E-book

Quattro motivi per cui firewall e VPN espongono le organizzazioni a violazioni

I problemi di oggi derivano dalle soluzioni di ieri

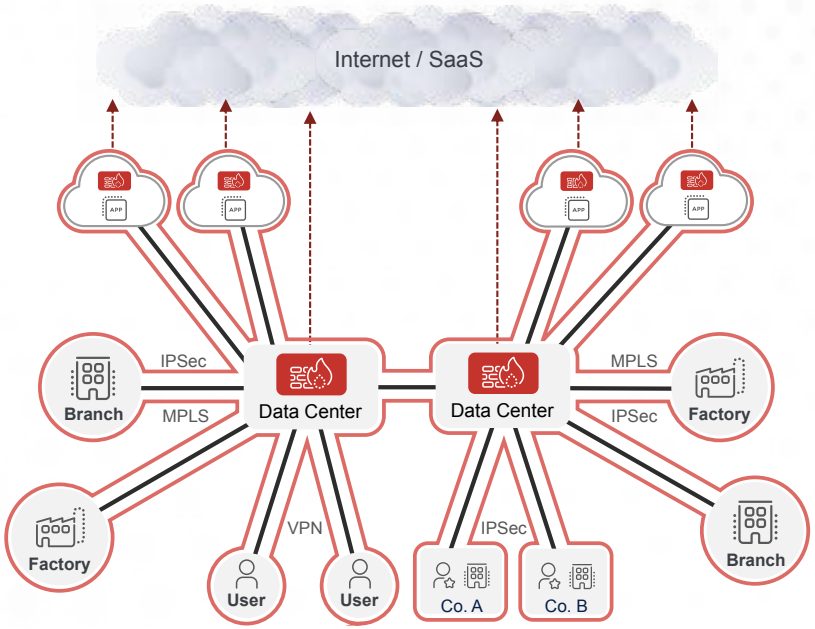
I firewall e le VPN espongono le organizzazioni alle violazioni. Può sembrare assurdo, dato che essi sono gli strumenti di sicurezza di riferimento ormai da decenni, ma il problema è proprio questo: sono stati progettati in un'epoca in cui il lavoro veniva svolto in modo molto diverso da oggi.
In passato, gli utenti e le app risiedevano on-premise (presso la sede principale o in una filiale) e le attività di sicurezza si concentravano sulla creazione di un perimetro attorno alla rete che li collegava. In altre parole, la rete "hub-and-spoke" era difesa da un modello di sicurezza di tipo "castle-and-moat".

Questo approccio viene chiamato in diversi modi, tra cui architettura basata sul perimetro, architettura incentrata sulla rete e architettura tradizionale o legacy. Indipendentemente dal nome, esso implica l'uso di strumenti come firewall e VPN, che vengono implementati nel tentativo di proteggere la rete tenendo fuori le entità dannose e ammettendo quelle legittime.

Le organizzazioni si sono evolute rapidamente negli ultimi anni, in gran parte a causa della pandemia di COVID-19. Per riuscire a preservare la propria produttività nel corso del 2020, esse hanno dovuto accelerare i tempi della trasformazione digitale, spostando le app nel cloud e consentendo ai lavoratori di essere operativi da remoto. Tuttavia, questa evoluzione non è compatibile con i firewall, le VPN e le architetture basate sul perimetro su cui si basavano questi strumenti, semplicemente perché non si può costruire un perimetro di sicurezza attorno a una rete estesa a un numero sempre maggiore di utenti, dispositivi, app e cloud off-premise.

Le organizzazioni che continuano ad affidarsi a un'architettura legacy nel mezzo della trasformazione digitale si trovano ad affrontare numerose sfide in termini di complessità, rigidità, costi e produttività. Per di più, questo modello incrementa il rischio informatico ed espone le organizzazioni al pericolo di subire violazioni attraverso le quattro modalità che verranno illustrate nelle pagine a seguire.

L'architettura incentrata su firewall e VPN



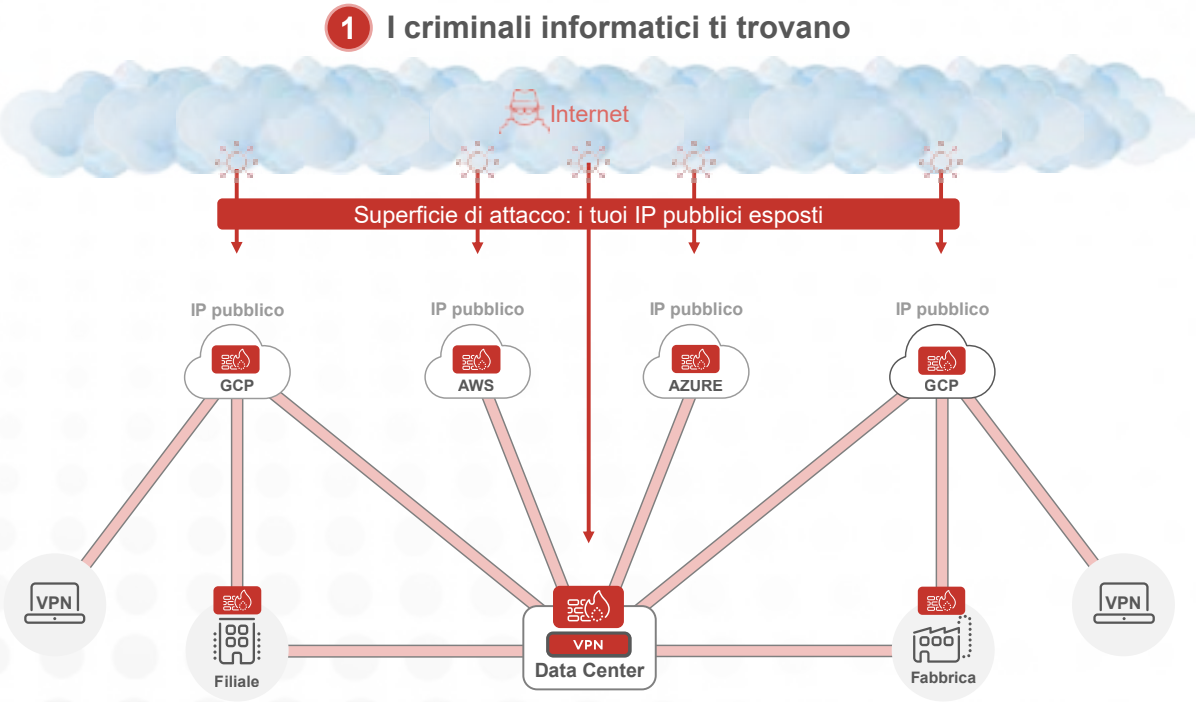
Una rete attendibile connette utenti, siti e app. La protezione dalle minacce e dei dati si concentra sulla protezione della rete.

#1 Firewall e VPN estendono la superficie di attacco

I criminali informatici sono costantemente alla ricerca di obiettivi da attaccare per penetrare le difese delle organizzazioni e portare a termine i loro piani. Purtroppo, non essendo adatte al modo di lavorare di oggi, le architetture basate sul perimetro estendono la superficie di attacco e permettono inavvertitamente agli aggressori di identificare obiettivi per loro interessanti.

Come accennato in precedenza, continuare a utilizzare una rete hub-and-spoke nel mondo moderno implica l'estensione costante di tale rete a un numero crescente di utenti in remoto, dispositivi, risorse con base cloud, filiali e altro. Una rete piatta e tentacolare è un tesoro di risorse interconnesse in continua espansione, e ci sono molte strade (app cloud, utenti in remoto ecc.) che i criminali informatici possono intraprendere per guadagnare punti di ingresso. In pratica, una rete che continua a espandersi si traduce in una superficie di attacco a sua volta in costante crescita.

Ecco in che modo le architetture basate su firewall e VPN aumentano i rischi



Purtroppo, i problemi legati alla superficie di attacco delle architetture basate sul perimetro vanno ben oltre quanto descritto in precedenza, e questo è dovuto ai firewall e alle VPN. Questi strumenti sono i mezzi attraverso cui i modelli di sicurezza di tipo "castle-and-moat" dovrebbero difendere le reti hub-and-spoke, ma il loro utilizzo genera conseguenze indesiderate.

Firewall e VPN hanno indirizzi IP pubblici che possono essere trovati sulla rete Internet pubblica per fare in modo che gli utenti legittimi e autorizzati possano accedere alla rete tramite il web, interagire con le risorse connesse al suo interno e svolgere il proprio lavoro. Tali indirizzi IP pubblici, però, possono essere trovati anche da utenti malintenzionati alla ricerca di obiettivi da attaccare per ottenere l'accesso alla rete.

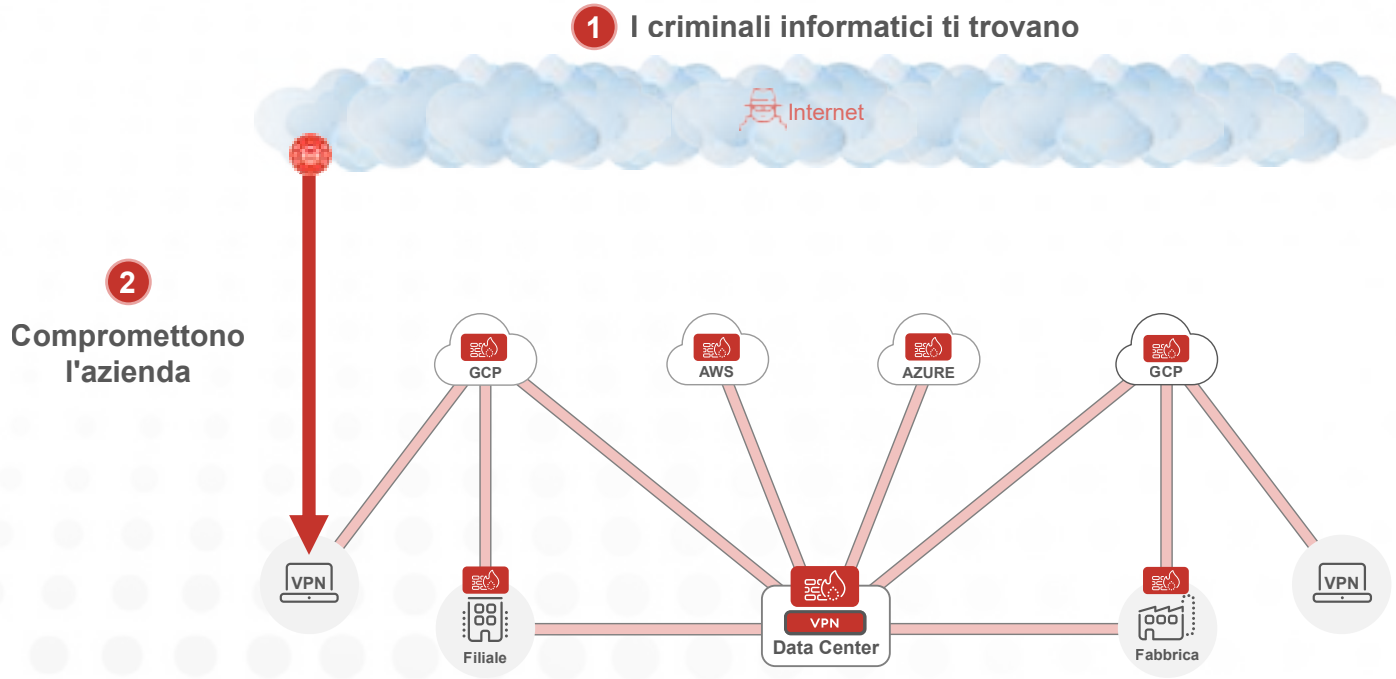
In altre parole, firewall e VPN forniscono ai criminali informatici più vettori di attacco, estendendo la superficie esposta dell'organizzazione. Paradossalmente, questo significa che la strategia standard basata sull'implementazione di ulteriori firewall e VPN per migliorare la scalabilità e la sicurezza, in realtà aggrava ulteriormente il problema ed estende ancora di più la superficie di attacco.

#2 I firewall e le VPN non sono in grado di prevenire le compromissioni

Una volta identificato con successo un obiettivo interessante, i criminali informatici lanciano i loro attacchi informatici nel tentativo di penetrare le difese dell'organizzazione. Purtroppo, ancora una volta, gli strumenti tradizionali come firewall e VPN non sono adatti a proteggere le imprese da questa fase della catena di attacco.

Per prevenire la compromissione è necessario l'uso di policy di sicurezza inline che blocchino le minacce in tempo reale, prima che possano entrare nell'ambiente di un'organizzazione e iniziare a causare danni. Per questo motivo, le organizzazioni devono essere in grado di ispezionare tutto il traffico delle loro operazioni in modo da poter identificare eventuali minacce. La capacità di ispezionare il traffico cifrato è quindi di fondamentale importanza, perché la stragrande maggioranza del traffico web di oggi, per esattezza oltre il 95%, è cifrata. Ma è proprio qui che sorge un problema legato a un ulteriore punto debole dell'architettura basata su firewall e VPN.

Ecco in che modo le architetture basate su firewall e VPN aumentano i rischi



L'ispezione del traffico cifrato è un processo che necessita di un ingente quantitativo di risorse, ed è quindi necessaria una notevole quantità di potenza di calcolo per decifrare, esaminare e cifrare nuovamente il traffico. I dispositivi di sicurezza come i firewall, però, faticano a svolgere questo compito a dovere, sia che vengano distribuiti come hardware on-premise o come dispositivi virtuali in un'istanza cloud.

Questi apparecchi dispongono infatti di capacità fisse per garantire un determinato livello del servizio, e non sono in grado di adattare le proprie prestazioni per soddisfare i requisiti sempre crescenti di un'organizzazione e riuscire a ispezionare il traffico in tempo reale, in particolare quando si tratta di traffico cifrato. Di conseguenza, nello scenario migliore, le realtà che si affidano a strumenti e architetture tradizionali si ritrovano con un'ispezione del traffico cifrato incompleta, e in quello peggiore, senza alcuna ispezione di questo tipo.

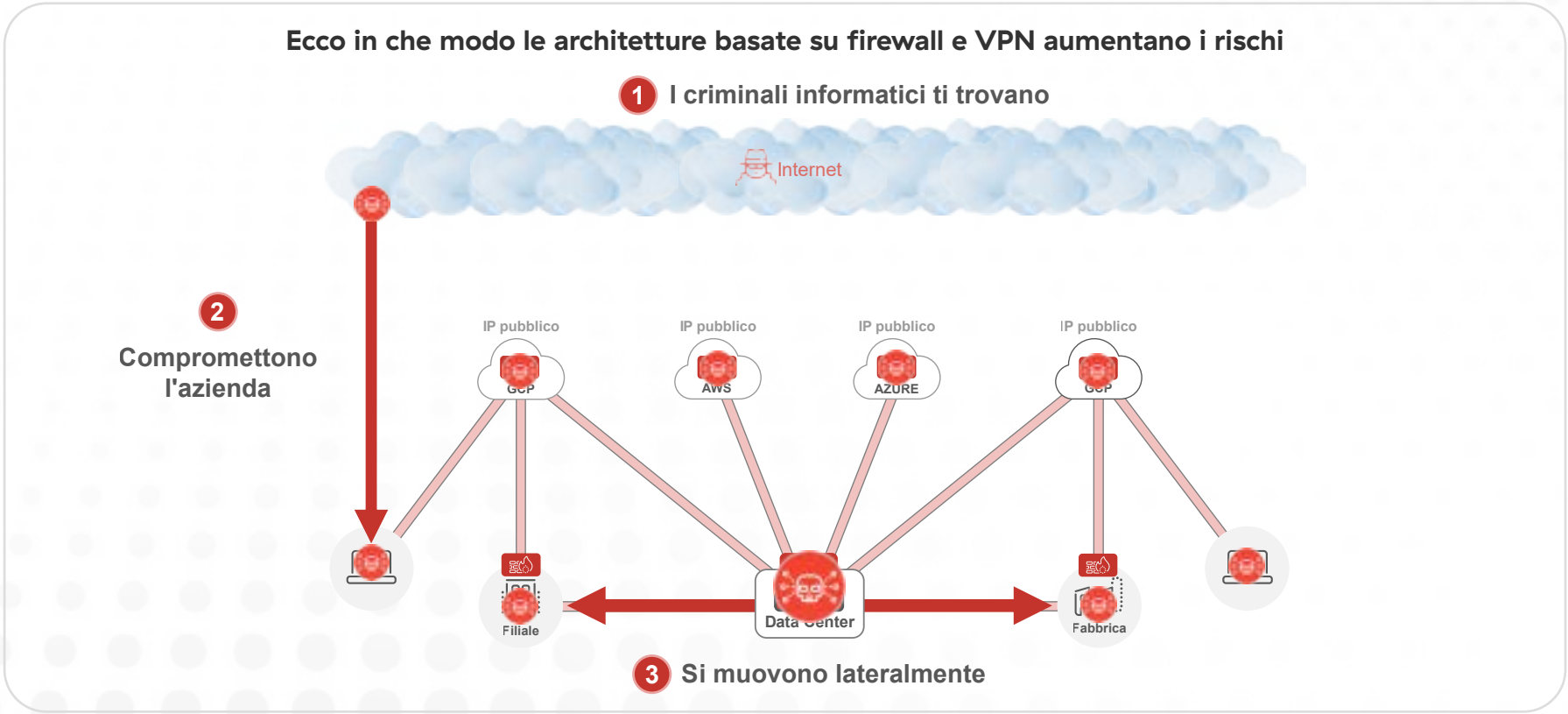
La mancata ispezione del traffico cifrato su larga scala consente alle minacce in grado di oltrepassare le difese senza essere rilevate e agli aggressori di portare a termine i propri piani. Gli utenti malintenzionati sono a conoscenza di questo, e hanno iniziato a utilizzare il traffico cifrato come mezzo principale per lanciare i loro attacchi. Oggi, circa l'86% degli attacchi informatici si nasconde nel traffico cifrato; quindi, senza un'ispezione completa non è possibile fermare la stragrande maggioranza delle minacce che tentano di violare le difese. In sintesi, le architetture basate su firewall e VPN non sono in grado di prevenire le compromissioni.

#3

I firewall e le VPN consentono il movimento laterale delle minacce

Se una minaccia informatica supera le difese di un'organizzazione, i punti deboli dei firewall e delle VPN sono evidenti. Il movimento laterale delle minacce, noto anche come propagazione laterale, si riferisce al modo attraverso cui le minacce presenti sulla rete riescono ad accedere alle varie risorse dell'organizzazione, siano esse applicazioni on-premise, workload su cloud privati o istanze di applicazioni SaaS. Quando una minaccia viola il perimetro di un'organizzazione, è raro che sia una sola applicazione a essere compromessa. Per comprendere il modo in cui si attua il movimento laterale di una minaccia, possiamo considerare l'analogia contenuta nell'espressione "sicurezza di tipo castle-and-moat" (ossia "castello e fossato").

Il fossato viene infatti utilizzato per difendere un castello e impedire agli aggressori di accedervi al fine di proteggere le risorse preziose e le persone al suo interno. Se gli aggressori riescono a superare il fossato, il meccanismo di difesa principale del castello risulta inutile e i nemici sono liberi di saccheggiare l'intera roccaforte.



La stessa debolezza è presente quando si utilizzano firewall e VPN. Questo è dovuto alla natura altamente interconnessa delle reti hub-and-spoke che alcune organizzazioni ancora usano e al fatto che il principale strumento su cui si fondano questi modelli di sicurezza è la difesa dell'accesso alla rete.

I firewall possono quindi essere considerati il fossato, le VPN il ponte levatoio e la rete stessa il castello da proteggere. Se una minaccia informatica supera il fossato ed entra nel castello, l'utente malintenzionato può facilmente spostarsi da una risorsa connessa all'altra accedendo alle varie stanze dell'edificio.

Firewall e VPN consentono quindi il movimento laterale delle minacce e permettono ai criminali informatici di estendere la portata delle violazioni attraverso la rete, causando pesanti danni, gravi interruzioni e costi ingenti. La compromissione colpisce ogni cosa. Anche se la segmentazione della rete viene spesso presentata come la soluzione al problema, questa tattica comporta inevitabilmente l'acquisto di sempre più firewall e non tiene conto dei problemi architetturali insiti negli strumenti legacy basati sul perimetro.

#4 I firewall e le VPN espongono alla perdita dei dati

Nella stragrande maggioranza degli attacchi informatici, gli utenti malintenzionati non cercano di violare le organizzazioni solo per il gusto di farlo. Al contrario, hanno in mente un obiettivo specifico: rubare informazioni sensibili. I dati rubati possono infatti essere venduti sul dark web in cambio di profitti cospicui o utilizzati in uno schema a doppia estorsione per spingere le organizzazioni a pagare un riscatto. In ogni caso, le ripercussioni possono essere catastrofiche per qualsiasi organizzazione.

Quindi, se i criminali informatici individuano una superficie di attacco, compromettono le difese e avviano il movimento laterale (tutte e tre queste azioni rese possibili da firewall e VPN), cercheranno in seguito il maggior numero di dati possibile nella rete, dando priorità alle informazioni particolarmente sensibili o sottoposte a normative. Naturalmente a questo segue l'esfiltrazione dei dati.

Affidarsi a strumenti tradizionali per fermare questo anello finale della catena di attacco produce ancora una volta risultati rischiosi e consente la perdita dei dati.

Ecco in che modo le architetture basate su firewall e VPN aumentano i rischi

Come accennato in precedenza, oggi oltre il 95% del traffico web è cifrato, l'ispezione richiede una grande potenza di calcolo e le apparecchiature statiche non sono in grado di garantire la scalabilità necessaria per elaborare gli enormi volumi di traffico cifrato generati da organizzazioni in continua crescita. Questo problema (sia per l'hardware che per le apparecchiature virtuali) è rilevante non solo per le potenziali compromissioni, ma anche in relazione alla perdita dei dati. I criminali informatici sono consapevoli che le probabilità che vi siano punti ciechi sul traffico cifrato delle organizzazioni sono molto elevate, e proprio per questo è la principale via che utilizzano per l'esfiltrazione.

Non è solo a causa del problema della scalabilità che strumenti come i firewall non sono in grado di fermare l'esfiltrazione dei dati. Le tecnologie di tipo legacy sono state progettate per una realtà ormai passata in cui le app non erano sul cloud e i lavoratori non operavano da remoto. Di conseguenza, non sono in grado di proteggere i percorsi moderni attraverso cui si verifica la perdita di dati, per esempio la funzionalità di condivisione integrata nelle applicazioni SaaS come Google Drive, Box, Microsoft OneDrive e altre. Allo stesso modo, le risorse cloud configurate in modo errato, come i bucket AWS S3 impostati erroneamente su "pubblico", espongono i dati e non possono essere corrette con firewall, VPN o strumenti convenzionali per la prevenzione della perdita dei dati (DLP).

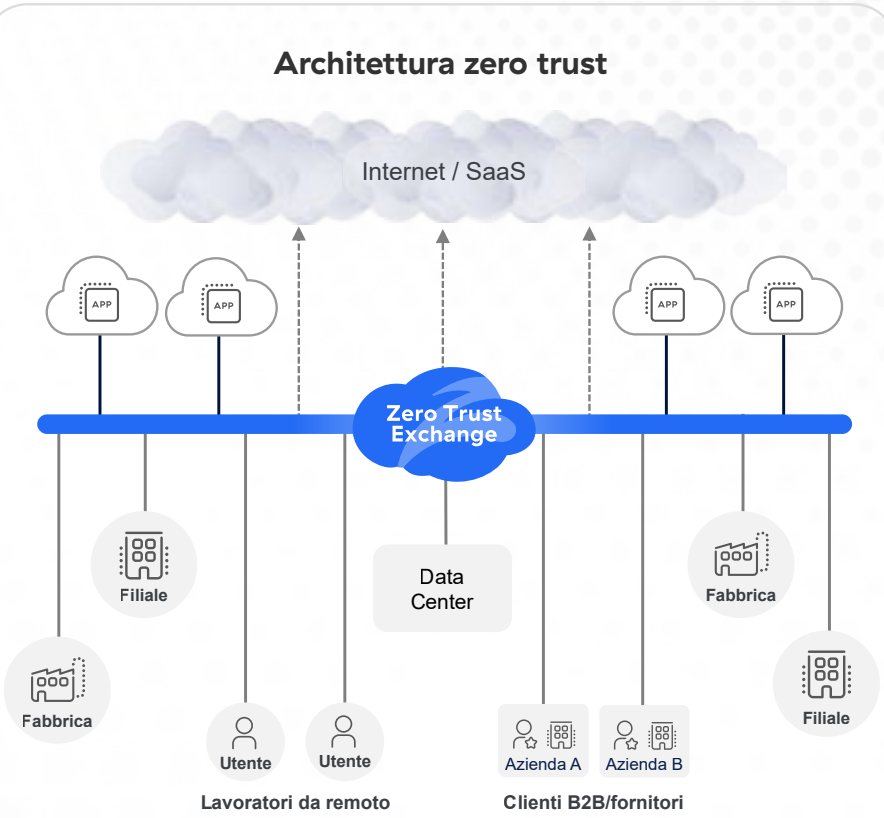
Gli aggressori esterni cercano di utilizzare questi e altri mezzi per rubare informazioni sensibili, ma è fondamentale ricordare che essi non rappresentano l'unica minaccia ai dati. Le organizzazioni devono fare i conti con la possibilità che anche eventuali utenti interni malintenzionati o negligenti possano far trapelare informazioni sensibili. Indipendentemente da chi sia l'aggressore, la sicurezza deve evolversi per garantire la protezione dei dati.

L'architettura zero trust è la risposta a tutti questi problemi

Lo zero trust non è solo un altro strumento incentrato sulla rete da aggiungere allo stack esistente. Non si tratta di un prodotto che si limita a ridurre i problemi delle architetture basate sul perimetro senza risolvere in concreto le cause sottostanti. Al contrario, lo zero trust è un'architettura a sé stante e basata sul principio dell'accesso a privilegi minimi, che si contraddistingue in modo radicale da un'architettura standard basata su firewall e VPN.

Adottando un'architettura zero trust, le organizzazioni possono ottenere una sicurezza sul cloud a livello globale che agisce come un centralino intelligente, connettendo in modo sicuro utenti, workload, dispositivi IoT/OT e partner B2B, senza estendere mai la rete a niente e nessuno. Allo stesso tempo, il cloud zero trust offre suite complete di soluzioni (come la protezione contro le minacce informatiche e la tutela dei dati) fornite come servizio all'edge, il più vicino possibile all'utente finale.

Con lo zero trust, la sicurezza e la connettività vengono separate dalla rete, e le architetture basate sul perimetro diventano un lontano ricordo del passato.



Le policy aziendali determinano chi può accedere a cosa su qualsiasi rete, e quest'ultima è solamente il mezzo di trasporto.

Con questa architettura moderna, le organizzazioni possono rimediare definitivamente ai quattro modi in cui firewall e VPN le espongono alle violazioni:

- **Riduzione al minimo della superficie di attacco:** usa lo zero trust per fermare l'estensione infinita della rete, eliminare firewall, VPN e i relativi IP pubblici, impedire le connessioni in entrata e nascondere le app dietro a un cloud zero trust.
- **Blocco delle compromissioni:** ispeziona tutto il traffico, incluso quello cifrato, sfruttando un cloud zero trust ad alte prestazioni che identifica le minacce e applica le policy di sicurezza in tempo reale.
- **Prevenzione del movimento laterale delle minacce:** connetti utenti, workload e dispositivi direttamente alle app, e non alla rete nel suo complesso, adottando il principio dell'accesso a privilegi minimi.
- **Blocco della perdita dei dati:** blocca la perdita dei dati a livello generale, sia attraverso il traffico cifrato che tutti gli altri percorsi, e tutela i dati inattivi sul cloud e quelli in uso sui dispositivi endpoint dei dipendenti.

Oltre a ridurre il rischio di violazioni, un'architettura zero trust riduce la complessità, incrementa la produttività degli utenti, fa risparmiare denaro e migliora il dinamismo dell'organizzazione, risolvendo una serie di problemi che affliggono le architetture basate su firewall e VPN.

Conclusione

Per coloro che necessitano di un'architettura zero trust, la scelta giusta è la piattaforma basata sull'IA Zscaler Zero Trust Exchange. Trattandosi del security cloud inline più grande e più diffuso al mondo, la sua portata e il suo successo parlano da soli:

Oltre 150
Data center globali

Oltre 360 MLD
Transazioni protette ogni giorno

Oltre 500 BLN
Segnali di telemetria ogni giorno

Oltre 70
Net Promoter Score

40%
percentuale delle aziende Fortune 500 che serviamo

Leader
Nel Gartner MQ per l'SSE

Per saperne di più, registrati al nostro webinar mensile, "Inizia da qui: un'introduzione allo zero trust". In questo webinar, illustreremo l'architettura zero trust in modo semplice per i meno esperti e condivideremo maggiori informazioni su Zscaler, per far sì che tutti abbiano gli strumenti per iniziare il proprio percorso verso lo zero trust in sicurezza.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su X (precedentemente Twitter) **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.it