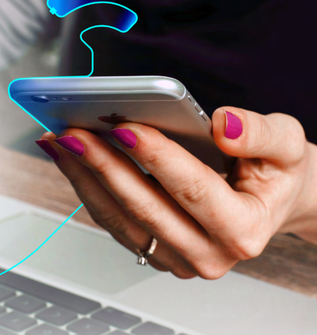
INFOGRAFICA

Firewall e VPN non sono adatti a supportare lo zero trust

L'abilitazione e la protezione della forza lavoro distribuita richiedono un approccio nuovo alla sicurezza.



Il modo in cui lavoriamo è cambiato.

Gli utenti, i dati e le applicazioni sono distribuiti ovunque.

300%
aumento della percentuale di dipendenti totali che lavorano da remoto.[1]

50%
di tutti i dati aziendali è archiviato sul cloud.[2]

70%
delle app aziendali utilizzate oggi dalle aziende è basato su SaaS.[3]

Perché non dovrebbe evolversi anche la sicurezza?

Proteggere il perimetro e considerare attendibile tutto ciò che è collocato all'interno della rete era un approccio efficace quando tutto si trovava on-premise. Ma oggi il perimetro è scomparso, e le modalità di protezione della rete del passato non sono più adeguate.

delle organizzazioni ritiene di dover aggiornare la propria sicurezza per proteggere meglio i lavoratori in ufficio e da remoto.[4]

delle aziende sta dando priorità all'adozione di un modello zero trust.[5]

La soluzione è lo zero trust.

Affinché le aziende siano in grado di supportare la forza lavoro moderna, rimanendo agili e competitive, le architetture di sicurezza devono evolversi. È giunto il momento di passare a una soluzione che autorizzi le connessioni in base al contesto e alle policy per ogni sessione, da ogni utente verso ogni applicazione e in ogni luogo.

Ma i firewall e le VPN non sono adatti a supportare lo zero trust. Perché?

Le minacce possono accedere e attuare con facilità tecniche di movimento laterale, perché i firewall richiedono ancora la connessione di utenti e dispositivi alla rete per consentire l'accesso alle applicazioni.

Le applicazioni sono pubblicate su Internet, e questo estende la superficie di attacco.

Le architetture di tipo "passthrough" dei firewall hanno una capacità limitata di ispezionare il traffico e proteggere i dati.

delle aziende non ritiene che le proprie tecnologie esistenti possano aiutarle a raggiungere lo zero trust. [5]

delle organizzazioni si fiderà erroneamente delle tecnologie esistenti e collocherà gli utenti sulla rete aziendale.[5]

Lo zero trust richiede un approccio radicalmente diverso.

A differenza degli approcci tradizionali, che considerano attendibile tutto ciò che si trova all'interno del perimetro di rete, lo zero trust si basa sul principio dell'accesso a privilegi minimi e sul concetto che nessuna applicazione o utente debba essere automaticamente ritenuto attendibile. Una vera soluzione zero trust collega in modo sicuro applicazioni e utenti tramite Internet sulla base di policy aziendali, e:

Eliminare il movimento laterale
Collega direttamente gli utenti e i dispositivi alle applicazioni, mai alla rete.

Ridurre al minimo la superficie di attacco
Rende gli utenti e le applicazioni invisibili a Internet. Se non possono essere individuati, significa che non vi è una superficie di attacco che gli aggressori possono sfruttare.

Blocco delle minacce e della perdita di dati
Offre un'ispezione completa, anche del traffico criptato, per una protezione efficace dalle minacce informatiche e dalla perdita di dati.

Zscaler: i leader dello zero trust.

Zero Trust Exchange, una soluzione Zscaler basata sul security cloud più grande del pianeta, aiuta i team IT ad adottare il modello zero trust per ridurre i rischi, aumentare l'agilità aziendale e offrire un'esperienza utente ottimale.

Ogni giorno, Zero Trust Exchange:

SICURA PIÙ DI 200 MILIARDI
di transazioni

PREVIENE PIÙ DI 7 MILIARDI
di incidenti di sicurezza e violazioni delle policy

PROCESSA PIÙ DI 200 000
aggiornamenti unici di sicurezza

Inizia il tuo percorso verso lo zero trust con Zscaler.

Zscaler ha aiutato più di 5000 aziende a trasformarsi in modo sicuro con lo zero trust.

Possiamo aiutare anche te.

Scopri come

1. *Grady, John. (2021). Lo stato delle strategie di sicurezza zero trust. Enterprise Strategy Group. https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies*
2. *Statista. Percentuale di dati e dati sensibili archiviati sul cloud in tutto il mondo. https://www.statista.com/statistics/1202541/sensitive-data-cloud-location*
3. *Better Cloud. (2021). The State of SaaSOps 2021. https://stateofsaasops.bettercloud.com/?_ga=2.164919740.241347015.1636678142-1969514686.1636678142*
4. *IDG Marketpulse Survey. (2020). Approcci alla sicurezza della rete e perché adottare lo zero trust. https://info.zscaler.com/industry-report-leading-cios-and-it-leaders-see-it-future-in-zero-trust*
5. *Cybersecurity Insiders. (2021). Report sui rischi delle VPN. https://info.zscaler.com/resources-industry-reports-vpn-risk-report-cybersecurity-insiders*

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408 533 0288
www.zscaler.it