I sette elementi di un'architettura zero trust di grande successo

Zero Trust Exchange di Zscaler: la guida degli architetti

Le architetture di sicurezza tradizionali rendono le aziende vulnerabili

Gli approcci alla sicurezza basati sul mantenimento dello status quo, che fanno uso di firewall e VPN, connettono gli utenti alla rete. Di conseguenza, consentono agli aggressori di compromettere utenti, dispositivi e carichi di lavoro e di spostarsi lateralmente per raggiungere risorse di alto valore ed esfiltrare i dati sensibili.

L'ambiente di lavoro ibrido di oggi richiede l'adozione di un approccio zero trust alla sicurezza.

Per proteggere le organizzazioni, i leader più innovativi stanno adottando lo zero trust, un approccio olistico alla sicurezza basato sull'accesso a privilegi minimi e sul concetto che utenti e applicazioni non debbano mai essere ritenuti automaticamente attendibili.

Come si implementa un'architettura zero trust?

Il vero approccio zero trust viene fornito tramite **Zscaler Zero Trust Exchange**, una piattaforma integrata e nativa del cloud che connette in modo sicuro utenti, dispositivi (IoT/OT) e carichi di lavoro alle applicazioni senza instaurare connessioni alla rete.

Gli elementi alla base di una vera architettura zero trust sono sette

Grazie a questo approccio unico nel suo genere, Zscaler elimina la superficie d'attacco, previene il movimento laterale delle minacce e protegge l'azienda dalle compromissioni e dalla perdita di dati.

1. Chi si sta connettendo?

Termina la connessione che viene richiesta, quindi verifica l'identità dell'utente, del dispositivo IoT/OT o del carico di lavoro.

2. Qual è il contesto dell'accesso?

Convalida il contesto di chi richiede la connessione esaminando attributi come il ruolo, la responsabilità, l'orario e le circostanze della richiesta.

3. Qual è la destinazione della connessione?

Conferma che la destinazione sia nota, compresa e contestualizzata per l'accesso. Se la destinazione è sconosciuta, viene segnalata affinché venga eseguita un'analisi più approfondita.

4. Valutazione del rischio

Utilizza l'IA per calcolare dinamicamente il punteggio di rischio associato alla connessione, in base a fattori come il profilo di sicurezza del dispositivo, le minacce, la destinazione, il comportamento e le policy.

5. Prevenzione delle compromissioni

Ispeziona il traffico e i contenuti inline per identificare e bloccare i contenuti dannosi.

6. Prevenzione della perdita di dati

Ispeziona il traffico in uscita per identificare i dati sensibili e impedirne l'esfiltrazione.

7. Applicazione delle policy

Applica le policy per ogni sessione e determina l'azione condizionale da intraprendere in relazione alla connessione richiesta. Una volta raggiunta la decisione di concedere l'autorizzazione, viene stabilita una connessione sicura a Internet, all'app SaaS o all'app interna.

Vuoi scoprire come implementare questi sette principi nella tua azienda per **eliminare la superficie di attacco, prevenire il movimento laterale delle minacce** e **proteggere l'organizzazione da compromissioni e perdite di dati con un progetto zero trust?**

Leggi l'e-book

Experience your world, secured.

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