E-book

Vuoi proteggere la tua forza lavoro flessibile con lo ZTNA?

Ricerca queste 10 funzionalità indispensabili

Contenuti

Introduzione

Il mondo del lavoro sta cambiando. Le modalità e i luoghi in cui i dipendenti sono più produttivi sono diversi rispetto a qualche anno fa. Le aziende stanno adottando il lavoro flessibile e da remoto, e per farlo spostano un numero crescente di applicazioni critiche sul cloud, in modo da poter sfruttare appieno la flessibilità, la scalabilità e l'efficienza che offre.

Ma la trasformazione degli ecosistemi IT genera anche nuove sfide nell'ambito della sicurezza. L'adozione su larga scala del lavoro flessibile e da remoto, insieme all'incremento dell'utilizzo del cloud e all'aumento dell'accesso mobile, possono estendere la superficie di attacco, soprattutto se questi cambiamenti non sono accompagnati dall'abbandono delle soluzioni legacy (come VPN e firewall) e degli approcci più obsoleti. Oltre a estendere la superficie di attacco, questi elementi limitano la visibilità dei team di sicurezza, rendendo più difficile l'investigazione degli incidenti e la risoluzione dei problemi.

È necessario dunque adottare un nuovo modello in grado di soddisfare le attuali esigenze di sicurezza e connettività e di proteggere realmente gli ambienti tecnologici. Lo zero trust offre esattamente questo, e attualmente è in rapida adozione in tutti i settori e intutte le aree geografiche.

Un numero crescente di organizzazioni sceglie lo ZTNA (Zero Trust Network Access) per rafforzare il proprio profilo di sicurezza e poter supportare così il lavoro flessibile. Lo ZTNA fornisce un framework chiaro e bendefinito da seguire nel proprio percorso verso lozero trust. Secondo quanto riferito dalla società di analisi Gartner, il mercato dello ZTNA si sta espandendo a un ritmo incredibile, con una crescita annuale chesupera il 60%.

Le organizzazioni citano la sostituzione delle VPN come motivazione principale dell'implementazione dello ZTNA.

Cos'è lo ZTNA (Zero Trust Network Access)?

Lo ZTNA è un insieme di tecnologie e funzionalità che consentono agli utenti in remoto di accedere in modo sicuro alle applicazioni interne e/o private.

Lo ZTNA opera secondo un modello di attendibilità adattivo, in cui l'attendibilità, o trust, non è mai implicita, e l'accesso viene concesso solo a coloro che ne hanno realmente bisogno e in base a privilegi minimi, secondo quanto definito da policy granulari.

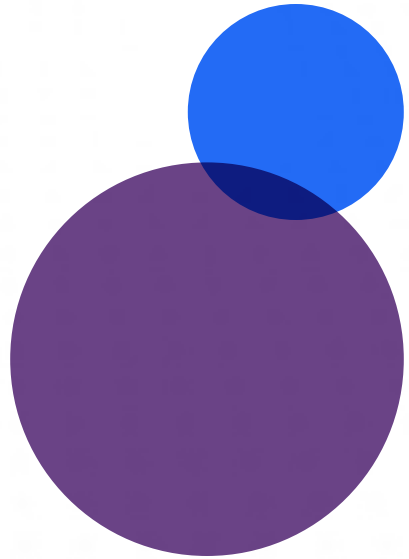
Un numero crescente di organizzazioni adotta applicazioni e infrastrutture distribuite sul cloud, e molte di esse cercano di unificare i servizi di sicurezza impiegando un'unica piattaforma distribuita sul cloud. Si tratta del Security Service Edge (SSE), che comprende il Secure Web Gateway (SWG), il CASB (Cloud Access Security Broker) e le funzionalità ZTNA. Gartner raccomanda ai responsabili della sicurezza e della gestione del rischio di avviare le proprie strategie di implementazione di un modello SSE partendo proprio dall'adozione dello ZTNA. Ecco perché lo ZTNA è spesso un primo passo fondamentale nel percorso verso la sicurezza fornita sul cloud.

Molte organizzazioni passano allo ZTNA per sostituire le infrastrutture VPN che non funzionano bene su larga scala o che espongono l'organizzazione a maggiori rischi di sicurezza, in quanto la loro stessa presenza comporta l'estensione della superficie di attacco. Ma lo ZTNA non rappresenta solamente un'alternativa alle VPN; offre alle organizzazioni l'opportunità di eliminare gli apparecchi legacy (e i relativi costi di gestione), fornisce agli utenti un accesso rapido e diretto alle app, è scalabile in modo semplice e migliora il controllo amministrativo e la visibilità.

Tuttavia, non tutti i prodotti o le soluzioni ZTNA presenti sul mercato sono uguali tra loro. Per poter usufruire di tutti questi e altri vantaggi, è necessario ricercare una soluzione in grado offrire le 10 funzionalità elencate di seguito.

N. 1: eliminare la superficie di attacco rendendo le app invisibili alla rete Internet pubblica.

Nelle architetture di rete tradizionali di tipo hub-and-spoke, le applicazioni possono essere facilmente individuate da qualsiasi aggressore che sia in grado di violare il perimetro di sicurezza.



Una volta che gli utenti malintenzionati si trovano all'interno della rete, le applicazioni e le altre risorse possono essere individuate molto facilmente con una semplice ricerca.

Con una vera soluzione ZTNA, l'accesso alle applicazioni viene concesso su base individuale attraverso la segmentazione. In questo modo, individuare le altre applicazioni nell'ambiente risulta impossibile, anche se un utente malintenzionato riesce ad accedere a una di esse.

Tutte le applicazioni sono nascoste dietro alla piattaforma ZTNA, che agisce da mediatrice per stabilire la connettività diretta. Dato che gli aggressori non sono in grado di colpire ciò che non riescono a vedere, una soluzione ZTNA dovrebbe nascondere le identità di origine offuscando i relativi indirizzi IP. In sostanza, queste connessioni inside-out, ossia dall'interno verso l'esterno, rendono l'intero ecosistema applicativo invisibile, e di conseguenza gli aggressori non sono in grado di lanciare attacchi mirati contro le singole app.

N. 2: consentire una connettività senza interruzioni da qualsiasi luogo.

Attualmente, il 77% delle organizzazioni ha adottato o sta cercando di supportare il lavoro flessibile.

Le architetture di rete legacy utilizzano costosi collegamenti MPLS tra le filiali e il data center centrale, e collegano gli utenti in remoto tramite le VPN. Con l'affermarsi del lavoro flessibile e da remoto, l'utilizzo delle VPN crea problemi prestazionali, perché questi strumenti non offrono scalabilità.

Lo ZTNA, invece, isola completamente l'accesso alle applicazioni dall'accesso alla rete, eliminando la necessità di collegamenti MPLS e VPN. Cerca servizi ZTNA forniti sul cloud, perché questa modalità elimina la necessità di effettuare il backhauling del traffico verso il data center aziendale, ed è possibile offrire agli utenti un accesso rapido e diretto alle applicazioni di cui hanno bisogno per rimanere produttivi.

Un provider di soluzioni ZTNA che vanta una presenza globale ed estesa di data center sarà in grado di individuare il percorso di connettività più breve tra utenti e applicazioni, e la possibilità di stabilire connessioni il più vicino possibile all'edge garantisce ai dipendenti un'esperienza utente ottimale.

N. 3: applicare l'accesso a privilegi minimi.

L'accesso a privilegi minimi è un principio chiave della filosofia zero trust. La sua definizione è molto semplice: agli utenti viene concesso solo il livello minimo di accesso necessario per svolgere le proprie mansioni lavorative, e nulla di più.

Costruire un'architettura di sicurezza in grado di supportare questo approccio può essere molto impegnativo senza la giusta soluzione ZTNA. Quest'ultima infatti deve incorporare rigorosi meccanismi di autenticazione dell'identità dell'utente, comprendere il contesto del dispositivo e includere la capacità di applicare una segmentazione molto granulare da utente ad applicazione. Per raggiungere questo obiettivo, lo ZTNA dove disporre di integrazioni avanzate con tutte le principali piattaforme dei provider di servizi di identità (IdP).

Cerca una soluzione ZTNA in grado di applicare le policy IT e aziendali per collegare gli utenti verificati solamente alle applicazioni che sono autorizzati a utilizzare, e non alla rete. Questo tipo di accesso deve essere esteso in egual misura agli utenti in remoto e a quelli in sede, indipendentemente dalla loro posizione, e i controlli di sicurezza devono essere identici per tutti gli utenti, ovunque.

Zscaler ha permesso di garantire la sicurezza di 18.000 dipendenti da remoto della Città di Los Angeles.

N. 4: preservare la produttività degli utenti, rilevando e risolvendo rapidamente i problemi di app, rete e dispositivi.

L'adozione dello zero trust, soprattutto quando si cerca di implementarlo utilizzando VPN legacy, richiede una segmentazione granulare della rete.

Dal punto di vista ingegneristico non si tratta di un compito facile, e anche l'esperienza utente si rivela problematica. Segmentando le reti in questo modo, per i team di rete e di assistenza è difficile, se non impossibile, ottenere le informazioni sulle prestazioni dei dispositivi e delle applicazioni degli utenti finali necessarie per garantire esperienze ottimali.

Una soluzione ZTNA dovrebbe fornire anche funzionalità in grado di aiutare i team a superare questa difficoltà. Dovrebbe raccogliere metriche sullo stato dei dispositivi degli utenti finali, sulle prestazioni della rete e sulla disponibilità delle applicazioni, quindi renderle disponibili all'interno di una dashboard facile da monitorare, attraverso cui i team di assistenza possono identificare e risolvere i problemi prima che si ripercuotano sugli utenti finali.

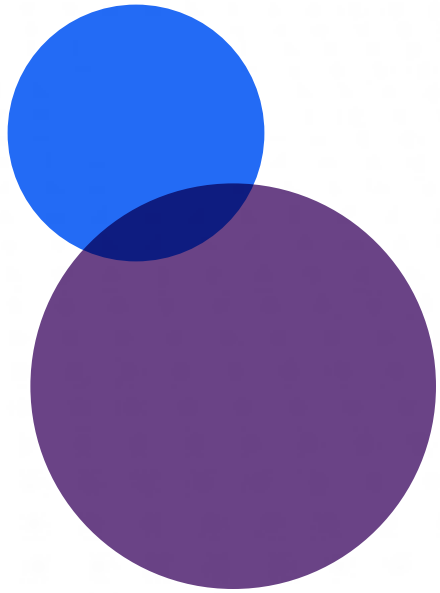
Careem ha migliorato il tempo medio di risoluzione (MTTR, Mean Time-to-Response) del 62% grazie al monitoraggio di Zscaler Digital Experience.

N. 5: prevenire il movimento laterale attraverso la microsegmentazione delle applicazioni.

Una soluzione ZTNA deve proteggere i dati, i flussi di lavoro, i servizi e le risorse attraverso una microsegmentazione definita da software che consenta di collegare gli utenti direttamente alle applicazioni, non alla rete.

Adottando questo approccio, i team di sicurezza non devono più preoccuparsi del movimento laterale attraverso la rete, e in caso di una violazione di un singolo account utente o di un'applicazione, l'aggressore non potrà spostarsi per compromettere altre risorse aziendali.

In un modello ZTNA, la creazione di una connessione a una singola app o risorsa non non deve mai consentire in automatico l'accesso ad altre.



N. 6: supportare l'accesso sicuro per i dispositivi personali (BYOD) e quelli di proprietà dell'azienda.

Careem ha migliorato il tempo medio di risoluzione (MTTR, Mean Time-to-Response) del 62% grazie al monitoraggio di Zscaler Digital Experience.

Cerca una soluzione ZTNA in grado di supportare sia l'accesso con agente che quello agentless per i dipendenti e le terze parti.

Cerca una soluzione ZTNA in grado di supportare sia l'accesso con agente che quello agentless per i dipendenti e le terze parti. In questo modo, lo ZTNA può permettere a partner e fornitori di accedere senza problemi alle risorse aziendali, e consentire al contempo ai dipendenti di utilizzare i propri dispositivi (compresi quelli mobili) per scopi lavorativi in modo sicuro.

Dato che i dispositivi non gestiti sono sempre più diffusi, è importante che la soluzione ZTNA sia in grado di supportare l'accesso clientless. In caso contrario, i dipendenti saranno protetti solo sui dispositivi aziendali. In un mondo in cui i dispositivi mobili vengono usati sempre più frequente, questa è una limitazione molto significativa.

N. 7: bloccare gli attacchi e le minacce sfruttando l'ispezione completa dei contenuti inline.

Per ottenere la visibilità integrale necessaria a bloccare tutte le minacce, una soluzione ZTNA deve essere in grado di eseguire un'ispezione completa dei contenuti inline.

Questo significa che il servizio sarà in grado di ispezionare tutto il traffico (compreso quello cifrato con SSL, utilizzato per mascherare la trasmissione di contenuti pericolosi come ransomware, spyware e virus) e di consentire il passaggio solamente alle comunicazioni legittime. L'ispezione inline deve fondarsi su informazioni di intelligence sulle minacce provenienti da un'ampia varietà di segnali globali, per essere in grado di bloccare le minacce ransomware, phishing e O-day attualmente più diffuse e gli attacchi avanzati.

Desideri sapere quali sono le minacce che lo ZTNA dovrebbe essere in grado di combattere? La OWASP Top 10 è il risultato di un ampio consenso degli esperti sui rischi di sicurezza più critici per le applicazioni web. Una soluzione ZTNA dovrebbe fornire una copertura completa contro le tecniche di attacco più comunemente utilizzate, tra cui SQL injection, cross-site scripting, scanner di ambienti e porte e cookie poisoning.

Zscaler consente di bloccare la OWASP Top 10 e gli altri rischi noti nell'ambito per la sicurezza delle applicazioni web, tra cui SQL injection e cross-site scripting.

N. 8: garantire un'integrazione perfetta con un'ampia varietà di fornitori di servizi e soluzioni per l'identità.

Zscaler dispone di integrazioni approfondite con i fornitori di servizi di identità, come Microsoft e Okta, e con le piattaforme di rilevamento e risposta degli endpoint (EDR), come CrowdStrike.

La sicurezza zero trust parte con la verifica dell'identità dell'utente che cerca di accedere a un'applicazione o a un'altra risorsa.

Il numero di organizzazioni che adottano strategie cloud-first per supportare gli ambienti moderni che prevedono la possibilità di lavorare da casa è in continua crescita. Per gestire l'autenticazione e le identità degli utenti per tutto il tempo necessario, queste realtà si rivolgono a un'ampia varietà di partner di gestione delle identità e degli accessi (IAM) e di governance e l'amministrazione delle identità (IGA).

Una soluzione ZTNA dovrebbe naturalmente integrarsi con gli attuali partner aziendali di IAM e IGA. Ma se si vuole essere davvero all'avanguardia con la propria strategia di identità e autenticazione, è fondamentale ricercare un fornitore che abbia stabilito solide relazioni con tutti i principali provider di soluzioni tecnologiche del settore.

N. 9: incorporare una tecnologia di deception integrata per sventare gli attacchi degli aggressori.

La tecnologia di deception è una nuova categoria di soluzioni di sicurezza informatica.

L'utilizzo di questa tecnologia consente di rilevare rapidamente le minacce del mondo reale, con tassi di falsi positivi molto bassi, e consiste nel distribuire esche realistiche (ad es. domini, database, directory, server, app, file, credenziali, breadcrumb) accanto alle risorse reali di una rete, con l'obiettivo di trarre in inganno gli aggressori. Quando un utente malintenzionato interagisce con un'esca, la tecnologia inizia a raccogliere informazioni che utilizzerà per generare avvisi altamente attendibili.

Sfruttare la tecnologia di deception permette di migliorare la capacità del team di sicurezza di rilevare le minacce, comprendere più approfonditamente i rischi che l'azienda deve affrontare in tempo reale e coprire meglio quelli che altrimenti sarebbero punti ciechi nell'ambiente aziendale. In un ambiente zero trust, le esche di deception agiscono da trappole, rilevando gli account utente compromessi o i tentativi di spostarsi lateralmente attraverso la rete.

Trattandosi di una tecnologia emergente, alcuni fornitori di soluzioni ZTNA devono ancora integrare piattaforme di deception, ma i leader del settore hanno già compiuto questo importante progresso.

KuppingerCole ha nominato Zscaler un'azienda leader nelle piattaforme distribuite di deception.

N. 10: consentire una distribuzione rapida e semplice.

A differenza di altre soluzioni tecnologiche che possono richiedere settimane o mesi per essere distribuite, lo ZTNA leader del settore può essere implementato da qualsiasi luogo in pochi giorni.

Zscaler ha permesso alla città di Los Angeles di fornire un accesso sicuro a 18.000 dipendenti da remoto in meno di due settimane.

Scopri perché Zscaler Private Access è la piattaforma ZTNA più utilizzata al mondo

Zscaler Private Access (ZPA) fa tutto questo e molto di più. ZPA è una soluzione basata sull'esclusiva architettura zero trust di Zscaler, che applica il principio dell'accesso a privilegi minimi per offrire agli utenti connessioni sicure e dirette alle applicazioni private, eliminando al contempo gli accessi non autorizzati e il movimento laterale. Grazie al fatto che è un servizio fornito sul cloud, può essere implementato in poche ore per sostituire le VPN e gli strumenti di accesso remoto legacy con una piattaforma zero trust moderna e olistica.

Zscaler Private Access offre:

- **Una sicurezza ineguagliabile, che surclassa quella ottenibile con VPN e firewall legacy:** gli utenti si collegano direttamente alle app, non alla rete, e ciò consente di ridurre al minimo la superficie di attacco ed eliminare il movimento laterale.
- **Niente più compromissioni delle app private:** una protezione delle app di alto livello che offre prevenzione inline, tecnologia di deception e isolamento delle minacce e riduce al minimo il rischio causato dagli utenti compromessi.
- **Produttività superiore per la forza lavoro flessibile di oggi:** accesso ultraveloce alle app private, che si estende anche a utenti in remoto, uffici aziendali e filiali e partner terzi.
- **ZTNA unificato per utenti, workload e dispositivi:** i dipendenti e i partner possono connettersi in modo sicuro ad app private, servizi e dispositivi OT/IoT sfruttando la piattaforma ZTNA più completa del settore.Qui con dii pos cerfit. C. Certusum

Desideri saperne di più? Richiedi oggi stesso una dimostrazione gratuita.

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 inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.it