Zero Trust Security: come superare le sfide più comuni



Zero Trust Security non è più un’opzione. Il ransomware continua ad accelerare. Gli attaccanti diventano sempre più sofisticati. L’intelligenza artificiale evolve senza sosta. Il panorama delle minacce informatiche si trasforma a una velocità che i principi di sicurezza tradizionali non riescono più a stare al passo. In questo scenario, adottare un’architettura Zero Trust è l’unica risposta concreta alle minacce di domani.

Migrare verso il modello Zero Trust può sembrare un’impresa titanica. Richiede un cambiamento radicale nel modo di concepire la sicurezza, mettendo in discussione ogni aspetto dell’architettura di rete. I controlli di sicurezza tradizionali aggiungono livelli di difesa sopra reti e sistemi operativi intrinsecamente aperti: le regole del firewall vengono applicate ai gateway per bloccare il traffico malevolo, le configurazioni sicure vanno a correggere impostazioni locali predefinite tutt’altro che robuste.

Zero Trust ribalta completamente questa logica.

In una rete moderna e sicura, tutti i punti di accesso sono chiusi per impostazione predefinita. L’accesso alla rete o ai suoi endpoint viene concesso solo in condizioni specifiche e ben definite.

Abbandonare il consolidato paradigma di sicurezza tradizionale non è un passo semplice. È comprensibile voler rimandare l’adozione dello Zero Trust, soprattutto per le organizzazioni che operano in ambienti già strutturati e rodati. Da dove si comincia a trasformare un’intera architettura di sicurezza? Come si convincono colleghi e vertici aziendali ad accettare

un cambiamento così profondo? E soprattutto, chi ne sostiene i costi?

Sono domande legittime che meritano risposte concrete e che, con la giusta pianificazione e gli strumenti adeguati, possono tutte trovare una soluzione.

Il tempo, però, stringe. Le vulnerabilità zero-day non aspettano che le reti si adeguino. Ogni infrastruttura prima o poi verrà attaccata: che l'attacco vada a segno o meno dipenderà, in larga misura, dall'aver compiuto o meno il salto verso Zero Trust.

Gli ostacoli lungo il percorso Zero Trust Security

Nel cammino verso l'adozione del modello Zero Trust si incontrano inevitabilmente ostacoli, sia tecnici che organizzativi. Ecco le sfide più frequenti e come ThreatLocker aiuta ad affrontarle.

Come evitare interruzioni operative?

Un approccio Zero Trust richiede di proteggere gli endpoint bloccando per default tutte le applicazioni e consentendo l'esecuzione solo di quelle esplicitamente autorizzate. Il principio del "nega tutto per impostazione predefinita" è un cardine dello Zero Trust, ma l'idea di bloccare qualcosa di essenziale per le operazioni è comprensibilmente fonte di preoccupazione.

Per evitare disservizi è fondamentale, prima di tutto, definire una baseline delle attività ordinarie su tutti gli ambienti applicativi. Comprendere il numero atteso di esecuzioni e installazioni in un dato arco di tempo permette di prendere decisioni consapevoli su quali applicazioni debbano rimanere autorizzate.

Come aiuta ThreatLocker

Con ThreatLocker, gli agenti non iniziano a bloccare le applicazioni finché non hanno completato una fase di apprendimento approfondita di tutto ciò che gira su ogni endpoint. Le policy di autorizzazione vengono create automaticamente e non vengono applicate fino a quando non si decide di attivarle. Nel frattempo, ogni esecuzione e installazione viene tracciata, evidenziando ciò che sarebbe stato bloccato. Endpoint e utenti continuano a operare normalmente, mentre la modalità di apprendimento cataloga silenziosamente tutto in background.

Non abbiamo personale sufficiente per gestire la migrazione.

Allocare le risorse disponibili in modo efficace è una delle sfide ricorrenti in qualsiasi progetto IT. I progetti si allungano o vengono accantonati di fronte a priorità concorrenti. Peggio ancora, distribuire le risorse oltre le proprie capacità rischia di compromettere l'intero deployment Zero Trust.

Per i team ridotti, una strada praticabile è un rollout graduale di agenti leggeri, partendo dai sistemi o dagli utenti a maggior rischio e ampliando progressivamente il perimetro man mano che le policy si consolidano. Introducendo l'enforcement per fasi controllate e gestendo le policy in modo centralizzato, si può rafforzare la postura di sicurezza senza sovraccaricare le risorse disponibili.

Come aiuta ThreatLocker

ThreatLocker elimina questo rischio attraverso un rollout strutturato e controllato. Il software agente può essere distribuito reparto per reparto, o addirittura macchina per macchina, accompagnando l'organizzazione verso l'architettura Zero Trust secondo ritmi compatibili con le esigenze

operative. Gli ambienti dotati di strumenti di remote monitoring and management (RMM) possono persino automatizzare il deployment degli agenti grazie alle decine di integrazioni native supportate dalla piattaforma.

Non disponiamo del supporto tecnico necessario.

Non tutte le organizzazioni hanno la fortuna di poter contare su esperti IT o di sicurezza interni. Le piccole e medie imprese spesso esternalizzano queste funzioni a managed service provider (MSP), i cui accordi contrattuali potrebbero non includere il supporto necessario per implementare o gestire servizi di sicurezza avanzati.

Chi dispone di supporto limitato può comunque partire dai principi ad alto impatto e bassa complessità: verificare ogni richiesta di accesso, applicare il principio del minimo privilegio, proteggere i sistemi critici prima degli altri. Un'implementazione graduale permette di migliorare la sicurezza senza richiedere fin dall'inizio una specializzazione tecnica approfondita.

Come aiuta ThreatLocker

Ogni deployment di ThreatLocker è accompagnato da un Solutions Engineer dedicato, in grado di orientarsi nel contesto specifico di ciascun cliente. Ogni fase del deployment viene pianificata durante un periodo di onboarding personalizzato sull'organizzazione, dall'installazione degli agenti alla fase di apprendimento fino all'attivazione del blocco delle applicazioni. Una volta completato l'onboarding, le eventuali lacune di competenza vengono colmate grazie all'accesso 24/7 al team Cyber Hero, con tempi di risposta in chat inferiori al minuto.

Il nostro ambiente ibrido è troppo eterogeneo per implementare Zero Trust.

Molte piccole imprese esitano ad adottare Zero Trust perché i loro ambienti sono un mosaico di server on-premise, piattaforme cloud, endpoint remoti e sistemi legacy nati prima che i moderni principi di sicurezza diventassero una priorità. La percezione che Zero Trust richieda una revisione architettonica completa blocca spesso il progetto ancora prima di cominciare.

In realtà, Zero Trust può essere applicato in modo coerente anche negli ambienti ibridi, senza necessità di ricostruire tutto da zero. Applicare controlli di accesso basati sull'identità e sul minimo privilegio, anziché sui perimetri di rete tradizionali, è un principio fondante dello Zero Trust e non richiede una riprogettazione dell'infrastruttura.

Zero Trust Security: come aiuta ThreatLocker

Ambienti cloud e reti che ospitano sistemi operativi eterogenei possono sembrare difficili da proteggere con un approccio Zero Trust, ma i prodotti ThreatLocker si adattano a qualsiasi contesto, distribuendo gli agenti con la stessa semplicità su dispositivi cloud e hardware fisici, su Windows, macOS e Linux. Mentre gli agenti ThreatLocker applicano i controlli Zero Trust sugli endpoint on-premise e cloud, ThreatLocker Cloud Control estende la copertura all'infrastruttura Microsoft 365: tentativi di connessione e autenticazione al tenant cloud vengono monitorati e bloccati salvo che non provengano da indirizzi esplicitamente attendibili.

Le diverse aree aziendali hanno esigenze di sicurezza differenti.

La struttura organizzativa può complicare qualsiasi implementazione tecnologica trasversale. Un'area di business potrebbe non aver bisogno delle stesse protezioni Zero Trust di un'altra. Un cliente di un MSP potrebbe voler gestire autonomamente il proprio stack di sicurezza, mentre un altro preferisce delegarlo completamente.

Un approccio efficace consiste nel definire confini logici chiari tra i reparti, limitando i controlli di sicurezza ai dispositivi, agli utenti e ai domini di ciascuno.

Come aiuta ThreatLocker

ThreatLocker gestisce qualsiasi framework organizzativo separando prodotti, policy e modalità di fatturazione Zero Trust su tutti i confini logici necessari alla rete. A supporto di ogni tipo di organizzazione, la piattaforma mette a disposizione migliaia di definizioni di applicazioni native per Windows, macOS e Linux, in grado di adattarsi a qualsiasi ambiente applicativo.

È possibile mantenere la conformità agli obblighi normativi?

I framework e le normative di compliance contengono spesso indicazioni molto specifiche su come soddisfare i requisiti di sicurezza inclusi. Le organizzazioni non possono permettersi di uscire dalla conformità, ma i principi dello Zero Trust sono pienamente compatibili con queste richieste.

Essendo all'avanguardia nella moderna architettura di sicurezza, l'adozione dello Zero Trust avvicina concretamente una rete alla conformità normativa, anche rispetto ai controlli tradizionali. Lo Zero Trust supporta per natura le

aspettative più comuni dei framework di compliance: verifica continua degli accessi, minimo privilegio e controllo degli accessi sono requisiti trasversali alla maggior parte delle normative di sicurezza vigenti.

Come aiuta ThreatLocker

Le protezioni Zero Trust offerte da ThreatLocker supportano la conformità a decine di diversi framework di sicurezza e la piattaforma è presente nel marketplace FedRAMP del governo federale statunitense.

Come convincere il management aziendale?

Il consenso della leadership è una sfida raramente considerata in fase di pianificazione, ma con conseguenze significative sull'intero progetto. Alcune iniziative non superano nemmeno la fase di proposta senza riuscire a coinvolgere i giusti interlocutori ai vertici. I principali stakeholder e i responsabili dei budget potrebbero chiedersi: "Perché investire in Zero Trust se non abbiamo mai subito una violazione?"

La domanda non è se si verrà colpiti, ma quando. Proteggere la rete ora costa molto meno che rimediare ai danni in seguito. In materia di cybersecurity, la protezione va inquadrata come un investimento: adottare lo Zero Trust equivale a ridurre i costi, migliorare la reputazione aziendale e rafforzare la fiducia dei clienti.

Come aiuta ThreatLocker

ThreatLocker ha semplificato le conversazioni con il management grazie al valore tangibile portato ai propri clienti, testimoniato da una riduzione pressoché totale degli incidenti di sicurezza gestibili. Questo report di Forrester illustra il ROI concreto raggiungibile dalle aziende dopo il

deployment delle protezioni Zero Trust di ThreatLocker.

Il cambiamento di mentalità: l’ultimo ostacolo

Per molti responsabili IT e di sicurezza, l’ostacolo più grande verso lo Zero Trust non è il deployment degli agenti: è lasciarsi alle spalle il modello di sicurezza che hanno padroneggiato nel corso dell’intera carriera. Cambiare è difficile, e ci vuole coraggio per trovare la volontà di adattarsi. ThreatLocker rende semplice il passaggio allo Zero Trust: spetta all’organizzazione prendere la decisione.

Scopri come ThreatLocker può semplificare la transizione verso lo Zero Trust con una prova gratuita di 30 giorni.

A cura di Justin Leonard, Technical Writer

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/zero-trust-security-threatlocker/