loro presenza negli endpoint degli utenti e nel percorso dei dati delle applicazioni. Questi vantaggi consentono ai provider di comprendere l'esperienza dalla prospettiva dell'endpoint dell'utente e di fornire informazioni diagnostiche più approfondite e maggiore scalabilità sfruttando l'infrastruttura del service edge pubblico.

Concentrati sui provider di soluzioni SSE che integrano una soluzione di monitoraggio (di solito chiamata **Monitoraggio dell'esperienza digitale** o DEM, Digital Experience Monitoring) nei loro agenti esistenti e nell'infrastruttura cloud. I provider che offrono soluzioni che richiedono ulteriori agenti, o che sono il risultato di acquisizioni scarsamente integrate, non saranno in grado di fornire lo stesso livello di visibilità e diagnostica.

La soluzione di monitoraggio offerta dal provider della soluzione SSE deve essere ampia, fornire visibilità end-to-end e assicurare la risoluzione dei problemi relativi alle prestazioni degli utenti finali, per qualsiasi utente o applicazione, indipendentemente dalla loro posizione. Inoltre, deve consentire ai team di rete, sicurezza, desktop e assistenza tecnica di effettuare il monitoraggio continuo, e di ottenere informazioni dettagliate sulle problematiche legate a dispositivi, reti e prestazioni delle applicazioni degli utenti finali. Infine, deve consentire flussi di lavoro reattivi, che aiutino a chiudere le richieste di assistenza per i problemi segnalati dai dipendenti, e flussi di lavoro proattivi, che consentano di identificare problemi macroscopici (come le interruzioni degli ISP regionali o periodi di inattività delle applicazioni globali), prima che gli utenti se ne accorgano. **Questa funzionalità deve fare uso di algoritmi di machine learning per il calcolo del punteggio che monitorino l'esperienza utente normale e anomala in base all'utente, all'applicazione, all'ufficio o alla geolocalizzazione**.

Il monitoraggio deve essere a più livelli, e deve includere il livello 7, per informazioni utili sui tempi di risposta delle applicazioni web, e il livello 3, per comprendere il comportamento della rete, con informazioni sul percorso, la latenza e la perdita di pacchetti. Questa analisi deve comprendere anche l'autodiagnosi del cloud del provider SSE, per identificare eventuali ritardi di hop. Infine, la soluzione deve fornire informazioni utili sullo stato del dispositivo endpoint dell'utente e identificarne gli eventi che contribuiscono al calo del punteggio **(vedi la Figura 13)**.

I provider di soluzioni SSE si trovano in una posizione favorevole per misurare e diagnosticare l'esperienza degli utenti finali grazie alla loro presenza negli endpoint degli utenti e nel percorso dei dati delle applicazioni.

Monitoraggio delle prestazioni di Microsoft Teams e Zoom e risoluzione dei problemi

Teams e Zoom sono diventate le principali piattaforme di collaborazione e comunicazione di molte aziende, e la valutazione e la diagnostica dei problemi di qualità audio/video sono diventate ancora più importanti. Le soluzioni di monitoraggio fornite dal provider della soluzione SSE dovrebbero essere in grado di interfacciarsi con le applicazioni UCaaS più popolari, come Zoom e Microsoft Teams, per acquisire metriche sulla qualità audio e video e associarle ad analisi approfondite e hop-by-hop della rete e dei dispositivi endpoint. Combinando questi set di dati, la soluzione di monitoraggio dovrebbe identificare i problemi di qualità e indicarne la causa principale.

Inoltre, il monitoraggio deve sfruttare la scalabilità del cloud del provider SSE e utilizzarlo come proxy per effettuare e memorizzare test telemetrici, in modo che si possano raccogliere dati granulari da ogni utente finale, a intervalli di pochi minuti, con un impatto minimo sulle applicazioni.

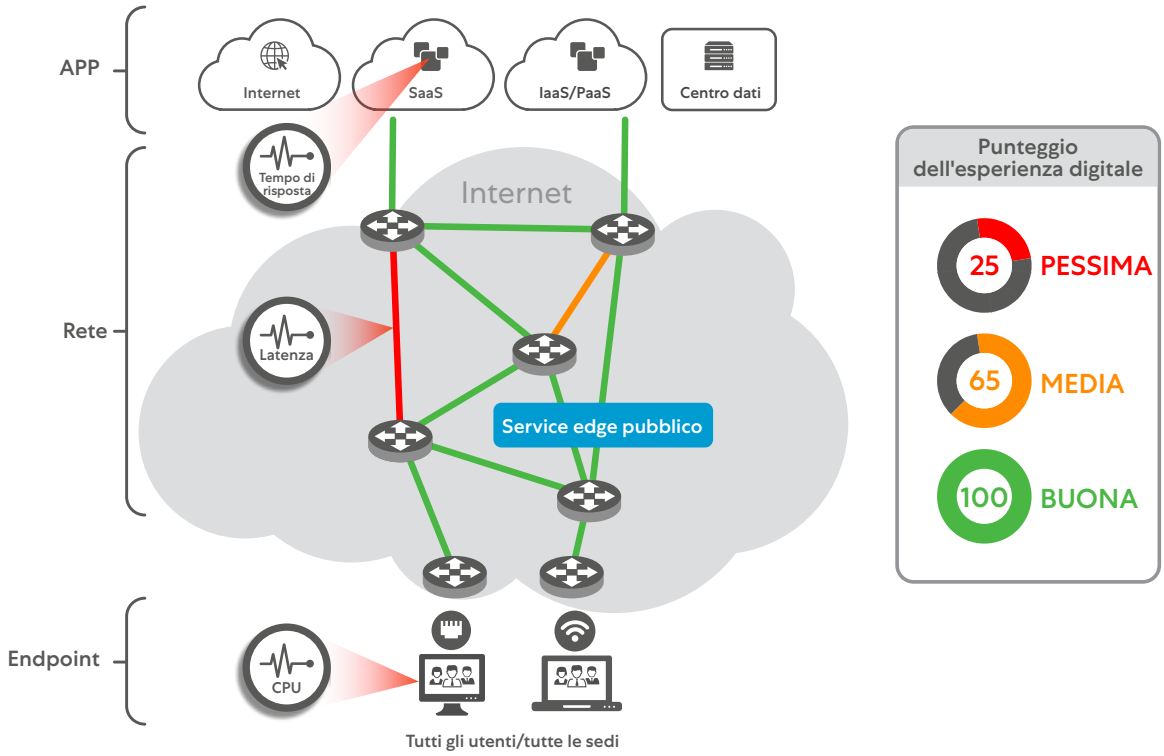

Figura 13: una soluzione di monitoraggio integrata nella piattaforma SSE deve fornire una visibilità unica sulla qualità dell'esperienza utente dalla prospettiva dell'utente finale e identificare i problemi relativi a endpoint, rete e applicazioni

Diffida degli strumenti di monitoraggio legacy che adottano un approccio incentrato sul data center per monitorare e raccogliere metriche da posizioni fisse, anziché direttamente dal dispositivo dell'utente. Questo approccio non fornisce una visione unificata delle prestazioni basata sul dispositivo dell'utente, sul percorso di rete o sull'applicazione, e offre poca visibilità quando utenti e applicazioni non si trovano sul data center o sulla rete aziendale. Questi strumenti creano silos di informazioni e non condividono alcun tipo di contesto, offrono una visibilità frammentata dell'esperienza utente e ritardano la risoluzione dei problemi. Gli strumenti di monitoraggio indipendenti, ottimizzati per i data center, presentano delle lacune di visibilità e ostacolano il rilevamento, la risoluzione e la diagnosi dei problemi prestazionali dell'utente finale su Internet; al contrario, una soluzione di monitoraggio moderna, integrata in una piattaforma SSE, offre una vasta selezione di dati per l'analisi delle cause principali dei problemi (vedi la Figura 14).

La soluzione di monitoraggio deve identificare gli utenti che riscontrano problemi di qualità e indicare la causa principale del peggioramento delle prestazioni.

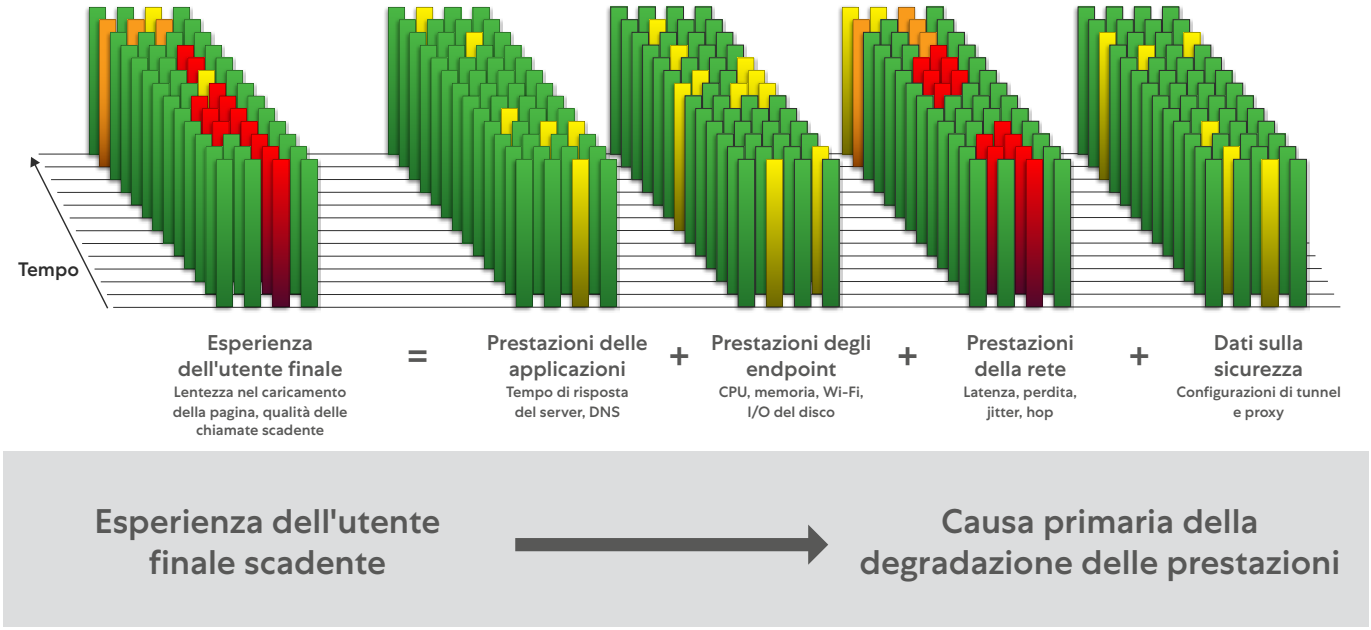

Figura 14: una soluzione di monitoraggio integrata nella piattaforma SSE deve fornire una visibilità unica sulla qualità dell'esperienza utente dalla prospettiva dell'utente finale e identificare i problemi relativi a endpoint, rete e applicazioni

Ottimizzazione dell'esperienza utente per M365

Oltre a monitorare l'esperienza utente finale, una soluzione SSE completa può arrivare a ottimizzare le prestazioni delle principali applicazioni SaaS, come Microsoft 365. In questi casi, la difficoltà è rappresentata dal fatto che molte aziende instradano il traffico a livello centrale, attraverso reti di tipo "hub and spoke" ed ExpressRoute. Inoltre, il traffico degli utenti di M365 incrementa l'utilizzo della rete del 40% e le infrastrutture del traffico in uscita su Internet della maggior parte delle aziende non sono in grado di adattarsi a questa richiesta; così, l'esperienza utente ne risente. Microsoft suggerisce di instaurare connessioni dirette a Internet e di accertarsi che l'architettura del provider SSE consenta di utilizzare punti di accesso a Internet locali per ottenere prestazioni ottimali e ridurre i costi.

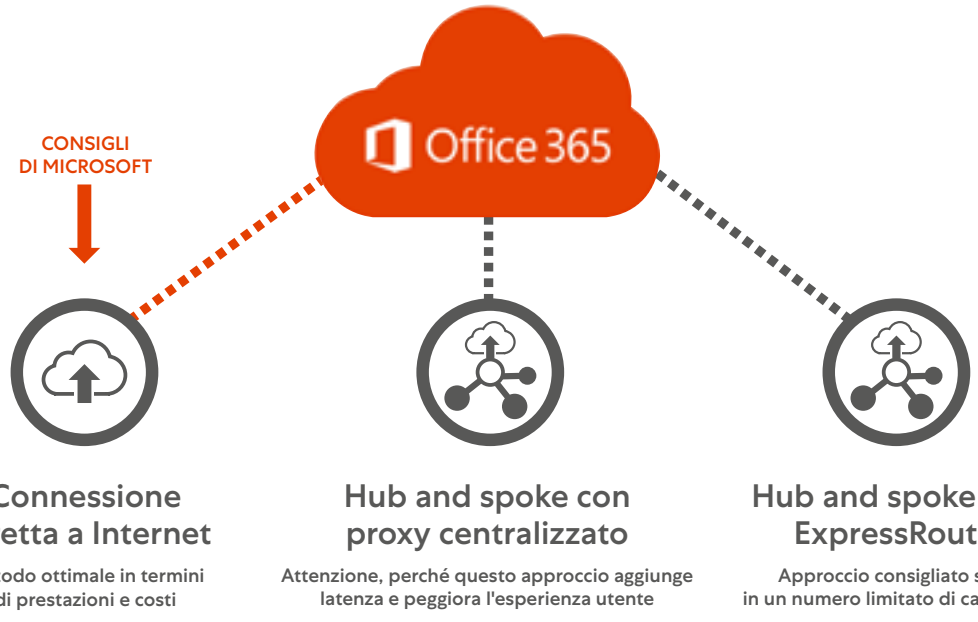

Figura 15: Microsoft suggerisce di instaurare connessioni dirette a Internet per ottenere prestazioni ottimali e costi ridotti, in linea con i principi del Security Service Edge (fonte: microsoft.com).

Ma l'architettura fa la differenza. I punti di presenza in tutto il mondo del provider della soluzione SSE e le relazioni di peering con provider e fornitori di applicazioni devono avvicinare l'edge agli utenti, per una connettività veloce e un accesso a bassa latenza. Cerca provider di soluzioni SSE che eseguano il peering mediante la fibra direttamente a Microsoft 365 nella maggior parte degli Internet Exchange principali per ridurre la latenza a circa 1-2 ms come tempo di round trip, che siano in grado di offrire scalabilità per gestire l'elevato numero di connessioni di lunga durata, che consentano download rapidi dei file e che forniscano una risoluzione DNS veloce con meno hop. (vedi la Figura 15).

Le transazioni di M365 sono particolarmente importanti nelle soluzioni SSE, perché l'ispezione di applicazioni come OneDrive e SharePoint aiuta a prevenire la perdita di dati sensibili. Fornisce inoltre un audit trail completo di ogni comunicazione, da e verso le applicazioni M365. Tuttavia, ricorda che alcune applicazioni M365, come Teams, potrebbero non dover essere ispezionate, dato che gran parte del traffico è in formato voce/video tramite UDP.

⚠ A cosa fare attenzione:

Nel nostro mondo in cui si lavora da qualsiasi luogo, ci sono molti anelli deboli nell'insieme di reti cablate e wireless che dovrebbero garantire le prestazioni ottimali delle applicazioni. L'ottimizzazione dell'esperienza utente è un'operazione complessa anche per le architetture di livello superiore e per i set di strumenti dedicati alle attività di valutazione e diagnostica. È essenziale stabilire delle aspettative ragionevoli con gli utenti finali su ciò che costituisce un'esperienza utente accettabile per le applicazioni critiche. Queste aspettative devono quindi essere utilizzate come base di riferimento da monitorare e gestire.

La diagnosi dei problemi dell'esperienza utente è più un'arte che una scienza. Richiede un'architettura e degli strumenti d'eccellenza, ma anche le giuste competenze per interpretare e agire sui dati. Se da un lato gli strumenti di monitoraggio offerti dai provider SSE aiutano a identificare la maggior parte delle cause dei problemi (Wi-Fi, ISP, backbone, endpoint o problemi DNS), alcuni di questi problemi richiederanno ulteriori azioni e set di dati aggiuntivi. Ad esempio, potrebbero essere necessari log e tracce di pacchetti per individuare le cause principali di alcuni di questi problemi, mentre ce ne saranno altri che non si riusciranno a risolvere, e questo rientra comunque nella normalità delle cose.

Diffida dei venditori che effettuano l'hairpinning del traffico. I data center di un provider SSE dovrebbero essere tutti in grado di eseguire l'elaborazione e l'ispezione, per consentire un'esperienza utente più rapida e fluida. L'architettura nativa del cloud non dovrebbe effettuare l'hairpinning del traffico verso delle posizioni centralizzate per l'ispezione. Ad esempio, se un utente si connette a Melbourne, l'ispezione del traffico dovrebbe avvenire localmente con servizi di prevenzione delle minacce e protezione dei dati, senza che si verifichi il backhauling in altre regioni, come Sydney o Singapore. I provider di soluzioni SSE che gestiscono il loro cloud con strumenti di iperscalabilità (o hyperscaler) spesso finiscono con l'effettuare l'hairpinning del traffico degli utenti. Un hyperscaler può avere 120 punti edge, ma è probabile che l'80% di essi sia costituito da percorsi on-ramp per portare il traffico verso un numero inferiore di data center hyperscaler in cui è possibile applicare il controllo delle policy SSE. È importante capire quanti data center sono su percorsi on-ramp e quanti sono effettivamente in grado di applicare le policy.

Esiti:

Il successo di qualsiasi trasformazione, sia essa digitale, della rete o della sicurezza, è guidato dall'esperienza dell'utente finale. L'obiettivo finale di qualsiasi progetto SSE è quello di migliorare l'esperienza dell'utente finale, riducendo l'esposizione alle minacce e proteggendo i dati sensibili. Quindi, è ideale che la capacità della soluzione SSE di migliorare l'esperienza utente possa essere valutata con strumenti di monitoraggio. Questo dovrebbe essere un compito facile, perché l'abbandono dell'hairpinning verso i data center e delle VPN sono metodi consolidati per migliorare l'esperienza utente:

- La soluzione SSE dovrebbe modernizzare l'esperienza utente e il processo di assistenza tecnica. Con un approccio proattivo al monitoraggio dell'esperienza utente, i team di assistenza possono intervenire prima di ricevere lamentele da parte degli utenti.
- La soluzione SSE dovrebbe fornire informazioni utili sulle prestazioni audio e video in tempo reale per le piattaforme di collaborazione come Teams e Zoom.
- La soluzione SSE deve raccogliere le metriche a livello di applicazione, endpoint e rete, per individuare le anomalie e consentire la determinazione delle cause principali.
- Il provider della soluzione SSE deve fornire un numero minimo di hop tra il cloud e le destinazioni più popolari, come Microsoft 365.

N. 6
Errore

Scegliere una soluzione SSE senza un set completo di integrazioni e orchestrazioni con un ecosistema di fornitori terzi

Considera invece provider di soluzioni SSE che:

- Si integrino tramite API solide con altre soluzioni d'eccellenza dell'ecosistema, (come CSP, SD-WAN, IAM, SOAR/SIEM, EDR, ecc.) per garantire una protezione ottimale e un'esperienza utente di alto livello.
- Utilizzino queste integrazioni per abilitare l'automazione e l'orchestrazione e ridurre la complessità operativa e i costi.
- Non incrementino il debito tecnico generato dalla combinazione incoerente di un insieme di soluzioni scarsamente integrate, sia tra loro che verso terzi.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

La maggior parte delle organizzazioni alle prese con un debito tecnico sa che questo è dovuto all'implementazione, nel corso degli anni, di tecnologie che non riescono a operare in concerto.

Per non parlare delle cosiddette "piattaforme" offerte da provider singoli che non sono realmente integrate, ma che consistono in una raccolta di prodotti indipendenti che non condividono nulla tra loro, se non la dashboard. Spesso, queste tecnologie richiedono competenze specializzate per riuscire a instaurare e gestire la fragile coesistenza con altre tecnologie complementari. Il Security Service Edge è in grado di eliminare gran parte di questo debito tecnico, grazie a una piattaforma di sicurezza unificata nel cloud offerta da un unico provider. Partendo da questa visione di base, il Security Service Edge è comunque il risultato della combinazione di varie tecnologie complementari, e l'obiettivo principale dei provider deve essere quello di garantire l'interoperabilità all'interno di questo ecosistema, che è costituito da strumenti di sicurezza, di rete e cloud (**si veda la Figura 16**).

Figura 16: non isolarti scegliendo un provider che non abbia un ricco ecosistema di integrazioni con terze parti. Questo genererebbe un debito tecnico, interoperabilità limitata e un set fragile (e non agile) di servizi di sicurezza.

Per garantire una distribuzione e un'integrazione che siano rapide, semplici e sicure, il fornitore di SSE deve fornire integrazioni con i leader in:

- Provider di servizi cloud (CSP), sia IaaS/PaaS che SaaS
- Rilevamento e risposta degli endpoint (Endpoint detection and response, o EDR)
- SD-WAN
- Gestione delle identità e degli accessi (Identity and Access Management, IAM)
- SIEM (Security Information and Event Management)/SOAR (Security Orchestration, Automation, and Response)
- Strumenti di orchestrazione

Queste integrazioni devono consentire l'orchestrazione tra il provider della soluzione SSE e altri provider, per ridurre la complessità, il costo totale di proprietà e migliorare il profilo di sicurezza (vedi la Figura 17).

Provider di servizi cloud (IaaS/PaaS e SaaS)

Per le applicazioni interne native del cloud o che vi vengono spostate, la soluzione SSE deve integrare i principali provider IaaS/PaaS, come AWS, GCP e Azure, per fornire una connettività basata sull'accesso remoto sicuro e zero trust alle applicazioni. Così facendo, queste ultime non vengono mai esposte a Internet, e rimangono completamente invisibili agli utenti non autorizzati. La connessione avviene tramite una connettività dall'interno verso l'esterno e basata su policy, e non tramite l'estensione della rete.

Questo approccio assicura l'accesso diretto al cloud senza una VPN di accesso remoto, con la possibilità di sfruttare i vantaggi di scalabilità del provider di servizi cloud senza aggiungere la complessità della segmentazione della rete. Inoltre, non si basa su dispositivi virtuali o fisici e offre i vantaggi dello zero trust per eliminare la superficie di attacco.

Per le applicazioni SaaS più diffuse, i provider di soluzioni SSE dovrebbero offrire integrazioni semplificate. Nel caso di Microsoft 365, l'integrazione dovrebbe mappare tutti gli intervalli IP e i domini di Microsoft per le app di M365 elencate e consentire l'inoltro trasparente del traffico degli utenti finali al relativo cloud. Inoltre, il peering con Microsoft 365 riduce il tempo di round trip, migliora la scalabilità e consente download dei file e risoluzione DNS più veloci.

L'integrazione del Security Service Edge con altri fornitori SaaS, come ServiceNow, può migliorare la protezione dati. Durante la scansione dei dati nuovi ed esistenti di ServiceNow, il provider della soluzione SSE deve identificare i dati sensibili all'interno dei file in base alle policy di prevenzione della perdita dei dati e bloccarne il caricamento in uscita. L'integrazione con ServiceNow Security Incident Response consente di orchestrare le azioni di risposta, tra cui l'aggiornamento di liste di blocco personalizzate. IP, domini e URL rischiosi possono essere bloccati senza l'intervento manuale, mentre gli errori di configurazione del cloud possono essere risolti per ridurre il rischio di violazioni.

Rilevamento e risposta degli endpoint (Endpoint Detection and Response, o EDR)

Il provider della soluzione SSE deve integrarsi con diversi partner per la sicurezza degli endpoint, per condividere i dati telemetrici, migliorare la visibilità reciproca e orchestrare le risposte. Queste integrazioni consentono di implementare strategie di difesa avanzata che permettono di adottare l'approccio zero trust in modo efficace ed efficiente.

L'integrazione dovrebbe permettere di valutare l'identità, la posizione e il comportamento del dispositivo dell'utente per implementare automaticamente le policy di accesso condizionale appropriate. Inoltre, la correlazione e il flusso di lavoro multipiattaforma permettono di accelerare le indagini e la risposta. Ciò comporta:

- La valutazione dello stato dei dispositivi e l'implementazione automatica delle policy di accesso appropriate.
- L'identificazione delle minacce 0-day e la correlazione con la telemetria degli endpoint, per identificare i dispositivi interessati e mettere in atto risposte rapide utilizzando flussi di lavoro con quarantena multipiattaforma.
- L'indagine sulle minacce con il contesto degli endpoint e della rete per incrementare l'efficienza del rilevamento e del processo decisionale.

SD-WAN

Il provider della soluzione SSE deve integrarsi con i provider di SD-WAN per semplificare l'instradamento del traffico dalla filiale e la creazione di punti di accesso locali a Internet sicuri.

Una soluzione SSE/SD-WAN congiunta può consentire un accesso sicuro e basato su policy a Internet e alle applicazioni fondamentali e fornire una protezione identica a tutti gli utenti, ovunque e per ogni connessione alle applicazioni cloud e alla rete Internet aperta. Le soluzioni SD-WAN possono essere integrate con il Security Service Edge tramite le API. Grazie a questa soluzione combinata, gli uffici delle filiali aziendali sono in grado di gestire l'aumento del traffico cloud e Internet senza dover ricorrere al backhauling verso la DMZ centralizzata nel data center, utilizzando un'architettura WAN ibrida per trasformare la rete e un robusto sistema di sicurezza.

I provider di soluzioni SSE dovrebbero essere indipendenti dalla rete, e non legati in modo esclusivo a una rete underlay. In realtà, molti dei vantaggi della rete SD-WAN derivano dalla sua funzionalità "software-defined", ma non necessariamente dalla WAN, che estende intrinsecamente la rete aziendale e consente il movimento laterale delle minacce. I responsabili delle decisioni sul Security Service Edge dovrebbero valutare attentamente i motivi per cui continuano a estendere la rete aziendale alle filiali e iniziare a considerare degli approcci alternativi più sicuri, come l'utilizzo della sola rete Internet.

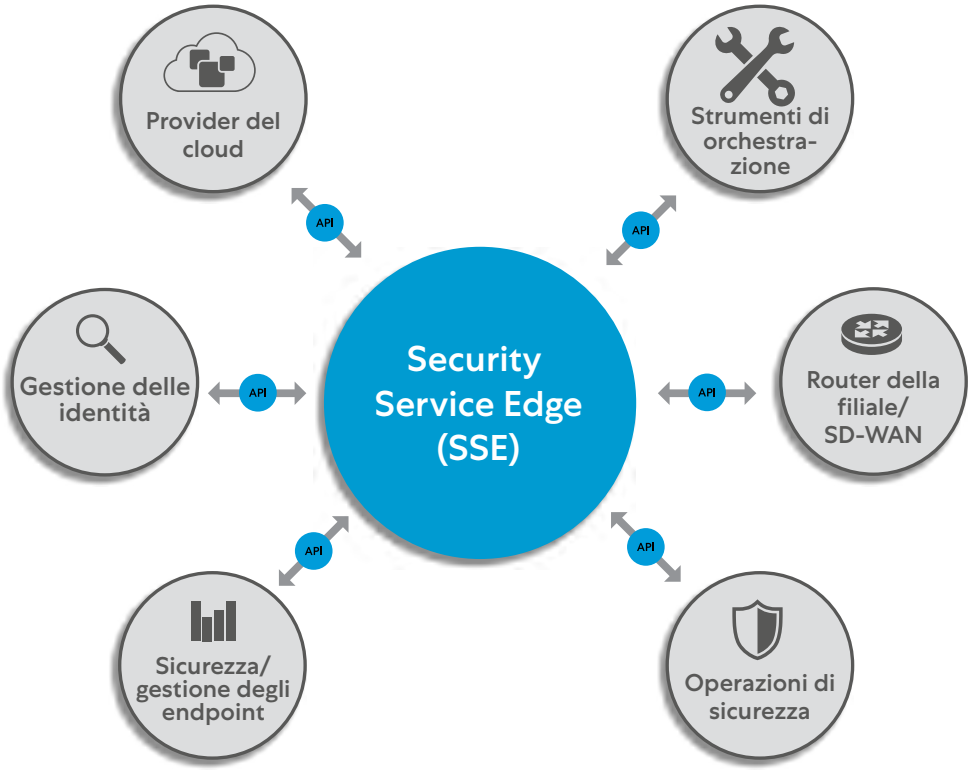

Figura 17: i provider di soluzioni SSE devono offrire integrazioni con gli operatori e le soluzioni migliori del settore.

Gestione delle identità e degli accessi (Identity and Access Management, o IAM)

I provider di soluzioni SSE dovrebbero fornire integrazioni con soluzioni di gestione delle identità e degli accessi, per applicare un accesso zero trust basato sul profilo del dispositivo e offrire una protezione dalle minacce più efficace a livello aziendale.

Utilizzando standard come il Security Assertion Markup Language (SAML), la distribuzione dell'integrazione dovrebbe essere semplice. Gli utenti dovrebbero essere in grado di autenticarsi e godere di un accesso sicuro a Internet e alle applicazioni interne. Le soluzioni IAM gestiscono l'accesso degli utenti finali alle applicazioni tramite una combinazione di Single Sign-On e autenticazione a più fattori, mentre il provider della soluzione SSE si occupa di proteggere la connessione. Il supporto del protocollo SCIM (System for Cross-domain Identity Management, sistema per la gestione delle identità tra domini) consente di mantenere sincronizzate tra i due sistemi tutte le informazioni relative agli utenti, come i cambi di gruppo, di ruolo, e le cancellazioni degli account per gli utenti che lasciano l'azienda.

SIEM e SOAR

I provider di soluzioni SSE dovrebbero prevedere integrazioni con i provider SIEM (Security information and event management) e SOAR (Security orchestration, automation and response), al fine di consentire una gestione efficiente ed efficace dei rischi e della conformità con l'automazione e l'arricchimento delle informazioni.

I provider delle soluzioni SSE devono essere in grado di inviare i dati di log, praticamente in tempo reale, alle soluzioni SIEM/SOAR in cloud e on-premise, per agevolare la correlazione dei log da più origini, consentendo così alle aziende di analizzare i modelli di traffico su tutte le loro reti. Inoltre, le aziende devono essere in grado di usare i dati di log nel SIEM per eseguire analisi storiche estese (> 6 mesi). In questo modo si garantisce la conformità ai requisiti normativi attraverso l'archiviazione locale dei log.

Strumenti di orchestrazione

Poiché infrastruttura come codice (IaC) e DevSecOps costringono i team di sicurezza ad attuare strategie di "shift-left", i provider di soluzioni SSE devono fornire le API per l'orchestrazione. In questo ambito, l'attenzione è rivolta alle applicazioni interne in cui l'implementazione dell'accesso zero trust fa parte del ciclo di distribuzione delle applicazioni, attraverso script di orchestrazione (come Ansible o Terraform), in particolare per le configurazioni relative alla segmentazione da utente ad applicazione o da carico di lavoro a carico di lavoro. Un'orchestrazione di questo tipo consente alle funzionalità zero trust di essere allineate con i metodi agili utilizzati dagli sviluppatori di software.

Poiché infrastruttura come codice (IaC) e DevSecOps costringono i team di sicurezza ad attuare strategie di "shift-left", i fornitori di SSE devono fornire le API per l'orchestrazione

⚠ A cosa fare attenzione:

I responsabili delle decisioni sul Security Service Edge, devono valutare se le integrazioni delle API sono avanzate e con quanta frequenza vengono effettuati gli aggiornamenti. Inoltre, è necessario prestare attenzione ai cambiamenti nel mercato che potrebbero ostacolare future integrazioni (come nel caso in cui un provider acquisito diventi parte della concorrenza). Tieni a mente anche l'eventuale scarsità di competenze nella tua azienda, poiché l'implementazione di queste integrazioni, in particolare nel caso di utilizzo con strumenti legacy, richiederà conoscenze specializzate.

Esiti:

I provider di soluzioni SSE che offrono solide integrazioni API con terze parti, permettono di ottenere un'efficienza maggiore, grazie alla capacità di coordinare le migliori soluzioni del settore e di ridurre l'isolamento derivante dall'utilizzo di un unico fornitore.

- I provider SSE che si integrano con le principali soluzioni dell'ecosistema (come CSP, SD-WAN, IAM, SOAR/SIEM, EDR, ecc.) fanno sì che la loro tecnologia sia a prova di futuro e riducono il debito tecnico.
- Un ecosistema orchestrato di fornitori integrati riduce la complessità operativa e i costi e può diminuire gli errori imputabili all'operatore.
- I provider di soluzioni SSE che raggruppano un insieme incoerente di soluzioni diverse attraverso le acquisizioni tendono a rimanere indietro nell'innovazione dei prodotti e spesso non offrono interoperabilità con terze parti.

N. 7
Errore

Scegliere una soluzione SSE non in grado di rivelare rapidamente il proprio valore con un'esecuzione pilota in un ambiente di produzione

Considera invece provider di soluzioni SSE che:

- Consentano di testare con semplicità la soluzione con un singolo agente unificato, con l'accesso a un set globale di service edge (vicini all'utente) e un'interfaccia utente centralizzata e facile da usare.
- Consentano di testare i molti aspetti della piattaforma SSE con requisiti minimi di distribuzione aggiuntiva.
- Siano in grado di garantire che la loro soluzione funzionerà come previsto al momento della distribuzione completa, con uno sforzo post-vendita minimo.

Figura 18: assicurati che il test del provider SSE sia con la soluzione reale e non con una replica fittizia. Solo un'esecuzione pilota in un ambiente di produzione può dimostrare l'effettivo valore della soluzione SSE.

Ecco cosa contraddistingue i provider di soluzioni SSE vincenti:

L'adozione di una piattaforma SSE richiede il ripensamento dell'architettura di sicurezza; quindi, la scelta della soluzione non deve essere presa alla leggera. È fondamentale comprendere la reale capacità del provider della soluzione di operare nel tuo ambiente di produzione. La facilità con cui ciò avviene è rappresentativa dell'architettura della piattaforma.

Durante la scelta di una piattaforma SSE, è necessario comprendere i passaggi necessari per avviare un'esecuzione pilota. Idealmente, il processo dovrebbe consistere nel trovare un modo per inoltrare il traffico al service edge SSE, dove subentra il cloud del provider SSE. I passaggi dovrebbero essere minimi per l'amministratore del Security Service Edge, il quale dovrebbe limitarsi a definire un meccanismo di inoltro, configurare le policy di base e occuparsi di autenticazione e reportistica. Naturalmente, le configurazioni di policy avanzate richiederanno più tempo.

L'esecuzione pilota deve rivelarsi all'altezza rispetto a una serie di obiettivi aziendali e coinvolgere i membri di vari team, tra cui sicurezza, rete e desktop (ad esempio per l'installazione degli agenti endpoint). Tuttavia, il coinvolgimento attivo di questi team dovrebbe essere minimo, perché sono alla ricerca di una soluzione che fornisca loro una serie di servizi. Diffida dei provider SSE che richiedono un intervento significativo dei team, in particolare di quelli di rete, per gestire degli scenari di routing complessi nell'esecuzione pilota.

Durante la pianificazione di un'esecuzione pilota completa della soluzione SSE, adotta un approccio sequenziale che rifletta gli obiettivi aziendali:

1. Esamina il profilo di sicurezza, le policy, l'infrastruttura di rete e i requisiti delle applicazioni, la tecnologia di autenticazione, le opzioni di inoltro del traffico e la capacità.
2. Identifica un insieme di utenti/servizi di origine e un insieme di applicazioni di destinazione su cui lanciare un'esecuzione pilota.
3. Abilita l'inoltro del traffico per gli utenti selezionati; di solito si utilizza un singolo agente, ma è anche possibile creare dei tunnel dalla posizione della filiale, quindi distribuisci una o più macchine virtuali davanti alle applicazioni private scelte
4. Configura l'autenticazione degli utenti con il provisioning di un'integrazione con il provider dell'identità.
5. Configura la prevenzione delle minacce e della perdita di dati utilizzando modelli standard di protezione dalle minacce, policy per sandbox, policy di controllo del browser, policy per gli URL, policy per le app cloud, controllo dei tipi di file e integrazione delle API per le policy SaaS e firewall.
6. Configura il rilevamento dei server per applicazioni privatee le policy di accesso per tali app. Questa può essere una policy *.* per l'esecuzione pilota.
7. Configura l'ispezione SSL/TLS, le policy avanzate e le funzionalità aggiuntive, come CBI, DEM o CSPM.

Il provider della soluzione SSE dovrebbe essere in grado di mettere in atto tutti questi passaggi facilmente e in breve tempo (solitamente qualche giorno) e senza importanti modifiche del routing o della configurazione. Sebbene la distribuzione completa richieda ulteriori passaggi, come la configurazione di policy avanzate, la considerazione di diversi tipi di applicazioni ed endpoint e l'integrazione con altri agenti e tecnologie, il provider dovrebbe riuscire a mostrare il valore della piattaforma attraverso un'esecuzione pilota semplice, ma ben eseguita.

Durante l'esecuzione pilota, il provider della soluzione SSE deve essere in grado di dimostrare quanto segue, in linea con le sei pratiche precedenti descritte in questo documento:

- **Infrastruttura cloud globale con latenza minima per l'utente finale con disponibilità e prestazioni elevate.** Il provider deve dimostrare la propria capacità di far funzionare questo cloud adattandosi alla crescita del traffico e dimostrare l'effetto del failover.
- **Approccio zero trust per ogni sessione utente**, con protezione delle applicazioni private e pubbliche e persino delle comunicazioni tra carichi di lavoro (se l'esecuzione pilota lo richiede).
- **Protezione dalle minacce avanzate e DLP avanzata tramite peering nel traffico criptato**. La gestione dei certificati potrebbe richiedere ulteriori passaggi nell'esecuzione pilota, ma la capacità del provider di eseguire l'ispezione SSL/TLS con un'aggiunta di latenza minima costituisce un ottimo modo per contraddistinguerlo da un eventuale concorrente.
- **Opzioni di distribuzione flessibile**. Sebbene ciò non faccia parte dell'esecuzione pilota, il provider della soluzione SSE deve fornire un piano per proteggere tutti gli utenti, indipendentemente dalla posizione o dall'applicazione. Ciò potrebbe comportare la distribuzione di service edge privati o della funzionalità di isolamento del browser cloud per i collaboratori. È importante verificare che il provider sia in grado di soddisfare i requisiti della forza lavoro e delle applicazioni attraverso i propri modelli di distribuzione.

- **Esperienza utente ottimale**. Questa metrica riguarda la facilità d'uso (come funziona l'interfaccia dell'utente finale con l'agente fornito, ad esempio), e l'esperienza di accesso generale dell'utente alle applicazioni pubbliche e private sulla piattaforma SSE. Il provider dovrebbe essere in grado di valutare e diagnosticare un'ampia varietà di problemi prestazionali dell'utente finale (Wi-Fi, ISP, CPU, e altro). Questa capacità di valutare/diagnosticare dovrebbe essere integrata direttamente nella piattaforma SSE, senza la necessità di distribuire nuovi agenti.
- **Integrazione con fornitori terzi**. Anche se questo potrebbe non essere parte dell'esecuzione pilota, il provider deve fornire metodi per integrare i dati di log in uno strumento SIEM esterno o offrire l'integrazione con uno strumento di EDR esistente. Una volta iniziata la distribuzione effettiva, il provider della soluzione SSE dovrebbe analizzare l'ecosistema di strumenti esistenti e fornire consigli per l'integrazione.

Data la carenza di competenze e di personale che il settore si trova ad affrontare, ti consigliamo di concentrarti sui provider di soluzioni SSE che richiedono il minor carico di lavoro possibile.

Il vantaggio di passare a un modello di sicurezza SaaS è quello di potersi affidare alla soluzione SSE per svolgere compiti generalmente gestiti dal personale interno: l'esecuzione pilota dovrebbe fornire un'indicazione chiara di quanto impegno è richiesto per la distribuzione, la gestione e l'aggiornamento della soluzione SSE.

⚠ A cosa fare attenzione:

- Le esecuzioni pilota che non sono in grado di rispondere a eventi e problematiche impreviste che potrebbero sorgere durante la distribuzione effettiva.
- Verifica che il provider della soluzione SSE faccia attenzione alle esigenze del cliente e mostri il desiderio di superare gli eventuali problemi di distribuzione che si presentano.
- Ricorda che, molto probabilmente, non avrai la possibilità di testare la scalabilità in un'esecuzione pilota ed eventuali problematiche in questo senso potrebbero non essere immediatamente visibili. I provider di soluzioni SSE potrebbero riuscire a evitare i problemi di rete o di routing durante l'esecuzione pilota, e questi problemi potrebbero rivelarsi solo durante la distribuzione effettiva. Il provider giusto non deve fare affidamento su un particolare percorso di rete per poter funzionare.
- Considera anche il carico operativo richiesto e in che percentuale è suddiviso tra la tua azienda e il provider. Calcola l'intervento necessario per la distribuzione di produzione e per la manutenzione a lungo termine della soluzione.
- Alcuni provider SSE potrebbero non essere realmente SaaS. È necessario accertarsi che la gestione della soluzione SSE abbia il costo totale di proprietà più basso. Questo è particolarmente importante data la carenza di competenze a cui deve far fronte la maggior parte delle organizzazioni IT.

Esiti:

Un'esecuzione pilota efficace dimostrerà che la soluzione SSE è facile da distribuire, funziona nell'ambiente di produzione ed è in linea con gli obiettivi del cliente

- I provider di soluzioni SSE che consentono di testare integralmente la propria soluzione si riveleranno i migliori quando si procederà con le distribuzioni complete. Grazie al basso costo di proprietà, al singolo agente unificato, all'accesso a un set globale di service edge e all'interfaccia utente centralizzata e facile da usare, la manutenzione a lungo termine della soluzione è semplice. Tutte le distribuzioni su larga scala richiedono tempo e impegno, ma l'obiettivo deve essere quello di collaborare con il provider, affinché questi aspetti siano ridotti al minimo.
- L'architettura di una soluzione SSE dovrebbe fare in modo che aggiungere funzionalità sia facile, e che le distribuzioni aggiuntive siano minime (ad esempio agenti o VM aggiuntive). In questo modo, i clienti possono adottare un approccio graduale al Security Service Edge, sapendo che il passaggio da una fase all'altra non richiederà modifiche significative.
- In definitiva, è necessario avere la certezza che il provider della soluzione SSE consenta una distribuzione veloce in un ambiente di produzione e che sarà a disposizione qualora si verifichino problemi. I provider orientati al cliente che dispongono di un'architettura collaudata rappresentano la scelta migliore per assicurarsi che il proprio investimento per la sicurezza e la trasformazione della rete si riveli un successo.

Cosa dicono di noi

I momenti di massima espansione, che consentono alle aziende di effettuare investimenti significativi, sono molto rari. È per questo che le imprese devono considerare un approccio misurato per distribuire il Security Service Edge. Il campo di applicazione del Security Service Edge aziendale (come condiviso pubblicamente su https://trust.zscaler.com), che interessa tutti i possibili utenti, server, dispositivi, ecc., è delineato nel 2° errore. Ecco come gli attuali operatori del settore hanno affrontato l'adozione del modello SSE:

Prima testimonianza

Il cliente ha distribuito la piattaforma SSE di Zscaler per controllare con un approccio zero trust:

- L'accesso granulare ai servizi privati per gli utenti finali
- La sicurezza Internet dell'utente finale, con l'ispezione inline e la protezione dei dati
- La trasformazione della rete, che ha rimosso completamente gli utenti dalla rete
- La protezione di carichi di lavoro, Internet e accesso privato
- I limiti di accesso di terze parti

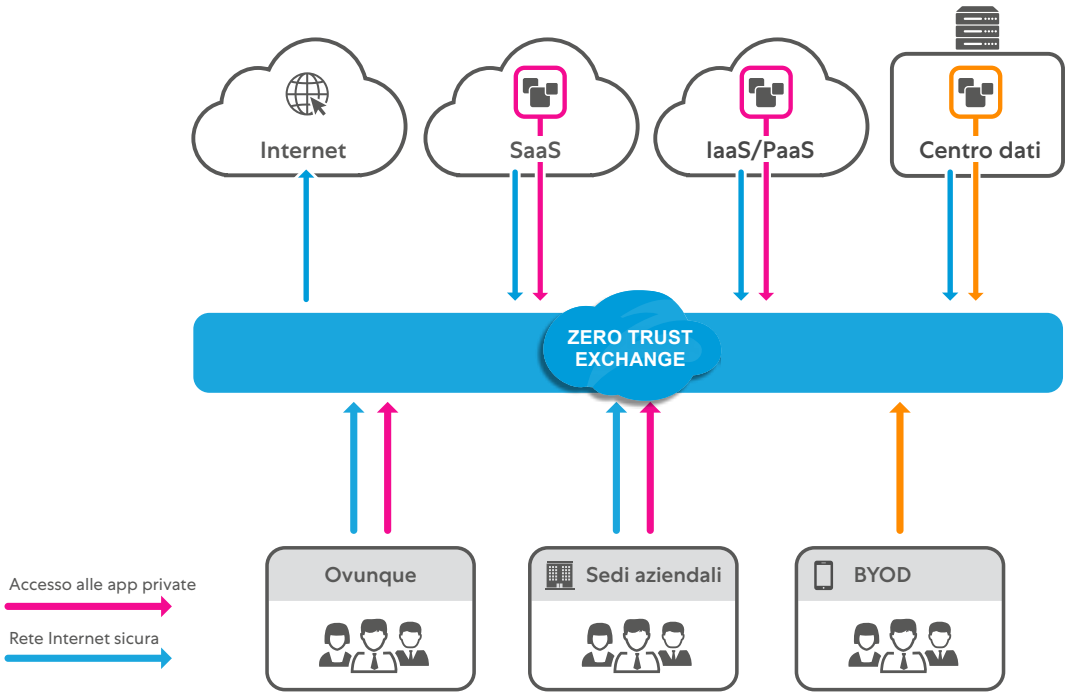

Figura 19: rappresentazione della connettività distribuita a livello aziendale con Zscaler

"In meno di cinque giorni, abbiamo trasferito in remoto 20.000 dipendenti, in modo fluido, sicuro e conveniente, sostituendo le VPN con la soluzione ZTNA di Zscaler".

Michael Alvmarken, Service Manager for Cybersecurity and Technology, Sandvik Group

"Sfruttando l'infrastruttura cloud di Zscaler e le integrazioni native con ZIA e ZPA, siamo riusciti a ottenere informazioni migliori sui dati degli utenti finali".

John Dawes, Director Enterprise Architecture, Reckitt Benckiser

"Rimuovendo il backhauling del traffico e utilizzando direttamente Internet, prevediamo di poter ridurre i costi del 70%".

Frederik Janssen, VP Global IT Infrastructure Portfolio, Siemens

Seconda testimonianza

- Il cliente ha implementato la piattaforma SSE di Zscaler per ottenere:
- Visibilità completa dell'accesso a tutti i servizi Internet (cloud e non solo)
- Controllo completo inline per limitare la perdita della proprietà intellettuale aziendale
- Monitoraggio dell'esperienza digitale dell'accesso degli utenti in remoto

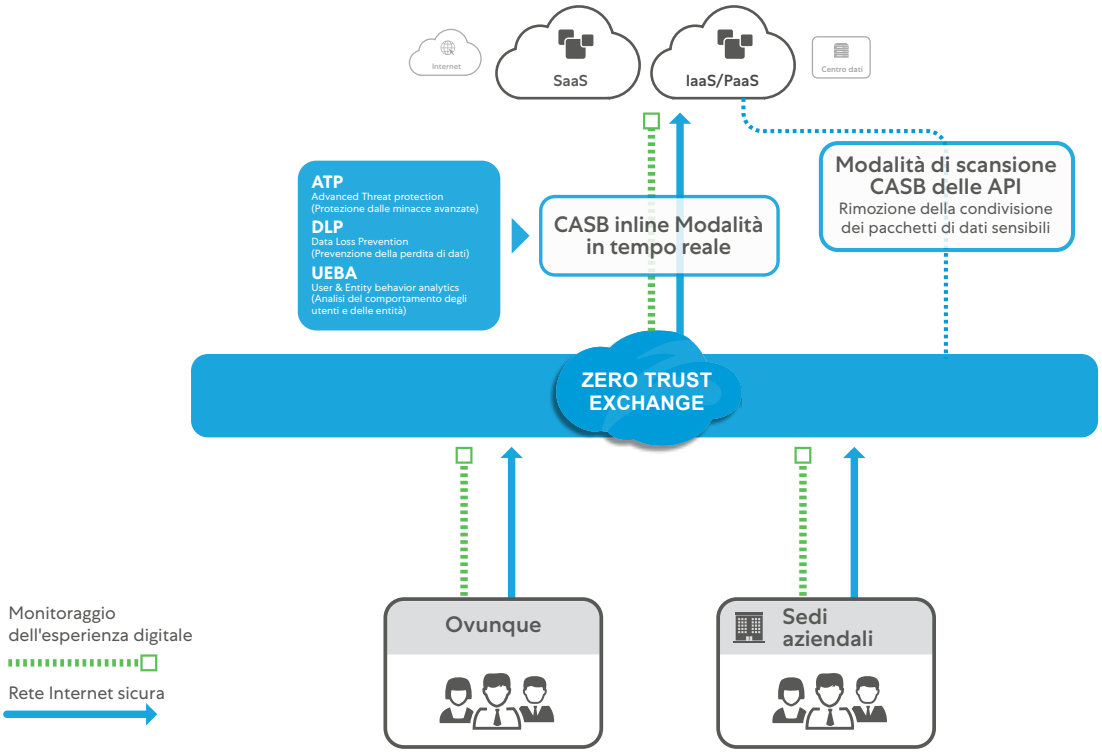

Figura 20: esempio di ispezione inline e monitoraggio dell'esperienza con Zscaler.

"Consideriamo Zscaler Digital Experience un servizio fondamentale per offrire un'esperienza produttiva ai lavoratori a distanza. In passato, riuscivamo a malapena a risolvere il 25% dei problemi degli utenti. Ora, ZDX è il punto di partenza per risolvere tutti i nostri problemi relativi all'esperienza utente, e siamo in grado di individuare le cause principali il 95% delle volte".

Ed DeGrange, Principal Security Architect, Ciena

"Che si tratti di un problema commerciale o di frode, indipendentemente che sia imputabile a un sito web o a una frode interna, tutto ha un impatto finanziario ed è per questo che la sicurezza informatica ha un ruolo cruciale".

Frederik Janssen, VP Global IT Infrastructure Portfolio, Siemens

"La funzionalità Advanced Cloud Sandbox di Zscaler ci consente di alleggerire il carico di lavoro per il reparto IT, che è fondamentale, perché le figure professionali con competenze mirate oggi scarseggiano, e le assunzioni sono estremamente difficoltose".

Mark Ferguson, CISO, Bombardier

Terza testimonianza

Il cliente ha implementato una protezione granulare dei servizi non IT, utilizzando la piattaforma Zscaler:

- Zero trust per la tecnologia operativa (OT), sia per i dipendenti che per i terzi
- Da OT a carico di lavoro
- Da cloud a carico di lavoro

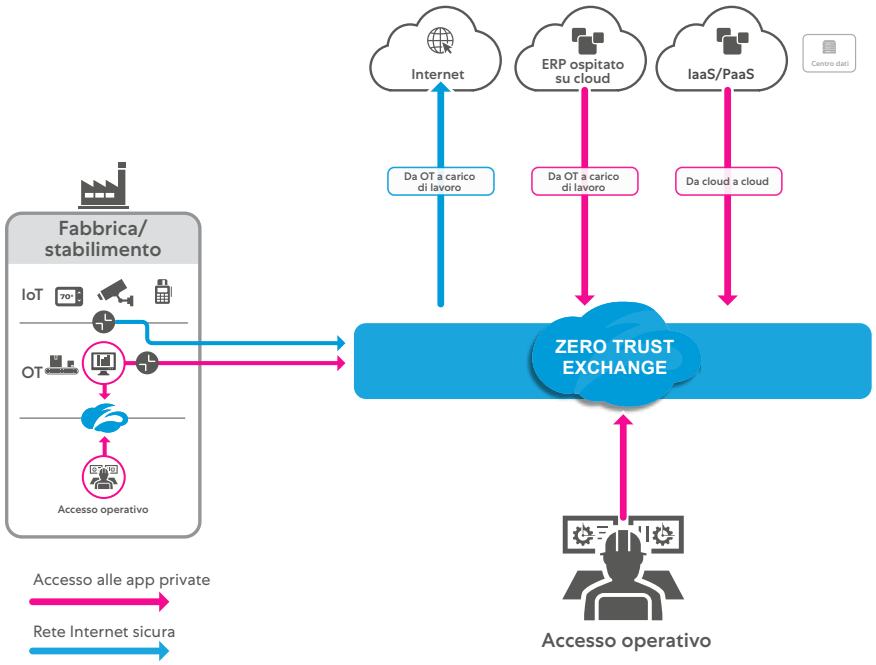

Figura 20: esempio di ispezione inline e monitoraggio dell'esperienza con Zscaler

Punti chiave da ricordare

- ☐ Il provider della soluzione SSE deve offrire accordi sul servizio documentati in base alla perdita o alla riduzione del servizio.
- ☐ La soluzione SSE deve offrire l'applicazione in tutte le sedi, inline, a livello globale e all'interno di punti di peering neutrali, garantendo il percorso più efficace verso i clienti.
- ☐ Il provider della soluzione SSE deve fornire controlli zero trust per tutti gli utenti, i carichi di lavoro e i dispositivi aziendali autorizzati, attraverso qualsiasi protocollo.
- ☐ La soluzione SSE deve fornire un servizio in modo indipendente su qualsiasi rete.
- ☐ La soluzione SSE deve fornire un'ispezione inline tramite un'architettura cloud proxy che garantisca una latenza minima e una visibilità completa su tutto il traffico web (fino al protocollo TLS 1.3 incluso).
- ☐ La soluzione SSE deve fornire più controlli di sicurezza attraverso un'architettura single-pass, per offrire vantaggi di scalabilità unici per la decriptazione su larga scala.
- ☐ Il provider della soluzione SSE deve fornire una soluzione con una gestione centralizzata e distribuibile in più forme, per rispondere alla specificità di posizione, regione, località e funzioni del cliente.
- ☐ La soluzione SSE deve essere ampliata per proteggere i dispositivi personali non gestiti (BYOD) e l'accesso di terze parti e dei partner, con lo stesso livello di controllo granulare a cui sono soggetti i dipendenti.
- ☐ Il provider della soluzione SSE deve ottimizzare l'esperienza utente monitorando e diagnosticando i problemi relativi alle prestazioni dei servizi aziendali (Team, Zoom, ecc.)
- ☐ La soluzione SSE deve raccogliere metriche dai percorsi delle applicazioni, dagli endpoint e dai livelli della rete, per identificare le anomalie e fornire informazioni ai team di supporto.
- ☐ Il provider della soluzione SSE deve integrarsi con i migliori strumenti dell'ecosistema (come CSP, SD-WAN, IAM, SOAR/SIEM, EDR, ecc.), per offrire controllo e sicurezza completi e avanzati all'intero panorama aziendale.
- ☐ La soluzione SSE deve essere integrata con questi fornitori per offrire un'orchestrazione che riduca al minimo il carico operativo.
- ☐ I provider di soluzioni SSE devono essere in grado di lanciare un'esecuzione pilota che testi le funzioni e le posizioni di cui l'azienda ha bisogno in produzione.
- ☐ La soluzione SSE deve poter essere estesa in tutta semplicità, senza la necessità di hardware o agenti aggiuntivi, e consentire alle aziende di aumentarne gradualmente l'utilizzo.

Per ulteriori informazioni sul Security Service Edge, vai su SSE Zscaler 2022

Informazioni sugli autori

Sanjit Ganguli (VP, Transformation Strategy / Field CTO) e Nathan Howe (VP, Emerging Technology & 5G), hanno carriere maturate in tutto il mondo e hanno fatto parte di aziende come Gartner, Nestlé, Riverbed e Verizon. La loro leadership è all'insegna dell'innovazione su cloud, sicurezza, trasformazione e tecnologie emergenti.