Cos'è il vero zero trust?

Le aziende stanno adottando lo zero trust per accelerare la trasformazione digitale sicura, ma navigare nel mare delle soluzioni "zero trust" può rivelarsi molto complesso. È importante saper distinguere una vera soluzione zero trust da una che ne utilizza unicamente il nome.

Il vero zero trust

COSA NON FA

Non utilizza firewall perimetrali e VPN per estendere una rete piatta agli utenti in remoto, ampliando così la superficie di attacco.

Non concede l'attendibilità implicita

Non considera attendibili tutti gli utenti, le app e i dispositivi conosciuti

Non colloca gli utenti sulla rete

Non utilizza una rete instradabile per il traffico degli utenti e delle app, che faciliterebbe il movimento laterale.

Non consente il passaggio del traffico "passthrough"

Non consente al traffico criptato di procedere senza essere ispezionato per individuare eventuali minacce e dati sensibili.

COSA FA

Considera tutto come ostile o compromesso, concedendo l'accesso solo se può anche:

Verificare l'identità e il contesto

Interrompe la connessione e verifica l'identità e il contesto per ottenere maggiori informazioni sulla richiesta

Controllare i contenuti e l'accesso

Valuta il rischio associato alle richieste di connessione e **ispeziona il traffico** alla ricerca di minacce informatiche e dati sensibili

Eseguire le policy, con decisione e applicazione definite per sessione

Applica le policy prima di instaurare la connessione alle app interne o esterne.

Scopri il One True Zero Trust: Zscaler Zero Trust Exchange

Prova lo zero trust senza compromessi e offri alla tua azienda un'architettura zero trust fluida, sicura ed economica che trasformi l'infrastruttura IT in un acceleratore della trasformazione digitale.

Leggi il white paper

Experience your world, secured.™

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