White paper

Perché i responsabili IT dovrebbero prendere in considerazione una strategia ZTNA

Favorire il business digitale proteggendo i dati

Sebbene la tecnologia sia da tempo considerata il motore alla base del progresso aziendale, oggi sono tutti d'accordo nel considerarla essenziale per raggiungere nuovi livelli di efficienza e opportunità di profitto. Il ruolo dei responsabili IT si è evoluto in modo analogo, e CISO, CIO e CTO sono entrati a far parte dei gruppi dirigenziali per guidare e concentrarsi su nuove iniziative nell'ambito della tecnologia.

I principali fattori che hanno favorito questo cambiamento sono stati l'esplosione dell'adozione del cloud pubblico aziendale, come Azure, AWS e Google Cloud, e l'uso diffuso dei dispositivi mobili personali (BYOD) per il lavoro. Le imprese stanno sfruttando queste tecnologie per ottimizzare i processi aziendali e fornire prodotti e servizi più rapidamente e a un costo complessivamente inferiore.

Ma che dire del rischio che presentano?

A causa del passaggio al cloud e della sempre maggiore mobilità degli utenti, il perimetro di sicurezza tradizionale che una volta proteggeva gli utenti e i servizi che si trovavano sulla rete aziendale è scomparso.

Per questo motivo, quando si richiede lo stanziamento di somme per le iniziative IT volte a supportare il cloud e la mobilità, è importante che il consiglio di amministrazione sia a conoscenza dei rischi e del loro potenziale impatto sui ricavi dell'azienda. È necessario fornire informazioni chiare sul costo potenziale di una violazione dei dati, di tempi di inattività dell'infrastruttura critica e della perdita reputazionale del marchio. I responsabili IT devono quindi affrontare queste tematiche dal punto di vista del valore aziendale, in un modo che sia comprensibile per i dirigenti.

L'IT deve innanzitutto essere consapevole dei rischi per l'azienda e della capacità di quest'ultima di contrastarli. Ad esempio, le applicazioni fondamentali, ovvero quelle considerate critiche per l'azienda, potrebbero essere conformi ai requisiti SOC1 o ISO 27001, e richiedere ulteriori livelli di sicurezza. Inoltre, alcuni Paesi, come la Cina, devono essere isolati da altri Paesi. Con un'infrastruttura legacy che necessita di una valutazione continua per l'applicazione delle patch, una configurazione firewall mancante potrebbe causare gravi problemi all'azienda.

Le sfide da superare per i responsabili della tecnologia

Per supportare le iniziative aziendali principali e colmare il divario tra le esigenze dell'impresa e le funzionalità IT, i responsabili IT devono scegliere una tecnologia che li aiuti a superare gli ostacoli e che consenta loro di:

1. Semplificare il lavoro e ridurre al minimo lo stress per i dipendenti
2. Offrire un'esperienza utente di livello superiore a dipendenti e terze parti
3. Ridurre i rischi per la produttività, la proprietà intellettuale e la reputazione dell'azienda
4. Offrire agilità e adattabilità per favorire l'evoluzione aziendale continua
5. Accelerare la trasformazione digitale attraverso l'adozione del cloud pubblico

Identificare le tecnologie in grado di raggiungere questi obiettivi è un compito arduo, perché i risultati che si desiderano da una soluzione potrebbero ostacolarne un'altra, aggiungendo complessità. La decisione di adottare servizi cloud e tecnologie mobili, ad esempio, consente di semplificare l'esperienza utente, ma può aumentare il rischio di attacchi informatici. I responsabili IT devono trovare un equilibrio tra la rapida adozione di nuove tecnologie e la sicurezza dei dati sensibili. Scegliere la tecnologia giusta al momento giusto è quindi fondamentale.

Il valore dello ZTNA per il business

Gartner consiglia ai responsabili IT di adottare l'approccio ZTNA nell'ambito di una strategia SSE (Security Service Edge), per fornire una connettività flessibile e sicura alla forza lavoro ibrida.
I servizi ZTNA offrono un accesso sicuro alle applicazioni aziendali private per gli utenti che lavorano in remoto e dall'ufficio, senza la necessità di utilizzare le tecnologie VPN tradizionali.

I servizi ZTNA creano un confine ad accesso logico basato sull'identità e sul contesto attorno a un'applicazione o a una serie di applicazioni.
Le applicazioni rimangono nascoste, e l'accesso viene limitato a una serie di entità definite tramite un broker di negoziazione dell'attendibilità.
Quest'ultimo verifica l'identità dell'utente, il contesto e l'adesione alle policy dei partecipanti interessati prima di consentire la connessione.
In questo modo, le applicazioni vengono rese invisibili a Internet e si riduce in modo significativo la superficie di attacco.

Gartner

Entro il 2025, almeno il 70% delle nuove distribuzioni di accesso remoto avverrà prevalentemente tramite servizi ZTNA, e non attraverso servizi VPN, una percentuale che era inferiore al 10% alla fine del 2021

In precedenza, abbiamo elencato i cinque aspetti principali che i responsabili IT devono prendere in considerazione quando adottano nuove tecnologie. Vediamo ora come lo ZTNA può favorire il raggiungimento di questi obiettivi:

1. Migliore produttività:

Quest'anno, 3 dipendenti su 4 che lavorano full-time dalle sedi aziendali **hanno intenzione di licenziarsi,** aggiungendosi così alle decine di milioni di persone che hanno già cambiato lavoro in seguito all'ondata di dimissioni causata dalla pandemia. In questa situazione, i datori di lavoro stanno ripensando il modo in cui attraggono e trattengono i professionisti. I responsabili IT possono contribuire a motivare i dipendenti a restare grazie alla tecnologia e gettare al contempo le basi per il lavoro del futuro.
La facilità d'uso dello ZTNA offre vantaggi significativi agli utenti, in quanto elimina il problema dell'utilizzo di un client VPN ogni volta che l'utente si collega alla rete, mantiene alta la produttività e riduce al minimo la frustrazione. La semplicità dello ZTNA, che è distribuito sul cloud ed è solo software, ne facilita la configurazione e la distribuzione, e permette all'IT di mettere in sicurezza le applicazioni cloud, anche sui dispositivi mobili, massimizzando al contempo la produttività del personale IT e dell'intera organizzazione.

2. Fornire un'esperienza utente di livello superiore:

Oggi gli utenti lavorano da qualsiasi luogo: in ufficio, da casa e persino mentre sono in viaggio. Questi utenti sono spesso costituiti da dipendenti e collaboratori terzi, ed entrambe queste categorie si aspettano un accesso senza ostacoli alle applicazioni, indipendentemente dal dispositivo, dalla posizione o dalla rete che utilizzano. Lo ZTNA assicura che ogni utente goda di un'esperienza rapida e totalmente fluida. Inoltre, elimina la necessità di una VPN e di scomodi login, favorendo il lavoro di utenti terzi su tutti i tipi di dispositivi, senza la necessità di un agente sull'endpoint.

Inoltre, lo ZTNA sfrutta l'accesso alle applicazioni private in base alle policy e aumenta la produttività, perché gli utenti possono collegarsi alle applicazioni da qualsiasi dispositivo, indipendentemente dalla loro posizione.

3. Ridurre il rischio:

La sicurezza rimane la più grande preoccupazione nell'ambito dell'adozione del cloud e del lavoro mobile, in quanto una gestione non attenta può incrementare la probabilità di un attacco alle app e all'infrastruttura critica per l'impresa. Le tecnologie tradizionali incentrate sulla rete, come VPN e firewall, concedono l'attendibilità in modo eccessivo, e dovrebbero per questo essere evitate. Queste soluzioni collocano gli utenti in remoto direttamente sulla rete, e richiedono quindi che i server VPN ascoltino le chiamate in entrata da Internet. Questo è il motivo per cui le VPN sono diventate un cavallo di Troia per i ransomware; infatti, sia da remoto che in locale, in questo modo l'utente può muoversi lateralmente su tutta la rete. Questo è vero sia per i dipendenti che per gli utenti terzi, che potrebbero adottare pratiche di sicurezza più deboli. I servizi ZTNA utilizzano policy basate sullo zero trust per fornire la connettività solo agli utenti autorizzati (in base all'identità e al profilo del dispositivo) e solo a specifiche app private situate su cloud pubblico, privato o sul data center.
La recente evoluzione dello ZTNA, che è passato dall'offrire la connettività a fornire una sicurezza completamente integrata per proteggere le applicazioni dalle minacce interne e dagli aggressori avanzati, aiuta le organizzazioni a migliorare il proprio approccio complessivo alla sicurezza.

4. Agilità e scalabilità fornite sul cloud:

Oggi, la quantità di dipendenti, dispositivi degli utenti, applicazioni e traffico continua a crescere. I servizi ZTNA forniti sul cloud sono ospitati dal provider, quindi l'adattabilità delle prestazioni non rappresenta più un problema per l'IT.
Quando la domanda aumenta, il servizio ZTNA gestisce automaticamente il carico aggiuntivo. Non è necessario distribuire firewall hardware o virtuali aggiuntivi che rallentano l'adozione del cloud pubblico. Un livello maggiore di adattabilità e scalabilità è fondamentale per il successo di un responsabile IT, e lo ZTNA è in grado di fornirlo.

5. Accelerare la trasformazione digitale:

Oggi il cloud e la mobilità costituiscono una priorità per la maggior parte dei team aziendali, ma con le soluzioni sbagliate possono essere necessari mesi o addirittura anni per implementare il cloud in modo sicuro su una base di utenti globale. Ciò è dovuto in parte alla complessità dell'utilizzo della tecnologia di rete e di sicurezza tradizionale per fornire l'accesso alle app cloud dai dispositivi utente non gestiti.
Lo ZTNA utilizza il software per ridurre la complessità, riducendo così i tempi di implementazione da mesi o addirittura anni ad alcune ore. Grazie allo ZTNA, le organizzazioni possono sfruttare più rapidamente i vantaggi del cloud e della mobilità.

> “Grazie alle modifiche che abbiamo apportato al nostro percorso verso il cloud, sono certo che saremo in una posizione solida che ci consentirà di gestire tutto ciò che ci riserverà il futuro. Questa esperienza avrà un impatto duraturo e cambierà definitivamente gli approcci legacy. Stiamo aprendo gli occhi a nuovi modi di lavorare, e questa evoluzione dimostra l'impatto della tecnologia, la resilienza e la creatività della nostra forza lavoro”.
>
> — **Alex Philips,** CIO, National Oilwell & Varco

Scopri di più su ZTNA

I servizi ZTNA sono uno strumento prezioso per i responsabili IT dell'azienda. Zscaler ha sviluppato un servizio ZTNA chiamato Zscaler Private Access (ZPA). Questo servizio sfrutta il nostro cloud globale per fornire un accesso fluido e sicuro alle applicazioni interne; esattamente ciò di cui l'IT ha bisogno per passare dall'essere considerato solo un costo per l'azienda al diventare un valido alleato della dirigenza.

Leggi la storia di Paychex raccontata da Carlos Cong, Senior Manager della funzione Enterprise Technology Services, sulla semplificazione e l'accelerazione dell'integrazioni IT nell'ambito di fusioni e acquisizioni grazie allo ZTNA.

Guarda la storia di CMA-CGN

Consenti al tuo team di approfittare di un periodo di prova gratuito di 7 giorni della soluzione ZTNA di Zscaler.

Inizia una prova di 7 giorni dello ZTNA

Hai altre domande? Contatta direttamente i nostri esperti di ZTNA all'indirizzo **sales@zscaler.com.**

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security in linea del mondo. Scopri di più su **zscaler.it** o seguici su Twitter su **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it