



SICUREZZA SENZA
COMPROMESSI PER L'ACCESSO
REMOTO

ZTNA

Datasheet



Le aziende del Gruppo MEET IT



Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com



Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
infoonline.it | www.ntonline.it



Le VPN client-to-site, anche integrate con MFA, non sono sufficienti per garantire una sicurezza adeguata nel contesto dello smart working.

La soluzione? Zero Trust Network Access (ZTNA)

Le tradizionali VPN di accesso remoto hanno servito le aziende per anni, ma con la diffusione dello smart working e la crescente complessità delle minacce informatiche, emergono sempre più limiti e vulnerabilità. **Zero Trust Network Access (ZTNA)** è la soluzione moderna per garantire connessioni sicure, selettive e monitorate, eliminando i rischi legati all'accesso implicito e migliorando il controllo su utenti e dispositivi.

COME FUNZIONA

ZTNA si basa sul principio "*Mai fidarsi, verificare sempre*". Ogni utente, dispositivo o applicazione deve superare un rigoroso controllo di identità e conformità prima di accedere alle risorse aziendali. L'accesso non avviene più all'intera rete, ma solo alle applicazioni specifiche necessarie, riducendo i rischi di intrusioni e movimenti laterali delle minacce.

PROCESSO DI ACCESSO



Identificazione dell'utente

Autenticazione basata su credenziali e fattori multipli.



Verifica dello stato del dispositivo

Controllo della conformità e integrità prima della connessione.



Accesso mirato

Connessione solo alle applicazioni autorizzate, senza accesso generalizzato alla rete.



Sicurezza avanzata



Zero Trust elimina il rischio di accesso implicito



Controlli continui su identità e dispositivi.



Micro-segmentazione per bloccare movimenti laterali delle minacce.

Migliore esperienza utente



Accesso trasparente senza necessità di connessioni VPN manuali



Nessun impatto negativo sulle prestazioni di rete



Gestione delle autorizzazioni semplice e automatizzata

Gestione IT semplificata



Facile registrazione di nuovi utenti e rimozione di accessi obsoleti



Integrazione con altre soluzioni di cybersecurity



Monitoraggio in tempo reale di accessi e utilizzo delle applicazioni



PERCHÉ SCEGLIERE ZTNA RISPETTO ALLE VPN TRADIZIONALI?

Caratteristica	VPN Tradizionale	ZTNA
Accesso alla rete	Completo	Selettivo e controllato
Sicurezza	Attendibilità implicita	Controllo continuo
Facilità di gestione	Complessa	Semplificata e automatizzata
Esperienza utente	Latenze e problemi di connessione	Fluida e trasparente

AMBITI DI UTILIZZO



Smart working e accesso remoto

Garantisce connessioni sicure per i dipendenti ovunque si trovino, senza necessità di VPN complesse.



Protezione delle applicazioni aziendali

Difende le risorse interne da accessi non autorizzati e attacchi ransomware.



Gestione dinamica degli accessi

Facile inclusione e rimozione di utenti e dispositivi in scenari aziendali in evoluzione.

CONCLUSIONI

ZTNA rappresenta l'evoluzione naturale delle soluzioni di accesso remoto, combinando sicurezza avanzata, esperienza utente migliorata e gestione IT semplificata. Adottare ZTNA significa proteggere le risorse aziendali in modo moderno, efficace e senza compromessi.

Passa a ZTNA e rivoluziona il modo in cui proteggi il tuo business!

VISITA IL SITO [MEETIT.CLOUD](https://meetit.cloud) 