Guida all'acquisto di una soluzione di sicurezza SASE

Come scegliere una piattaforma SASE che mette i dati in primo piano

Forcepoint

Guida all'acquisto

Sommario

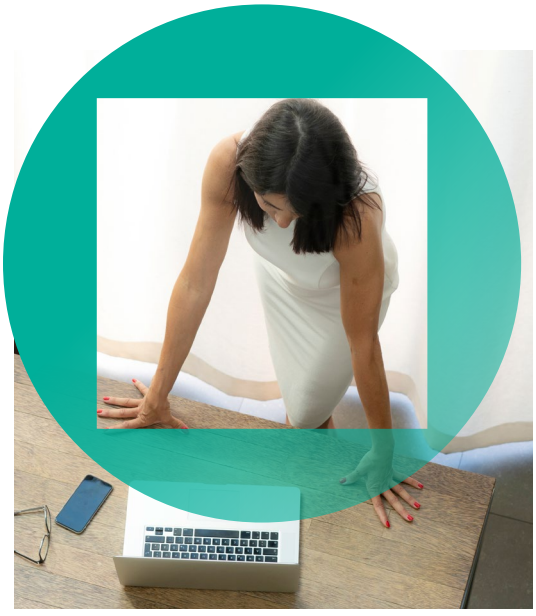
Prefazione

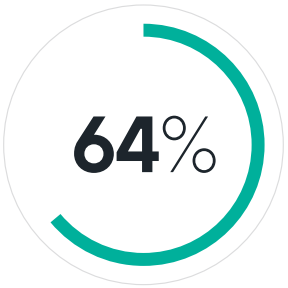
Smart working significa lavorare ovunque: a casa, in ufficio o mentre sei in viaggio. Ciò che conta oggi è la capacità di connettere le persone ai dati e proteggere entrambi con una soluzione di sicurezza costante.

Persone, applicazioni e dati spesso si trovano oltre il tradizionale perimetro di difesa dell'azienda e i team di sicurezza sono chiamati a offrire protezione laddove occorre, sostenendo allo stesso tempo la produttività del lavoratore ovunque si trovi e riducendo il carico operativo. Studiata per affiancare tecnologie di sicurezza e tecnologie di rete divergenti e offrirle sotto forma di servizi convergenti erogati dal cloud, l'architettura Secure Access Service Edge (SASE) di Gartner offre una soluzione decisamente interessante.

Alcune strategie SASE sono focalizzate sulla connessione tra persone e applicazioni; gli accessi, però, costituiscono soltanto il modo con cui le persone ottengono in sicurezza i dati necessari per svolgere il proprio lavoro. Il compito della cyber sicurezza è proteggere anche l'uso dei dati, dall'edge al cloud.

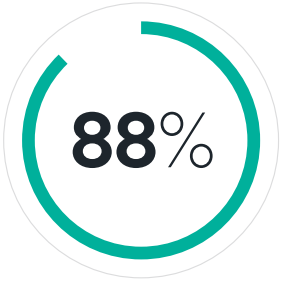
Questa guida permette di capire i vari approcci alle funzionalità e alla sicurezza SASE che può offrirti una piattaforma SASE di fiducia.



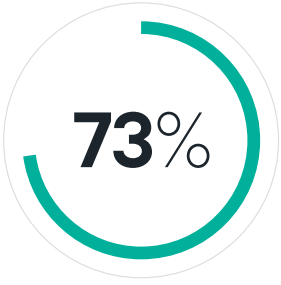


Il **64%** delle imprese afferma che la sicurezza di rete oggi è più complessa[1]

Il **53%** dei dipendenti lavora da remoto, rispetto al 20% dell'era pre-COVID[1]



L'**88%** degli utenti SASE ritiene di avere visibilità su tutto l'utilizzo del cloud nella loro impresa[1]



Il **73%** degli utenti che hanno raggiunto la maturità SASE elimineranno le VPN[1]

Due tipologie di SASE

L'approccio SASE riprende dei prodotti hardware divergenti per la sicurezza e la rete e li ripropone come servizi cloud convergenti che, in linea generale, seguono due scuole di pensiero, descritte di seguito.

Il SASE incentrato sugli accessi

- **Pro:** come suggerisce il nome, il SASE incentrato sugli accessi punta soprattutto a connettere in sicurezza utenti, applicazioni e dati, che siano sul web, sul cloud oppure in data center privati interni. Solitamente erogato come cloud, questo tipo di SASE offre un controllo centralizzato su chi può utilizzare i sistemi aziendali cruciali e offre protezione da hacker, malware, ransomware e altre minacce avanzate.
- **Contro:** il SASE incentrato sugli accessi è focalizzato sulle connessioni tra gli utenti e le applicazioni necessarie per la loro interazione con i dati aziendali, ma non offre un controllo costante sull'uso di tali dati. Altre soluzioni, poi, operano come prodotti di punta mal gestiti, richiedono molteplici endpoint agent per diversi servizi di sicurezza e quindi creano caos e conflitti tra gli agenti.

SASE Data-First

- **Pro:** una soluzione SASE che dà priorità ai dati offre un controllo costante sul loro utilizzo oltre ad assicurare agli utenti l'accesso sicuro ai dati. In più alcune soluzioni SASE si sono evolute per capire in che modo interagiscono gli utenti con i dati, i sistemi digitali e fisici e identificano i comportamenti che creano un rischio e che possono sfociare in una violazione. Quando i dati sono il punto focale del SASE, le policy di sicurezza possono essere attuate automaticamente in base al rischio presentato da un utente in qualsiasi dato momento. L'obiettivo del SASE Data-First è uniformare ovunque l'attuazione automatizzata delle policy – sugli endpoint, nella rete, sul web e nel cloud – affinché questo approccio diventi l'ideale per l'impresa distribuita in cui i dipendenti lavorano e usano i servizi cloud al di fuori delle mura aziendali.
- **Contro:** anche se tutte le piattaforme SASE consentono di implementare una funzionalità per volta, un approccio Data-First al SASE è più efficace quando la sicurezza dei dati è considerata prioritaria a livello dell'intera organizzazione. Per ottenere tutti i vantaggi di un approccio che mette i dati in primo piano, le policy di sicurezza per la proprietà intellettuale e le informazioni sensibili devono essere comprese e supportate dalle procedure e dai processi di management e business.

5 passi per l'adozione del SASE

1.

Proteggere i lavoratori in smart working sia sul web che nel cloud

La sicurezza SASE deve permettere alle persone di lavorare in sicurezza, ma senza ostacolare la produttività. L'"anywhere worker" deve poter lavorare liberamente sempre, ovunque si trovi.

2.

Controllare gli accessi alle app cloud e private senza VPN

Ogni utente deve avere accesso soltanto alle risorse che è esplicitamente autorizzato a usare, e sempre sotto l'occhio vigile dell'azienda.

3.

Tutelare l'uso dei dati ovunque

Il SASE deve assicurare il controllo costante sull'utilizzo dei dati critici e della proprietà intellettuale una volta che sono stati scaricati dalle app. Solo così, infatti, è possibile evitare che i dati finiscano nel cloud, sul web o in account privati, intenzionalmente o meno.

4.

Connettere e proteggere filiali e sedi remote

Gli utenti presso le sedi remote devono poter accedere a web, cloud e app private velocemente e in sicurezza, senza i costi o le complessità delle linee MPLS private e senza i disagi di una rete di backhaul con il quartier generale. L'integrazione semplice con i servizi SASE è fondamentale per la gestione di scala.

5.

Monitorare continuamente il rischio correlato agli utenti

Il controllo sull'uso dei dati, soprattutto sui dispositivi remoti e i servizi cloud, è possibile solo a patto di sapere costantemente che cosa fanno le persone e se il loro comportamento crea rischi che potrebbero trasformarsi in violazioni.

Che cosa cercare in SASE Data-First

Facendo convergere le funzionalità in una piattaforma erogata su cloud, il SASE va a colmare le lacune create da diversi prodotti mirati, riduce i costi e migliora le efficienze, offrendo sicurezza ovunque siano utilizzati i dati. La differenza tra l'approccio SASE incentrato sui dati e quello focalizzato sugli accessi si riduce a una sola questione, ovvero se, dopo l'accesso, i dati siano o meno protetti costantemente. Per una corretta valutazione del SASE, considera le seguenti caratteristiche e cerca quelle funzionalità SASE avanzate che aumentano l'automazione e la gestibilità, mettendo sempre in primo piano i dati.

Funzionalità chiave

- → **Protezione dei dati:** il SASE Data-First deve offrire protezione sugli accessi e sull'uso di dati sensibili e proprietà intellettuale. Cerca soluzioni SASE che offrono un singolo set di policy per la sicurezza dei dati, attuabili in modo uniforme dall'endpoint a tutta la rete, web e cloud inclusi. Dei controlli del traffico di livello enterprise impediscono le fughe dei dati dai dispositivi dei dipendenti, ad esempio vietando il passaggio (e anche la stampa o la copia) dei dati su un dispositivo USB o su un servizio cloud.
- → **Protezione dalle minacce:** le difese sono multistrato e abbinano protezione dell'edge, ispezione avanzata dei contenuti, rilevamento dei malware avanzati e isolamento remoto dei browser per creare una barriera dagli attacchi esterni. Una protezione completa, erogata direttamente dal cloud e quindi senza l'uso di appliance hardware, ti permette di innalzare velocemente le protezioni per le filiali quando occorre.
- → **Sicurezza delle applicazioni:** il SASE è stato studiato per offrire visibilità e controllo su applicazioni, IT Shadow e dispositivi non gestiti e gestiti dall'azienda, con funzioni come il filtraggio degli URL, l'ispezione avanzata dei contenuti e la visibilità delle app cloud. Bloccando l'uso di servizi cloud non autorizzati, di fatto impedisci ai dipendenti di aggirare le policy di sicurezza. Un controllo granulare e completo sull'uso delle app e sulle attività semplifica la compliance nel cloud.
- → **Sicurezza di rete:** una sicurezza globale, che include servizi firewall locali e su cloud, consente l'accesso sicuro a internet, l'ispezione del traffico crittografato e le difese dalle minacce avanzate di rete.

- → **Connettività di rete:** l'SD-WAN collega gli uffici di filiale direttamente a internet, dove i servizi SASE possono offrire una sicurezza trasparente; un agente per gli endpoint collega similmente i dipendenti che lavorano da remoto.

Funzionalità di nuova generazione

- → **Policy unificate per la sicurezza dei dati.** Le policy di sicurezza possono essere definite una volta sola e poi applicate ovunque, dall'endpoint al cloud.
- → **Agenti unificati.** Gli agenti unificati integrano i software degli endpoint per l'accesso sicuro alle risorse, attuando le policy e monitorando le attività sui dispositivi degli utenti.
- → **Funzionalità di distribuzione flessibili.** Queste funzionalità integrano tutta una serie di controlli contestualizzati, delle implementazioni ibride laddove sussistono requisiti speciali (ad es. la conformità con regolamenti sulla sovranità dei dati) e una SD-WAN sicura, senza bisogno di utilizzare altri prodotti.
- → **Applicazione delle policy in base al rischio.** Questa funzione modula automaticamente la sicurezza a seconda del rischio che scaturisce dal comportamento di ogni singolo utente quando usa dati, app e sistemi.

Fatti chiave da considerare

1. Quali passaggi ti occorrono per passare a un modello di forza lavoro ibrida?
2. Come fanno oggi gli smart worker ad accedere alle app private e su cloud?
3. Che cosa hai dovuto modificare nella tua infrastruttura o struttura operativa per supportare l'home working?
4. Come potrai sostenere l'home working?
5. Quali applicazioni autorizza la tua organizzazione oggi?
6. Hai visibilità sulle applicazioni non autorizzate che includono delle funzionalità di condivisione dati?
7. Hai la capacità di controllare la sicurezza su cloud / internet per i tuoi lavoratori da remoto?
8. Sei in cerca di modi per consolidare l'hardware sull'edge di rete (negli uffici, nelle filiali ecc.)?
9. Quale strategia hai adottato per proteggere gli accessi alle app private e interne?
10. Come proteggi o controlli i dati e quali sono le lacune tra i requisiti di legge e le tue capacità?
11. Qual è l'esposizione al rischio della tua organizzazione riguardo alla "perdita" di dati nel cloud, all'esposizione dei dati al pubblico o all'esfiltrazione diretta?
12. Se potessi ripartire da zero, che cosa faresti diversamente per proteggere reti, dati e accessi al cloud?

Il risultato: protezione dei dati ovunque

I lavoratori in smart working avranno sempre più autonomia nell'azienda decentralizzata moderna. Il mondo è cambiato irreversibilmente e oggi le opzioni per accedere a risorse e servizi e per proteggerci da minacce sofisticate e violazioni accidentali sono, almeno in apparenza, infinite.

In quanto professionista della sicurezza, sei responsabile di permettere la trasformazione senza vincolarti a soluzioni specifiche che non sono in grado di adattarsi a frontiere digitali sempre più inconsistenti. Se stai leggendo questo articolo, significa che sei in cerca di nuovi modi per favorire efficacemente la produttività e, allo stesso tempo, proteggere persone e dati fondamentali ovunque. Oggi la sicurezza più efficace è cloud nativa e di natura ibrida.

Trova un partner in grado di aiutarti a identificare rapidamente le opportunità di creare un'infrastruttura di sicurezza integrata, e che ti segua passo dopo passo. Un partner che ti offra la flessibilità per adattarti a un ambiente che evolve senza sosta.

In quanto professionista della sicurezza, sei responsabile di permettere la trasformazione senza vincolarti a soluzioni specifiche che non sono in grado di adattarsi a frontiere digitali sempre più inconsistenti.

Passi successivi

Scopri di più e scarica il white paper *5 passi per l'adozione del SASE*.

Scarica ora

[1] ESG Research Insights Report, Quantifying the Benefits of SASE, marzo 2021

Forcepoint

forcepoint.com/contact

Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è tutelare le aziende e guidare la crescita e la trasformazione digitale. Le soluzioni human-centric di Forcepoint si adattano in tempo reale alle modalità di interazione uomo / dati, consentono un accesso sicuro e, allo stesso tempo, permettono ai dipendenti di creare valore. Dalla sua sede di Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.

[SASE Security Buyers Guide-IT] Jun2021