E-BOOK

In che modo le SD-WAN tradizionali permettono gli attacchi ransomware e come fermarli

Introduzione

Le sfide legate alla sicurezza sono aumentate costantemente, ma le architetture di rete non si sono evolute abbastanza rapidamente per rimanere al passo. Secondo il Report sui ransomware del 2024 di Zscaler ThreatLabz, si è registrato un aumento record nei pagamenti dei riscatti e un incremento del 58% su base annua nel numero di aziende che hanno subito estorsioni. Il ransomware si diffonde rapidamente nelle organizzazioni per una ragione semplice: le reti tradizionali (legacy) si basano su una fiducia implicita verso tutto ciò che è connesso, consentendo ai ransomware di muoversi liberamente dai dispositivi infetti negli uffici remoti fino alle applicazioni più critiche dell'azienda.

In passato, le organizzazioni si affidavano a un modello di sicurezza di tipo "castle-and-moat", che significa "a castello e fossato", in cui tutto il traffico all'interno della rete era considerato sicuro automaticamente e i controlli di sicurezza venivano applicati solo al perimetro. Man mano che le organizzazioni sono diventate più distribuite e incentrate sul cloud, hanno semplicemente esteso le loro reti private a filiali e cloud utilizzando SD-WAN (Software-Defined Wide Area Network) e VPN da sito a sito. Si sono così create grandi reti ritenute affidabili in cui gli aggressori possono muoversi lateralmente nonostante il gran numero di firewall distribuiti ovunque.

Nel frattempo, il numero di dispositivi IoT presenti nelle reti continua a crescere. Si stima che 55,7 miliardi di questi dispositivi saranno connessi alle reti aziendali entro il 2025, generando 80 miliardi di zettabyte di dati ogni anno,[1] con un'espansione del perimetro digitale che crea una superficie di attacco sempre più ampia e rende le organizzazioni più vulnerabili. Tutte queste tendenze fanno sì che gli approcci alla sicurezza basati sul perimetro siano sempre più inadatti. Di conseguenza, anno dopo anno, il numero (e il costo) delle violazioni dei dati continua ad aumentare e l'attività dei ransomware continua a crescere.

Per proteggere la propria infrastruttura da queste crescenti minacce, le organizzazioni di tutti i settori stanno adottando sempre più spesso un approccio per la sicurezza informatica.

Aumento del 17,8% degli attacchi ransomware dal 2023 al 2024.[2]

75 milioni di dollari: il risarcimento record per un attacco ransomware segnalato nel 2024.[2]

Aumento del 104% del numero di vittime di violazioni dei dati dal 2023 al 2024.[3]

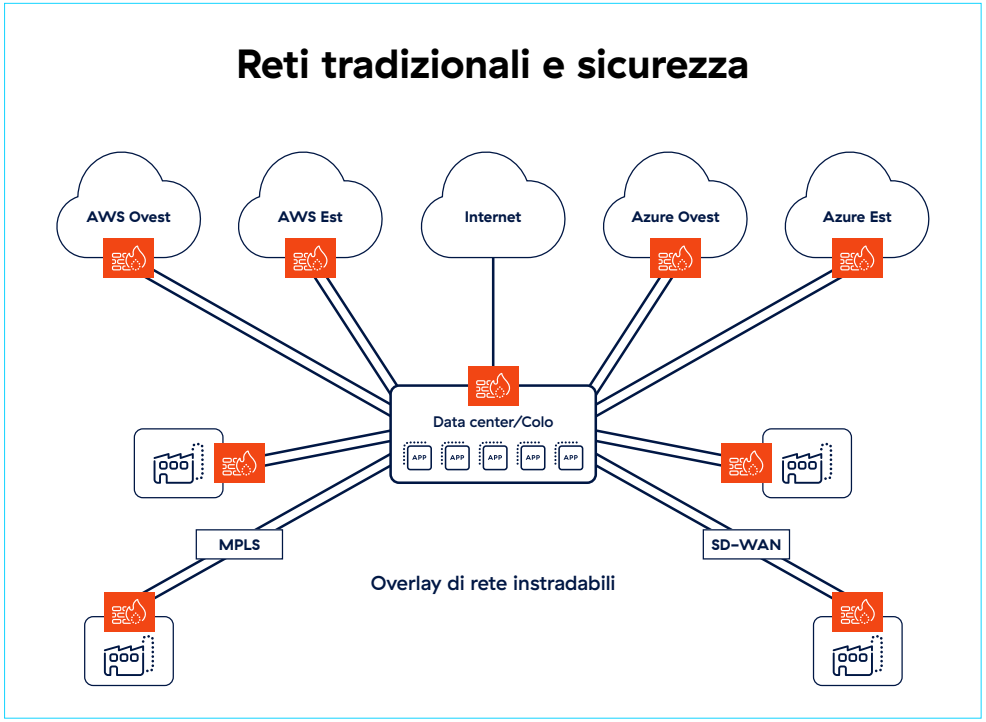
Il costo medio globale di una violazione dei dati ha raggiunto il massimo storico di **4,88 milioni di dollari** nel 2024.[4]

1: IDC Research, Future of Industry Ecosystems: Shared Data and Insights, 2021.
2: Zscaler ThreatLabz 2024 Ransomware Report.
3: Identity Theft Resource Center, H1 2024 Data Breach Analysis.
4: IBM, Cost of a Data Breach Report 2024.

Cos'è e cosa non è la SD-WAN tradizionale.

La SD-WAN utilizza l'automazione per instradare il traffico di rete sul percorso più efficiente attraverso diversi servizi di trasporto e infrastrutture di rete. I protocolli di routing basati sulle applicazioni migliorano le prestazioni di queste ultime assegnando la priorità al traffico tra le app critiche.

Le soluzioni SD-WAN tradizionali estendono semplicemente la rete aziendale alle filiali e ai data center. Progettata per semplificare la connettività, la tecnologia SD-WAN consente ai dispositivi presenti in qualunque luogo, tra cui filiali, stabilimenti e siti terzi, di comunicare con le app nel data center o nel cloud pubblico. Costituite da una rete di dispositivi e VPN site-to-site, queste architetture offrono una protezione minima, se non nulla, contro il movimento laterale delle minacce e i ransomware.



Abilita lo spostamento laterale delle minacce e facilita gli attacchi ransomware

Espande la superficie di attacco a filiali, stabilimenti e cloud

Aumenta i costi, la complessità e i tempi di distribuzione

Le SD-WAN sono state progettate per migliorare la connettività, rendendo più rapido e semplice l'accesso alle risorse da parte degli utenti. Ma connettività non è sinonimo di sicurezza. Al contrario, un approccio zero trust richiede che l'identità e lo stato di sicurezza vengano verificati prima di consentire la connettività. La fiducia implicita delle reti legacy non fa che renderle più difficili da proteggere, agevolando la rapida diffusione dei ransomware.

Per raggiungere lo zero trust su una SD-WAN tradizionale, un'organizzazione deve implementare ulteriori dispositivi di sicurezza, strumenti e punti di applicazione delle policy. Il risultato è un mosaico di firewall, mesh di VPN e altri strumenti, come il controllo degli accessi alla rete (NAC), le soluzioni di sicurezza DNS, ecc. Questa architettura è complessa e la sua gestione richiede risorse finanziarie e umane eccessive.

> La connettività basata sulla fiducia automatica è in contrasto con il modello zero trust "

Che cos'è lo zero trust?

Lo zero trust è una strategia di sicurezza che si fonda sul concetto che nessuna entità (utente, app, servizio o dispositivo) deve essere considerata attendibile automaticamente. Segue inoltre il principio dell'accesso a privilegi minimi e, prima di autorizzare una connessione, l'attendibilità viene vagliata considerando il contesto e il profilo di sicurezza dell'entità, quindi costantemente rivalutata per ogni nuova connessione, anche per le entità già autenticate in precedenza.

I primi passi con lo zero trust

Partire da una rete aperta e lineare e aggiungere punti di applicazione econtrolli di sicurezza per ottenere un modello zero trust è un'operazione complessa e costosa dal punto di vista operativo. I progetti di segmenta-zione della rete durano mesi o addirittura anni, e spesso irequisiti cambiano prima che essi vengano completati. E se invece procedessi al contrario? Se le tue filiali potessero essere ambienti più semplici, senza una rete instradabile che le collega alle applicazioni aziendali nel cloud?

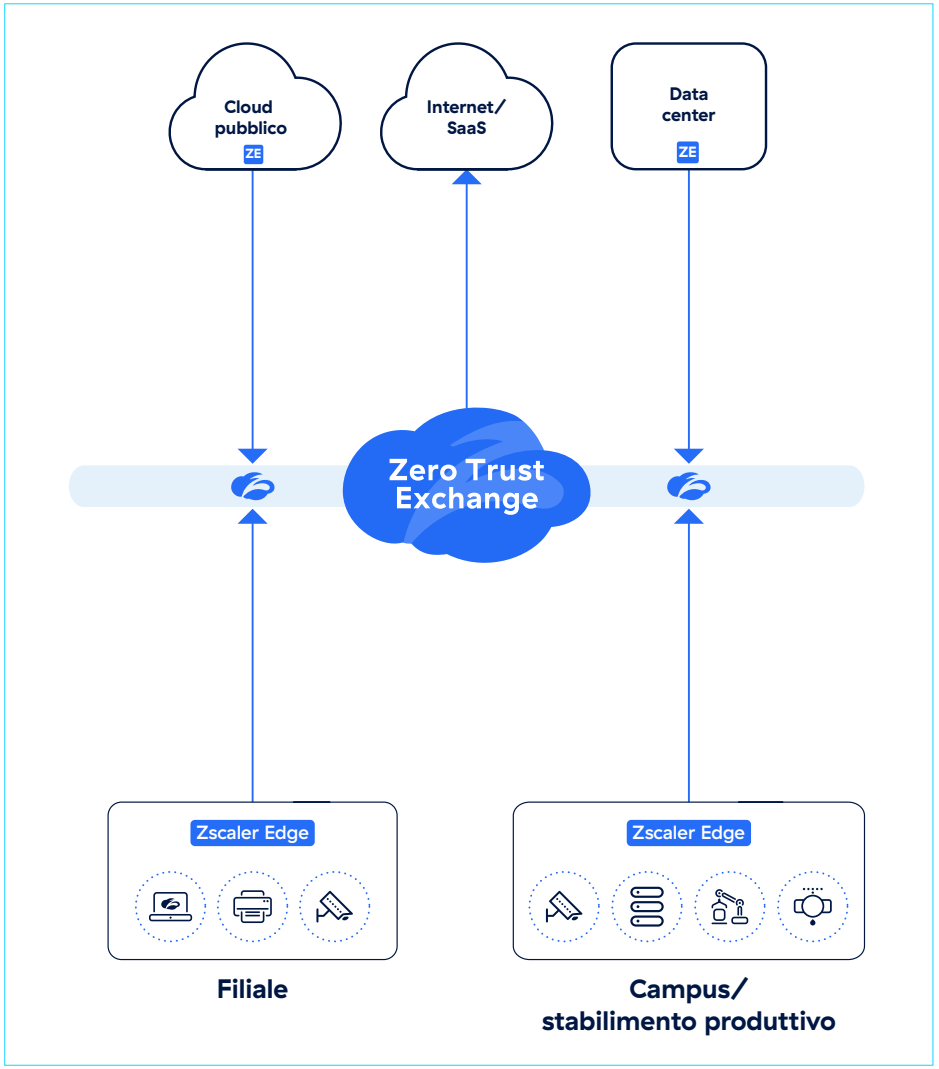
Utenti e dispositivi vengono collegati alle applicazioni in base alle policy, non in base alla presenza in rete, garantendo al contempo una sicurezza solida e la semplicità operativa.

Si tratta di un approccio nativo di tipo zero trust che rende impossibile il movimento laterale, poiché utenti e dispositivi (inclusi i dispositivi IoT e OT) non sono mai direttamente connessi alle applicazioni. La comunicazione avviene tramite la piattaforma Zscaler Zero Trust Exchange™, che facilita la protezione completa dei dati e la difesa dalle minacce informatiche con solidi controlli di accesso basati sull'identità e sul contesto.

> Zero Trust SD-WAN è un nuovo modo per fornire alle filiali e ai data center un accesso rapido e affidabile a Internet, applicazioni private e servizi cloud senza dover estendere la rete aziendale ovunque."

Questo approccio zero trust:

- **Migliora le prestazioni delle applicazioni.**
  Le aziende possono sostituire le complesse VPN site-to-site con una semplice architettura direct-to-cloud che offre prestazioni rapide e costanti per supportare la produttività.
- **Riduce al minimo la superficie di attacco di Internet.**
  Le soluzioni WAN legacy espongono le porte VPN all'Internet pubblica, lasciando la rete vulnerabile agli attacchi. Con Zero Trust SD-WAN, le applicazioni sono protette da Zero Trust Exchange e non possono essere rilevate o attaccate da Internet.
- **Impedisce lo spostamento laterale delle minacce.**
  Le VPN site-to-site creano una grande rete instradabile in cui un malware può essere trasmesso da un singolo dispositivo a tutto ciò che è presente sulla rete. Con Zero Trust SD-WAN, le connessioni vengono effettuate direttamente alle applicazioni, non alla rete; in questo modo, lo spostamento laterale è impossibile.
- **Riduce i costi e la complessità.**
  Questo approccio elimina la necessità di più firewall, VPN, NAC e altre soluzioni stratificate. Il risultato èun'architettura più semplice, meno costosa e molto più facile da configurare e gestire.



Zscaler affronta e risolve le sfide della tradizionale SD-WAN

Affidandosi a Zero Trust Exchange per connettere in modo sicuro filiali, stabilimenti e data center, Zscaler garantisce un accesso zero trust uniforme e coerente per tutti gli utenti, i dispositivi IoT/OT e le applicazioni.

	SD-WAN zero trust	SD-WAN tradizionale
Riduce la superficie di attacco e arresta il movimento laterale delle minacce	Sì	No
Riduce la complessità delle regole per firewall e ACL	Sì	No
Elimina i compromessi tra sicurezza e prestazioni	Sì	No
Elimina la necessità di firewall nella filiale	Sì	No

La flessibilità di Zscaler Zero Trust SD-WAN permette di supportare più opzioni di distribuzione che non richiedono una sostituzione completa. Può funzionare insieme all'infrastruttura SD-WAN esistente della tua filiale esistente e creare overlay zero trust per Zero Trust Exchange. In questo modo, si garantisce un accesso sicuro e performante dai dispositivi delle filiali alle applicazioni private in altre sedi e nel cloud, senza permettere lo spostamento laterale delle minacce.

Se vuoi adottare un nuovo approccio alle esigenze di connettività della tua organizzazione, inizia con un'architettura zero trust nativa per ridurre la complessità ed eliminare la necessità di aggiungere innumerevoli firewall. Zscaler Zero Trust SD-WAN è in grado di gestire le connessioni ISP e indirizzare in modo intelligente il traffico delle applicazioni, per offrire ai tuoi utenti un'esperienza sicura in modo semplice e proteggere al contempo la tua organizzazione dagli attacchi ransomware.

Ferma gli attacchi ransomware con zero trust

Lo zero trust è fondamentale per affrontare le sfide di sicurezza odierne e ridurre il rischio di attacchi ransomware. Con Zscaler Zero Trust SD-WAN, la tua organizzazione può proteggere tutte le comunicazioni ed eliminare la possibilità di movimento laterale delle minacce, senza incorrere nei costi e nella complessità operativa degli approcci legacy. Inoltre, le ottime esperienze digitali manterranno produttivi e soddisfatti i clienti, i dipendenti e gli altri utenti.

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 di dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la piattaforma di cloud security inline più grande del mondo. Per saperne di più, visita il sito **www.zscaler.com/it**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/it