Edizione targata:

netskope

Security Service Edge (SSE)

for dummies

Progettare le risorse IT per il futuro della sicurezza cloud-based

Ottenere le funzioni CASB, SWG, ZTNA e Firewall attraverso un'unica piattaforma

Diventare esperti di SSE per l'architettura SASE e Zero Trust

Edizione speciale Netskope

Jason Clark

Steve Riley

Informazioni su Netskope

Netskope, il leader dell'architettura SASE, connette gli utenti direttamente a Internet, a qualsiasi applicazione e alla propria infrastruttura da qualunque dispositivo in rete e fuori rete in modo sicuro e veloce. Con CASB, SWG, FWaaS e ZTNA integrati nativamente in un'unica piattaforma, la tecnologia brevettata di Netskope Security Cloud garantisce un contesto altamente dettagliato per consentire l'accesso condizionato e migliorare la consapevolezza dell'utente, il tutto applicando i principi Zero Trust per proteggere i dati e prevenire le minacce, ovunque. Diversamente da altri vendor che propongono solo compromessi tra sicurezza e prestazioni di rete, il cloud privato di sicurezza globale di Netskope garantisce capacità di calcolo complete a livello edge.

Netskope è veloce ovunque, centrata sui dati e smart sul cloud, con una cittadinanza digitale di buona qualità e un costo totale di proprietà più contenuto. Maggiori informazioni su www.netskope.com.

Vogliamo ringraziare le persone che hanno reso possibile questo book:

In Netskope: Amanda Anderson, Lauren Baker, Chad Berndtson, Jeff Brainard, Tim Chiu, Tom Clare, Catie Halliday, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Sasi Murthy, Shamla Naidoo, Lauren Polito, Zoe Revis,

James Robinson, James Yokota, Svetlana Rubin

In Evolved Media: David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Security Service Edge (SSE)

for dummies®

Security Service Edge (SSE)

Edizione speciale Netskope

di Jason Clark e Steve Riley

for dummies®

Security Service Edge (SSE) For Dummies®, Edizione speciale Netskope

Editore
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-89721-7 (pbk); ISBN 978-1-119-89722-4 (ebk)

Ringraziamenti dell'editore

Fra coloro che hanno contribuito alla pubblicazione di questo book, si ringraziano:

Editore di progetto: Elizabeth Kuball

Direttore acquisizioni: Ashley Coffey

Caporedattore senior: Rev Mengle

Rappresentante sviluppo aziendale: Jeremith Coward

Direttore di produzione: Tamilmani Varadharaj

Assistenza speciale: Nicole Sholly

Indice

Introduzione

La transizione generale delle aziende verso il cloud sta avvenendo a una velocità molto superiore alle previsioni. Questo ha fatto sì che gran parte di loro continuasse ad affidarsi a piattaforme di sicurezza di un mondo ormai passato, dominato dai data center on-premise. La pandemia di COVID-19 ha ulteriormente accelerato e complicato la situazione sottoponendo a grande stress i responsabili della sicurezza a livello centrale (CISO), che devono proteggere il personale operativo da casa – che forse non tornerà mai a lavorare a tempo pieno in ufficio.

La buona notizia è che SASE (*Secure Access Service Edge*), un framework di architettura di sicurezza, indica la via verso una soluzione basata sul cloud in grado di garantire il livello di protezione necessario a qualsiasi azienda, indipendentemente da dove si trova il personale. Ma non finisce qui: SSE (*Security Service Edge*), ossia l'insieme dei servizi di sicurezza alla base di SASE, garantisce le funzioni richieste per proteggere i dipendenti da remoto, la tecnologia in cloud, nonché le applicazioni e le infrastrutture esistenti on-premise.

SASE è un quadro di riferimento. SSE è un insieme di servizi che possono essere acquistati subito. Questo book spiega cos'è SSE esplorando le sue fondamenta, sviluppate su concetti innovativi come Zero Trust e la sicurezza adattiva basata sul contesto e su nuovi approcci alla progettazione della rete. Nella seconda parte, spiega come diversi servizi si uniscono in SSE a nuove tecnologie avanzate, in grado di migliorare significativamente la sicurezza.

Informazioni su questo book

È tempo di ridefinire il panorama attuale della sicurezza. Conoscere meglio SSE consentirà allo staff della sicurezza e del business di prepararsi ai passi necessari per trasformare la sicurezza aziendale – attualmente considerata un collo di bottiglia– in un elemento amplificante e abilitanteamplificatore e della trasformazione digitale. Questo book prepara il terreno spiegando cosa sono SASE e SSE, per poi proporre una roadmap per dare vita al nuovo approccio alla sicurezza – un passaggio irrinunciabile per qualsiasi azienda che intende avvalersi del cloud. Nelle prossime pagine, spieghiamo come riuscirci.

Qualche presupposto scontato

Hai esperienza con Internet e la sicurezza. Sei consapevole di come il tradizionale modello di sicurezza utilizzato da tutti abbia raggiunto i suoi limiti. Sei consapevole anche di come il cloud possa essere al tempo stesso un incentivo alla produttività e sia un luogo pericoloso, dove le credenziali e i dati di utenti e aziende sono sotto attacco. Infine, ti interessa rendere meno difficile la sfida per l'azienda, i dipendenti, gli azionisti, i clienti e i partner commerciali grazie ai potenti strumenti SASE e SSE.

Icone usate in questo book

Le informazioni più importanti sono evidenziate in tutto il book con delle icone.

SUGGERIMENTO

L'icona Suggerimento mette a disposizione scorciatoie e altre informazioni per rendere più semplice la lettura.

RICORDA

L'icona Ricorda segnala fatti particolarmente importanti da sapere.

ATTENZIONE

L'icona Attenzione è importante per non farsi sfuggire nulla.

Oltre il book

Per ulteriori informazioni sulle soluzioni Netskope, visitare `www.netskope.com`. Per saperne di più su SSE (*Security Service Edge*), visitare `www.netskope.com/security-defined/security-service-edge-sse`.

IN QUESTO CAPITOLO

- **Esploreremo il futuro della sicurezza**
- **Comprenderemo gli effetti della trasformazione digitale della sicurezza**
- **Scopriremo come creare il "paradiso" della sicurezza che tutti vorremmo**

Capitolo 1
Come contesto ed integrazione accelerano la trasformazione digitale della sicurezza

Le organizzazioni stanno adottando applicazioni in cloud per gli evidenti vantaggi offerti in termini di velocità, efficienza e maggiore fruibilità delle informazioni. Per proteggere efficacemente dati, persone e applicazioni cloud, la sicurezza non può più essere fatta di semplici decisioni binarie "sì/no", come quando la rete regnava incontrastata e la maggior parte dei dipendenti lavorava in un unico luogo. La sicurezza, oggi più che mai, deve essere resa più dinamica ed intelligente, sulla base di un contesto dettagliato in che sia in grado di creare la protezione giusta per l'organizzazione, indipendentemente da dove si trovano i dipendenti. La sicurezza deve seguire i dati ovunque essi si trovino e deve essere semplice da applicare per non rallentare le attività.

Che direzione ha preso la sicurezza

Stiamo vivendo in un'epoca in cui la sicurezza ha un ruolo fondamentale. Le possibilità e la qualità delle tecnologie nel campo della sicurezza informatica stanno facendo passi da gigante. Mai come oggi, i professionisti del settore hanno dovuto fare i conti con così tanti cambiamenti in così poco tempo o hanno avuto l'opportunità di trasformare la sicurezza per aumentare il business. Dati,

applicazioni e dipendenti sono già migrati nel cloud. La sicurezza deve seguire questo cambiamento.

Le aziende che adottano un modello di sicurezza in cloud per rendere possibile la trasformazione digitale affronteranno questo cambiamento in modo più veloce e sicuro rispetto a quelle che rimarranno radicate a tecnologie tradizionali. Intravediamo una nuova era in cui i professionisti della sicurezza finalmente guadagneranno un vantaggio sugli attaccantie assisteranno le proprie aziende proprio mentre la trasformazione digitale spinta dal cloud sarà al suo apice.

I tentativi di portare a ogni costo i vecchi sistemi di sicurezza nel cloud si stanno rivelando vani. Come descritto dalle linee guida del SASE (*Secure Access Service Edge*), la sicurezza si sta trasformando per rispondere alle esigenze del luogo di lavoro ibrido e basato sul cloud.

ATTENZIONE

Anche i migliori prodotti e servizi di sicurezza tradizionali non funzioneranno nel cloud. E non servirà neanche modernizzare o etichettare diversamente la vecchia tecnologia per "abilitarla" al cloud.

Oggi, invece, i vendor di tecnologie per la sicurezza propongono nuovi prodotti e servizi cloud nativi capaci di offrire protezione quando si archiviano dati e si eseguono applicazioni su infrastrutture che le società stesse non controllano. Le nuove tecnologie per la sicurezza devono proteggere non solo l'*accesso* ai dati, ma anche il loro *uso*.

È utile guardare alla sicurezza cloud-ready sulla base di quattro concetti fondamentali:

- Il **SASE** è un modello architetturale di sicurezza aziendale basato sul cloud, che ha come obiettivo la convergenza per le funzioni di rete e sicurezza. Unisce concetti come Zero Trust, SD-WAN e SSE (*Security Service Edge*) per guidarci verso configurazioni di sicurezza e di rete che proteggono e governano il cloud e il nuovo ambiente di lavoro distribuito. Gli analisti riconoscono che questa nuova architettura fornisce una sicurezza totale per un mondo cloud-centrico (ved. *Designing a SASE Architecture For Dummies* di Netskope per un'introduzione completa).
- L'**SSE** è il modo in cui tutti i servizi di sicurezza necessari per il SASE – che prima consistevano in applicazioni, prodotti o servizi separati, spesso di vendor diversi – si presentano in forma unificata e integrata per offrire maggiore capacità ed efficienza, e ridurre complessità e costi. L'SSE rappresenta capacità di

sicurezza profondamente integrate, consapevoli le une delle altre, che lavorano bene insieme e sono fornite da un unico vendor. Netskope definisce ulteriormente un set di capacità estese che chiamiamo SSE vero e proprio (ved. capitolo 3).

- Il **contesto** determina in che modo le capacità di sicurezza integrate dell'SSE si applicano come meccanismo di controllo per mantenere dati, applicazioni e utenti al sicuro in ogni momento. Il contesto – ossia, una comprensione profonda di *chi* sia la persona, di *che cosa* stia cercando di fare e del *perché* (oltre al quando e al come) - rende inoltre possibile applicare policy di sicurezza adattive per mitigare i rischi in tempo reale. Prima le uniche opzioni erano "consenti" o "blocca". Ora invece un contesto ricco supporta variazioni al controllo degli accessi, come "consenti, con condizioni", per fornire una sicurezza solida senza interferire con la produttività. La qualità e la portata del contesto sono fondamentali elementi differenzianti tra i vendor.
- I principi **Zero Trust** differenziano le policy veramente adattive da una semplice autenticazione condizionata basata sulla familiarità. L'obiettivo non è solo fornire l'accesso e le autorizzazioni utili per eseguire un dato compito, secondo il livello di confidenza derivato da una valutazione in tempo reale dell'identità del dipendente e del metodo di accesso. L'accesso adattivo richiede informazioni approfondite su ciò che succede *dopo* il login: segnali ambientali che variano nel tempo, comportamento storico e attuale e le caratteristiche dei dati stessi. In Netskope, consideriamo lo Zero Trust il punto di partenza (nessuna fiducia all'inizio di ogni interazione) e puntiamo a raggiungere la *fiducia adattiva continua*, ossia via via commisurata al livello di confidenza e ai segnali ambientali stabiliti.

Questo libro spiega come tali concetti si fondono in un SSE applicato in modo efficace per creare un nuovo paradiso della sicurezza (ved. capitolo 3). Alla fine, le aziende avranno una sicurezza basata sul cloud con tutto ciò che è necessario per proteggere un mondo cloud-centrico di dati e applicazioni accessibili agli utenti, che sono – e rimarranno – in luoghi diffusi e spesso lontano da una sede centrale.

Forzare la trasformazione della sicurezza

I boom in molte aree della trasformazione digitale stanno rimodellando il mondo del business. La trasformazione della sicurezza è fondamentale per dare il giusto risultato all'impegno verso la trasformazione digitale.

RICORDA

Tecnologie come il cloud, l'IoT (Internet delle cose), il machine learning/l'intelligenza artificiale (ML/IA) e l'analitica sostanzialmente migliorano i risultati delle aziende. Se la sicurezza non riesce a tenere il passo, quel progresso è a rischio.

- **Il boom dei dati:** entro il 2025, IDC prevede che nel mondo ci saranno 175 zettabyte (ZB) di dati (ossia, una quantità fino a 25 volte superiore a quella del 2010). Come si può leggere sui giornali, i pirati informatici sottraggono dati alle aziende con intenzioni malevole: venderli, modificarli illecitamente o usarli per ricattare. Netskope Threat Labs ha scoperto che il cloud è un terreno fertile per gli attaccanti e che nel 2021 il 68% dei malware è stato diffuso attraverso il cloud (rispetto a meno della metà solo nel 2020). La crescita vertiginosa degli accessi ai dati dal cloud si traduce in più obiettivi da colpire per gli attaccanti e in più sfide per chi deve difendersi.
- **Il boom del cloud:** le aziende stanno adottando infrastrutture e applicazioni in cloud per migliorare in termini di velocità, flessibilità e agilità. Secondo Netskope Threat Labs, un'azienda media utilizzapiù di 800 diverse applicazioni SaaS (*Software-as-a-Service*), di cui ben il 97% è "shadow IT", ossia non gestito (e non visibile) dall'IT. Inoltre, le impostazioni di sicurezza predefinite di molte applicazioni cloud sono aperte, altro motivo per cui gli attaccanti considerano il cloud un obiettivo particolarmente interessante.
- **Il boom dei dispositivi:** le stime riguardo al volume dei dispositivi connessi a Internet variano enormemente, da 25 miliardi nel 2030 a nientemeno che circa 75 miliardi entro il 2025. Più dispositivi e più connettività creano un patrimonio tecnologico più vasto, e anche una superficie d'attacco più estesa. Ciò nonostante, questo fenomeno spesso porta a un'accelerazione nelle innovazioni.

RICORDA

La trasformazione della sicurezza consiste nel creare un nuovo sistema per gestire tutti questi fenomeni e quindi permettere alle aziende di fare il necessario per non avere problemi.

Le organizzazioni che non riescono a portare avanti la trasformazione della sicurezza basata sul cloud si trovano ad affrontare un rischio crescente. Anche se la sua efficacia diminuisce, l'attuale panorama della sicurezza è diventato troppo complesso, con ingenti spese per le aziende in conto capitale (CapEx) e operativo (OpEx) nonché costi del personale. I vendor devono, pertanto, ricostruire le funzioni in sistemi che collaborano fra loro.

Creazione di un paradiso della sicurezza

Le aziende che oggi pianificano il futuro della propria sicurezza devono immaginare come sarà il paradiso a cui aspirano, in generale e nel dettaglio. Efficienza e praticità, non il marketing o (se c'è differenza) le mode, dovrebbero guidare le loro decisioni.

Partendo dall'alto, ecco come potrebbe avvenire questa transizione:

1. **Trasformazione della rete.**

   La rete deve spostare i dati nel modo più efficiente possibile tra tutti i punti, inclusi i servizi cloud e il data center, senza scendere a compromessi sulla sicurezza in cambio di migliori prestazioni ed esperienze utente. Il traffico è instradato attraverso una rete costruita per supportare SSE e che consiste in punti di presenza (PoP) distribuiti a livello globale. Il personale in ufficio, a casa o al bar può godere di una sicurezza e prestazioni di alto livello, e i dati aziendali rimangono protetti.

2. **Consolidamento dei servizi di sicurezza.**

   Una suite unificata di un unico vendor che offre un SSE completo si sostituisce al mix di vecchie appliance di sicurezza. Le capacità combinate semplificano la gestione e l'amministrazione, garantiscono l'applicazione coerente delle policy e snelliscono l'elaborazione del traffico.

3. **Estensione dell'uso di SSE e implementazione di servizi di sicurezza avanzati.**

   Con SSE, i team addetti alla sicurezza possono introdurre potenti funzioni, come l'isolamento del browser da remoto (RBI), la gestione delle configurazioni di sicurezza del cloud (CSPM) e la gestione delle configurazioni di sicurezza SaaS (SSPM). Le capacità avanzate come la prevenzione della perdita di dati (DLP) e la protezione avanzata dalle minacce (ATP) funzionano meglio rispetto ai vecchi modelli, che sono frenati da un'integrazione minima e una visibilità limitata.

4. **Protezione dei dati nel cloud e nei dispositivi aziendali.**

   Lo stesso vendor SSE dovrebbe inoltre fornire un FWaaS (*FireWall-as-a-Service*) per proteggere le applicazioni cloud-based, dei dispositivi aziendali e delle repository di dati.

5. **Trattamento del data center come una qualsiasi altra destinazione.**

   Il data center tradizionale, un tempo l'unica destinazione attraverso cui veniva riportato tutto il traffico tramite backhaul, diventa ora una delle tante verso cui e da cui l'SSE instrada il traffico. L'eliminazione dell'hairpinning abbatte i costi, riduce la complessità e incrementa le prestazioni.

6. **Applicazione dei principi di Zero Trust per raggiungere uno stato di fiducia adattiva continua.**

   Poiché SSE monitora costantemente il traffico una volta dato l'accesso, i professionisti della sicurezza possono svolgere un'accurata analisi contestuale della sessione, prendere decisioni informate grazie alla risk intelligence di terze parti, rilevare le variazioni nei profili di rischio e neutralizzare le azioni pericolose. Le notifiche possono istruire i dipendenti su come migliorare le proprie abitudini ai fini della sicurezza.

7. **Miglioramento della gestione del rischio in tutta l'azienda con una visibilità maggiore.**

   La possibilità di vedere, guidare e controllare l'attività di tutti in azienda migliora considerevolmente la consapevolezza e la capacità di rilevare i rischi. Il team dedicato può concentrarsi sulle aree ad alto rischio e distribuire rapidamente delle policy migliorate nell'SSE. Mentre i leader della sicurezza godranno di una posizione migliore per decidere le strategie relative all'azienda e ai rischi.

La trasformazione della sicurezza non è impresa da poco. Il capitolo 4 mostra in che modo i principi di Zero Trust consentono un passaggio incrementale verso la piena implementazione della sicurezza cloud-based. Il capitolo 5 mette in evidenza gli errori più comuni e i principi del successo descrivendo inoltre un esempio che molte organizzazioni seguiranno se approcceranno SSE, Zero Trust e, in ultima istanza, SASE nel modo giusto.

IN QUESTO CAPITOLO

- **Rivedremo la storia del firewall**
- **Analizzeremo perché il cloud è una realtà destinata a rimanere**
- **Discuteremo i limiti dei prodotti monofunzione**
- **Scopriremo come integrare la sicurezza e seguire i dati**
- **Capiremo il ruolo di SSE nella sicurezza**

Capitolo 2
Come il cloud ha cambiato radicalmente il modello di sicurezza tradizionale

Una decina di anni fa, pochi leader avevano previsto con quale rapidità il cloud, in tutte le sue forme, avrebbe preso piede. Secondo Netskope Threat Labs, le aziende ora usano, in media, oltre 800 applicazioni SaaS (*Software-as-a-Service*).

Il cloud e l'edge computing spingono sempre più i carichi di lavoro fuori dal data center. Le iniziative di lavoro ubiquo, accelerate dalla pandemia di COVID-19, hanno portato più persone, dispositivi, applicazioni, servizi e dati a superare i tradizionali confini del data center aziendale. Adesso, il cloud è fondamentale per la produttività, ma quando si presentano nuovi rischi, ci costringe anche a rivedere la sicurezza.

Immaginiamo di essere genitori di bambini piccoli: per la loro sicurezza, copriamo le prese elettriche, mettiamo cancelletti alle scale,

fermi alle ante degli armadietti e alla tavoletta del water. Proteggiamo il perimetro interno della nostra abitazione con un dispositivo di allarme che scatta ogni volta che si apre una porta, e quello esterno con un recinto. Una volta che i figli vanno all'asilo, a scuola e all'università, vogliamo sempre proteggerli, ma il nostro ruolo è cambiato.

Analogamente, proteggere il cloud significa riconoscere che l'obiettivo della sicurezza – ovvero salvaguardare dati, applicazioni e utenti–, è sempre lo stesso. La differenza è che i dati, le applicazioni e gli utenti hanno lasciato il perimetro,; e ciò fa passare il ruolo del firewall in secondo piano. Allo stesso tempo, le minacce in più rapida crescita sono dirette al cloud, non al data center. Di conseguenza, le strategie di sicurezza devono cambiare.

Quando il firewall dominava la sicurezza

Tempi addietro, il firewall era il punto di controllo più importante della sicurezza centrale e, probabilmente, la voce più costosa del budget. La maggior parte delle aziende sviluppava le architetture di sicurezza di rete intorno al data center, entro un perimetro ben definito. Essere al sicuro significava proteggere la rete.

Nell'era pre-cloud, quell'approccio aveva senso. Dopotutto, il data center era l'unico posto dove un'organizzazione custodiva le sue preziose risorse digitali. Come un'abitazione con un buon sistema di allarme, un'azienda erigeva un perimetro (per lo più) impenetrabile per il suo data center. Un robusto cancello fatto di dispositivi di sicurezza ad accesso strettamente limitato. Una volta installati gli allarmi ai punti d'ingresso, nell'era pre-cloud si aveva un controllo sostanziale sulla sicurezza.

I dipendenti si muovevano attraverso una rete privata esclusiva che li connetteva alle aree di cui avevano bisogno; la stessa che usavano per collegarsi da filiali lontane, o comunque da remoto: digitando un codice di allarme, ottenevano l'autorizzazione ad accedere non solo alle applicazioni e ai dati interni, ma anche a tutte le destinazioni esterne collegate. Tuttavia, reinstradare il traffico da remoto attraverso il data center centralizzato (backhauling) comportava costi, complessità e inefficienza.

La sicurezza del firewall vecchio stile si basava sul semplice consentire o negare l'accesso. Una volta data l'autorizzazione, la presenza e le buone intenzioni dell'utente si davano per scontate. Sulla base di queste premesse, le aziende adottavano una sicurezza progettata per contrastare minacce singole o intere categorie di minacce man mano che emergevano. Se si intravedeva una minaccia, si compravano nuovi dispositivi. Nel modello on-premises, un'azienda poteva avere dieci dispositivi di sicurezza collegati tra loro da un cavo.

Ogni dispositivo eseguiva un'ispezione specifica – ad esempio per rilevare malware, confrontare le signature e bloccare le intrusioni, filtrare la posta elettronica, cercare dati sensibili, proteggersi dagli attacchi DNS, bloccare porte e protocolli con ACL – per poi instradare i pacchetti alla funzione successiva, ma questo aumentava la latenza e la complessità.

Il cloud ha cambiato tutte le assunzioni.

In che modo il cloud è un vantaggio per le aziende

Il cloud computing offre una flessibilità e un valore di business così evidenti da non poter più tornare indietro. E qualsiasi "proclama di ritorno" al data center, fatta eccezione per scenari rari e specifici, è privo di senso. Il cloud è allettante per CEO, CFO, CIO e aziende in generale perché la maggior parte dell'infrastruttura è standardizzata e pronta all'uso. In più, aiuta a risparmiare tutto il tempo e denaro necessari per mettere a punto una propria infrastruttura. Si sottoscrive in abbonamento, si attiva, si personalizza in base alle necessità specifiche dell'organizzazione e lo si usa. Il cloud aiuta le aziende a centrare l'obiettivo di generare più ricavi e diventare più redditizie.

Piace anche ai dipendenti pieni di impegni, i quali trovano particolarmente interessanti le innumerevoli applicazioni SaaS con piattaforme moderne e talvolta divertenti per collaborare, comunicare, concludere le vendite, gestire le finanze e anche le relazioni con i clienti. Queste applicazioni cloud di terze parti offrono un'esperienza utente migliore e sono più veloci ed efficaci di qualsiasi altra soluzione proposta dalle vecchie applicazioni aziendali strettamente confinate nel data center.

ATTENZIONE

Ma qui sta il tranello, e il pericolo: La maggior parte delle applicazioni cloud non è approvata, e tanto meno controllata, dall'IT aziendale – e non è affatto sicura. Si è ancora tenuti a proteggere, ma non si ha più il tipo di controllo a cui si è abituati. Passare al cloud è come mandare i figli a scuola o addirittura all'università: non sono più sotto i nostri occhi né possiamo sapere cosa stanno facendo.

Nell'era del cloud, il firewall non è più il mezzo di controllo della sicurezza per eccellenza perché non protegge in modo completo l'azienda dalle minacce presenti. Senza adeguati sistemi volti a proteggere processi digitali, dipendenti, clienti e (ahimé) risorse, in questo nuovo panorama aperto gli sforzi per l'accelerazione digitale saranno rischiosi. Ora il compito della sicurezza è permettere all'azienda di fruire del valore che deriva dal cloud gestendo le responsabilità intrinseche.

I prodotti monofunzione aiutano in circostanze specifiche ma non risolvono i problemi più importanti

Con l'avanzare del lavoro da remoto e il passaggio delle applicazioni al cloud, gli strumenti di sicurezza tradizionali del data center si sono rivelati incapaci di "vedere" cosa succede al di là del perimetro. Per essere utili, le applicazioni SaaS devono usare dati custoditi dentro le mura aziendali ma trovandosi al di fuori devono migrare i dati, che quindi non sono più sotto il controllo e la protezione dell'azienda.

Per sfruttare in modo sicuro le applicazioni basate sul cloud serviva un cambiamento. Le aziende hanno configurato sulle reti private e sul cloud nuovi prodotti mirati ad affrontare i problemi di sicurezza e i punti deboli più urgenti legati al cloud, tra cui:

- Cloud Access Security Broker (**CASB**): I CASB aiutano a governare e proteggere i dati aziendali conservati nel computer di qualcun altro. Un modo onesto per concettualizzare il cloud.
- Secure Web Gateway (**SWG**): I SWG proteggono dipendenti e organizzazioni dalle minacce sul web, ovvero le pagine visitate quando si è online e si naviga in siti pubblici.

- Zero Trust Network Access (**ZTNA**): I prodotti ZTNA proteggono dall'accesso pubblico le applicazioni di un'azienda rendendole invece disponibili a un gruppo di dipendenti noti.

Questi strumenti rappresentano la prima generazione di sicurezza cloud, alla quale però è mancato un aspetto fondamentale: l'integrazione.

Integrare la sicurezza è un must

I prodotti per la sicurezza cloud di prima generazione spesso provenivano da fornitori diversi, e quindi non erano integrati fra loro. Ognuno offriva la propria console e richiedeva policy che andavano a sovrapporsi alle altre (ad es., DLP). Poteva anche richiedere un agente dedicato, creando problemi di distribuzione e instradamento del traffico. In più, richiedeva trattative contrattuali e accordi di acquisto distinti.

Proviamo a immaginare come sarebbe se i nostri cinque sensi – udito, olfatto, gusto, tatto e vista – fossero collegati a cervelli diversi. Senza interazione, nel caso di un incendio, vedremmo le fiamme, percepiremmo l'odore del fumo o sentiremmo il sibilare del fuoco, ma non sapremmo cosa fare perché i nostri vari cervelli non condividerebbero le informazioni e quindi non metterebbero in correlazione tra loro i vari input.

Tornado all'infrastruttura di sicurezza, abbiamo molti sistemi diversi, ognuno con un cervello nel suo specifico dominio. Ad esempio, il CASB è un cervello incentrato principalmente sull'accesso dei singoli dipendenti a un'applicazione SaaS.

<remember>

Proprio come il nostro cervello acquisisce informazioni da tutti i sensi per decidere sul da farsi, i servizi di sicurezza devono essere completamente integrati per prendere decisioni efficaci a supporto della strategia cloud. SSE è il cervello che integra tra loro categorie di sicurezza disparate. Invece di operare separatamente in sequenza, SSE consente a tutti i "sensi" di sicurezza di attivarsi in parallelo. Il risultato è una sicurezza più veloce ed efficiente. Inoltre, SSE è molto più facile da acquisire perché tutte le funzionalità (CASB, SWG, ZTNA e correlate) sono già incluse.

La sicurezza deve seguire i dati

Come abbiamo spiegato nel capitolo 1, SASE (*Secure Access Service Edge*) descrive una visione in cui il tradizionale perimetro aziendale non esiste più. Invece, l'intero portafoglio di funzioni di rete e di sicurezza si sposta nel cloud, vicino agli utenti, ai dati archiviati e alle applicazioni SaaS.

SASE permette di adeguare la nostra prospettiva a un mondo basato sul cloud e sul lavoro ubiquo, dove la vecchia nozione di perimetro fisico è svanita. In questo nuovo mondo, la sicurezza deve andare ben oltre i confini del data center. Ora deve seguire la risorsa più importante di un'azienda – i dati – con un livello di consapevolezza contestuale sufficiente a proteggere le informazioni ovunque si trovino e indipendentemente dal tipo di accesso.

Per ottenere una sicurezza a misura di cloud, si devono mettere in atto nuove ipotesi e funzionalità di sicurezza. La sicurezza deve:

- seguire i dati.
- essere basata su un contesto ricco.
- adeguarsi alle caratteristiche specifiche del contesto di un utente.

L'altra considerazione chiave da fare sul modello SASE è l'equilibrio tra sicurezza ed efficienza della rete. Non possiamo sacrificare l'una per l'altra: abbiamo bisogno di entrambe. Le persone sono più produttive quando hanno a disposizione una tecnologia semplice da usare e fluida. Se gli strumenti di sicurezza rallentano le reti, l'efficienza viene meno e la produttività ne risente. Nell'ipotesi peggiore, i dipendenti cercano di aggirare del tutto i controlli di sicurezza, con gli enormi rischi e l'esposizione che ciò comporta.

Il passo cruciale verso un tale equilibrio consiste nello spostare le funzionalità di rete e sicurezza essenziali nel cloud, eliminando al tempo stesso le appliance basate sul perimetro e (preparandosi a respingere al mittente) tutti i prodotti tradizionali.

Tale approccio fornirà un accesso sicuro e affidabile a servizi web, applicazioni e dati, con i principi Zero Trust applicati ovunque per ottenere una fiducia adattiva continua a ogni interazione.

SSE: alla guida della sicurezza nel percorso SASE

SASE e SSE sono il modo in cui la sicurezza passa al cloud e diventa più efficace di qualsiasi soluzione precedente.

SASE è la visione globale che sostiene la transizione verso il cloud delle funzionalità di rete e sicurezza. SSE è il cervello che integra, identifica ed esegue i servizi di sicurezza necessari per realizzare SASE. L'insieme dei servizi integrati diventa il principale punto in cui tutto il traffico è sottoposto a ispezioni e controlli di sicurezza coerenti. SSE non elimina il firewall, che rimarrà, ma si sostituisce a esso a livello di sicurezza centrale.

Sicuramente, CASB, SWG, ZTNA e altri servizi correlati offrono valore anche in versione standalone. La maggior parte delle aziende ne ha già implementati uno o due. Tuttavia, per sfruttare appieno il valore del cloud, questi servizi devono essere integrati e collaborare tra loro.

Secondo Netskope, le funzioni SSE essenziali possono essere aumentate con molte caratteristiche ora assenti ma cruciali per proteggere in modo affidabile le risorse digitali oltre i confini del data center. Queste includono:

- **Classificazione:** Identifica ed etichetta le informazioni sensibili, idealmente quando vengono create ma anche attraverso scansioni periodiche degli archivi di dati.
- **Prevenzione della perdita di dati (DLP):** Monitora e controlla attivamente il movimento di informazioni sensibili.
- **Consapevolezza e neutralizzazione delle minacce (nota anche come protezione avanzata dalle minacce o ATP):** Identifica i segnali di un ambiente compromesso e interviene per ridurre o eliminare le probabilità di attacchi futuri.
- **Gestione dello stato di sicurezza nel cloud (CSPM):** Valuta la configurazione delle risorse cloud ti tipo Iaas (Infrastructure-as-a-Service) e PaaS (Platform-as-a-Service) e interviene per correggere le configurazioni errate che potrebbero portarea compromissioni dell'ambiente.

- **Gestione dello stato di sicurezza SaaS (SSPM):** Valuta la configurazione delle applicazioni SaaS ed elimina le configurazioni errate che potrebbero consentire la sottrazione illecita di dati, l'impersonificazione o altri tipi di attacchi.

Gestione dell'esperienza digitale (DEM): Analizza i dati raccolti per motivi di sicurezza insieme ad altri segnali di disponibilità ed efficienza per misurare l'esperienza degli utentie aiutare a risolvere rapidamente i problemi.

RICORDA

SSE, che combina tutte queste funzionalità in un unico prodotto di sicurezza integrato ed erogato dal cloud(dove è più vicino ad utenti, dati e applicazioni), diventa il punto di ispezione più importante per la protezione dell'azienda, come vedremo nel dettaglio nel Capitolo 3.

Abbiamo bisogno di sicurezza per il futuro, non per il passato

Dobbiamo implementare strumenti compatibili con il cloud, un fattore chiave per creare valore aziendale e ricavi. Dobbiamo implementare strumenti capaci di resistere agli avversari. Per finire, dobbiamo implementare strumenti che non ostacolano le operazioni. Immaginando di mandare nostro figlio o nostra figlia all'asilo nido, a scuola o all'università con una guardia del corpo invisibile, quella guardia del corpo si chiamerebbe SSE.

IN QUESTO CAPITOLO

- **Capiremo perché SSE è necessario**
- **Esploreremo le capacità e i requisiti di SSE**
- **Valuteremo i benefici di SSE**

Capitolo 3
Security Service Edge: un piano per il futuro della sicurezza cloud-based

SASE (*Secure Access Service Edge*) modifica la nostra percezione di come viene garantita la sicurezza in un mondo cloud-based, dove i dati sono accessibili da dovunque. Quando i dipendenti lavorano da remoto, quando le applicazioni diventano SaaS (*Software as a Service*) e quando i dati si spostano nel cloud, anche tutte le attività per la cybersicurezza devono trasferirsi nel cloud. Se implementato correttamente, SASE mostra che la sicurezza deve essere il più possibile vicina ai dati e ai relativi punti di accesso. Con SASE, gli interessi di un'organizzazione saranno protetti grazie a controlli coerenti a qualsiasi distanza, senza compromettere la connettività di rete e l'esperienza utente.

SASE implica il consolidamento e l'integrazione della sicurezza, ossia l'essenza stessa di SSE.

SSE trasferisce i punti critici di controllo e ispezione nel cloud, sede operativa di fatto delle attività aziendali. Questo spostamento porta la sicurezza vicina a dati, applicazioni e utenti– ossia, dove si cela il pericolo. Con SSE, i servizi di ispezione e controllo per SaaS, web e

dati, uniti a sofisticate funzioni di rilevamento e neutralizzazione delle minacce, funzionano come un solo sistema coerente e interoperabile.

<tip>

Il problema non è la sicurezza della rete. Il problema è la sicurezza del cloud. L'unica cosa di cui è sensato parlare in termini di rete riguarda la realizzazione di un'architettura in grado di rendere SSE il punto di ispezione primario nel cloud.

SSE offre capacità che trascendono dai firewall tradizionali. Un SSE implementato nel modo giusto è in grado di distinguere anche il contesto – ossia, a quali dati è possibile accedere, come e perché –, in modo da prendere decisioni calibrate in tempo reale. SSE fa convergere tutti i "sensi" della sicurezza verso un solo cervello che interpreta i dati, è consapevole della portata dei rischi e contratta il giusto livello di accesso in qualsiasi momento e scenario.

Più avanti, vedremo come funziona l'SSE.

Vediamo perché SSE è necessario

Il vecchio approccio alla sicurezza si basava su un perimetro ben definito e su un firewall capace di respingere gli attaccanti che prendevano di mira un data center aziendale. Poiché, tuttavia, nessuna misura di sicurezza garantisce l'inviolabilità, un attaccante tanto abile da violare il perimetro avrebbe potuto spostarsi lateralmente nella rete, rendendo di fatto dati e applicazioni inermi.

Le architetture SASE si basano ancora sulla gestione delle identità e degli accessi per autenticare i dipendenti e su piattaforme di protezione degli endpoint per tutelare i dispositivi. Ma una architettura SASE efficace si avvale anche dei principi Zero Trust che garantiscono l'accesso e monitorano l'attendibilità in base a una serie di condizioni. Nel cloud, il perimetro diventa il contesto che circonda la persona.

L'approccio Zero Trust è una filosofia basata su tre presupposti fondamentali per SSE, e quindi anche per SASE:

- L'utilità della fiducia implicita tipica dei sistemi tradizionali è venuta meno. L'approccio Zero Trust inverte l'ordine: da "fidati ma controlla" a "prima controlla e poi fidati". L'identità e il contesto di qualsiasi persona o azione che richiede l'accesso ai

dati devono essere verificati ogni volta, in modo da raggiungere un determinato livello di attendibilità. Senza eccezioni.

- Garantire esclusivamente l'accesso minimo, detto anche privilegio minimo, adeguato al livello di attendibilità previsto. L'accesso è limitato a una risorsa specifica e non può essere esteso ad altre.
- Il contesto deve essere costantemente rivalutato in base a segnali come l'identità del dipendente e del dispositivo,lo stato di sicurezza del dispositivo, l'ora del giorno, la geolocalizzazione, il ruolo aziendale, la sensibilità dei dati. Ogni modifica deve avviare una nuova valutazione. (Netskope chiama questo approccio *fiducia adattiva continua*, di cui parleremo più approfonditamente nel Capitolo 4.)

SASE mette a disposizione un quadro di riferimento per un programma Zero Trust efficace, che include gli ambienti dove si trovano le persone, le applicazioni e i dati. Ma, come vedremo nel Capitolo 4, l'approccio Zero Trust è costituito da un insieme di principi, non da un'architettura tecnica volta a implementare in modo unificato le diverse funzioni di sicurezza.

Tale architettura viene garantita da SSE, che unifica, integra e coordina numerosi servizi di sicurezza, ne migliora le capacità e garantisce alte prestazioni ai dipendenti e alle aziende in modo integrato e personalizzato sulla base del contesto. Per conseguire i risultati attesi, SSE offre:

- Un contesto dettagliato, completo di storia dell'utente, rete, dati, dispositivo, applicazione e persino motivo della richiesta.
- Informazioni sulle risorse alle quali l'utenteha accesso per soddisfare la richiesta, che SSE può raccogliere dall'autorizzazione e dai relativi diritti.
- Informazioni molto dettagliate che classificano la sensibilità delle diverse risorse (per evitare perdite di dati).
- Istruzioni e un insieme dettagliato di policy che descrivono il risultato atteso in base a diverse combinazioni di persone, dati, applicazioni e altre informazioni contestuali.

Il problema è che molti dei risultati di sicurezza, come la funzione DLP, il rilevamento e la neutralizzazione delle minacce, richiedono la collaborazione tra più componenti.

ATTENZIONE

Implementare separatamente ciascun servizio vuol dire ripetere svariate operazioni di sicurezza nelle console di gestione di ogni strumento, uno dopo l'altro. Si tratta di un lavoro immane e passibile di errori mentre in ballo c'è una vendita, se non addirittura una vita.

SSE elimina tutte queste ripetizioni. Se ben implementato, unifica i servizi di sicurezza permettendo loro di condividere il contesto, i diritti, le policy di sicurezza, la risk intelligence, l'isolamento del browser, la codifica/decodifica dei dati, e altro ancora. Tale coesione dà il potere di elaborare tutte le transazioni in un unico passaggio, per concedere rapidamente l'accesso giusto.

Scopriamo come SSE riunisce i servizi di sicurezza sotto un unico tetto

SSE è basato sull'integrazione tra molti servizi di sicurezza supportati da numerose funzioni correlate. Esiste il modo giusto per costruire SSE, ma ce ne sono tanti sbagliati.

ATTENZIONE

Con il diffondersi di SSE, farà rapidamente la sua comparsa anche un marketing ingannevole. Un'implementazione SSE sbagliata si riconosce facilmente dalla scarsa integrazione. Gli approcci che si limitano a collegare processi discreti o ad aggiornare intere serie di vecchie appliance svelano in realtà sistemi fatti di componenti distinti sviluppati secondo stili pre-cloud obsoleti, ed eventualmente acquistati da diversi vendor. Questi sistemi appiccicati tra loro introducono grande latenza, non offrono i benefici ad ampio raggio di SSE e non costituiscono un significativo passo in avanti nel passaggio al SASE.

SSE non consisterà mai in una serie di appliance o una sequenza di processi discreti che fanno passare i dati attraverso un motore DLP, un motore di valutazione delle liste di controllo degli accessi, un gateway web e così via. Ciò nonostante, può essere utile esaminare una a una le caratteristiche di un'implementazione SSE pienamente integrata.

Sicurezza single-pass, analisi di ogni fase

RICORDA

In una architettura SSE ideale, i servizi di sicurezza integrati operano in parallelo. Tutte le ispezioni vengono eseguite contemporaneamente, in tempo reale, a prescindere dalla provenienza del traffico – web, cloud o data center aziendale.

Una singola azione garantisce un filtro sempre più fine per proteggere dati e applicazioni. Pensiamo ad esempio a un imbuto.

Un'architettura SSE adeguata distingue le applicazioni aziendali (ad esempio Salesforce, Workday) da quelle personali (come un account Gmail) e da applicazioni/servizi di terzi (come le istanze aziendali di Microsoft Office 365 o Dropbox). Sulla base di ciò consente le connessioni utili a proteggere ogni applicazione o servizio secondo le policy.

Inoltre valuta il contesto, ad esempio regolando l'accesso in base al fatto che un medico (si veda il Capitolo 4) sta utilizzando un tablet di proprietà dell'ospedale in una sala di degenza oppure lo smartphone personale dal Wi-Fi del bar o il computer di gioco nella stanza del figlio.

Un'architettura SSE adeguata si avvale di policy per evitare perdite o furti di dati, con controlli in grado di prevenire il download di documenti, l'acquisizione di screenshot, l'immissione di dati in moduli web o la pubblicazione di post sui social.

Un'architettura SSE adeguata offre un monitoraggio continuo. Mentre il dipendente porta avanti le sue solite attività, SSE è attento a eventuali anomalie. Una volta classificati gli oggetti di dati, SSE può distinguere i contenuti sensibili da quelli che non lo sono, modificando dinamicamente i permessi di accesso e le attività consentite. SSE può inizializzare un allarme, mandare avvisi o chiedere più informazioni al dipendente per guidare le attività in sicurezza.

Alimentato da servizi condivisi

Le funzioni di sicurezza di alto livello – come DLP, il rilevamentoe neutralizzazione delle minacce, la gestione dell'esperienza digitale (DEM) e altre ancora – possono avvalersi di tutti i servizi e le tecniche qui descritte per ottenere i risultati di sicurezza attesi:

- **Contesto condiviso:** Tutti gli elementi SSE condividono un'enorme raccolta di metadati che identificano la persona, il dispositivo e la posizione. Si procede identificando il sito web di destinazione, l'applicazione o il servizio, assegnando un livello di rischio e valutando le attività. Viene preso in considerazione qualsiasi dato richiesto o creato dall'utente e dall'applicazione. Il ricco contesto SSE include una valutazione del comportamento dell'utente, anche sulla base delle interazioni passate, per analizzare l'attività attuale. Questo panorama contestuale

costantemente aggiornato determina le azioni intraprese e le policy applicate da tutti gli elementi SSE (In SSE di Netskope, questo servizio è detto Cloud XD).

- **Fiducia adattiva continua:** L'accesso ai dati e alle applicazioni non è una semplice decisione binaria. Deve essere flessibile, basato su requisiti e contesti mutevoli. Un'implementazione SSE adeguata pone in relazione il livello di fiducia e il valore delle risorse, basandosi sulla grande quantità di segnali contestuali disponibili e sulla propensione al rischio dell'organizzazione definita nella policy.
- **Amministrazione basata su policy:** Nell'ambito della sicurezza single-pass, un'implementazione SSE adeguata è caratterizzata da policy dettagliate e condivise che consentono all'azienda di stabilire i confini della sua propensione al rischio e di definire chiaramente i risultati di sicurezza attesi. Questo è molto diverso rispetto alle migliaia di regole tipiche dei firewall. I componenti SSE fanno riferimento alle policy per controllare attività e dati su tutte le applicazioni, le categorie di applicazioni e i servizi web.

SSE: caratteristiche più interessanti

Una volta descritti i componenti di SSE, possiamo esaminare le loro capacità. Alcune risulteranno più familiari e magari già implementate in altra forma, quindi è probabile che col tempo verranno sostituite da SSE.

RICORDA

L'obiettivo di SSE è consentire a persone e attività di operare con la massima rapidità e sicurezza. Funzionando ovunque, SSE mette fine a inutili tentativi di estendere la sicurezza nel data center per seguire dati, applicazioni e persone trasferiti sul cloud.

La Tabella 3-1 mostra i requisiti minimi in termini di capacità per poter definire un prodotto come SSE secondo diversi analisti nel 2021.

TABELLA 3-1 **Requisiti minimi delle capacità SSE**

Capacità	Cosa fa	Come viene migliorata da SSE
SWG	Controlla gli accessi e protegge esclusivamente dalle minacce web.	Estende la protezione alle minacce native in cloud e i rischi legati ai dati per le istanze personali delle applicazioni gestite, per migliaia di applicazioni shadow IT e per i servizi cloud.
CASB	Un punto di applicazione delle policy di sicurezza situato tra gli utenti e i fornitori del servizio cloud dove vengono applicate le policy di sicurezza aziendali in caso di accesso a risorse nel. Valuta i comportamenti ed è consapevole della funzionalità dell'applicazione SaaS per impostare l'accesso giusto per un dato utente.	Elimina la duplicazione delle policy (tra SWG e CASB), semplifica l'amministrazione (un solo agente per SWG, CASB e STNA) e garantisce visibilità su tutti i flussi di traffico.
ZTNA	Applica la premessa in base alla quale nessuno gode di cieca fiducia e può accedere alle risorse aziendali fino alla convalida dell'autorizzazione. Supporta l'implementazione dell'accesso con privilegio minimo, ossia consentito solo alle risorse richieste da singoli o gruppi, e nulla più.	Potenzia ZTNA con capacità di accesso adattivo. Uniforma le policy a livello di amministrazione e decisioni con altri componenti SSE, pur mantenendone distribuita l'applicazione.
Isolamento del browser da remoto (RBI)	Separa i dispositivi dei dipendenti dalla navigazione in Internet trasferendo ed eseguendo tutte le relative attività in un container remoto cloud-based. Grazie a questo sandboxing protegge dati, dispositivi e reti da qualsiasi tipo di minaccia proveniente da siti web malevoli.	Consente a RBI di sfruttare la classificazione dei dati e il contesto dei ruoli. Aggiunge l'isolamento all'array di azioni policy-based in SWG e CASB.

(continuazione)

TABELLA 3-1 *(continuazione)*

Capacità	Cosa fa	Come viene migliorata da SSE
Firewall-as-a-Service (FWaaS)	Sicurezza di rete per tutte le porte e i protocolli in uscita allo scopo di accedere direttamente a Internet in modo sicuro tramite un agente sui dispositivi gestiti o tramite GRE e IPsec nel caso di uffici. Un solo motore di policy e una sola piattaforma di sicurezza per gestire in modo semplificato gli utenti e le sedi remote da un'unica console.	Consente alle organizzazioni di aggregare il traffico proveniente da fonti diverse: data center on-site, siti remoti, dipendenti in mobilità o infrastrutture cloud. Garantisce l'applicazione coerente delle policy per tutte le postazioni e i dipendenti, e al tempo stesso totale visibilità e controllo di rete senza implementare appliance fisiche.

Capacità di SSE: presto disponibili per il team di sicurezza

Grazie alla maturità raggiunta dai prodotti e al proliferare delle iniziative cloud-first, SSE si evolverà con capacità ancora maggiori. Un'architettura SSE adeguata include ben più della definizione originale, ossia:

- Classificazione potenziata a supporto della funzione DLP
- Gestione dello stato di sicurezza per cloud e SaaS
- Rilevamento e neutralizzazione delle minacce
- Gestione dell'esperienza digitale

Nei prossimi paragrafi le vedremo una a una.

Classificazione migliorata a supporto della funzione DLP

DLP è un termine ombrello per una funzione volta a prevenire la sottrazione dei dati intenzionale o accidentale. Rileva i movimenti delle informazioni sensibili, ne previene la diffusione verso posizioni indesiderate, interrompe l'azione degli utenti con pop-up educativi per porre fine a esposizioni non intenzionali e incorpora il machine learning per valutare il livello di rischio dei dipendenti.

SUGGERIMENTO

SSE migliora la funzione DLP identificando e classificando attivamente i dati, e quindi permettendo di tenere traccia e applicare con più precisione le regole sul movimento dei dati sensibili.

Gestione dello stato di sicurezza per cloud e SaaS

La gestione dello stato di sicurezza nel cloud (CSPM) e la gestione dello stato di sicurezza SaaS (SSPM) consentono di scoprire e sanare le configurazioni errate nei cloud (la forma più comune di errori nella sicurezza del cloud). Sulla base del contesto fornito da SSE, i controlli abilitati API (*Application Programming Interface*) e la valutazione in tempo reale delle architetture cloud pubbliche, CSPM e SSPM mitigano i rischi analizzando la configurazione, suggerendo modifiche che riducono – se non addirittura eliminano – la probabilità di potenziali attacchi e monitorando la conformità normativa.

SUGGERIMENTO

Nelle implementazioni SSE adeguate, CSPM e SSPM riconoscono le minacce e adottano attivamente contromisure mirate al miglioramento dello stato di sicurezza di un'organizzazione.

Ad esempio, alcune implementazioni CSPM e SSPM possono identificare non conformità quando una policy richiede di default la crittografia di tutti i dati sul cloud. Si tratta di un atteggiamento molto forte che richiede la corrispondenza tra i controlli di accesso: l'identità di una persona deve essere presente sia sulla lista di controllo degli accessi per un oggetto crittografato sia sulla lista per la relativa chiave di crittografia. CSPM e SSPM riconoscono quando una persona ha accesso a una ma non all'altra e segnalano l'incoerenza.

Rilevamento e neutralizzazione delle minacce

Il rilevamento e la neutralizzazione delle minacce identifica gli attacchi riusciti e genera allarmi per contenere il pericolo. Le evidenze più comuni includono le attività di rete anomale, le modifiche alla configurazione e l'eliminazione dei file di log. L'analisi forense determina la presenza nell'ambiente di minacce attive. La neutralizzazione delle minacce è l'esempio perfetto di un servizio che trae beneficio dalle funzioni condivise dell'architettura SSE e contemporaneamente fornisce loro evidenze.

Gestione dell'esperienza digitale (DEM)

Un aspetto forte di SSE che sta emergendo è la sua capacità di valutare l'esperienza dell'utente e le prestazioni dell'applicazione, tanto più ora che i confini della rete si estendono al cloud e oltre. Grazie al monitoraggio continuo del traffico, gli utentibeneficiano di una visibilità end-to-end sul comportamento della rete e delle applicazioni aziendali, con informazioni in tempo reale processabili basate sulle reali attività umane, per garantire che SSE dia buoni risultati senza scendere a compromessi sulle prestazioni. Quando ci sono problemi con dispositivi, reti o applicazioni, DEM contribuisce a identificare le cause in tempi brevi, accelera la risoluzione dei ticket dell'help-desk e attiva contromisure per evitare che problemi di lieve entità diventino rilevanti con conseguente impatto sull'operatività.

Anche la rete deve evolversi

Fino a ora, ci siamo focalizzati sulle caratteristiche e sulle capacità di sicurezza che l'SSE può offrire al mondo cloud-first. Ma sono necessarie ulteriori trasformazioni, che vanno oltre ciò che consideriamo sicurezza.

RICORDA

L'accesso alla rete deve essere distribuito per consentire ai dipendenti e alle organizzazioni di ottenere il massimo valore dai sistemi cloud-based protetti da SSE, come mostrato nella Figura 3-1.

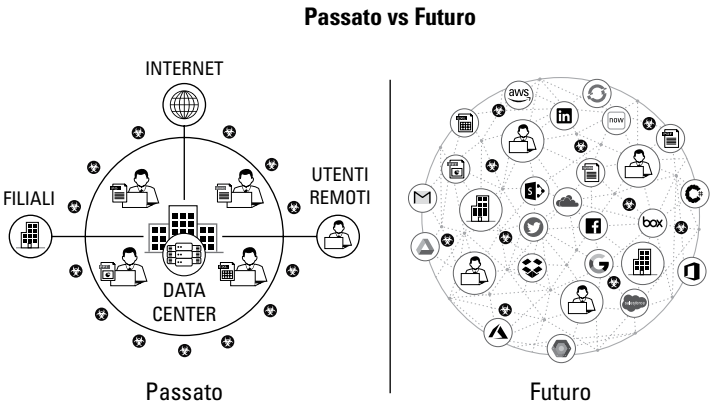

FIGURA 3-1: Il vecchio modello di accesso era inefficiente e inefficace rispetto a quello nuovo, che consente l'accesso da ovunque.

Prima infatti i dipendenti si connettevano a una rete protetta da un perimetro ben definito. I siti remoti mantenevano la connessione al data center tramite costose reti private, diventate un ostacolo con il prosperare delle attività prima sul web e poi sul cloud. L'unica opzione sicura era instradare il traffico dei dipendenti attraverso lo stack di sicurezza del data center, prima dell'interazione con le risorse sul cloud e sul web.

Un approccio inefficiente e inefficace. Consentire ai dipendenti di interagire direttamente con le risorse sul cloud migliora di gran lunga le performance e la produttività, ma sovverte il controllo e la visibilità del data center. Persistere nell'uso del vecchio modello creando, mantenendo e monitorando reti private per raggiungere tutto ciò che il cloud può offrire è complesso, costoso e in definitiva non consente la scalabilità in un'era che chiede di dare alla sicurezza la massima priorità a qualsiasi livello aziendale, incluso il Consiglio di Amministrazione.

Il nuovo modello di rete prevede un'architettura costruita per il lavoro da remoto, che consente agli utenti di connettersi da qualsiasi luogo e di interagire con altri utenti e informazioni principalmente sul cloud. Per garantire prestazioni eccellenti e la migliore esperienza d'uso delle applicazioni, la rete di un provider SSE deve:

- Avere numerose relazioni di peering con le destinazioni più importanti
- Avere un numero sufficiente di punti di presenza dotati ciascuno di completa capacità di calcolo e distribuiti strategicamente, in modo che gli utenti non siano mai distanti

SUGGERIMENTO

Il modo migliore di ottenere connessioni rapide e fluide è lavorare con un provider che offra una rete dotata di molte relazioni di peering direttocon le destinazioni più importanti. Al crescere delle connessioni migliorano le prestazioni, la resilienza e la soddisfazione degli utenti.

RICORDA

Un provider ben connesso offre prestazioni migliori, una resilienza maggiore e un'esperienza d'uso eccellente. L'esperienza d'uso dell'utente è fondamentale! La trasformazione digitale ha successo quando la rete e la sicurezza si fondono in una partnership coesa fin dall'inizio. È inaccettabile che la sicurezza obblighi a rinunciare alle prestazioni di rete o a scendere a pericolosi compromessi fra sicurezza e produttività.

Come tutti gli aspetti di SASE e SSE, la trasformazione della rete viene ottimizzata nel tempo. Il vendor deve colmare il divario tra la sicurezza che si ha oggi e quella che si vuole domani. Deve offrire SSE, abilitare nuove modalità d'accesso alla forza lavoro distribuita e integrarsi trasparentemente con l'infrastruttura e i processi di rete esistenti.

Vantaggi di SSE in termini di sicurezza

Adottando l'architettura SASE centrata sui principi Zero Trust e collaborando con un vendor SSE in grado di offrire servizi di sicurezza critici in modo distribuito, si possono ottenere benefici notevoli:

- Maggiore tranquillità in caso di accesso a dati e applicazioni all'esterno del data center
- Sicurezza flessibile basata sulla conoscenza dei rischi, con policy e funzioni di controllo adattive su attività specifiche, create su misura per ogni applicazione
- Capacità di estendere i principi Zero Trust alle applicazioni web e SaaS
- Accesso a ulteriori servizi di sicurezza come le funzioni RBI e DLP avanzate, in base al livello di rischio o fiducia valutato
- Monitoraggio continuo di eventuali modifiche al contesto, che avviano automaticamente una rivalutazione della fiducia e dell'accesso, e di conseguenza delle policy di sicurezza
- Una riduzione della superficie di attacco eliminando l'esposizione di protocolli e servizi alla rete Internet pubblica
- Cloud configurati correttamente che eliminano la forma più comune di falle nella sicurezza.

Tutti questi benefici rappresentano diversi aspetti del paradiso della sicurezza di cui abbiamo parlato nel Capitolo 1. Il Capitolo 4 analizza i vantaggi aziendali ottenuti grazie all'implementazione SSE appropriata e i passaggi necessari per realizzarla.

IN QUESTO CAPITOLO

- **Capiremo come otterremo uno stato di fiducia adattiva continua con i principi Zero Trust**
- **Impareremo come implementare SSE in quattro passaggi**
- **Scopriremo i vantaggi di SSE per l'azienda**

Capitolo 4
Usare i principi Zero Trust per SASE

Come abbiamo visto nel Capitolo 2, portare la sicurezza dell'azienda sul cloud è diventato importante perché il cloud è diventato importante per l'azienda. Il passaggio al cloud procede spedito, molto più di quanto anche le organizzazioni più lungimiranti avessero previsto solo cinque anni fa. Le aziende si stanno spostando sul cloud per garantirsi uno sviluppo rapido, accedere a risorse on-demand, godere di una scalabilità elastica e snellire di molto i carichi amministrativi per innovare e creare nuovi prodotti e servizi in tempi record.

Gli attaccanti si stanno spostando sul cloud per seguire le aziende. Quindi, fare in modo che i dati, le applicazioni e lo staff siano protetti sul cloud deve essere una preoccupazione comune a tutti.

ATTENZIONE

Se il cloud non è protetto, i vantaggi che offre restano inafferrabili.

Chi è alla guida di questa nuova tendenza sarà tra i primi a dover portare avanti innanzitutto l'idea che proteggere il cloud è importante ed inoltre, che SASE, SSE e la riconfigurazione della rete consentiranno di gestire meglio i rischi riducendo i problemi legati alla sicurezza. I piani di supporto devono spiegare perché valga la pena portare avanti un cambiamento di tale portata, prevedere i vantaggi specifici per l'azienda e definire come misurarli.

Partendo da quanto detto su questa trasformazione, SASE e SSE, questo capitolo descrive il percorso verso il paradiso della sicurezza che tutti vogliamo, dove dati, applicazioni e staff sono sicuri sul cloud e possono creare un valore sostanziale e inequivocabile per l'azienda. Quel percorso ora include inesorabilmente l'applicazione dei principi Zero Trust alla progettazione della sicurezza.

Da Zero Trust alla fiducia adattiva continua

Un'implementazione SASE e SSE riuscita è ben più che un semplice cambio di tecnologia. Come visto nel Capitolo 3, Zero Trust riconsidera alcuni presupposti di base della sicurezza. Nel modello on-premise, si parte dal presupposto che la rete sia sicura e sia necessario verificare l'identità di un utente prima di consentire l'accesso. Il paradigma tipico consentiva all'utente l'accesso a tutto o a niente: le uniche due scelte erano "consenti" o "blocca". Zero Trust modifica questo modello come segue:

- **La richiesta di accesso da parte di un utente viene valutata sulla base di diverse condizioni.** L'identità è una di queste, ma il sistema prende in considerazione anche dove si trova l'utente, l'ora del giorno, il dispositivo, il tipo di connessione di rete e molte altre variabili.
- **L'applicazione a cui l'utente si sta connettendo fa parte di quel contesto.**
- **Il livello di servizio voluto è un fattore importante.** Si tratta di usare un'applicazione per una questione di vita o di morte oppure di divertirsi un po' con un videogame?
- **La protezione del percorso di rete può cambiare in base all'applicazione usata.** Se si esegue l'accesso all'account e-mail personale, si usa una connessione ordinaria a Internet dove la protezione TLS (*Transport Layer Security*) viene negoziata tra il server mail e il client di posta. Se un medico sta consultando la cartella clinica di un paziente, viene stabilito un percorso sicuro, crittografato e autenticato, indipendentemente dalle capacità della rete o dell'applicazione sottostante.

In base a questo contesto, viene determinato il livello di attendibilità della sessione di un utente, che godrà di una fiducia limitata o estesa.

Un utente che richiede l'accesso a un'applicazione molto sensibile a un'ora insolita e da una postazione altrettanto insolita (un'istanza con basso livello di attendibilità) dovrà probabilmente sottoporsi a un processo di autenticazione muti-fattore. L'accesso potrebbe essere limitato a un numero ridotto di dati e funzioni, e comunque in modalità di sola lettura. A un dipendente che esegue l'accesso alla solita ora da una posizione sicura (un'istanza con alto livello di attendibilità), potrebbe essere garantito l'accesso completo a tutti i dati e a tutte le funzioni dell'applicazione.

L'esempio del medico che accede alle cartelle cliniche elettroniche mostra il funzionamento dei principi Zero Trust in SSE.

> Un medico ha con sé un tablet dell'ospedale durante il giro di visite in corsia: in base alla sua identità, alla posizione, al dispositivo e ad altri fattori, SSE decide se è sicuro concedere l'accesso completo alla cartella clinica di un paziente.
>
> Poi, il medico va a prendere un caffè di fronte all'ospedale. Accende il laptop, si collega alla rete Wi-Fi del bar e cerca di consultare la stessa cartella clinica. SSE riconosce il medico ma si accorge che il laptop non è di proprietà dell'ospedale ed è collegato a una rete sconosciuta; quindi consente di visualizzare e commentare la cartella ma non di modificare i dati.
>
> Il medico, arrivato a casa per cena, viene avvisato di una crisi in corso e chiede al figlio di cedergli il posto al PC di casa per collegarsi alla cartella clinica del paziente. SSE si accorge del minore livello di sicurezza del PC rispetto al tablet dell'ospedale. Invece di negare direttamente l'accesso, propone una serie di verifiche che consentono al medico di dimostrare ulteriormente la propria identità e chiarire per quale motivo deve accedere. Quindi, mette a sua disposizione un insieme di risorse per rispondere all'emergenza, ad esempio una sessione isolata del browser sotto il controllo di SSE.

Probabilmente l'accesso Zero Trust alla rete (ZTNA) non suona nuovo; infatti, è una scelta eccellente per potenziare la rete virtuale privata (VPN) e far fronte a più scenari di accesso remoto. ZTNA non consente al dipendente l'accesso a un intero segmento di rete che potrebbe consentire connessioni a diversi servizi, garantisce invece solamente la connessione all'applicazione che vuole usare – come nel caso del medico – e solo l'accesso minimo richiesto per eseguire l'attività specifica.

Un'analisi più approfondita di questo modello e del relativo funzionamento nella sua forma più avanzata evidenzia alcuni importanti concetti che possono guidarci:

- **Contesto:** Nella sicurezza pre-SASE la rete definiva il perimetro, una barriera da attraversare per avere l'accesso. Secondo una certa linea di pensiero, con Zero Trust il nuovo perimetro è l'identità, che deve essere convalidata per consentire l'accesso; ma si tratta di un concetto riduttivo. Un approccio migliore prevede invece di valutare l'intero contesto, ossia l'identità e molte altre variabili, per determinare il tipo di accesso.
- **Privilegio minimo:** Zero Trust cerca sempre di concedere solo l'accesso minimo richiesto per un determinato lavoro. La forma più avanzata di Zero Trust cerca anche continuamente di scoprire se sono stati dati troppi privilegi e di eliminare l'eccesso di fiducia dal sistema.
- **Metrica di rischio:** Quando i dipendenti interagiscono con le applicazioni, SSE crea una storia delle attività che può essere analizzata per costruire un modello di attività normali e rilevare in tempo reale quelle sospette. Questa analisi genera metriche di rischio per un dipendente, un'applicazione o un sito web che ampliano ulteriormente il contesto usato per determinare il tipo di accesso da concedere.
- **Occultamento delle risorse:** L'accesso basato su ZTNA non espone gli indirizzi IP pubblici ai quali tutti possono connettersi. La connettività viene concessa solo dopo aver valutato il contesto. Tutto viene occultato di default (eh già, l'oscurità ha un ruolo nella sicurezza, diversamente da quanto spesso insegnato nei corsi infosec).
- **Fiducia adattiva continua (probabilmente l'idea migliore della lista):** La fiducia adattiva continua consiste nel monitorare una connessione adattando continuamente i permessi in base ai cambiamenti del contesto. Se, per esempio, un utente abituale di Salesforce cerca di accedere al sistema di tesoreria del CFO, il sistema riduce accesso e autorizzazione, aumenta la metrica di rischio e sollecita l'intervento di qualcuno. Se, invece, un'altro utente cerca di accedere a un sito web pericoloso. Il sistema visualizza un avviso prima di concedere l'accesso. L'obiettivo è reagire costantemente ai cambiamenti del contesto per proteggere nel modo giusto dati, applicazioni e utenti.

RICORDA

Implementare SSE con i principi Zero Trust restringe la superficie di attacco e consente di prendere decisioni guidate dai dati, aspetto che migliora notevolmente lo stato di sicurezza. Poiché il livello di rischio posto da un utente, un'applicazione o un sito web viene costantemente rivalutato, la sicurezza si adatta in tempo reale in base ai cambiamenti del contesto.

Una volta sviluppato un solido approccio alla fiducia adattiva continua, possiamo iniziare a parlare di come implementare SSE nel modo giusto.

Implementare SSE in quattro semplici passaggi

Per gran parte delle organizzazioni, SSE significa passare da un concetto di sicurezza on-premise, che vede la rete come il perimetro, a una concetto di sicurezza basato sul cloud, dove invece il perimetro costituisce il contesto. Partiremo da un punto che riflette la situazione attuale in gran parte delle aziende: un firewall on-premise che include VPN per l'accesso remoto, un Secure Web Gateway (SWG) on-premise che controlla l'accesso al web ed eventualmente un Cloud Access Security Broker (CASB) autonomo che protegge l'uso delle applicazioni SaaS.

Passaggio 1: Migrare i dipendenti mobili per avere nuovamente visibilità

Prima di tutto, è necessario valutare cosa fanno i dipendenti e misurare il livello di rischio corrente. Il modo più facile per riuscirci è partire dalla popolazione di utenti mobili, che potenzialmente presentano i rischi maggiori. Il loro traffico deve essere instradato attraverso le funzioni SWG e CASB di SSE, configurato per aderire il più possibile alle policy esistenti. E poi si osserva.

Questo esercizio genera un quadro più chiaro di cosa fanno i dipendenti. Le aziende che non usano ancora CASB o SWG scopriranno una quantità enorme (e potenzialmente allarmante) di attività. Anche le aziende che già usano CASB e SWG scopriranno informazioni utili.

Molto probabilmente, si scoprirà che i dipendenti mobili accedono ad applicazioni e servizi di cui non si era a conoscenza. Si saprà dove lavorano e quali tipi di rete tendono a usare.

Per il resto, il passaggio 1 riguarda la migrazione dalle VPN a ZTNA in SSE degli accessi ai sistemi interni nel data center. Ciò migliora l'esperienza del dipendente aumentando al tempo stesso la sicurezza. Pensiamo a quando un idraulico viene a casa nostra mentre siamo al lavoro. Nel fare avanti e indietro dal furgone al bagno, ha l'accesso completo a tutta la proprietà. Magari lascia aperta la porta d'ingresso. Per tutto questo tempo, non abbiamo idea di cosa stia succedendo. Con ZTNA è come avere un pulsante magico per il teletrasporto. Una volta arrivato l'idraulico, lo si può teletrasportare dal furgone al bagno, senza fermate intermedie. Questo è il controllo dell'accesso perfezionato per l'era del cloud.

Passaggio 2: Migrare tutti gli altri dipendenti e applicare la classificazione dei dati all'intera azienda

Il secondo passaggio implica lo spostamento di tutti i dipendenti on-premise sotto la protezione di SSE per controllare l'accesso ad applicazioni e servizi in cloud. Ciò significa trasformare l'architettura di rete. A questo punto, tutti i dipendenti attraversano il punto di presenza più vicino del provider SSE, il quale poi invia il traffico alla destinazione in modo ottimale – spesso con meno hop rispetto alla rete Internet pubblica. Ora è possibile semplificare la rete e rinunciare alle costose reti private, che potrebbero non servire più. Durante questa transizione, si può introdurre una rete SD-WAN (*Software-Defined Wide-Area Networking*) per deviare selettivamente il traffico proveniente dagli uffici remoti.

L'obiettivo è capire fino in fondo quali dati, applicazioni, siti web e altri servizi interessano ai dipendenti. In questa fase, la capacità di SSE di catturare e analizzare le attività aumenta enormemente l'ambito e la profondità del contesto. il controllo di sicurezza espresso dalle policy SSE in questa fase dovrebbe probabilmente essere analogo a quello già presente nel prodotto legacy. È importante raggiungere la corrispondenza con uno stato conosciuto prima di aggiungere nuove capacità, che possono richiedere formazione e addestramento.

Con questo nuovo contesto a disposizione, è possibile gettare le basi per una migliore sicurezza classificando dati, applicazioni e utenti a seconda del rischio e del comportamento. Una volta fatto questo, SSE può usare dati interni ed esterni per calcolare in tempo reale le metriche di rischio di dipendenti, applicazioni e siti web. Ora è

possibile rinunciare a gran parte dell'infrastruttura di sicurezza legacy e procedere al passaggio successivo, nel quale SSE raggiunge un nuovo livello di sicurezza.

Passaggio 3: Implementare la fiducia adattiva continua e dei servizi estesi

Fino a questo punto, l'esperienza d'uso dei dipendenti è rimasta pressoché identica. Il cambiamento avverrà nel passaggio 3, quando la sicurezza si adatta in base al contesto.

RICORDA

La fiducia adattiva continua valuta il contesto per bilanciare il rischio e garantire il tipo di accesso giusto in qualsiasi momento. Consente di definire policy di sicurezza molto più dettagliate. Inoltre, quando gli utenti stanno per fare qualcosa di pericoloso, avvisi e suggerimenti si fanno più frequenti per segnalare le azioni approvate.

Con SSE, i professionisti della sicurezza sanno quali dati sono sensibili e quali applicazioni e siti web rappresentano un rischio. Unendo questa consapevolezza a capacità come il DLP, possono eseguire un controllo minuzioso sull'uso che lo staff fa dei dati sensibili – a un livello senza precedenti. L'accesso ora si trova su un continuum di possibilità, non è più questione di decidere se dare o negare l'autorizzazione.

La fiducia adattiva continua consente inoltre di aggiungere altri servizi. Ipotizziamo, ad esempio, che un medico voglia visitare un sito considerato rischioso. Dopo un avviso, il medico insiste nel suo intento. A questo punto, SSE potrebbe spostarlo in una sessione RBI, dove il browser viene eseguito all'interno di un ambiente virtuale presso il provider SSE, riducendo ulteriormente i rischi. A seconda delle necessità, è possibile aggiungere altri servizi avanzati.

Passaggio 4: Gestire attivamente i rischi con analisi dinamica e metrica

Nel passaggio 4, il team che gestisce SSE può avviare il processo di identificazione attiva dei rischi per eliminarli dall'ambiente. Un metodo per misurare i progressi è tenere traccia delle metriche di rischio per utenti, applicazioni e siti web; l'obiettivo è mostrare una riduzione del traffico verso siti pericolosi e delle azioni rischiose. Un altro metodo prevede di ridurre i diritti tenendo traccia dei modelli d'uso ed eliminando i privilegi in eccesso

A questo punto, è possibile focalizzarsi su alcuni dei controlli di sicurezza di livello più elevato, come la funzione DLP e la neutralizzazione delle minacce, aumentando le capacità di CASB, SWG, ZTNA e *Firewall-as-a-Service* (FWaaS). Questi controlli funzionano meglio in SSE delle rispettive versioni on-premise, e consentono di fare molto di più. Ad esempio, i classificatori basati su machine learning consentono alla funzione DLP di identificare documenti sensibili e reagire di conseguenza in tempo reale.

SUGGERIMENTO

La Digital Experience Management (DEM), la Cloud Security Posture Management(CSPM) e la SaaS Security Posture Management(SSPM) migliorano ulteriormente la gestione del rischio, aggiungendo metodi avanzati che garantiscono disponibilità e prestazioni coerenti e consentono di identificare e correggere eventuali errori di configurazione. In futuro, SSE consentirà ulteriori servizi avanzati di questo tipo.

RICORDA

Sarà la situazione specifica a stabilire i dettagli nei vari passaggi. Ma nel complesso, questo è il processo che gran parte delle aziende deve seguire per ottenere la piena implementazione SSE.

Trasformare la rete e il resto della sicurezza

SUGGERIMENTO

L'implementazione SSE è un passo in avanti importante e non negoziabile verso SASE. Ma per il paradiso che ci siamo proposti di raggiungere, l'intero panorama della sicurezza deve evolvere in modo che tutte le componenti importanti collaborino tra loro. Gran parte delle organizzazioni sta passando a un modello di lavoro ubiquo, per il quale i vantaggi della sicurezza sempre e ovunque sono ben chiari. Questo si allontana naturalmente dalla connettività basata su VPN e reti private, e offre la semplicità e i vantaggi economici di SSE.

L'aspetto più importante di cui tenere conto è che SSE (e SASE) semplifica l'infrastruttura tecnologica complessiva. Nel vecchio modello, i controlli di sicurezza per proteggere accessi non autorizzati erano applicati all'interno della rete aziendale, che costituiva l'unico percorso verso i dati. In quello nuovo, i diversi punti di presenza del provider SSE diventano i percorsi verso i dati, offrendo non solo il controllo degli accessi ma anche la completa ispezione del traffico. La rete sottostante può quindi concentrarsi sul trasferimento dei bit in modo rapido ed efficiente.

I sistemi di gestione dell'identità e accesso (IAM) hanno l'importante compito di autenticare i dipendenti. Molti di questi sistemi sono già altamente configurabili tramite API (*Application Programming Interface*), ma sono progettati per integrarsi anche con altri sistemi – una caratteristica necessaria per qualsiasi implementazione SSE. I miglioramenti alla tecnologia IAM garantiscono capacità ancora più avanzate di elaborare, monitorare e autenticare il contesto, che risulteranno vantaggiose anche per SSE e SASE. Le piattaforme di protezione degli endpoint (EPP) sono un ulteriore vantaggio per SSE: raccolgono importanti segnali (generando altro contesto), eseguono un monitoraggio minuzioso e includono meccanismi per controllare il comportamento e la configurazione di sicurezza. Sincronizzando il piano di implementazione SSE con una corrispondente evoluzione EPP è possibile ottenere il massimo dagli investimenti nella sicurezza.

SASE e SSE accelerano il cambiamento di ruolo del data center. Quando il cloud ha preso il sopravvento, il data center ha perso la sua posizione di centro delle attività di sicurezza. SSE sposta la sicurezza dal data center al cloud.

RICORDA

I data center avranno comunque un ruolo importante in molte aziende per le più svariate ragioni, come la pressione sui costi, i requisiti normativi, la gestione dei rischi e l'utilità di alcuni tipi specifici di infrastrutture di calcolo. Il data center diventerà una delle varie posizioni dove trovare importanti applicazioni protette da SSE.

Vantaggi di SSE per l'azienda

Il rischio informatico è una priorità per gran parte dei direttivi aziendali, ma come abbiamo precisato nel Capitolo 2, la sicurezza non è fine a sé stessa. La sua missione è proteggere il valore creato dai sistemi che supportano le attività aziendali. Le aziende si sono trasferite sul cloud perché per loro è una mossa sensata. Il compito di un'architettura SASE, SSE incluso, è proteggere applicazioni, dati e utenti. Ecco come si traduce in valore per l'azienda:

- **La sicurezza non è più un ostacolo alla produttività aziendale.** L'agilità aziendale è supportata e gli addetti alla sicurezza non rappresentano più dei limiti invalicabili perché ora qualsiasi attività può essere protetta in modo adeguato. Il freno posto dalla sicurezza si allenta notevolmente. I processi di sviluppo e manutenzione dei prodotti risultano ottimizzati

grazie alla maggiore facilità con cui è possibile incorporare la sicurezza. Un'implementazione SSE cloud-based è perfetta per proteggere un ambiente multi-cloud.

- **Il Consiglio di Amministrazione ora ha molta più fiducia nella corretta gestione e analisi dei tipi di controlli richiesti per usare in sicurezza le risorse sul cloud.** Il processo di gestione dei rischi relativi agli, ai dati e alle applicazioni diventa molto più sofisticato, così come i meccanismi usati per mitigare i rischi stessi. Con SSE, i rischi possono essere identificati in modo attivo ed eliminati sistematicamente. La sicurezza in senso stretto segue i dati, il che garantisce una certa tranquillità riguardo alla protezione delle risorse più importanti.
- **Il team di sicurezza diventa molto più unificato e focalizzato sull'attività.** Invece di avere una risorsa dedicata al SWG, una dedicata al CASB e una dedicata al Firewall, ci sarà un team focalizzato sul quadro generale, più informato e in grado di intervenire attivamente.

RICORDA

Implementare SSE significa creare un mondo di sicurezza molto migliore, e tutti in azienda ne trarranno beneficio.

Capitolo **5**

Dieci cose (più o meno...) da fare e non fare nel passaggio a SSE

Una parte importante del passaggio a un cloud sicuro e agile consiste nell'accettare che l'organizzazione IT attualmente in uso non è progettata per questo scopo. Per sua natura l'organizzazione IT rispecchia l'architettura della tecnologia. Pertanto, se i singoli individui o team accolgono con favore i Cloud Access Security Broker (CASB), i Secure Web Gateway (SWG), le reti private virtuali (VPN) e firewall, insieme o come parte di un Security Operation Center (SOC) e di un Network Operation Center (NOC) –, si incontrerà una certa resistenza alla messa in esercizio di una nuova architettura che integra *Secure Access Service Edge* (SASE) e *Security Service Edge* (SSE), e in più unisce sicurezza e networking in un fronte di difesa compatto. Le persone resistono al cambiamento per natura, talvolta per paura di perdere il controllo su un ambito che hanno imparato a conoscere a fondo con molta fatica.

SASE e SSE offrono benefici dal punto di vista tattico, che migliorano la qualità e la portata dei servizi per la sicurezza, e anche strategico, in quanto acceleranoaccelerare il business. I prossimi paragrafi forniscono una guida per adottare con successo SASE e SSE. Inizieremo con quattro principi da seguire per accelerare il passaggio e concluderemo con quattro errori da evitare.

Mettere i dati al centro

Con SSE, la sicurezza segue i dati ovunque. Poco importa, quindi, se i dati sono creati in Google Workspace e Microsoft 365, in un'applicazione *Software-as-a-Service* (SaaS) o in un oggetto di cloud storage: SSE sarà sempre lì a proteggerli.

Poiché SSE diventa un punto di ispezione primario capace anche di facilitare la classificazione dei dati, è importante stabilire lo scopo e la posizione di tutti i dati. Sfruttando queste informazioni per dare la priorità alla protezione e a un uso appropriato dei dati sensibili, ovunque si trovino, si può essere sicuri di aver dato precedenza all'aspetto più importante.

Aprirsi al concetto di integrazione

A ogni fase di risposta agli incidenti è importante sviluppare la capacità di automatizzare e integrare le componenti di sicurezza per riuscire a mettere a punto un ingranaggio finemente calibrato. Questo processo richiede di estrarre informazioni da più sistemi, integrarle per analizzare la situazione, formare la squadra giusta e adottare azioni automatizzate quando possibile.

SSE integra i servizi fondamentali per proteggere il cloud, ma è parte di un più ampio ecosistema di importanti servizi per la sicurezza. I sistemi di gestione delle identità e degli accessi (IAM), le piattaforme di protezione degli endpoint (EPP) e gli strumenti per la gestione delle informazioni di sicurezza e degli eventi (SIEM) sono alcuni dei componenti chiave che lavorano insieme a funzioni specifiche di SSE per fornire una sicurezza esaustiva e supportare una diagnosi rapida dei problemi e la relativa risposta.

Non dimenticare che nel cloud c'è posto anche per i cattivi

SSE e SASE rappresentano un grande balzo avanti in termini di portata e qualità della sicurezza. È ragionevole sentirsi soddisfatti dopo aver messo in campo gli elementi fondamentali. Ma è necessario ricordare che anche gli attaccanti hanno sfruttato il cloud per passare a un livello superiore. Secondo il *Cloud and Threat Report* di Netskope, la percentuale di malware diffuso tramite applicazioni cloud è passata dal 50% del 2° trimestre 2020 a un massimo storico

del 68% nel 2° trimestre 2021, (www.netskope.com/blog/july-2021-netskope-cloud-and-threat-report). SSE ci proietta davanti ai cattivi, ma servono un apprendimento e un adattamento costanti se vogliamo mantenere il vantaggio.

Riconoscere che la sicurezza è parte fondamentale della strategia aziendale

La sicurezza deve essere parte della strategia aziendale fin da subito. L'entusiasmo per le applicazioni e il cloud non ha senso se non si è in grado di proteggere queste soluzioni e quanti le usano per lavoro. La buona notizia è che, con SSE, i team per la sicurezza arriveranno più facilmente a generare business. Di fatto, se il team comprende gli obiettivi aziendali e le implicazioni per la sicurezza, accetterà i cambiamenti più di buon grado perché avrà più potere per proteggere tutto ciò che l'azienda vorrà fare.


SUGGERIMENTO

Perché un'adozione di SASE e SSE abbia successo, i promotori del programma devono spiegare che la sicurezza del cloud è importante a livello strategico. Il messaggio è che l'investimento nel cloud mira a trasformare l'azienda per ottenere risultati migliori, e quindi va protetto. Realizzare e mantenere questi risultati sarà l'incoraggiamento migliore per accettare il passaggio a SASE e SSE con entusiasmo.

Non ragionare a compartimenti stagni

SASE e SSE risolvono gli spinosi problemi che tendono ad accompagnare i progetti cloud. Evitiamo i tentativi di implementare CASB e SWG e Accesso Zero Trust alla rete (ZTNA) come progetti indipendenti: non faranno che attrarre altri vendor di nicchia con promesse illusorie, solo causa di distrazione. L'obiettivo è proteggere il cloud con una piattaforma integrata sensibile al contesto. Il cambiamento insito in SASE e SSE incontrerà certamente resistenza.


ATTENZIONE

Un grosso errore consiste nel rallentare il processo affrontando la questione con il classico modo di ragionare a compartimenti stagni dell'IT, che trascina nel presente vecchi modi di pensare. La sicurezza non dovrebbe più essere categorizzata come una semplice questione di rete. È bene evitare le discussioni che associano la rete e i problemi di sicurezza. SSE è diventato il punto cruciale in termini di visibilità e controllo della sicurezza in quanto parte dell'architettura SASE a funzionalità piena.

Non trascinarsi dietro le vecchie regole

Spesso le persone sono spaventate dal firewall, perché hanno accumulato strati di regole create molto tempo prima da persone che non sono più in azienda. Lo stesso può valere per altre tecnologie di sicurezza, che richiedono regole e configurazioni complesse per ottenere i risultati voluti. SSE è diverso. Anche se sono ancora necessarie regole e configurazioni, gran parte del lavoro è fatto attraverso la definizione di policy che descrivono i risultati. Se implementato in modo efficace, SSE gestisce autonomamente i dettagli delle interazioni tra le regole. Quindi, non dovremo più preoccuparci per la configurazione della tecnologia precedente. Potremo invece concentrare l'attenzione sui risultati in termini di sicurezza e avvalerci di SSE per ottenerli.

RICORDA

La maggior parte dei prodotti SSE è inoltre in grado di gestire le configurazioni di sicurezza cloud e SaaS aiutando così a prendere la decisione giusta e a mantenerla nel tempo.

Non disprezzare il data center

Adesso che la scelta è caduta su SASE e SSE, è facile pensare che il data center tradizionale non sia più importante. Esisterà sempre una qualche forma di data center: dopo tutto il cloud non è altro che una raccolta di data center, alla quale si accede tramite interfacce di programmazione delle applicazioni (API). Lo scopo del data center in questo nuovo modello è quello di un luogoper carichi di lavoro e applicazioni di calcolo importanti. Sebbene il data center non sia più il leader dell'infrastruttura di sicurezza, ne è ancora un importante elemento di supporto.

Non temere il cambiamento

Non facciamoci frenare dalla paura per SASE e SSE. L'architettura è sì diversa, e si dovranno gestire prodotti nuovi – un compito impegnativo visto che interessano tutti in azienda, ma SSE fornirà maggiori informazioni su utenti, dati e applicazioni interni e anche sui siti e sulle applicazioni di terzi. Queste informazioni, a loro volta, apriranno le porte a una maggiore automazione che mira a individuare errori e mettere in atto risposte efficaci. Rispetto allo stato della sicurezza attuale, questo nuovo mondo sarà come un paradiso.

SSE è lo stack di sicurezza che determina la buona riuscita di un'architettura SASE. Il book spiega come implementare SSE oggi.

Il passaggio a SASE richiede partner affidabili con una piattaforma realmente integrata, non venditori di fumo che sfoggiano scritte "SASE" o "SSE" a caratteri cubitali. Questo book vuole essere una guida pratica al passaggio verso SSE e SASE, con tanto di ragioni per cui entrambi i concetti sono fondamentali per creare le architetture di sicurezza e di rete del futuro centrate sul cloud, e tanto di spiegazioni su come investire e progettare oggi per SSE (*Security Service Edge*).

In questo book, scopriremo...

- cosa sono SASE e SSE
- il ruolo critico di Zero Trust
- come proteggere i dati aziendali critici sul cloud
- come mettere il turbo alla forza lavoro remota
- come evitare problemi di progettazione di SSE e SASE

Sul sito Dummies.com®
è possibile trovare video, esempi passo passo e guide dettagliate... o semplicemente fare acquisti!

netskope

Jason Clark (CSO e CMO) e **Steve Riley** (Field CTO), i leader di Netskope, sono autorità ampiamente riconosciute nei campi della tecnologia cloud computing, della cybersicurezza e delle reti, con decenni di esperienza in organizzazioni globali come Gartner, Optiv, Riverbed, e Websense.

ISBN: 978-1-119-89721-7

for dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.