Utilizzare lo ZTNA per offrire l'esperienza che gli utenti desiderano

Come consentire alla forza lavoro di accedere alle app da qualsiasi dispositivo, da qualsiasi luogo e in qualsiasi momento.

zscaler™

"Non vogliamo che le persone debbano preoccuparsi di come possono accedere alle proprie app, desideriamo supportare quella capacità il più rapidamente possibile, riducendo al minimo gli ostacoli".

- Mike Towers, CSO presso Takeda

La base di utenti si è evoluta

Nel 2020, la forza lavoro non è più confinata in ufficio. Opera da casa, dagli hotel e dagli aeroporti. I dispositivi impiegati non sono più dispositivi BlackBerry gestiti dal team endpoint. Si tratta di smartphone, tablet e laptop BYOD personali, utilizzati sia per il tempo libero che per il lavoro.

Ci si trova pertanto a essere responsabili non solo di proteggere i dipendenti, ma anche terze parti che non sono stipendiate dall'azienda. Tutti questi utenti hanno bisogno di un accesso identico alle app private indipendentemente dai dispositivi, dalle posizioni e dai tipi di applicazione. Fornire l'accesso da tali dispositivi, senza compromettere la sicurezza, un tempo era impossibile. Ma oggi non è più così.

Uno sguardo al portafoglio di utenti

Con una forza lavoro diversificata, distribuita a livello globale, l'accesso sicuro alle applicazioni private è diventato una sfida per i team IT. Sebbene la forza lavoro possa apparire diversa da quella di 15 anni fa, c'è comunque un elemento in comune: tutti gli utenti hanno bisogno di un accesso rapido e affidabile alle applicazioni private per consentire all'azienda di operare in tutta semplicità. La forza lavoro moderna può essere all'incirca così:

Il viaggiatore

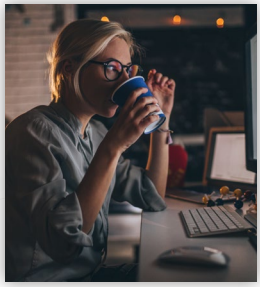
Sam Davis, VP del Dipartimento vendite

"Probabilmente trascorro in viaggio circa il 75% del mio tempo. Spesso mi trovo in un aeroporto, in un hotel o presso le sedi dei clienti e cerco di lavorare durante i periodi di attesa. Anche se il mio ambiente di lavoro può cambiare continuamente, ho comunque bisogno di accedere rapidamente alle nostre risorse aziendali, in modo da poter servire al meglio i clienti."

Chi è in sede

Danielle Allen, Dirigente della gestione finanziaria

"Opero dalla nostra sede centrale a San Jose, in California, e sono per la maggior parte del tempo una dipendente che lavora dall'ufficio. Ricevo ogni giorno richieste degli altri dipendenti in merito al propri pagamenti. Uso costantemente le nostre applicazioni finanziarie e ho bisogno di accedervi rapidamente in modo da poter rimanere al passo con le richieste".



L'appaltatore

Elaina thalin, Appaltatore per lo sviluppo Web

"Opero a contratto per l'azienda da circa 8 mesi. Anche se non sono una dipendente o non opero dall'ufficio, ho comunque bisogno di accedere ad alcune applicazioni private per portare a termine il mio lavoro. Se non riesco ad accedervi, non posso di fatto operare".

Chi lavora da casa

Justin miller, Dirigente marketing

"Vivo in Florida e, spesso, vengo influenzato dagli avvisi meteorologici, inclusi gli uragani. Durante quei periodi, ho bisogno di garantire la mia sicurezza e quella della mia famiglia, pur rispondendo alle mie responsabilità lavorative".

Indipendentemente dal tipo di utente o dal ruolo lavorativo ricoperto, la forza lavoro deve comunque essere in grado di accedere alle applicazioni private in modo rapido e sicuro, ovunque si trovi. L'IT deve essere potenziata con la tecnologia giusta, per poter rendere questo aspetto possibile e garantire che la sicurezza non sia in contrasto con la produttività degli utenti. Ecco perché la VPN non è la scelta ideale per la forza lavoro moderna.

Gli utenti meritano di più della VPN

Dato che la VPN è stata sviluppata oltre 30 anni fa, essa non è più adeguata all'uso che ne viene fatto dalla forza lavoro moderna, in quanto dispone di una struttura di sicurezza carente, che offre un'esperienza utente di scarso livello.

Elevata latenza, scalabilità limitata ed esperienza scadente
Le VPN sono state progettate per proteggere l'accesso alla rete. Ciò significa che tutto il traffico utente viene sottoposto al backhauling prima di tutto verso il datacenter, anche se le app ora vengono eseguite nel cloud pubblico. Questo fa sì che la rete ricada in un loop di rimbalzo dei dati, che a sua volta crea latenza per gli utenti. Inoltre, gli apparecchi VPN hanno limitazioni in termini di capacità utente e possono collassare se troppi utenti accedono contemporaneamente al server VPN.

Accessi ripetitivi e connessioni interrotte
Ogni volta che si verifica un cambiamento di rete o un'inattività, la connessione VPN si interrompe. Per la forza lavoro mobile di oggi, questo può verificarsi molto spesso, con conseguente frustrazione da parte dell'utente e perdite di tempo in termini di produttività.

Confusione su quando usare o meno la VPN.
Gli utenti potrebbero non sapere nemmeno quale sia la differenza tra le applicazioni pubbliche e private. Oggi, con le applicazioni che passano sul cloud, c'è ancora più confusione per l'utente, che si trova a non sapere quando, dove e come dovrebbe usare la VPN. Inutile dire che la VPN non è semplice o intuitiva per gli utenti.

Netflix non avrebbe funzionato se fosse stata costruita collegando migliaia di lettori DVD. Allo stesso modo, le soluzioni di accesso alle applicazioni private da qualsiasi luogo, in qualsiasi momento, devono essere create ad hoc. Devono essere sempre disponibili, altamente scalabili e incentrate sull'utente. Adattare gli apparecchi VPN nel data center, virtualizzandoli o inserendoli nel cloud, non risolverà le problematiche relative all'esperienza utente o alla sicurezza della rete create dal mondo mobile. **È necessario un nuovo approccio.**

"Entro il 2023, il 60% delle imprese dismetterà gradualmente la maggior parte delle reti private virtuali (VPN) di accesso remoto a favore dello ZTNA".

Gartner, Market Guide for Zero Trust Network Access
Steve Riley, Neil MacDonald, Lawrence Orans, aprile 2019

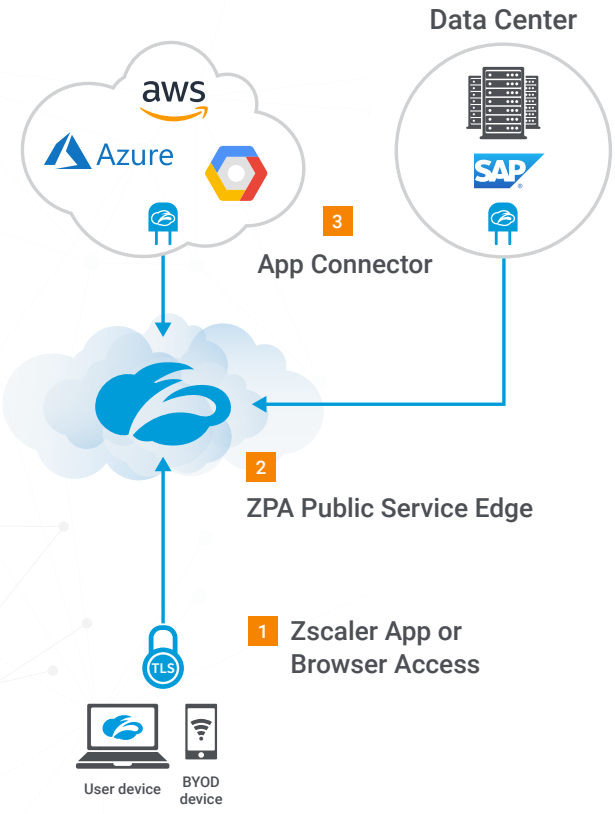
Garantire la produttività degli utenti grazie allo ZTNA

Che si tratti di accedere a SAP nel cloud pubblico, SSH, RDP, intranet personalizzata o a un'app del foglio di presenza basata sul Web, l'esperienza utente deve essere sempre senza soluzione di continuità. Questo è il motivo per cui Gartner consiglia alle organizzazioni di adottare tecnologie **ZTNA (Zero Trust Network Access, accesso alla rete zero trust)** in sostituzione delle VPN di accesso remoto.

Nella maggior parte dei casi, i servizi ZTNA sono ospitati sul cloud e impiegano delle policy per determinare quali utenti autorizzati hanno accesso a una specifica applicazione privata. Queste politiche prendono in considerazione l'identità dell'utente, del suo gruppo, la posizione del dispositivo e diversi altri criteri.

Poiché molti servizi ZTNA sono completamente erogati sul cloud, consentono agli utenti di connettersi a uno dei molti punti di presenza globali del servizio, che poi negozia la connessione sicura a un'applicazione privata. Ciò fornisce una disponibilità più ampia e una scalabilità decisamente maggiore rispetto a un dispositivo VPN. Gli utenti non vengono mai inseriti nella rete, pertanto il traffico non viene più reindirizzato verso un data center. Ciò significa che il servizio ZTNA consente un accesso fluido all'utente finale, permettendo al contempo di ridurre al minimo i rischi per l'azienda.

Architettura ZTNA (Zero trust network access)



1 App Zscaler o accesso al browser

- Reindirizza il traffico al provider IDP per l'autenticazione
- Client Connector instrada automaticamente il traffico al Service Edge pubblico
- L'accesso al browser elimina la necessità di client sul dispositivo quando si accede ad applicazioni basate sul Web

2 Service Edge pubblico ZPA

- Protegge la connessione da utente ad app
- Applica tutte le policy amministratore personalizzate

3 App Connector

- Si colloca di fronte alle applicazioni private nel cloud e/o al data center
- Risponde solo alle richieste da parte del Service Edge pubblico ZPA
- Nessuna connessione in entrata. Risponde solo con connessioni dall'interno verso l'esterno.



Come iniziare a offrire l'esperienza che gli utenti desiderano

Nel cercare di rendere gli utenti produttivi si dovrebbe prendere in considerazione un servizio ZTNA.

Scopri come Steve Day, EGM di Infrastruttura, cloud e luogo di lavoro presso la National Australia Bank, ha permesso ai suoi utenti di essere produttivi.

Guarda la Storia della National Australia Bank

Qual è il prossimo passo? Prova il nostro servizio ZTNA.

Inizia una prova di 7 giorni e scopri lo ZTNA

Informazioni su Zscaler

Zscaler consente alle organizzazioni leader nel mondo di trasformare in sicurezza le proprie reti e applicazioni tramite un'ottica mobile e cloud-first. I suoi servizi di punta, Zscaler Internet Access™ e Zscaler Private Access™, creano connessioni veloci e sicure tra utenti e applicazioni, indipendentemente dal dispositivo, dalla posizione o dalla rete. I servizi di Zscaler sono forniti al 100% sul cloud e offrono la semplicità, la sicurezza avanzata e l'esperienza utente migliorata che i dispositivi tradizionali o le soluzioni ibride non sono in grado di eguagliare. Utilizzata in oltre 185 Paesi, Zscaler gestisce una piattaforma cloud di sicurezza multitenant distribuita, che protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati. Scopri di più su **zscaler.com** o seguici su Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com