Akamai

GUIDA PER GLI ACQUIRENTI

Come scegliere un SWG (Secure Web Gateway) basato sul cloud

Protezione dei dipendenti remoti e semplificazione della sicurezza aziendale

Sommario

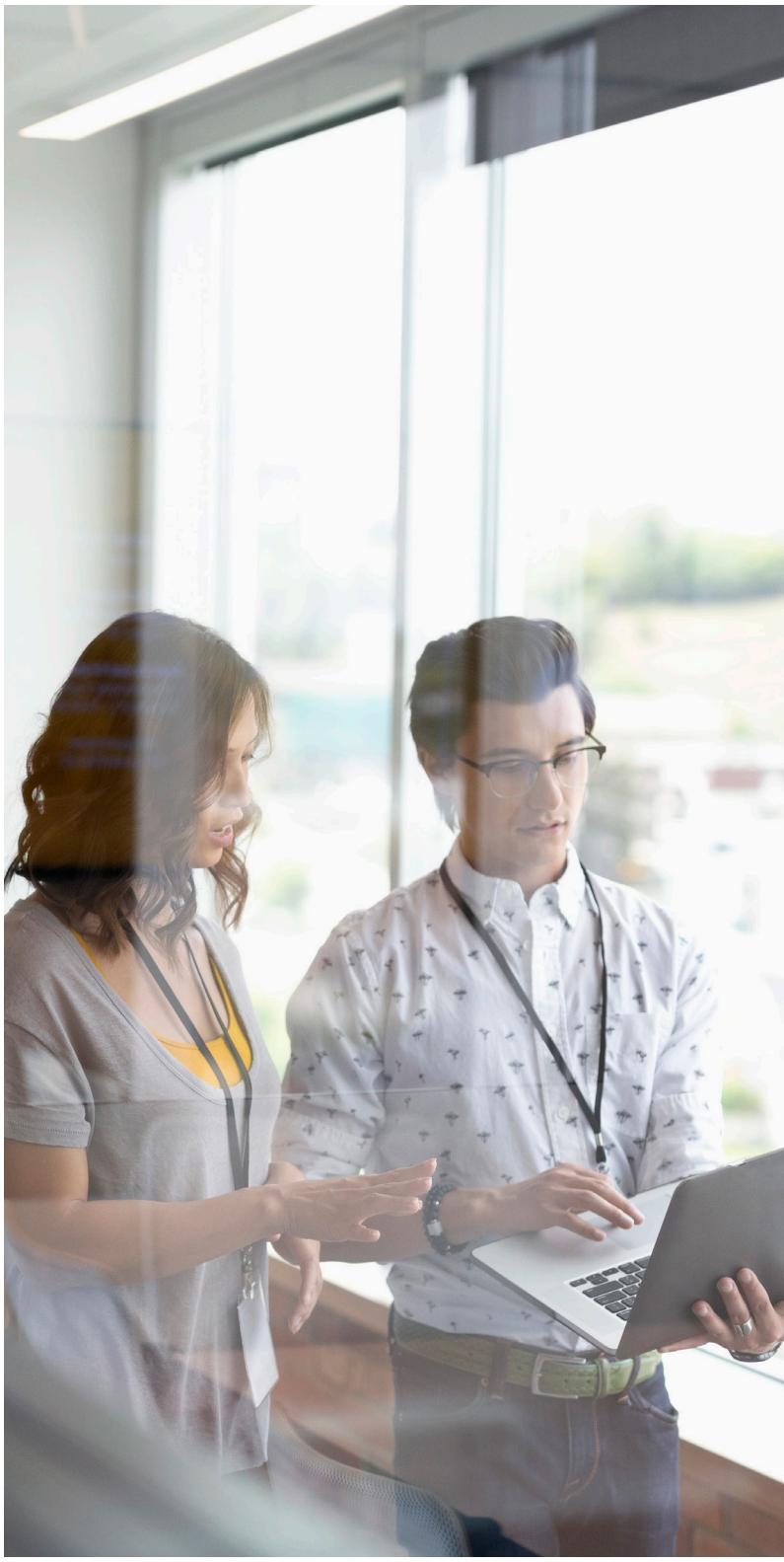
Proteggere le moderne imprese con una nuova concezione del backhaul del data center

Cloud computing, SaaS (Software-as-a-Service), mobilità e architetture di rete aggiornate hanno rivoluzionato le prassi aziendali. Tuttavia, hanno anche profondamente sconvolto il lavoro dei team IT, impegnati come non mai a proteggere il personale senza incidere sulla portata di queste nuove tecnologie. Oggi si aggiunge una sfida ulteriore. Indipendentemente dalla fase della trasformazione digitale in cui si trovavano, molte aziende hanno dovuto adottare rapidamente nuove misure per supportare un drastico aumento degli utenti remoti nel 2020.

Un SWG (Secure Web Gateway) è un componente fondamentale della protezione dei dipendenti, ma molte aziende utilizzano ancora dispositivi fisici distribuiti nei data center. Questi dispositivi hardware richiedono gestione, manutenzione e aggiornamenti continui e utilizzano un complicato backhaul del traffico per ispezionare e controllare il traffico web, riducendo così le performance.

Ma la necessità di proteggere l'ambiente aziendale distribuito che si sta configurando impone alle organizzazioni l'adozione di un approccio moderno e semplificato. La soluzione: eliminare i dispositivi hardware e spostare l'SWG (Secure Web Gateway) nel cloud.

Questa guida all'acquisto descrive i vantaggi dell'SWG (Secure Web Gateway) basato sul cloud e quali funzionalità cercare in una moderna tecnologia di gateway web.



L'aumento del lavoro remoto crea nuove esigenze IT e di sicurezza

Negli ultimi dieci anni, i dipendenti remoti delle organizzazioni sono aumentati costantemente. Il COVID-19 ha semplicemente accelerato una tendenza che secondo le previsioni continuerà ben oltre la pandemia. Gartner ha rilevato infatti che il 74% dei CFO intervistati trasferirà almeno il 5% dei dipendenti che in precedenza lavorava in sede a posizioni permanentemente remote dopo la fine della pandemia.[1]

Allo stesso tempo, il numero di attacchi mirati sofisticati come phishing, ransomware e malware è aumentato vertiginosamente. Il 53% degli intervistati in un recente sondaggio ha affermato di aver assistito a un aumento dell'attività di phishing dall'inizio della pandemia di COVID-19.[2] Un recente avviso del Dipartimento del Tesoro degli Stati Uniti ha affermato che la richiesta di riscatto per attacchi ransomware è aumentata durante la pandemia di COVID-19 in quanto i cybercriminali prendono di mira i sistemi online a cui le persone si affidano per continuare a condurre le proprie attività.[3]

Tradizionalmente, le organizzazioni garantivano l'accesso a Internet agli utenti presso le sedi centrali e le filiali e anche ai dipendenti remoti installando appliance di sicurezza, come Secure Web Gateway, nei propri data center. Successivamente eseguivano il backhaul di tutto il traffico web in tale posizione centrale per l'ispezione e il controllo.

Le aziende utilizzavano questi Secure Web Gateway per filtrare il malware indesiderato dal traffico web avviato dagli utenti, impedire agli utenti di accedere a siti web dannosi e applicare le policy aziendali e normative.

Queste soluzioni gateway sono state originariamente progettate e implementate in ambienti in cui la maggior parte dei dipendenti utilizzava dalla propria scrivania dispositivi gestiti dall'azienda. Tuttavia, con l'aumento del numero di utenti che lavorano in remoto e nelle filiali e l'incremento del traffico sull'Internet pubblico per l'accesso alle applicazioni SaaS, le organizzazioni hanno iniziato a installare più Secure Web Gateway ridondanti nel data center centrale per garantire performance soddisfacenti. L'acquisto e la gestione di questi sistemi sono diventati sempre più complessi, costosi e dispendiosi in termini di tempo.

> **"La percentuale del budget IT speso per i data center è diminuita negli ultimi anni e oggi rappresenta solo il 17% del totale".**
>
> Gartner, Dati sulle metriche chiave dell'IT 2019

In alternativa, le organizzazioni aggiungevano dispositivi SWG alle proprie filiali eseguendo il backhaul del traffico per tutti gli utenti remoti. Tale ridondanza ha portato a un ulteriore aumento delle appliance e dei relativi costi, nonché ad aumentare notevolmente il carico di lavoro di implementazione e gestione.

Inoltre, è diventato sempre più difficile mantenere policy per la sicurezza coerenti per un elevato numero di posizioni. Anche il ricorso alla virtualizzazione per ridurre la proliferazione di appliance doveva comunque prevedere l'uso di dispositivi hardware aggiuntivi.

Un terzo approccio è consistito nell'implementazione ibrida, in cui le organizzazioni hanno continuato a utilizzare SWG locali per le sedi principali inviando il traffico web delle filiali a un SWG basato sul cloud e continuando ad eseguire il backhaul del traffico per i dipendenti remoti. Questo approccio ha preservato gli investimenti hardware esistenti nelle apparecchiature locali. Tuttavia, ha aggiunto complessità perché le organizzazioni si sono trovate a dover gestire sistemi disparati. Le apparecchiature aggiuntive e la gestione supplementare non solo erano molto più costose di un approccio cloud puro, ma era anche difficile mantenere policy coerenti tra i sistemi locali e quelli basati sul cloud.

> **Gartner prevede che, entro il 2025, l'80% delle aziende chiuderà i propri data center tradizionali.[4]**

A peggiorare le cose, durante la fase di adozione di queste soluzioni sempre più complesse, le organizzazioni hanno iniziato a fare i conti con la scarsità di risorse per la cybersicurezza. Uno studio di (ISC)[2] ha rilevato che sarebbe necessario un aumento del 62% per colmare l'attuale carenza di dipendenti richiesti nel settore della sicurezza negli Stati Uniti.[5]

Perché scegliere un SWG (Secure Web Gateway) basato sul cloud?

Le organizzazioni necessitano di un approccio moderno alla sicurezza web, che si adatti alla strategia cloud aziendale e che supporti e consenta lo smart working. Un SWG basato sul cloud offre alle organizzazioni un elevato livello di sicurezza riducendo la complessità tramite la connessione diretta a Internet per evitare la necessità di più appliance e di backhaul.

Con un SGW basato sul cloud, le organizzazioni possono trarre vantaggio da:

Riduzione della complessità della sicurezza: come servizio nel cloud, questi SGW eliminano la necessità di distribuire dispositivi hardware o virtuali, nonché di configurare, gestire e sostituire/aggiornare l'hardware ogni tre anni.

Riduzione al minimo dei colli di bottiglia delle performance: un SWG basato su Internet elimina la necessità di aggiungere ulteriori dispositivi per far fronte all'aumento dei carichi di traffico web e all'incremento dei livelli di traffico crittografato. I clienti possono semplicemente aggiungere servizi aggiuntivi in base alle necessità con un impatto minimo sulle performance.

Riduzione di un costoso backhaul/hairpinning del traffico: gli SWG basati sul cloud applicano la sicurezza al traffico web senza backhaul del traffico per consentire la connessione diretta a Internet, riducendo così i costi di rete per il Multi-Protocol Label Switching (MPLS).

Migliore efficienza del team di sicurezza: poiché gli SWG basati sul cloud non richiedono la manutenzione continua di hardware o software, le scarse risorse per la sicurezza hanno più tempo per concentrarsi su altre misure di sicurezza proattive.

Policy per la sicurezza coerenti: le organizzazioni possono utilizzare policy gestite centralmente ma distribuite a livello globale, per tutti gli utenti che si connettono da qualsiasi dispositivo. Anche se l'organizzazione ha policy diverse per regioni diverse, può utilizzare la stessa interfaccia utente per gestirle tutte.

Requisiti chiave di un SWG (Secure Web Gateway)

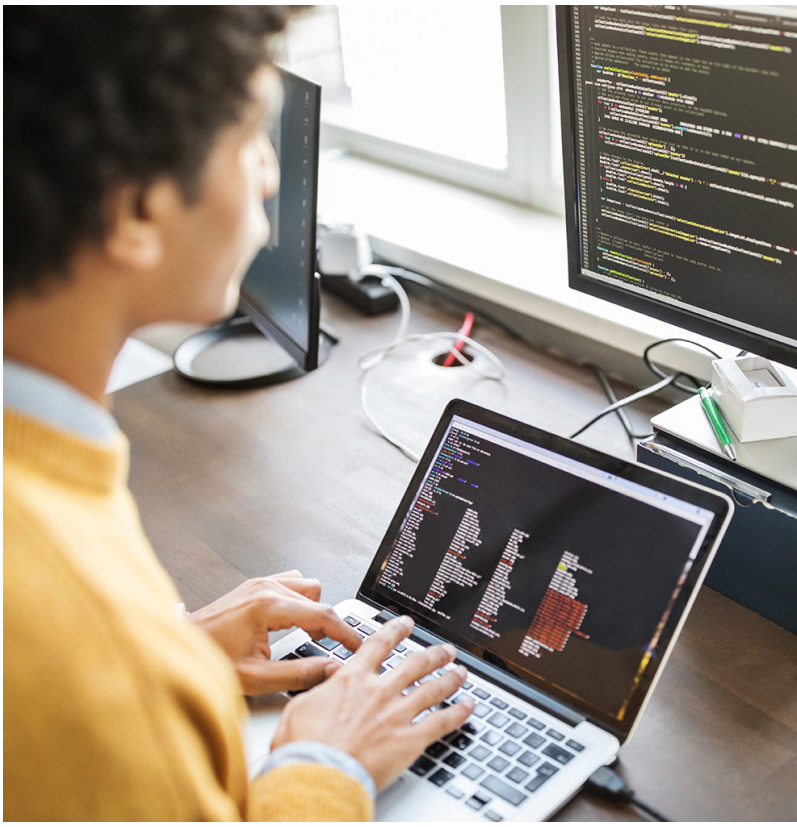
Quando si sceglie un SWG basato sul cloud, è importante comprendere che la sicurezza è il requisito fondamentale. Molti SWG legacy includono funzionalità che risolvono problemi non più esistenti. Ad esempio, includono il controllo della larghezza di banda, una funzione progettata per un periodo in cui la larghezza di banda era costosa. Oppure impediscono ai dipendenti di utilizzare YouTube o Facebook durante l'orario di lavoro. Oggi, queste funzionalità non sono più necessarie, perché la larghezza di banda è abbondante e gli utenti che utilizzano i dispositivi mobili sono talmente tanti che le organizzazioni non si preoccupano più di bloccare questi servizi sui dispositivi aziendali.

Le organizzazioni oggi necessitano di un SWG basato sul cloud progettato specificamente per gestire i moderni problemi di sicurezza. In particolare, la soluzione dovrebbe seguire una strategia di difesa approfondita che utilizzi più misure di sicurezza per fornire il massimo livello di protezione. Un tale approccio dovrebbe includere tutti gli aspetti della cybersicurezza e fornire misure di sicurezza ridondanti. In questo modo, se una linea di difesa viene compromessa, sono disponibili ulteriori livelli di difesa per impedire agli attacchi di sfruttare le vulnerabilità. Questo approccio a più livelli garantisce di bloccare nella fase iniziale e più velocemente minacce come malware, ransomware e phishing prima che il dispositivo dell'utente venga compromesso.

Un SWG che implementa una strategia di difesa approfondita dovrebbe offrire le seguenti funzionalità di sicurezza:

Valutazione di tutte le richieste DNS e URL

Una soluzione SWG basata sul cloud dovrebbe valutare tutte le richieste URL e DNS in base all'intelligence sulle minacce in tempo reale e



bloccare le richieste dannose nelle prime fasi della kill chain. Se la soluzione SWG può bloccare le minacce prima che venga stabilita una connessione in uscita, la risorsa web non deve aprire o ispezionare alcun contenuto restituito. Questa efficienza evita un processo a elevata intensità di elaborazione e riduce la quantità di traffico che l'SWG deve analizzare nella fase di payload. Il risultato? Migliori performance complessive dell'SWG.

L'intelligence sulle minacce dovrebbe proteggere da malware, ransomware, phishing ed esfiltrazione di dati basata su DNS a bassa velocità effettiva. Dovrebbe anche essere appositamente progettata per offrire una protezione che sia effettiva, pertinente e fornisca bassi tassi di falsi positivi.

Molteplici tecniche di analisi dei payload

Poiché tutte le minacce sono diverse e quindi nessuna tecnica o approccio di rilevamento singolo può affrontare tutti i tipi di malware, la soluzione SWG dovrebbe includere più motori di analisi del malware. Questi motori dovrebbero analizzare i payload HTTP e HTTPS sia online che offline utilizzando una varietà di tecniche di identificazione, tra cui quelle con e senza firma, apprendimento automatico e sandbox. Una simile analisi è in grado di fornire una protezione zero-day completa contro file potenzialmente dannosi come file eseguibili e file di documenti.

Rilevamento degli attacchi di phishing zero-day

I dipendenti remoti continuano a rilevare un aumento degli attacchi di phishing dall'inizio dell'epidemia di COVID-19. Gli utenti malintenzionati lanciano questi attacchi tramite e-mail, social media e applicazioni di messaggistica istantanea, nonché tramite la condivisione di file online e canali di collaborazione, per rubare le credenziali aziendali che consentono loro di accedere alla rete aziendale. Da lì, gli autori di attacchi possono spostarsi lateralmente per trovare ed esfiltrare dati e proprietà intellettuale o avviare campagne di ransomware.

Per identificare e bloccare l'accesso a una pagina di phishing, la maggior parte dei fornitori di servizi di sicurezza effettua le seguenti operazioni:

1. **Osserva il traffico insolito che colpisce un dominio**
2. **Analizza tale dominio**
3. **Determina se si tratta di un dominio di phishing**
4. **Lo aggiunge alla blocklist**
5. **Invia l'aggiornamento della blocklist ai clienti**

Questo processo può richiedere ore. E, peggio ancora, i cybercriminali di oggi utilizzano kit di phishing per creare e lanciare facilmente attacchi di breve durata, rendendo il rilevamento ancora più difficile. Quando viene individuato il dominio o l'URL di phishing, l'attacco è terminato. Infatti, più sofisticato e mirato è l'attacco di phishing, più breve sarà la sua durata.

Tuttavia, sebbene queste campagne possano terminare rapidamente, un motore di rilevamento del phishing zero-day avanzato può identificarle e bloccarle. Gli elementi ricorrenti di questi attacchi basati su kit possono essere osservati nel codice delle pagine di phishing. Utilizzando queste informazioni, è possibile identificare le "impronte digitali" per queste pagine che consentono un'identificazione accurata.

Una soluzione SWG dovrebbe includere un motore di rilevamento del phishing zero-day in grado di analizzare le pagine web richieste e di confrontarle con le "impronte digitali" di pagine di phishing visualizzate in precedenza.

Ispezione del traffico crittografato

Internet è un canale intrinsecamente non sicuro per il trasferimento dei dati. Di conseguenza, la crittografia del traffico web è ormai onnipresente per impedire agli aggressori di intercettare, commettere falsificazioni o manomettere il traffico. Transport Layer Security (TLS) è lo standard di crittografia più utilizzato per fornire una navigazione web sicura. TLS crea un tunnel sicuro tra due endpoint, come un browser client e un server web.

> **La percentuale di traffico web crittografato su Internet è aumentata costantemente, da circa il 50% nel 2014 all'80%-90% di oggi. La maggior parte (96%) dei principali 100 siti al mondo utilizza HTTPS per impostazione predefinita.**
>
> - Google Transparency Report, 2020

Ma non tutto il traffico HTTPS è legittimo. Gli autori di attacchi e di malware utilizzano la crittografia anche per nascondere le proprie attività, impedire agli utenti di accedere ai file (tramite ransomware) e proteggere le comunicazioni di rete dannose. Uno studio recente ha rilevato che quasi un quarto dei malware che ha effettuato una connessione Internet ha utilizzato TLS per comunicare.[6]

Per ispezionare e controllare in modo proattivo il traffico web HTTPS, è necessario cercare all'interno del tunnel protetto ed esaminare il traffico crittografato, utilizzando un server proxy (intermediario affidabile). Il server proxy dovrebbe decrittografare il traffico HTTPS in testo normale, analizzarlo, crittografarlo nuovamente e quindi creare un'altra connessione sicura con una tecnica chiamata Machine-In-The-Middle (MITM). La tecnica MITM ispeziona gli URL richiesti per determinare se sono sicuri o dannosi, fornire visibilità sul traffico crittografato tramite TLS e proteggere l'azienda dalle minacce mantenendo la riservatezza e l'integrità del traffico verso i siti web di origine.

Le ispezioni MITM richiedono una notevole capacità di elaborazione. Di conseguenza, la navigazione sul web può rallentare a causa della latenza. L'SWG dovrebbe offrire servizi che migliorano le performance delle applicazioni. Dovrebbe includere una rete distribuita a livello globale di server e software intelligenti situati vicino agli utenti e ai data center di tutto il mondo per consentire ottimizzazioni web che migliorano le performance e la disponibilità delle applicazioni.

Inoltre, la tecnica MITM verifica che il fornitore dell'SWG sul cloud conservi un elenco centralizzato di domini e URL che non funzionano correttamente e devono essere ignorati. Infine, l'SWG sul cloud dovrebbe essere in grado di aggirare l'ispezione MITM per tipi specifici di contenuti web sensibili, come i servizi finanziari e l'assistenza sanitaria.

Prevenzione della perdita di dati integrata

Prevenire in modo proattivo la perdita di informazioni di identificazione personale (PII) e altri dati aziendali riservati è fondamentale data la potenzialità di perdite finanziarie o di reputazione. L'SWG sul cloud dovrebbe includere la prevenzione della perdita di dati integrata che sia facile da configurare e veloce da implementare. I dizionari aggiornati di frequente dovrebbero includere le normative sulla privacy e sulla protezione dei dati, come PII, PCI - DSS e HIPAA, mentre le organizzazioni dovrebbero essere in grado di creare facilmente dizionari personalizzati.

Identificazione e gestione di applicazioni IT nascoste

Gli utenti hanno a disposizione centinaia di migliaia di applicazioni da scaricare, installare e utilizzare sui dispositivi gestiti, a insaputa del team di sicurezza aziendale. Tuttavia, l'uso di applicazioni non autorizzate può espandere in modo significativo la superficie di attacco dell'organizzazione e aumentare il suo profilo di rischio.

> **Un'azienda media utilizza oltre 1.295 app e servizi cloud. Più del 95% di questi non sono gestiti, senza diritti di amministrazione IT.**
>
> - Cybersecurity Insiders,
> Cloud Security Report, 2019

Un SWG sul cloud dovrebbe essere in grado di identificare le applicazioni utilizzate, rilevare il numero di utenti che hanno installato applicazioni specifiche e individuare le applicazioni che possono rappresentare un rischio per la sicurezza potenzialmente grave. Una volta identificata, la soluzione dovrebbe essere in grado di bloccare l'intera applicazione o specifiche operazioni dell'applicazione (ad esempio, consentendo i caricamenti ma non i download).

Protezione ovunque per qualsiasi dispositivo

Negli ultimi dieci anni si è osservata una significativa tendenza al rialzo della flessibilità dello stile di lavoro. Gli utenti ormai lavorano ovunque, su qualsiasi dispositivo. Inoltre, in conseguenza al lavoro da casa durante la pandemia, il 59% delle attività informatiche degli utenti finali per le aziende si sta spostando su dispositivi mobili, aumentando o sostituendo PC e laptop. Si prevede che questo cambiamento continui anche dopo il ritorno al lavoro in ufficio.[7]

Il passaggio ai dispositivi mobili e un maggiore utilizzo delle reti Wi-Fi possono creare vulnerabilità nel sistema di sicurezza di qualsiasi organizzazione. Le aziende devono essere in grado di applicare un livello di sicurezza uniforme e universale, senza compromettere le performance dei dispositivi.

Un SWG sul cloud dovrebbe identificare, bloccare e mitigare in modo proattivo minacce mirate come malware, ransomware, phishing, esfiltrazione di dati DNS e attacchi zero-day su qualsiasi dispositivo (iOS, Android OS, Chrome OS), su tutte le reti utilizzate dagli utenti. La soluzione gateway dovrebbe fornire controlli onnipresenti e una gestione semplificata, a livello globale, mantenendo al contempo performance ottimali dei dispositivi.

Accesso sicuro a tutte le applicazioni aziendali

Un SWG sul cloud protegge utenti e dispositivi dai malware quando accedono alla rete Internet pubblica. Tuttavia, costituisce solo una tessera del mosaico della sicurezza per un'azienda.

Per creare un approccio alla sicurezza aziendale olistico, le organizzazioni devono anche proteggere dagli utenti malintenzionati le applicazioni gestite e di proprietà dell'azienda, indipendentemente dal fatto che risiedano nel data center aziendale o in un ambiente IaaS. Gli strumenti per la sicurezza delle reti tradizionali proteggono il perimetro della rete, ma se gli autori di attacchi violano il perimetro (ad esempio, rubando le credenziali dell'utente o installando malware su un dispositivo dell'utente) possono spostarsi liberamente all'interno della rete.

Le organizzazioni necessitano di un SWG sul cloud che offra anche una tecnologia ZTNA (Zero Trust Network Access) per proteggere le applicazioni aziendali. ZTNA è un componente fondamentale dell'adozione della sicurezza Zero Trust, che garantisce agli utenti l'accesso solo ad applicazioni specifiche (non a intere reti o segmenti) in base all'identità dell'utente. La soluzione protegge l'identità degli utenti tramite l'integrazione con tecnologie di gestione delle identità e degli accessi, MFA (Multi-Factor Authentication) e Single Sign-On. Utilizzando uno strumento ZTNA, le organizzazioni eliminano la complessità della gestione sicura dei dispositivi o del mantenimento di una di rete WAN complessa o della connettività di rete privata virtuale. Una volta autenticati correttamente, agli utenti viene concesso l'accesso solo alle applicazioni e ai dati necessari, riducendo a zero la superficie di attacco

delle applicazioni e minimizzando il rischio di movimento laterale. Quando le organizzazioni valutano un SWG sul cloud, dovrebbero prendere in considerazione le funzionalità del servizio ZTNA del fornitore. Il servizio può fornire l'accesso alle moderne applicazioni web e a quelle non web legacy? È possibile integrare il servizio con il servizio del provider di identità esistente dell'organizzazione? Supporta l'MFA?

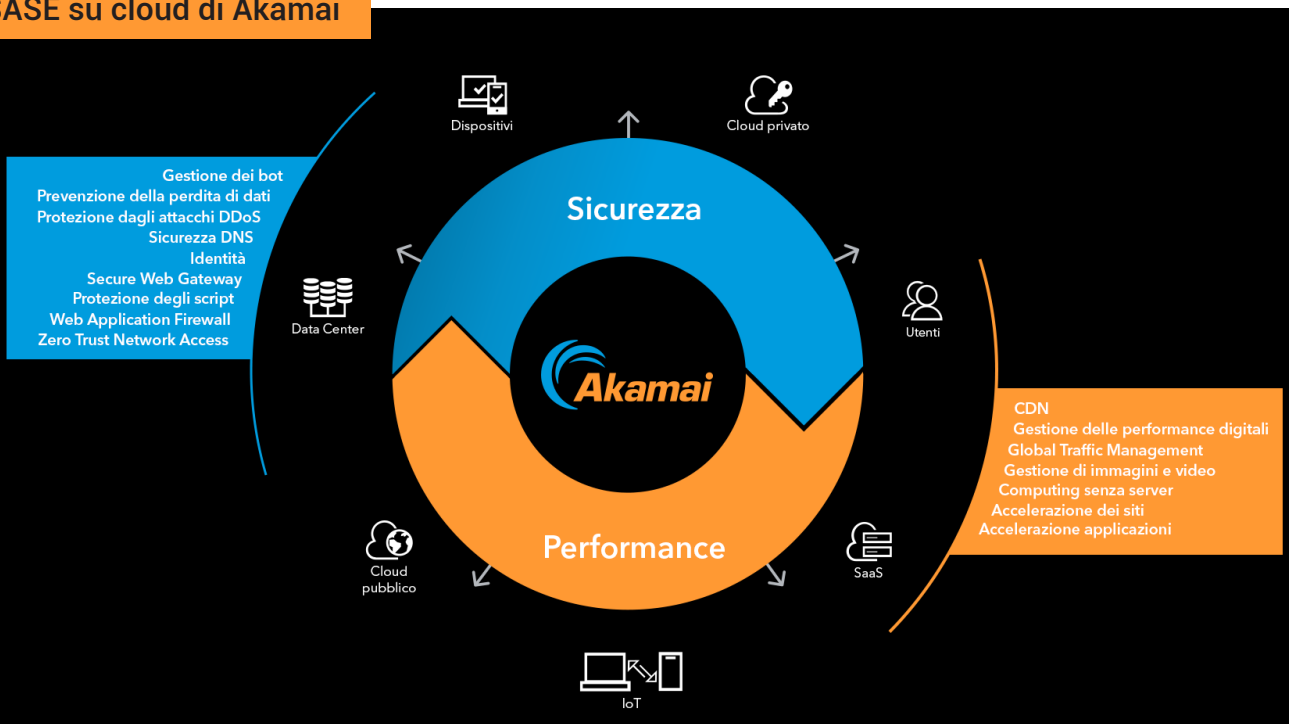
Il Secure Web Gateway dovrebbe integrarsi e funzionare in combinazione con il servizio ZTNA in modo tale che, se si rileva che un dispositivo è compromesso, gli sarà impedito l'accesso a qualsiasi applicazione aziendale. I registri di un SWG possono rafforzare altri segnali di minaccia per fornire un'immagine più accurata del livello di sicurezza di un dispositivo. Ad esempio, se il dispositivo effettua una chiamata ai server di comando e controllo, la soluzione dovrebbe utilizzare tale chiamata come un segnale per limitare l'accesso all'applicazione fino a quando il dispositivo non viene ripristinato.

Aggiungendo l'SWG e le funzionalità ZTNA, le organizzazioni compiono un passo avanti verso l'adozione di un framework SASE (Secure Access Service Edge). Un sistema SASE allontana il fulcro della strategia di sicurezza di un'organizzazione dalle architetture di sicurezza incentrate sul data center e sulle appliance hardware che non sono più adatte all'ambiente di lavoro e aziendale altamente distribuito di oggi. Invece, una soluzione SASE fornisce un accesso basato su policy in base all'identità dell'utente e/o del dispositivo. Offre anche una vasta gamma di controlli di sicurezza aggiuntivi, tra cui firewall per applicazioni web, sicurezza API, gestione dei bot e protezione da attacchi DoS (Denial-of-Service) distribuiti per applicazioni web.

> **Il sistema ZTNA migliora la flessibilità, l'agilità e la scalabilità dell'accesso alle applicazioni, consentendo alle aziende digitali di prosperare senza esporre le applicazioni interne direttamente a Internet e riducendo così il rischio di subire attacchi.**
>
> Gartner, Market Guide for Zero Trust Network Access, Steve Riley, Neil MacDonald, Lawrence Orans, 8 giugno 2020

Inoltre, i controlli di sicurezza vengono forniti sulla piattaforma SASE a un hop Internet di distanza dall'utente per fornire un accesso a bassa latenza a utenti, dispositivi e servizi cloud ovunque.

SASE su cloud di Akamai



Performance ottimali

Sebbene la sicurezza sia fondamentale, non può compromettere l'user experience con performance lente. Oltre a fornire un approccio approfondito alla difesa, un SWG basato sul cloud dovrebbe fornire i servizi riportati sopra senza introdurre latenza.

Per evitare la latenza, l'SWG sul cloud deve essere distribuito a livello globale con PoP (Points of Presence) vicini alla posizione di connessione di tutti gli utenti. Dopotutto, non ha molto senso sostituire un tipo di backhaul con un altro.

La piattaforma cloud dovrebbe anche consentire una rapida scalabilità per evitare di influire sull'user experience dell'utente finale, anche in condizioni di picco. Questa funzionalità è particolarmente importante quando si tratta di ispezionare il traffico HTTPS, che sta crescendo in modo esponenziale e arriverà a comprendere quasi il 100% dell'intero traffico web. L'ispezione del traffico crittografato con un impatto minimo sugli utenti finali è fondamentale, poiché la stragrande maggioranza dei malware viene attualmente distribuita tramite HTTPS. La piattaforma deve anche offrire uno SLA con disponibilità del 100%.

> **Attualmente, gli utenti di Office 365 rappresentano oltre la metà dell'81% delle organizzazioni totali che sono passate ai servizi cloud.[8]**

Integrazione di Office 365: garantire un livello elevato di sicurezza e performance per Microsoft Office 365 è particolarmente importante, poiché molte organizzazioni utilizzano questo servizio come suite di produttività essenziale. Una delle sfide dell'implementazione di un SWG sul cloud è rappresentata dal fatto che O365, come molte altre comuni applicazioni SaaS, funziona male quando gli utenti accedono alle sue applicazioni tramite un proxy di inoltro che esegue l'ispezione MITM TLS.

Per evitare di compromettere le performance di O365, è fondamentale che l'SWG sul cloud venga distribuito tramite una piattaforma edge globale in grado di:

- Utilizzare l'IP di origine della richiesta per indirizzare la richiesta al data center di Microsoft O365 geograficamente più vicino, anziché a soluzioni DNS backhaul che indirizzerebbero la richiesta al data center più vicino al resolver DNS aziendale; ad esempio, un utente che accede a O365 da Singapore e viene indirizzato a un server O365 a New York avrebbe un'user experience pessima

- Assicurare che le posizioni del Secure Web Gateway siano situate vicino ai data center di Microsoft O365 e che, idealmente, questi server e data center siano interconnessi

- Fornire un'impostazione di ottimizzazione del traffico di O365 con un clic che utilizza un elenco di domini O365 e indirizzi IP pubblicati e aggiornati da Microsoft; le richieste a questi domini devono essere inviate direttamente ai server O365 in linea con i consigli di Microsoft, il che consente di risparmiare tempo e fatica eliminando la necessità di aggiornare manualmente i firewall e altri prodotti di sicurezza quando Microsoft aggiunge nuovi domini o indirizzi IP

Spostamento della sicurezza sull'edge

I dipendenti remoti in rapida crescita sono sempre più vulnerabili agli attacchi informatici che, a loro volta, stanno diventando più frequenti e gravi. Le migliori soluzioni SWG (Secure Web Gateway) basate sul cloud si concentreranno esclusivamente sulla soddisfazione di queste moderne esigenze di sicurezza offrendo comprovate funzionalità di difesa approfondite. Supporteranno inoltre i moderni modelli di sicurezza aziendale come Zero Trust e SASE, garantendo l'accesso a Internet a tutti gli utenti, indipendentemente da dove si trovino.

Un SWG sul cloud completo dovrebbe valutare tutte le richieste DNS e URL, fornire più tecniche di analisi del payload, far fronte al phishing zero-day, ispezionare il traffico crittografato, integrare la prevenzione della perdita di dati, identificare e gestire le applicazioni IT nascoste e fornire protezione ovunque per qualsiasi dispositivo, offrendo al contempo un elevato livello di performance e integrandosi con le tecnologie di sicurezza delle applicazioni aziendali. Con una tale soluzione, le organizzazioni possono ridurre la complessità della sicurezza, eliminare costosi backhaul, migliorare l'efficienza del team addetto alla sicurezza e supportare policy di sicurezza coerenti.

Scoprite di più su Secure Internet Access, la soluzione SWG (Secure Web Gateway) basata sul cloud di Akamai, e usufruite di una prova gratuita all'indirizzo akamai.com.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services