SOPHOS

2025

White Paper

ZTNA

ZERO TRUST NETWORK ACCESS

La nuova frontiera della sicurezza degli accessi aziendali

www.yourwebsite.com

ZTNA: sicurezza garantita, accesso controllato

Negli ultimi anni, il perimetro aziendale è diventato sempre più difficile da definire. Lavoro da remoto, applicazioni cloud, dispositivi personali e fornitori esterni hanno trasformato l'idea tradizionale di rete aziendale in un ecosistema fluido, distribuito e costantemente esposto. In questo contesto, le soluzioni di sicurezza nate per proteggere ambienti statici e centralizzati – prima fra tutte la VPN – si rivelano oggi inefficaci o addirittura controproducenti.

La Zero Trust Network Access (ZTNA) non è semplicemente una nuova tecnologia: rappresenta un cambio di paradigma. Basata sul principio "never trust, always verify", questa filosofia di sicurezza **elimina la fiducia implicita negli utenti, nei dispositivi e nelle connessioni di rete. In sua vece, adotta un modello dinamico, adattivo e granulare, che autorizza l'accesso solo in seguito a una verifica continua dell'identità, dello stato del dispositivo e delle policy applicative.**

L'obiettivo di questo documento è fornire una panoramica chiara e approfondita su cos'è lo ZTNA, quali problemi risolve rispetto alle VPN tradizionali e perché rappresenta un investimento strategico per la cybersecurity delle organizzazioni moderne.

LOGO AZIENDA

Contenuti

Contattaci

Nome azienda
Indirizzo
CAP e città

Telefono
email

Il problema delle VPN tradizionali

Per decenni, le Virtual Private Network (VPN) hanno rappresentato la soluzione standard per consentire l'accesso remoto ai sistemi aziendali. Il principio di base era semplice: creare un tunnel criptato attraverso cui un utente remoto potesse collegarsi alla rete interna come se fosse fisicamente presente in ufficio. In un'epoca in cui le applicazioni e i dati risiedevano all'interno di un data center centrale, questo approccio risultava logico ed efficace.

Tuttavia, il panorama IT è radicalmente cambiato. Le aziende utilizzano oggi applicazioni distribuite su ambienti cloud, ibridi o multi-cloud. I dipendenti lavorano da casa, da coworking, da aeroporti o da qualsiasi altro luogo dotato di una connessione. Le reti sono diventate liquide e i perimetri indefinibili. In questo nuovo scenario, la VPN si rivela non solo obsoleta, ma anche rischiosa.

Uno dei problemi principali risiede nella fiducia implicita che la VPN concede una volta stabilita la connessione. L'utente, una volta "dentro", ha spesso accesso esteso a molteplici risorse aziendali, indipendentemente dal fatto che ne abbia effettivamente bisogno. Questa esposizione eccessiva favorisce il movimento laterale all'interno della rete, facilitando l'operato di malware e attori malevoli.

A ciò si aggiunge la mancanza di consapevolezza sullo stato del dispositivo che accede: la VPN non verifica se l'endpoint sia aggiornato, compromesso o conforme alle policy aziendali. Infine, la gestione di una VPN su larga scala richiede uno sforzo non indifferente in termini di configurazione, manutenzione e supporto utenti.

Il modello Zero Trust

Il concetto di Zero Trust nasce per rispondere a questi limiti strutturali. Non si tratta di una tecnologia specifica, bensì di un approccio strategico che rifiuta ogni forma di fiducia automatica all'interno della rete. **Ogni richiesta di accesso viene trattata come potenzialmente pericolosa e viene autorizzata solo dopo un processo di verifica dettagliato.**

Nel contesto dello ZTNA, ciò si traduce in una serie di meccanismi di controllo:

L'identità dell'utente viene verificata tramite sistemi di autenticazione robusta, spesso con l'uso dell'autenticazione a più fattori (MFA).

Lo stato del dispositivo viene controllato per assicurarsi che sia aggiornato, non compromesso e conforme alle policy di sicurezza.

L'accesso viene concesso solo alle applicazioni specificamente autorizzate per quell'utente, escludendo ogni tipo di accesso alla rete nel suo complesso.

In altre parole, **lo ZTNA non permette all'utente di "entrare in rete", ma solo di "collegarsi a un'applicazione", e lo fa attraverso canali sicuri e segmentati.**

ZTNA come alternativa alla VPN

Implementare lo ZTNA significa adottare un accesso granulare, che sostituisce la logica del “castello con il ponte levatoio” tipica delle VPN con una struttura fatta di perimetri micro-segmentati.
Ogni applicazione diventa un’isola, accessibile solo previa verifica delle credenziali e del contesto di sicurezza.

L’utente remoto non viene più “trasportato” nella LAN aziendale. Al contrario, gli viene concessa una connessione criptata diretta solo alla risorsa specifica necessaria per il suo lavoro. In questo modo si elimina il rischio di movimento laterale, si limita l’esposizione in caso di compromissione e si riduce la superficie di attacco in modo significativo.

Inoltre, lo ZTNA consente un’esperienza utente più fluida: non richiede tunnel manuali, configurazioni complicate o client VPN dedicati.
Le connessioni vengono stabilite in modo trasparente, a richiesta, e sono spesso più performanti perché non obbligano il traffico a passare da un punto centrale prima di raggiungere il cloud.

Benefici strategici dello ZTNA

L'adozione di un'architettura ZTNA genera vantaggi su più livelli:

1. Sicurezza proattiva:
La verifica continua dell'identità e dello stato del dispositivo riduce drasticamente il rischio di accesso non autorizzato, anche in caso di furto delle credenziali.

2. Riduzione della superficie di attacco:
Ogni utente vede solo le applicazioni a cui ha accesso. Nessuna visibilità sulle altre risorse di rete significa meno possibilità di movimento laterale per eventuali attaccanti.

3. Maggiore conformità e auditabilità:
Grazie alla tracciabilità completa di ogni accesso, diventa più semplice rispettare normative come GDPR, NIS2 e ISO 27001. Ogni evento è loggato, verificabile e attribuibile.

4. Agilità operativa:
Le organizzazioni possono introdurre nuove applicazioni, utenti o dispositivi in modo rapido e sicuro, accelerando il time-to-market e l'onboarding digitale.

5. Ottimizzazione dell'esperienza utente:
Lo ZTNA consente un accesso fluido, senza le frizioni tipiche delle VPN, migliorando la produttività e riducendo il carico sul supporto tecnico.

ZTNA e Cyber Resilienza

In un'epoca segnata dalla crescita degli attacchi ransomware e dalla proliferazione di minacce avanzate persistenti (APT), la capacità di reagire rapidamente a un incidente è fondamentale.

ZTNA, combinato con strategie di monitoraggio continuo e threat hunting, consente alle organizzazioni di individuare segnali di compromissione in tempo reale e di revocare selettivamente gli accessi prima che l'attacco si propaghi.

Non solo previene l'ingresso di minacce, ma è anche uno strumento fondamentale per contenere i danni in caso di violazione.

La proposta Sophos

Nel panorama delle soluzioni ZTNA, un esempio di implementazione efficace è rappresentato dalla piattaforma proposta da Sophos. Integrata nativamente con il proprio ecosistema di sicurezza – endpoint, firewall, XDR, MDR – **la soluzione ZTNA di Sophos garantisce un approccio sinergico e coordinato alla protezione degli accessi.**

Oltre a supportare l'autenticazione forte, la verifica dello stato del dispositivo e la micro-segmentazione, il sistema è progettato per essere gestito centralmente da una console cloud intuitiva e scalabile. Questo consente di monitorare in tempo reale ogni tentativo di accesso, correlare eventi tra diversi layer di sicurezza e intervenire rapidamente in caso di anomalia.

Sophos ZTNA rappresenta dunque non solo una tecnologia avanzata, ma un vero e proprio pilastro della cybersecurity moderna, capace di accompagnare le aziende nella transizione verso modelli di lavoro ibridi e digital-first in piena sicurezza.

Conclusioni

La Zero Trust Network Access non è una moda passeggera, ma una necessità strutturale.
In un mondo in cui il rischio cyber non è più un'eventualità, ma una costante, adottare un modello ZTNA significa proteggere il cuore stesso del business: i dati, le persone, la reputazione.

Investire oggi in questo paradigma significa costruire una difesa resiliente, agile e consapevole. E scegliere il giusto partner tecnologico può fare la differenza tra una trasformazione efficace e un'infrastruttura fragile.

Grazie!
Contattaci per una consulenza gratuita

Contact Us

Nome Azienda
Indirizzo
CAP e città
Telefono
E.mail

www.companywebsite.com