Zero trust:
la base per la sicurezza aziendale

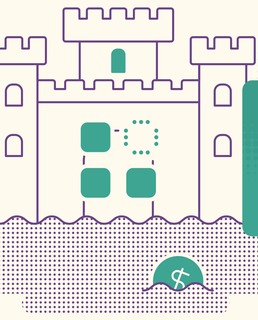
Di recente, gli analisti di IDC hanno esaminato il futuro dello zero trust e hanno condiviso le loro opinioni su come questo nuovo approccio influirà sulla sicurezza aziendale.

Il panorama delle minacce è in rapida evoluzione.

80% incremento degli attacchi ransomware nell'ultimo anno[1]

314% incremento degli attacchi sui canali criptati[2]

436% incremento degli attacchi di phishing nei settori del commercio al dettaglio e all'ingrosso[3]

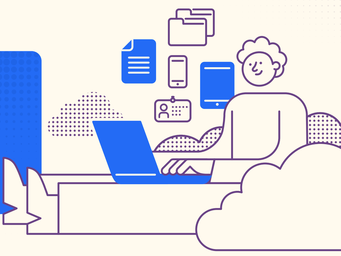


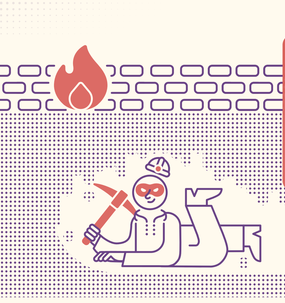
Le architetture di sicurezza perimetrali sono state progettate per il passato.

La sicurezza basata sul perimetro è stata concepita per un'epoca in cui i dipendenti lavoravano principalmente nell'ufficio, da cui accedevano alle applicazioni e alle risorse presenti sul data center.[4]

Il luogo di lavoro ibrido di oggi è molto più complesso.

Gli utenti lavorano da qualsiasi luogo, utilizzano dispositivi diversi e accedono ad applicazioni e dati che sono distribuiti su SaaS, data center e cloud pubblici.





Le difese del passato non sono più all'altezza.

I firewall, i firewall virtuali, le VPN e le altre strategie di difesa orientate al perimetro non sono in grado di bloccare le minacce dinamiche e persistenti.[4]

Le imprese di oggi richiedono un nuovo approccio.

Le organizzazioni stanno adottando lo zero trust per affrontare queste sfide. A differenza degli approcci basati sulla sicurezza perimetrale, lo zero trust si fonda sul principio dell'accesso a privilegi minimi e sul concetto che nessun utente e nessuna applicazione debbano essere intrinsecamente ritenuti attendibili.

Gli elementi fondamentali dello zero trust

Lo zero trust non è una tecnologia singola, ma una vera e propria strategia su cui si fonda l'intero ecosistema di sicurezza. Secondo IDC, lo zero trust si basa su sei elementi principali[4]:

- Autorizzazione granulare
- Identità e autenticazione solide
- Policy basate sul contesto
- Applicazione universale dello zero trust
- Rilevamento e protezione costante dalle minacce
- Accesso consentito solo in base alla necessità di accedere a una determinata risorsa

I vantaggi dell'adozione dello zero trust

Un'architettura zero trust consente alle organizzazioni di ridurre i rischi aziendali **abbattendo i costi, semplificando l'IT e migliorando l'esperienza utente.**

Costruire le basi per il successo

Scopri perché un'architettura zero trust costituisce una base sicura per la trasformazione digitale.

Leggi l'Analyst Brief di IDC

[1] Zscaler, report del 2022 di ThreatLabz "Ultimi dati sul ransomware".
[2] Zscaler, report del 2021 di ThreatLabz sugli attacchi criptati.
[3] Zscaler, report del 2022 di ThreatLabz sugli attacchi di phishing.
[4] IDC Analyst Brief, sponsorizzato da Zscaler, "Implementing Zero Trust as a Foundation for Secure Business Enablement". Documento #US49043922, aprile 2022.

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