Scegli la giusta soluzione SASE per la tua forza lavoro ibrida

Sommario

Panoramica preliminare

Fornire un accesso sicuro e autenticato alle applicazioni e alle risorse critiche, indipendentemente dal fatto che i dipendenti si trovino on-premise, lavorino da casa o in qualsiasi luogo, è ormai un requisito imprescindibile per la maggior parte delle organizzazioni. Le soluzioni Secure Access Service Edge (SASE) offrono una soluzione affidabile e flessibile per l'ormai ineluttabile passaggio a un modello ibrido di lavoro agile. Le soluzioni SASE devono combinare accesso remoto sicuro, autenticazione avanzata per sessione e per applicazione e sicurezza di livello enterprise in un'unica soluzione basata su cloud che può essere utilizzata ovunque, estendendo ai lavoratori remoti le stesse protezioni e prestazioni che sperimentano quando lavorano in un ufficio tradizionale on-premise.

Tuttavia, non tutte le soluzioni SASE sono uguali: l'accesso specifico alle applicazioni, le funzionalità e l'efficacia della sicurezza possono variare notevolmente. Inoltre, per le organizzazioni con una rete ibrida, l'aggiunta di un'ulteriore serie di tecnologie da gestire può sovraccaricare le limitate risorse IT, soprattutto quando si cerca di gestire l'ambiente da un capo all'altro per individuare i problemi e ottimizzare l'esperienza dell'utente. Le organizzazioni devono considerare attentamente diverse capacità critiche in vari casi d'uso principali quando valutano la tecnologia SASE per il proprio ambiente.

In che modo la forza lavoro ibrida di oggi influisce sulla sicurezza informatica

La forza lavoro ibrida è la nuova realtà per la maggior parte delle aziende: lo scorso annoè raddoppiata la percentuale di dipendenti in tutto il mondo che ora lavorano permanentemente da casa.[1] Un sondaggio mostra che l'83% dei responsabili aziendali e IT vede il lavoro ibrido come un pilastro delle operazioni future, e il 42% ritiene che più della metà della propria forza lavoro rimarrà definitivamente ibrida ora che la pandemia è alle spalle.[2]

Un altro dato di fatto del business moderno è il numero di applicazioni e servizi che si stanno spostando verso il cloud per ottenere maggiore efficienza, risparmio ed elasticità. Entro il 2025, ben la metà di tutta la spesa per applicazioni, software di infrastruttura, servizi dei processi aziendali e mercati dell'infrastruttura di sistema si sposterà verso il cloud.[3]

Ma questi rapidi cambiamenti nel modo di operare delle aziende hanno creato nuovi problemi per i team di sicurezza informatica. Un recente sondaggio rivela che l'80% dei responsabili della sicurezza e aziendali ritiene che le loro organizzazioni siano più esposte a rischi a causa del lavoro remoto.[4] Questa tendenza è confermata dai dati che mostrano che la quantità complessiva degli attacchi è aumentata del 31% rispetto lo scorso anno, a causa di cybercriminali che cercano di sfruttare i rapidi cambiamenti delle reti aziendali.[5] L'anno scorso è cresciuto anche il numero di violazioni di dati che hanno avuto successo, superando il precedente record annuale del 23%.[6]

Questi crescenti problemi sono spesso il risultato di una sicurezza obsoleta o insufficiente che non è mai stata progettata per affrontare le problematiche odierne. Ad esempio, molte aziende hanno scoperto nelle prime settimane della pandemia COVID-19 che le loro tradizionali reti VPN non erano basate su una strategia di connettività ideale per la loro forza lavoro remota in espansione. Le reti VPN non sono mai state concepite per operare su vasta scala, creando problemi di sicurezza.[7] Inoltre, comportano numerosi rischi, soprattutto se la rete è configurata in modo errato (l'attacco Colonial Pipeline è stato sferrato proprio attraverso una VPN di questo tipo).[8] Altre lacune nella sicurezza sono dovute alla mancanza di formazione sul cloud e all'elusione della sicurezza.[9]

La protezione degli ambienti di lavoro ibridi, oggi in rapida evoluzione, richiede una sicurezza solida e mirata, come una strategia basata su soluzioni SASE.

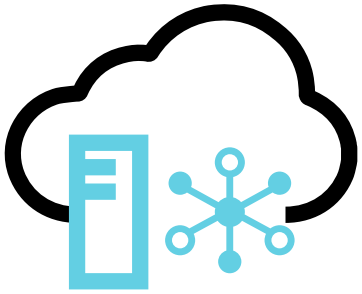
Ogni organizzazione ha una superficie di attacco in rapida espansione a causa di un maggior numero di ambienti ibridi, nuove opzioni di connettività e ulteriori applicazioni business-critical distribuite nel cloud.[10]

Adottare un approccio Single-Vendor SASE

Per assicurare connettività e sicurezza costanti per gli utenti dislocati ovunque, le soluzioni di rete e di sicurezza devono convergere ai perimetri e nel cloud. A livello più elementare, la tecnologia SASE combina più funzioni di Networking-as-a-Service (NaaS) e di Security-as-a-Service (SaaS) in un'unica soluzione. Questo può essere difficile da ottenere quando si cerca di integrare soluzioni di vendor diversi. Tuttavia, una soluzione SASE incentrata sulla piattaforma e su un unico fornitore consente di consolidare le tecnologie e di far convergere le funzioni di rete e di sicurezza per aumentare l'efficienza operativa. Ma le soluzioni SASE non operano in modo isolato. Per questo motivo, è fondamentale che le organizzazioni cerchino soluzioni SASE che possano essere perfettamente integrate nelle loro architetture di rete e di sicurezza, per assicurare una connettività sicura e affidabile e per offrire un'esperienza utente di livello superiore ovunque sia necessario.

Come per ogni nuova opportunità, immancabilmente spuntano vendor che cercano di soddisfare un'esigenza urgente e di conquistare una fetta del nuovo mercato. Tuttavia, molte di queste soluzioni non sono all'altezza dei vantaggi promessi. Alcune si basano su tecnologie immature o su funzionalità inadeguate. Molte operano come soluzioni isolate ed indipendentiche non si integrano con le tecnologie di sicurezza esistenti o con la rete ibrida in espansione. Poche consentono alle organizzazioni di realizzare una soluzione perfetta che riduca anziché complicare la dispersione delle soluzioni.

Per le organizzazioni che cercano di gestire una rete ibrida in rapida espansione ed estremamente dinamica, l'aggiunta di un'altra serie di tecnologie da gestire può sovraccaricare le limitate risorse IT. I controlli manuali, gli script e la threat intelligence limitata utilizzati da molti fornitori di tecnologie SASE non riescono a tenere il passo con il panorama delle minacce in rapida evoluzione, lasciando le organizzazioni vulnerabili.



Quello che SASE rappresenta è un modo migliore di fornire tecnologie di sicurezza informatica utilizzando una convergenza di software cloud e strumenti di rete.[11]

Scegliere la soluzione giusta: cosa cercare

Quando si tratta di valutare le funzionalità critiche e di selezionare la migliore soluzione SASE per proteggere la tua forza lavoro remota, ci sono sette considerazioni fondamentali di cui tenere conto:

1. Un approccio SASE offerto da un unico fornitore

Tentare di far interagire soluzioni di fornitori diversi come un'architettura SASE unificata non è solo difficile da realizzare, ma può richiedere molto tempo per la manutenzione e la risoluzione dei problemi. Un approccio SASE basato su un unico vendor fa convergere rete e sicurezza, in modo che la gestione, l'ottimizzazione e l'applicazione delle policy siano controllati da un'unica interfaccia. E idealmente, questo tipo di soluzione deve anche interoperare sulla rete distribuita, trasferendo senza problemi le connessioni tra il cloud e i dispositivi on-premise. Questo permette alle policy di accesso e sicurezza di seguire gli utenti e le applicazioni da un capo all'altro, anziché terminare la connettività e il controllo a uno dei perimetri della rete. Solo facendo convergere realmente rete e sicurezza in tutto l'ambiente aziendale le organizzazioni possono implementare un'architettura zero-trust completa che offra una sicurezza coerente e un'esperienza utente di livello superiore ovunque.

2. Un agente unificato per diversi casi d'uso

L'onboarding di differenti agenti per ogni caso d'uso può diventare rapidamente complesso e costoso da gestire. Una soluzione SASE efficace deve offrire un unico agente che supporti più casi d'uso, tra cui ZTNA, CASB (Cloud Access Security Broker) e protezione degli endpoint, reindirizzando automaticamente il traffico per proteggere le risorse e le applicazioni attraverso la sicurezza fornita dal cloud.

3. Accesso sicuro a Internet

Con il lavoro remoto che sta diventando la nuova normalità, gli utenti con accesso diretto a Internet ampliano notevolmente la potenziale superficie di attacco dell'organizzazione. Una soluzione efficace deve essere in grado di seguire, abilitare e proteggere gli utenti indipendentemente dalla loro posizione (o dalle loro applicazioni).

Una soluzione di sicurezza fornita nel cloud non deve limitarsi a offrire un tunnel crittografato (come le VPN tradizionali), ma deve offrire un portfolio di soluzioni di sicurezza di livello enterprise progettato per ispezionare il traffico e rilevare e rispondere agli attacchi noti e sconosciuti. In quest'ottica, una soluzione SASE di successo include funzionalità SWG (Secure Web Gateway) per monitorare e proteggere i dati e le applicazioni dalle tattiche di attacco basate sul web, oltre ad altre funzionalità come URL Filtering, sicurezza DNS, antiphishing, antivirus, antimalware, sandboxing e ispezione SSL approfondita.

4. Accesso privato flessibile e sicuro

Una soluzione SASE flessibile deve fornire una connettività sicura alle applicazioni aziendali, indipendentemente dal fatto che vengano distribuite in un data center privato o nel cloud pubblico. La tecnologia ZTNA integrata fornisce un accesso esplicito per applicazione agli utenti autenticati senza richiedere un tunnel persistente. La capacità di ZTNA di concedere l'accesso in base all'identità e al contesto, combinata con la convalida continua, assicura un controllo efficace su chi e cosa si trova in rete. La tua soluzione SASE deve inoltre integrarsi perfettamente con le soluzioni SD-WAN e NGFW per fornire funzionalità di indirizzamento intelligente e di instradamento dinamico attraverso il PoP SASE, assicurando un'esperienza utente di livello superiore grazie all'individuazione e alla protezione automatica del percorso più rapido verso le applicazioni aziendali. E idealmente, deve fornire tutto questo attraverso un unico agente per ZTNA, reindirizzamento del traffico, CASB e protezione degli endpoint.

5. Accesso SaaS sicuro

Una soluzione SASE efficace deve consentire un accesso sicuro indipendentemente dalla posizione di applicazioni, dispositivi, utenti e carichi di lavoro, una funzione fondamentale per una forza lavoro ibrida che si sposta regolarmente tra campus, filiali, uffici domestici e ambienti mobili. Inoltre, con la crescente dipendenza aziendale dalle applicazioni SaaS, una soluzione di sicurezza fornita nel cloud efficace deve anche proteggere i dati mission-critical e salvaguardare le informazioni basate su cloud con la stessa sicurezza di livello enterprise, indipendentemente dal fatto che gli utenti si trovino all'interno o all'esterno delle sedi aziendali. Deve anche supportare la tecnologia CASB dual-mode, con funzionalità in linea e basate su API, per identificare e superare le problematiche dello shadow IT, proteggendo al contempo i dati critici. Tenendo conto di tutto questo, le organizzazioni devono cercare una soluzione SASE che offra visibilità sulle applicazioni SaaS principali, report sulle applicazioni a rischio, un controllo granulare delle applicazioni per proteggere i dati sensibili e in grado di rilevare e risolvere le minacce informatiche presenti nelle applicazioni su dispositivi gestiti e non gestiti.

6. Consumo flessibile con onboarding semplificato

Le considerazioni per la scelta di una soluzione SASE non devono limitarsi alla tecnologia, ma devono includere anche le modalità di pagamento. La giusta soluzione SASE può aiutare le organizzazioni a spostare il consumo aziendale da un modello CAPEX a uno di tipo OPEX. Per farlo in modo efficace, deve offrire licenze semplici e differenziate che consentano alle organizzazioni di prevedere una correlazione tra costi e crescita aziendale e l'uso della sicurezza, anziché vincolare il capitale ad hardware in eccesso.

I controlli dei costi costanti possono anche essere legati ad aspetti come l'onboarding semplificato e i sistemi di gestione degli endpoint consolidati. La gestione centralizzata deve inoltre combinare operazioni efficienti con analisi granulari e includere report pre-generati e on-demand, tra cui registrazione ed eventi relativi a utenti, endpoint e VPN per una risoluzione efficiente dei problemi.

7. Gestione semplice basata su cloud

Un sistema di gestione SASE basato su cloud deve fornire visibilità, segnalazione, registrazione e analisi complete, contribuendo ad assicurare operazioni di sicurezza efficienti e riducendo al contempo il tempo medio di rilevamento (MTTD) e di risoluzione (MTTR). La sfida è che gli elementi di sicurezza SASE che operano come soluzioni monofunzionali in compartimenti stagni possono comportare oneri inutili per i team di sicurezza, soprattutto per le organizzazioni che gestiscono un ambiente ibrido con risorse IT limitate.

Questa integrazione può essere ancora più efficace se i componenti SASE distribuiti nel cloud interagiscono perfettamente con le soluzioni di sicurezza on-premise per un'orchestrazione e un'applicazione coerente delle policy.

Lavorare da qualsiasi luogo senza preoccupazioni

Poiché si stima che il 50% della forza lavoro statunitense continui a lavorare da casa a lungo termine,[12], le sfide legate alla necessità di garantire una forza lavoro ibrida sembrano essere una realtà ineluttabile che i team di sicurezza devono affrontare nel breve termine. Se implementata correttamente e con le funzionalità richieste per risolvere i casi d'uso principali, la giusta soluzione SASE può assicurare un accesso sicuro e affidabile a forze di lavoro eterogenee, fornendo al contempo una sicurezza di livello enterprise, fornita nel cloud, per proteggere le connessioni remote. Inoltre, una soluzione ben scelta può aiutare anche la tua azineda a concentrarsi sulle attività aziendali principali, eliminando la necessità di gestire manualmente integrazioni complesse, fornendo una postura di sicurezza coerente in tutti i tuoi ambienti IT ibridi in continua evoluzione.

[1] "Securing the hybrid workforce", Security Magazine, 7 gennaio 2022.

[2] "83% of IT leaders believe the hybrid workforce is here to stay", Tech Republic, 3 novembre 2021.

[3] "What is cloud computing? Everything you need to know about the cloud explained", ZD Net, 25 febbraio 2022.

[4] "Corporate attack surface exploding as a result of remote work", Help Net Security, 27 settembre 2021.

[5] "Cybersecurity Still A Challenge, And Improving Resiliency Is Essential", Forbes, 15 dicembre 2021.

[6] "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises", ITRC, 24 gennaio 2022.

[7] "Hybrid workforce model needs long-term security roadmap", Tech Target, 25 giugno 2021.

[8] "The Cybersecurity Challenges Of Working From Anywhere", Forbes, 2 marzo 2022.

[9] "Misconfigurations: Still the Biggest Threat to Cloud Security" Network Computing, 25 agosto 2021.

[10] "Predictions for 2022: Tomorrow's Threats Will Target the Expanding Attack Surface", Fortinet, 16 novembre 2021.

[11] "What's Driving The SASE Boom", Forbes, 11 novembre 2021.

[12] "83% of IT leaders believe the hybrid workforce is here to stay", Tech Republic, 3 novembre 2021.

FORTINET®

www.fortinet.com

ottobre 13, 2023 9:17 AM
1777526-0-0-IT