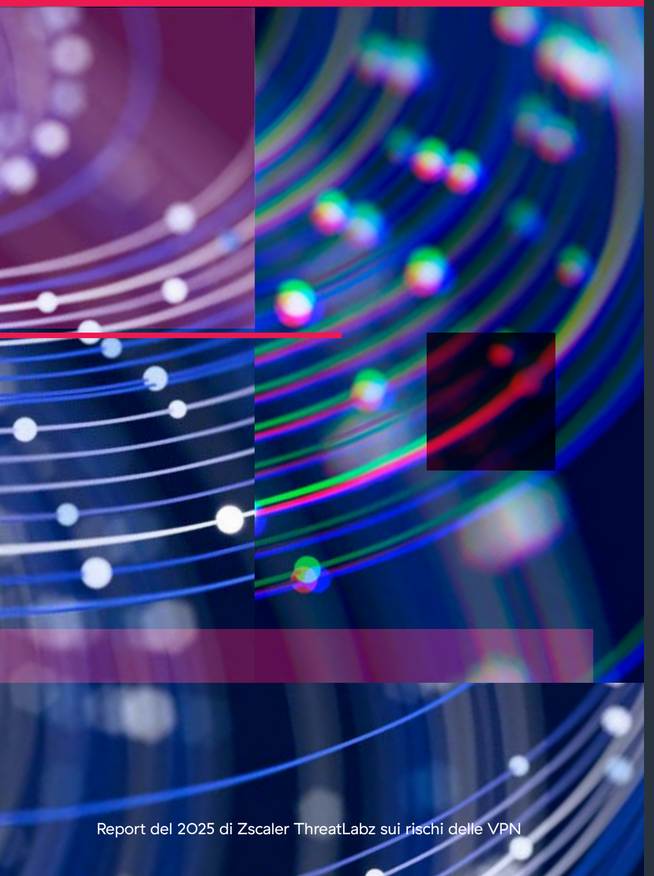
zscaler™ | Cybersecurity INSIDERS

Zscaler Report del 2025 di ThreatLabz sui rischi delle VPN



©2025 Zscaler, Inc. Tutti i diritti riservati.

Indice



Riepilogo esecutivo 3

I risultati principali 4

I rischi delle VPN: perché l'81% delle organizzazioni passerà allo zero trust entro il 2026 5

I problemi di sicurezza delle VPN 6

- L'obsolescenza delle VPN: rischi per la sicurezza e frustrazioni degli utenti 6
- Ransomware e VPN: una tempesta perfetta di rischi 7
- VPN e movimento laterale: l'impatto delle violazioni si estende 8

Le CVE delle VPN dal 2020 al 2025: un'ondata crescente di vulnerabilità molto gravi 9

- Le tendenze principali: tipi di impatto delle CVE 10
- Le tendenze principali: vulnerabilità critiche delle VPN 11

I problemi di sicurezza delle VPN (continua) 13

- Le sfide nell'implementazione della segmentazione 13
- Le VPN intensificano i rischi per la sicurezza informatica delle operazioni di fusione e acquisizione 14
- Accesso VPN di terze parti: una backdoor per gli aggressori 15

Criticità e lacune nelle misure di protezione legacy 16

- Gli strumenti tradizionali lasciano le applicazioni private esposte 16
- Implementazione del NAC negli ambienti VPN: una protezione limitata 17

I problemi della VPN negli ambiti della gestione e dell'esperienza utente 18

- I problemi prestazionali della VPN: utenti frustrati e sovraccarico dell'IT 18
- Gestire le VPN: sovraccarico per i team IT e vulnerabilità che aumentano l'esposizione 19
- Il peso della gestione delle VPN 20
- Controlli di accesso VPN troppo blandi: una falla critica nella sicurezza 21
- Sostituire la VPN: un passo verso l'accesso sicuro 22

L'adozione dello zero trust 23

- Lo zero trust sostituisce la VPN su larga scala 23
- Priorità che portano a scegliere lo zero trust: il lavoro da remoto favorisce l'adozione 24
- I vantaggi principali della sostituzione delle VPN con il modello zero trust 25

Le previsioni sui rischi delle VPN per il 2025 26

Le best practice per l'accesso sicuro 28

- Mitigazione dei rischi delle VPN e rafforzamento della sicurezza zero trust 28

In che modo Zscaler rivoluziona l'accesso sicuro 30

- I principali vantaggi di Zscaler Private Access (ZPA) 31

Metodologia e dati demografici 33

Di 34

©2025 Zscaler, Inc. Tutti i diritti riservati.

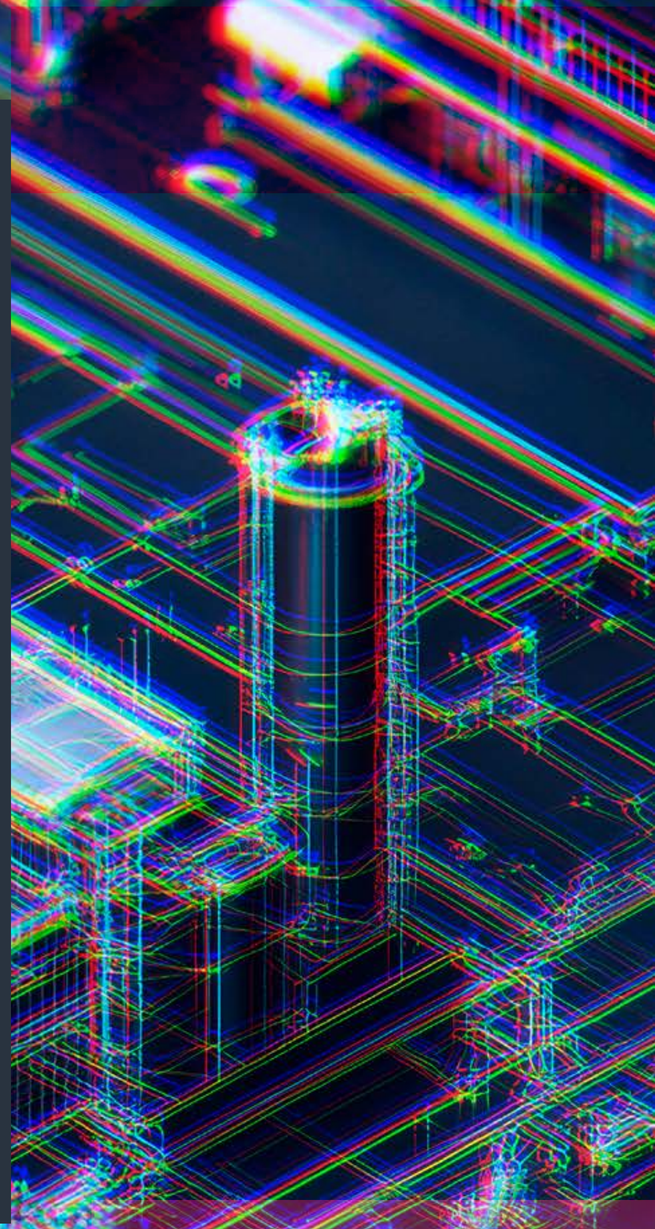
Riepilogo esecutivo

Il report del 2025 di Zscaler ThreatLabz sui rischi delle VPN offre un'analisi incisiva dell'evoluzione dei rischi associati alle reti private virtuali (Virtual Private Network, VPN) e mette in evidenza l'urgente necessità di adottare architetture zero trust, mentre le organizzazioni si impegnano per rendere la sicurezza a prova di futuro. Un tempo considerate la soluzione di riferimento per l'accesso remoto, le VPN sono sempre più prese di mira dalle minacce informatiche, e sono passate da strumenti essenziali a veri e propri generatori di rischi per la sicurezza delle organizzazioni di tutto il mondo. Questo report, che si basa sul contributo di oltre 600 professionisti nel campo dell'IT e della sicurezza, rivela una svolta cruciale nel panorama della sicurezza informatica: solo nell'ultimo anno, oltre la metà delle organizzazioni intervistate ha subito attacchi dovuti alle vulnerabilità delle VPN, un aspetto che evidenza l'urgente necessità di adottare un nuovo approccio negli ambienti di lavoro sempre più ibridi di oggi.

Nel 2025, l'insoddisfazione nei confronti delle VPN tradizionali ha innescato un cambiamento, e le aziende hanno realizzato che correggere le relative vulnerabilità è un'impresa vana. Questa consapevolezza sta favorendo l'adozione diffusa dei modelli zero trust, che promettono un controllo granulare dell'accesso e riducono significativamente i rischi per la sicurezza. In particolare, l'81% delle organizzazioni ha in programma di implementare strategie zero trust entro il 2026, mentre il 65% prevede di eliminare completamente le VPN nello stesso arco di tempo. Inoltre, criticità operative come connessioni lente, disconnessioni frequenti e processi di autenticazione complessi non hanno fatto altro che rimarcare l'urgenza di prendere i dovuti provvedimenti, alimentando un'impennata della domanda di soluzioni zero trust in grado di garantire un accesso fluido e sicuro.

Tutti questi cambiamenti avvengono in un contesto caratterizzato da minacce basate sull'AI, il cui aumento avrà un impatto senza precedenti sulla sicurezza delle VPN. Gli aggressori impiegano sempre di più l'AI per la ricognizione automatizzata delle vulnerabilità delle VPN, che risultano facilmente analizzabili tramite la rete Internet pubblica. Le tecniche come il password spraying intelligente e lo sviluppo rapido di exploit consentiranno agli aggressori di compromettere le credenziali VPN su larga scala. Più in là nella catena di attacco, le tecniche di elusione basate sull'AI renderanno ancora più difficile rilevare in tempo le intrusioni che sfruttano le VPN. Con l'aumento delle minacce basate sull'AI, i rischi per le VPN non faranno che aumentare, spingendo le aziende ad adottare misure di sicurezza proattive e accelerando il passaggio, già marcato, verso soluzioni zero trust.

Riconoscendo questi cambiamenti, il report di ThreatLabz non solo traccia il declino delle VPN, che sono passate dall'essere strumenti indispensabili a diventare veri e propri generatori di rischi, ma fornisce anche spunti pratici per le aziende affinché riescano a orientarsi in questo contesto in continua evoluzione.



©2025 Zscaler, Inc. Tutti i diritti riservati.

I risultati principali

1. **L'obsolescenza delle VPN accelera:**

   Il 65% delle aziende ha intenzione di sostituire i propri servizi VPN entro il prossimo anno, un aumento del 23% rispetto al 2024. Questa tendenza è dovuta principalmente all'incapacità delle VPN di soddisfare le esigenze di sicurezza e conformità delle aziende moderne, evidenziando il loro ruolo nell'esacerbare i rischi, anziché mitigarli.

2. **Escalation degli attacchi informatici che sfruttano le VPN e delle preoccupazioni per i ransomware:**

   Lo scorso anno si è registrato un preoccupante incremento degli incidenti informatici legati alle vulnerabilità delle VPN: il 56% delle organizzazioni ha segnalato di aver subito questo tipo di violazioni, registrando un aumento allarmante rispetto ai numeri degli anni precedenti. Al contempo, il 92% degli intervistati teme che le vulnerabilità non corrette delle VPN possano tradursi direttamente in attacchi ransomware. Questi risultati confermano la tendenza secondo cui, non riuscendo a rimanere al passo con il ritmo richiesto per la correzione delle vulnerabilità, le aziende devono ripensare la propria strategia di sicurezza per colmare queste lacune critiche e mitigare i rischi persistenti legati allo sfruttamento delle VPN.

3. **L'insoddisfazione degli utenti finali influenza il reindirizzamento della sicurezza:**

   La frustrazione degli utenti dovuta alle inefficienze delle VPN, che vanno da connessioni lente ad autenticazioni macchinose, complesse o malfunzionanti, influenza sempre di più le strategie delle organizzazioni. Questo malcontento degli utenti finali favorisce l'adozione di architetture zero trust in grado di garantire un accesso fluido e sicuro e di eliminare i tradizionali problemi associati alle VPN.

4. **Il passaggio dalle VPN allo zero trust: dal concetto all'implementazione:**

   A dimostrazione di un importante cambiamento di rotta nelle strategie adottate, l'81% delle organizzazioni si sta muovendo attivamente verso l'implementazione di framework zero trust entro il prossimo anno. Si tratta di una svolta cruciale, in quanto lo zero trust non viene più visto come un concetto astratto, bensì come una soluzione indispensabile per sostituire le VPN ed elevare la sicurezza di ambienti IT sempre più dinamici e distribuiti.



©2025 Zscaler, Inc. Tutti i diritti riservati.

I rischi delle VPN: perché l’81% delle organizzazioni passerà allo zero trust entro il 2026

Le VPN sono state progettate per fornire l’accesso remoto, ma i tempi sono cambiati, e con essi anche gli aggressori. Oggi, le VPN creano spesso punti di ingresso per attacchi ransomware, furti di credenziali e spionaggio informatico a causa di vulnerabilità difficili da risolvere in modo tempestivo, di modelli basati sull’attendibilità implicita che forniscono un accesso totale alla rete e di autorizzazioni di accesso troppo blande. Nel complesso, le vulnerabilità di sicurezza rappresentano la sfida più critica che le aziende devono affrontare in relazione alle VPN (secondo quanto riferito dal 54% degli intervistati), un dato che riflette il modus operandi degli aggressori, i quali sfruttano sistematicamente falle non corrette o aggirano le protezioni per penetrare nelle reti.

I rischi si intensificano se si guarda all’accesso VPN di terze parti. Il 93% degli intervistati esprime preoccupazione per le vulnerabilità di tipo backdoor introdotte dalle connessioni VPN esterne, in quanto gli aggressori sfruttano sempre più frequentemente credenziali di terze parti per violare le reti senza essere rilevati. Non si tratta solo dell’accesso iniziale; le VPN, infatti, rendono le violazioni anche molto più distruttive. A differenza delle soluzioni zero trust, che applicano policy granulari per impedire il movimento all’interno delle reti, le VPN concedono un accesso esteso, consentendo agli aggressori di muoversi lateralmente e incrementare i propri privilegi. Complessivamente, il 71% degli intervistati considera il movimento laterale una delle principali preoccupazioni, riconoscendo il modo in cui questo fattore amplifica la portata e l’impatto di una violazione.

Queste sfide, unite a problematiche quotidiane come prestazioni lente, autenticazione complessa e disconnessioni frequenti, rendono evidente il motivo per cui le aziende stanno abbandonando le VPN a favore dei modelli zero trust. Basato sulle informazioni provenienti da 632 professionisti operanti nell’IT e nella sicurezza informatica, il Report del 2025 sui rischi delle VPN vuole far luce sullo stato di utilizzo delle VPN nel 2025 al fine di comprenderne meglio i rischi e le criticità. Inoltre, si pone l’obiettivo di offrire alle aziende indicazioni sulle best practice da seguire per migliorare la propria strategia di sicurezza informatica e l’approccio all’accesso remoto sicuro.

I risultati di questo report offrono ai responsabili IT e della sicurezza informazioni basate sui dati sui motivi per cui è opportuno abbandonare le VPN obsolete e adottare un’architettura zero trust moderna e fornita sul cloud. Il passaggio dall’attendibilità implicita alla verifica continua non è più un optional, ma è invece essenziale per proteggere le aziende distribuite di oggi, ridurre la complessità dell’IT e garantire un’esperienza utente fluida.



©2025 Zscaler, Inc. Tutti i diritti riservati.

I problemi di sicurezza delle VPN

L’obsolescenza delle VPN: rischi per la sicurezza e frustrazioni degli utenti

Le organizzazioni che continuano a fare affidamento sulle VPN per l’accesso remoto si trovano sempre più esposte a lacune nella sicurezza, a inefficienze operative e all’insoddisfazione crescente degli utenti finali; tutto questo rafforza l’ormai diffusa convinzione che le VPN appartengano a un’epoca passata della sicurezza.

La principale sfida è rappresentata dai rischi per la sicurezza e la conformità, citati dal 54% degli intervistati, a rimarcare la vulnerabilità critica delle VPN di fronte a ransomware, escalation dei privilegi e attacchi basati sul movimento laterale. Gli aggressori considerano le VPN anelli deboli che possono essere sfruttati, mentre le organizzazioni faticano ad aggiornare questi sistemi obsoleti in modo sufficientemente rapido per stare al passo con le minacce più avanzate.

La frustrazione degli utenti ha raggiunto il punto di rottura: per il 51% degli intervistati le prestazioni scadenti delle VPN, che includono aspetti come connessioni lente, interruzioni e protocolli di autenticazione macchinosi, rappresentano un ostacolo alla produttività. Le VPN rappresentano una criticità anche sul piano operativo, con il 41% degli intervistati che segnala difficoltà nella gestione e il 37% che evidenzia i costi elevati per la manutenzione continua. Questi dati illustrano quanto le VPN siano diventate dispendiose in termini di risorse, prosciugando i budget IT e costringendo i team a dedicare tempo ad attività ripetitive per la risoluzione dei problemi.

Basta con gli approcci tradizionali: è tempo di zero trust

Una recente violazione mette in evidenza, in modo inequivocabile, la fragilità delle VPN. A gennaio del 2025, un gruppo cinese di spionaggio informatico è riuscito a sfruttare una vulnerabilità 0-day nella soluzione Pulse Secure VPN di Ivanti e a ottenere l’accesso non autorizzato alle reti aziendali. Questo attacco, uno dei tanti che hanno preso di mira la tecnologia VPN negli ultimi mesi, evidenzia il motivo per cui le organizzazioni non possono più permettersi di affidarsi a modelli di accesso legacy per difendere le proprie infrastrutture.

A fronte di queste sfide, numerosi fornitori di soluzioni VPN legacy hanno iniziato a commercializzare macchine virtuali fornite sul cloud, definendole in modo non corretto “soluzioni zero trust”. Tuttavia, dal punto di

Eliminare la dipendenza dalla VPN non è più un aggiornamento facoltativo dell’infrastruttura: è un’assoluta priorità. Le organizzazioni devono passare a veri e propri framework zero trust che offrano un accesso basato sull’identità con privilegi minimi e una segmentazione granulare. Queste architetture con base cloud contribuiscono a ridurre le superfici di attacco laterali, migliorare l’esperienza utente e ridurre drasticamente la complessità dell’IT: tre vantaggi che le VPN non sono in grado di eguagliare.

Quali sono le principali criticità insite nelle soluzioni VPN dell’organizzazione?

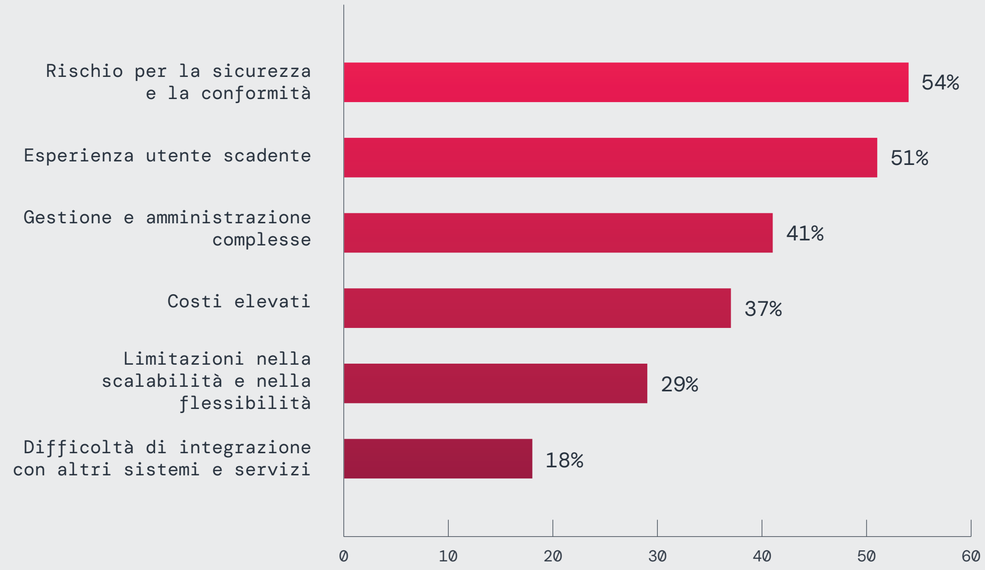


Figura 1: le principali criticità delle soluzioni VPN.

©2025 Zscaler, Inc. Tutti i diritti riservati.

vista architetturale, i servizi VPN ospitati sul cloud restano sostanzialmente gli stessi: sono comunque servizi connessi a Internet con un indirizzo IP pubblico che può essere violato. Un esempio concreto è dato dal fatto che, di recente, il settore ha assistito a un picco di attività nella scansione mirata di oltre ventimila indirizzi IP VPN pubblici ospitati da uno dei principali fornitori di soluzioni di sicurezza. In passato, questo tipo di attività è stato spesso il preludio di tentativi di sfruttamento di vulnerabilità non ancora divulgate presenti in risorse VPN target. In altre parole: se sei raggiungibile, sei violabile. Ecco perché, da una prospettiva architetturale, la tecnologia VPN con base cloud non sarà mai in grado di soddisfare realmente i principi dello zero trust, indipendentemente dal marchio.

Ransomware e VPN: una tempesta perfetta di rischi

I gruppi ransomware continuano a colpire le vulnerabilità delle VPN con una precisione devastante, sfruttando sia le problematiche O-day sia le debolezze note prima che le organizzazioni riescano a distribuire patch di sicurezza. Le VPN sono diventate un bersaglio facile per gli aggressori, a causa della loro adozione diffusa e della dipendenza da modelli obsoleti di attendibilità della rete.

Nel complesso, il 92% degli intervistati ha espresso un elevato livello di preoccupazione per i ransomware diretti alle vulnerabilità senza patch delle VPN, evidenziando l'urgente necessità di adottare meccanismi di protezione più solidi. Questi dati sottolineano il motivo per cui le VPN sono ormai considerate uno strumento dannoso, invece di una soluzione affidabile in grado di mitigare i rischi informatici di oggi.

La realtà dei fatti continua a corroborare questi timori. A gennaio del 2023, diverse organizzazioni sanitarie statunitensi sono state colpite da un attacco ransomware causato da una vulnerabilità di Citrix NetScaler non corretta (CVE-2023-4966). Questo exploit ha consentito agli aggressori di infiltrarsi nei sistemi, interrompere le operazioni ospedaliere, bloccare le cartelle cliniche dei pazienti e costringere le strutture a deviare cure critiche di emergenza, il tutto perché la vulnerabilità non era stata risolta in tempo. Questo incidente sottolinea il rischio diffuso rappresentato dall'impiego di VPN senza patch. Gli aggressori eseguono regolarmente scansioni dei sistemi esposti per assicurarsi di poter sfruttare le vulnerabilità prima che le organizzazioni riescano a correggerle, esponendo dunque queste ultime al rischio di subire compromissioni, interruzioni delle operazioni e perdite finanziarie.

Le organizzazioni devono uscire dall'infinita corsa all'applicazione di patch e adottare strategie difensive proattive, pensate per rispondere a minacce in continua evoluzione. I framework zero trust danno priorità al controllo degli accessi basato sull'identità e alla verifica continua, garantendo una significativa riduzione del rischio associato ai ransomware, anche quando le vulnerabilità rimangono irrisolte. I sistemi di rilevamento automatizzato e le policy dinamiche contribuiscono a rafforzare ulteriormente il contenimento delle potenziali violazioni, impedendo agli aggressori di muoversi lateralmente o di aumentare i propri privilegi.

Quanto è preoccupa l'organizzazione per la possibilità di essere vittima di ransomware a causa di vulnerabilità senza patch?

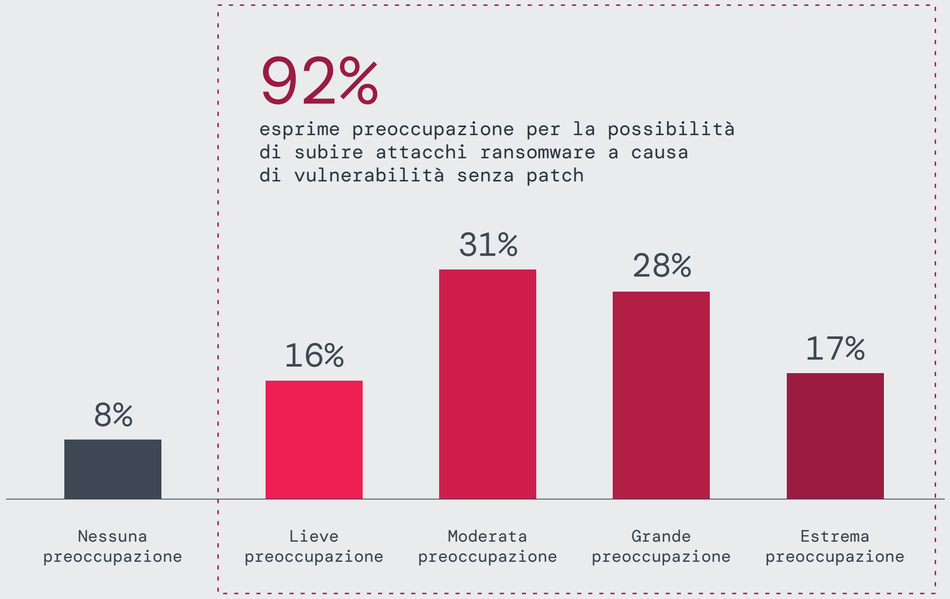


Figura 2: preoccupazioni di subire attacchi ransomware.

©2025 Zscaler, Inc. Tutti i diritti riservati.

VPN e movimento laterale: l'impatto delle violazioni si estende

Oltre a consentire la compromissione iniziale attraverso ransomware e altre minacce, le VPN facilitano il movimento laterale, una tecnica di attacco altamente pericolosa. Gli aggressori sfruttano l'esteso accesso fornito dalle VPN per aumentare i propri privilegi e infiltrarsi più a fondo nelle reti prese di mira, spesso con conseguenze devastanti.

Il 71% degli intervistati ha espresso un certo livello di preoccupazione per questo rischio, mentre il 32% ha indicato un livello di preoccupazione elevato. Questi timori sono ben fondati, perché le VPN, in genere, concedono un ampio accesso alla rete, consentendo agli aggressori di muoversi senza essere scoperti, aumentare i propri privilegi ed esfiltrare dati sensibili una volta al suo interno.

A settembre del 2024, alcuni aggressori hanno sfruttato diverse vulnerabilità 0-day nella soluzione Cloud Service Appliance (CSA) di Ivanti, in particolare la CVE-2024-8963 e la CVE-2024-8190, per violare i dati di diverse organizzazioni, come confermato dalla CISA (Cybersecurity and Infrastructure Security Agency) e dall'FBI. Gli aggressori sono riusciti ad aggirare i controlli amministrativi, quindi hanno eseguito comandi arbitrari, raccolto credenziali e impiantato web shell per consentire il movimento laterale tra le reti. Tralasciando i precedenti incidenti di sicurezza che hanno coinvolto le VPN di Ivanti, questi nuovi exploit dimostrano che l'applicazione di patch e la riprogettazione di soluzioni VPN legacy non consentono comunque di risolvere i difetti di sicurezza critici insiti nei modelli di accesso remoto basati sulla rete.

Quanto è preoccupata l'organizzazione per il fatto che, quando una VPN viene compromessa, gli aggressori possono muoversi lateralmente sulla rete?

89% esprime preoccupazione per la possibilità che gli aggressori riescano a muoversi lateralmente

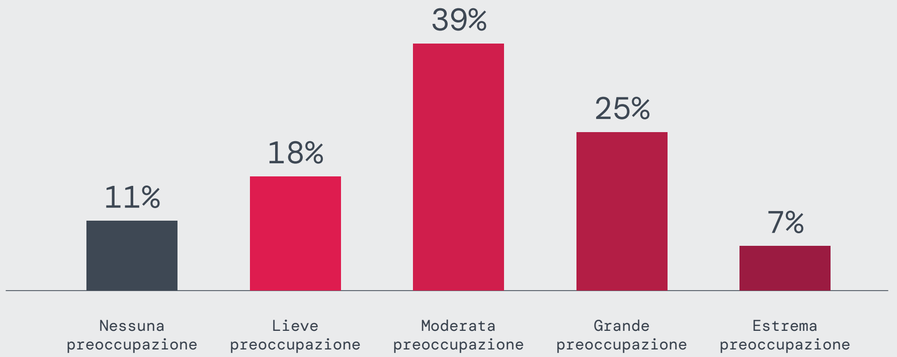


Figura 3: le preoccupazioni delle aziende che, in caso di compromissione della VPN, temono che la minaccia possa muoversi lateralmente sulla rete.

Per mitigare questi rischi, le organizzazioni devono passare dall'accesso basato su VPN allo ZTNA (Zero Trust Network Access) e implementare una segmentazione rigorosa. A differenza delle VPN, che concedono agli utenti un ampio accesso alla rete, lo ZTNA fornisce un accesso a livello di applicazione basato su identità e contesto, garantendo che gli utenti possano accedere solo alle risorse specifiche di cui hanno bisogno. Questo approccio impedisce il movimento laterale anche qualora gli aggressori dovessero riuscire a ottenere l'accesso iniziale, riducendo drasticamente la superficie di attacco e il potenziale impatto delle violazioni. Inoltre, l'implementazione della segmentazione di rete e della microsegmentazione rafforza la sicurezza, in quanto consente di isolare i sistemi critici e impedire le comunicazioni non autorizzate tra le risorse compromesse e quelle sicure.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Le CVE delle VPN dal 2020 al 2025: un'ondata crescente di vulnerabilità molto gravi

Nessun software è immune dalle vulnerabilità di sicurezza, né ci si dovrebbe aspettare che lo sia. Tuttavia, nel caso della tecnologia VPN le vulnerabilità, in particolare le minacce 0-day, possono essere particolarmente dannose, perché gli aggressori riescono a sondare con estrema facilità l'infrastruttura VPN interessata e sfruttarne le falle prima che venga rilasciata o applicata una patch. La segnalazione delle CVE è un'ottima pratica, in quanto questo impegno comunitario aiuta fornitori e clienti a seguire le best practice e migliorare la propria igiene informatica attraverso l'applicazione di patch e la divulgazione di informazioni. Il modo in cui queste CVE vengono scoperte e le informazioni che contengono riflettono i cambiamenti di un panorama di minacce in continua evoluzione.

Zscaler ThreatLabz ha analizzato 411 vulnerabilità ed esposizioni comuni (Common Vulnerabilities and Exposure, CVE) delle VPN dal 2020 al 2025, come riportato dal programma MITRE CVE. I risultati indicano un aumento progressivo delle vulnerabilità delle VPN nella prima metà di questo decennio. Queste CVE riguardano un'ampia gamma di falle delle VPN, che vanno da sfruttamento delle interfacce di gestione web a vulnerabilità di iniezione di comandi e convalida degli input, fino a problematiche crittografiche e agli attacchi DoS e DDoS. Le VPN sono state interessate da numerose vulnerabilità negli ultimi tempi, diverse delle quali hanno causato incidenti di sicurezza gravi e ben evidenti.

Molte di queste CVE sono risultate critiche. Nel 2024, ad esempio, il 60% delle 83 vulnerabilità delle VPN che sono state segnalate dal NIST aveva un punteggio CVSS elevato o critico. Al contempo, le vulnerabilità di esecuzione di codice remoto (Remote Code Execution, RCE), che consentono agli aggressori di eseguire comandi arbitrari e potenzialmente di compromettere il sistema, sono state le CVE più comuni. In altre parole, lungi dall'essere innocue, la maggior parte delle CVE delle VPN dell'ultimo anno ha reso i propri utenti estremamente vulnerabili a exploit che gli aggressori riescono a eseguire con relativa facilità. Inoltre, molte di queste CVE erano exploit 0-day. Sebbene nel 2025 le CVE siano ancora contenute, dall'inizio dell'anno sono già state divulgate vulnerabilità importanti, come due exploit 0-day: CVE-2025-0282 e CVE-2025-0283.

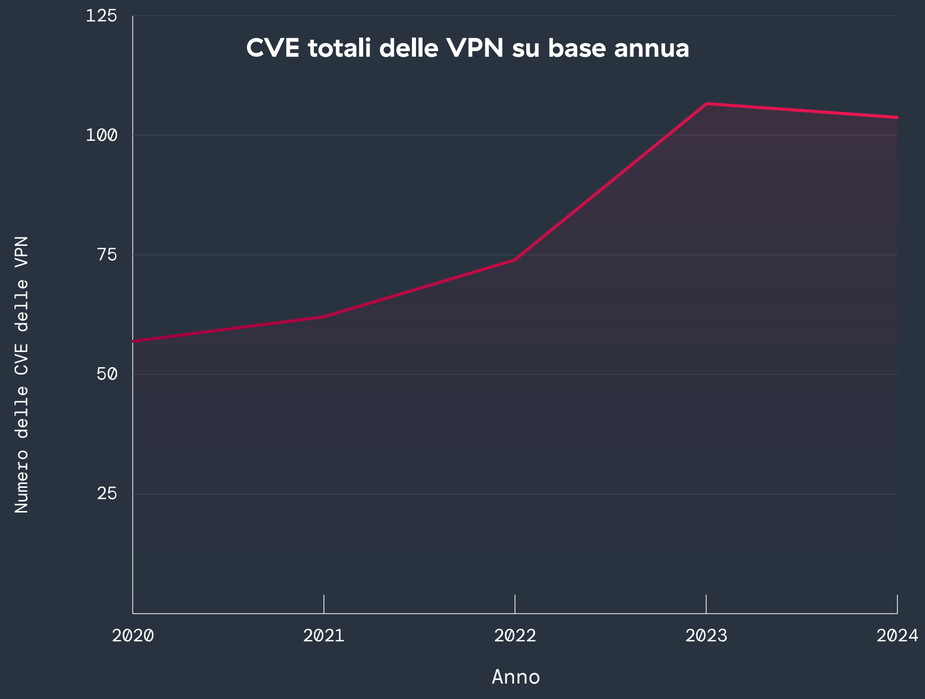


Figura 4: CVE totali delle VPN di ogni anno dal 2020 al 2024.

©2025 Zscaler, Inc. Tutti i diritti riservati.

1. L’RCE rimane la principale minaccia

- **Osservazione:** le vulnerabilità di tipo RCE sono in cima alla lista in tutti e quattro gli anni e, solo nel 2024, se ne contano 32. Se si considerano anche i dati del 2025, 149 CVE sono di tipo RCE, e questo le rende le vulnerabilità più frequenti e critiche.
- **Implicazione:** le vulnerabilità RCE consentono agli aggressori di eseguire comandi arbitrari sui dispositivi VPN, con il rischio di compromettere l’intero sistema. Le aziende dovrebbero dare priorità all’applicazione delle patch e alla protezione dei sistemi vulnerabili da tali exploit.

2. L’escalation dei privilegi cresce costantemente nel tempo

- **Osservazione:** si registra un aumento costante delle CVE di escalation dei privilegi (66,7%); il numero maggiore è stato registrato nel 2024, con 20 vulnerabilità.
- **Implicazione:** gli aggressori sfruttano sempre più spesso le falle delle VPN per aumentare i propri privilegi e ottenere il controllo amministrativo dei sistemi. Le aziende devono garantire configurazioni di sistema sicure e limitare rigorosamente l’accesso con privilegi.

3. Le vulnerabilità DOS (Denial of Service) registrano un forte aumento del 200%

- **Osservazione:** le CVE di tipo DoS sono triplicate, passando da 9 nel 2020 a 27 nel 2024 e diventando il secondo tipo di impatto degli ultimi anni, con 85 CVE in totale se si considerano anche i dati del 2025 già disponibili.
- **Implicazione:** gli attacchi DoS stanno diventando sempre più sofisticati, rendendo i sistemi VPN bersagli prediletti per causare l’interruzione delle operazioni. Per mitigare questi rischi, le aziende dovrebbero adottare misure per la limitazione, il controllo e la modellazione del traffico.

4. La fuga di informazioni sensibili è più rara, ma comunque critica

- **Osservazione:** sebbene relativamente meno comuni, con un totale di 41 CVE, le vulnerabilità associate alla fuga di informazioni sensibili espongono credenziali critiche, chiavi di crittografia e dati degli utenti.
- **Implicazione:** questo tipo di impatto è particolarmente dannoso per la riservatezza e la conformità. Le aziende dovrebbero implementare una crittografia solide, pratiche di sviluppo sicure e il monitoraggio del traffico per rilevare e prevenire le fughe dei dati.

5. Crescita costante delle vulnerabilità di aggiramento dell’autenticazione

- **Osservazione:** gli incidenti basati sull’aggiramento dell’autenticazione sono stati relativamente pochi, ma costanti, aumentando da 4 nel 2020, a un picco di 6 nel 2023, con fino a 4 vulnerabilità nel 2024, per un totale di 30 CVE nel periodo preso in esame.
- **Implicazione:** gli aggressori stanno prendendo di mira le debolezze dell’autenticazione a più fattori (MFA) e della logica di accesso per impersonare gli utenti. Le aziende dovrebbero rafforzare le configurazioni dell’MFA e monitorare eventuali comportamenti anomali di accesso.

Le tendenze principali: tipi di impatto delle CVE

Per comprendere i potenziali danni che queste vulnerabilità potrebbero causare, qualora venissero sfruttate, ThreatLabz ha valutato le CVE delle VPN in cinque categorie di attacco: esecuzione di codice remoto (RCE), escalation dei privilegi, fuga di informazioni, denial of service (DoS) e aggiramento dell’autenticazione. Alcune categorie sono raggruppamenti generici per tipi di attacchi distinti ma strettamente correlati: ad esempio, l’aggiramento dell’autenticazione include attacchi che possono aggirare l’autenticazione a due o più fattori (MFA), mentre altri aggirano le misure di autenticazione di base. In generale, qualsiasi vulnerabilità di tipo RCE sarà un elemento a elevata priorità da risolvere con urgenza per qualsiasi organizzazione.

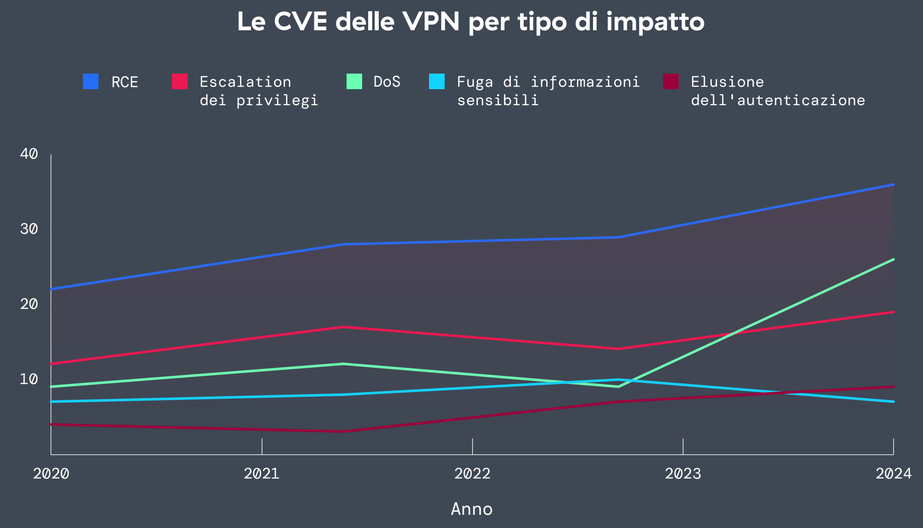


Figura 5: il tipo di impatto delle CVE delle VPN dal 2020 al 2024, prendendo in considerazione RCE, escalation dei privilegi, fuga di informazioni sensibili, DoS e aggiramento dell’autenticazione.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Le tendenze principali: vulnerabilità critiche delle VPN

Oltre ai tipi di impatto, ThreatLabz ha anche analizzato la gravità delle CVE delle VPN su base annua. **Nel complesso, ThreatLabz ha rilevato che le CVE con punteggi CVSS di grado ALTO o CRITICO sono aumentate del 38,9% dal 2020 al 2024.** Nello specifico, il 66,3% di tutte le CVE nel 2024 è stato classificato come di grado ALTO o CRITICO, a indicare il potenziale grave impatto sulle organizzazioni in caso di sfruttamento di queste CVE prima della correzione tramite patch. Inoltre, ThreatLabz ha analizzato le tendenze critiche relative a diversi tipi di vulnerabilità rappresentate nei dati sulle CVE che le aziende dovrebbero conoscere per difendersi al meglio da minacce in continua evoluzione dirette alle VPN.

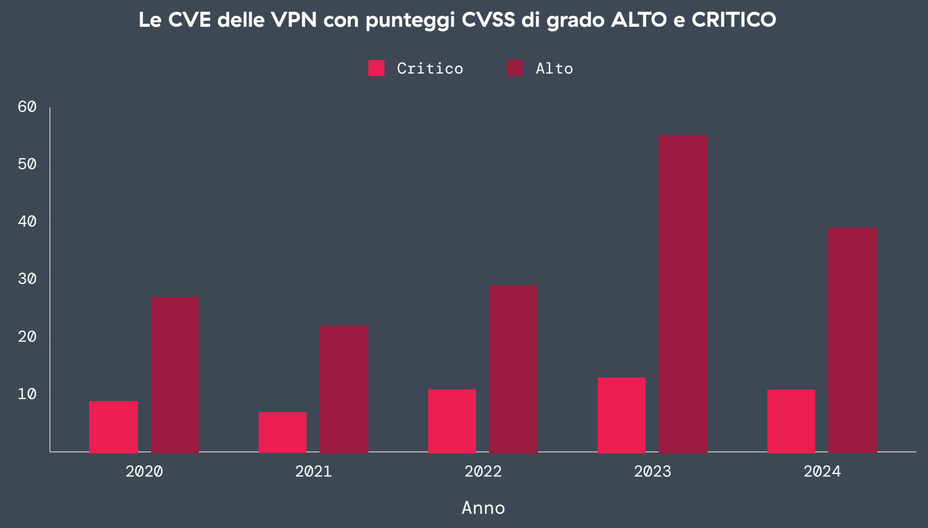


Figura 6: volume delle CVE delle VPN con punteggi CVSS di grado ALTO e CRITICO nel periodo 2020-2024.

1. Aumento dello sfruttamento delle interfacce di gestione con base web

- **Tendenza:** le vulnerabilità di iniezione di comandi, o command injection, e di convalida dell'input sono in costante aumento, a indicare la crescente attenzione degli aggressori verso i portali amministrativi e di gestione, sia dal punto di vista dell'amministratore che dell'utente finale. Dato che queste interfacce sono intrinsecamente esposte a Internet tramite la loro architettura, sono soggette allo sfruttamento da parte degli aggressori.
- **Escalation:** sebbene queste vulnerabilità fossero già presenti nel 2020–2021, si sono notevolmente intensificate dal 2022 in poi, a suggerire che gli aggressori considerano queste interfacce di gestione bersagli interessanti e accessibili, soprattutto a causa di pratiche inadeguate di sviluppo della sicurezza.

2. Autenticazione diffusa e aggiramento dell'MFA

- **Tendenza:** gli attacchi diretti specificatamente ai metodi di autenticazione, tra cui l'aggiramento dell'MFA e il dirottamento e la gestione impropria delle sessioni, sono in costante aumento.
- **Escalation:** negli anni passati (2020–2021), si è assistito principalmente all'aggiramento delle tipologie di autenticazione più semplici, mentre dal 2023 al 2025 questi attacchi si sono evoluti e sono diventati più avanzati, automatizzati e persistenti, diretti esplicitamente alle debolezze dell'MFA. Questo indica l'intenzione degli aggressori di scagliarsi anche contro le misure di sicurezza più efficaci.

3. Aumento degli exploit di escalation dei privilegi locali

- **Tendenza:** le vulnerabilità legate all'escalation dei privilegi locali sono diventate più diffuse e gravi.
- **Escalation:** quello che è iniziato come una piccola svista nella configurazione nel 2020–2021 si è intensificato nel 2024–2025, portando a metodi di escalation dei privilegi molto più sofisticati, come il DLL hijacking, che consentono agli aggressori di ottenere un accesso più profondo a livello di sistema.

©2025 Zscaler, Inc. Tutti i diritti riservati.

4. Crescente livello di sofisticatezza degli attacchi DoS e DDoS

- **Tendenza:** gli attacchi DoS si sono evoluti, passando dall'essere tecniche di base per l'esaurimento delle risorse (2020–2021) a sofisticate minacce di amplificazione DDoS (2024–2025).
- **Escalation:** gli aggressori sono passati da semplici interruzioni basate su pacchetti malformati ad attacchi amplificati più avanzati, riflettendo un'escalation strategica per massimizzare l'interruzione delle operazioni.

5. Errori crittografici persistenti e in aumento

- **Tendenza:** i problemi legati all'implementazione crittografica, come la convalida non corretta dei certificati, le chiavi divulgate e la verifica TLS insufficiente, sono aumentati considerevolmente.
- **Escalation:** a partire dal 2022 circa, si è registrato un notevole aumento delle vulnerabilità della crittografia, con un picco nel 2024–2025 caratterizzato da falle di elevata gravità. Questo incremento dimostra l'interesse strategico degli aggressori nello sfruttare le debolezze legate alla crittografia per minare la riservatezza delle VPN.



©2025 Zscaler, Inc. Tutti i diritti riservati.

I problemi di sicurezza delle VPN (continua)

Le sfide nell'implementazione della segmentazione

Considerati i rischi legati al movimento laterale, molte organizzazioni cercano di limitare la diffusione degli attacchi attraverso la segmentazione. Sebbene questa sia un meccanismo di difesa fondamentale per ridurre la superficie di attacco, la sua implementazione risulta spesso molto complessa.

L'indagine mette in luce queste sfide: il 51% delle organizzazioni prevede o riscontra complessità a livello di configurazione. Inoltre, il 39% segnala la mancanza di competenze e risorse, mentre il 24% riscontra colli di bottiglia nelle prestazioni, a dimostrazione del fatto che le architetture di rete legacy sono scarsamente attrezzate per supportare i controlli granulari dell'accesso necessari invece negli ambienti IT moderni.

Le difficoltà legate alla segmentazione hanno avuto un ruolo notevole nell'attacco ransomware a MGM Resorts del 2023, in cui gli aggressori hanno ottenuto l'accesso iniziale tramite tecniche ingegneria sociale, riuscendo poi a muoversi lateralmente a causa di una segmentazione insufficiente. Questa violazione ha interrotto le operazioni degli hotel, gli sportelli ATM e i sistemi di gioco dei casinò, costando all'azienda una cifra stimata pari a 100 milioni di dollari di danni. Questo caso evidenzia come una segmentazione scadente consenta agli aggressori di spostarsi tra sistemi critici, amplificando di conseguenza l'impatto di un'intrusione iniziale.

Per affrontare queste sfide, le organizzazioni dovrebbero implementare modelli di segmentazione basati sul cloud e sull'identità in grado di semplificare l'applicazione delle policy e di ridurre la quantità delle operazioni manuali necessarie. A differenza della segmentazione della rete tradizionale, che si basa su complesse regole dei firewall e configurazioni VLAN, un approccio zero trust consente una segmentazione dinamica basata sull'identità dell'utente, sul profilo di sicurezza del dispositivo e su valutazioni del rischio in tempo reale. In questo modo, è possibile garantire che solo gli utenti autorizzati possano accedere a determinate applicazioni, preservando al contempo la sicurezza della rete nel suo complesso.

Quali problemi ha incontrato o previsto la tua organizzazione durante l'implementazione della segmentazione?

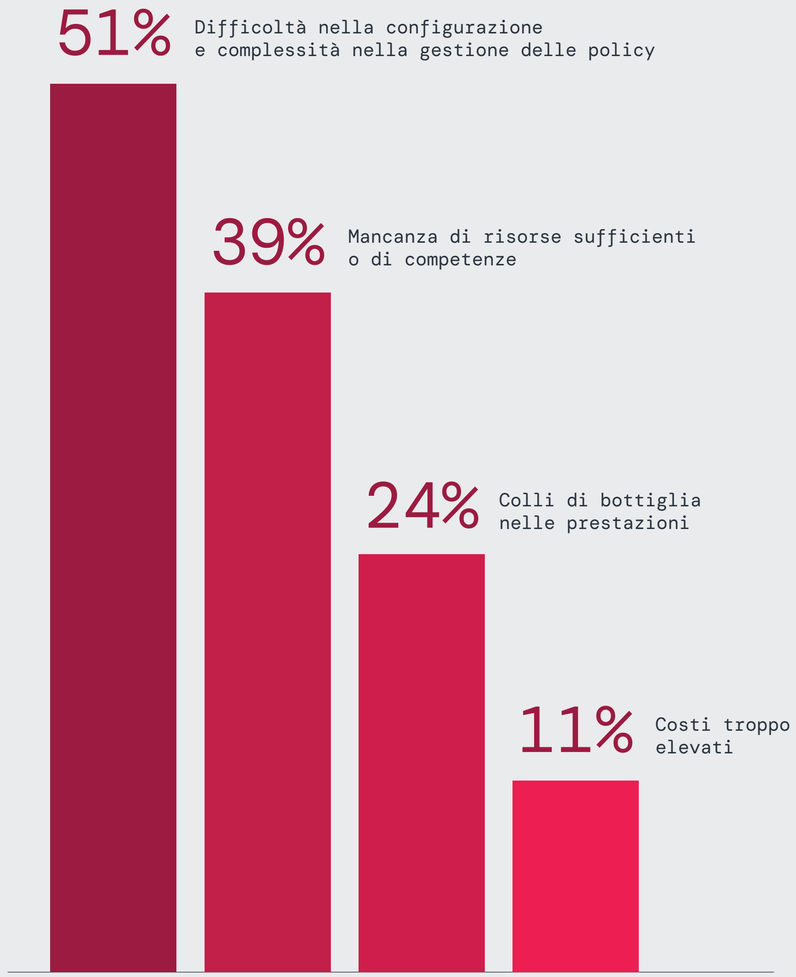


Figura 7: le principali sfide che le aziende devono affrontare quando implementano la segmentazione.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Le VPN intensificano i rischi per la sicurezza informatica delle operazioni di fusione e acquisizione

Oltre alle sfide quotidiane in materia di sicurezza, le operazioni di transizione importanti che interessano l'IT, come fusioni e le acquisizioni, pongono rischi aggiuntivi ed estendono le superfici di attacco. Queste transizioni spesso comportano il consolidamento di reti, applicazioni e identità diverse, il quale di conseguenza può portare a ereditare vulnerabilità, errori di configurazione e controlli di sicurezza scadenti.

Quasi due terzi (64%) degli intervistati hanno espresso preoccupazione per le minacce informatiche a seguito di operazioni di fusione e acquisizione, riconoscendo le lacune di sicurezza che si presentano durante le procedure di integrazione dell'IT.

Un esempio recente è la violazione dei dati di Capita del 2023, in cui gli aggressori hanno sfruttato le debolezze della sicurezza in seguito a un'acquisizione aziendale, ottenendo l'accesso non autorizzato ai dati sensibili. Questo incidente è stato causato da policy di sicurezza non allineate tra le entità interessate dalla fusione, che hanno consentito agli aggressori di muoversi lateralmente sulla rete appena integrata. Questa violazione sottolinea il modo in cui i controlli di sicurezza incoerenti, l'accesso VPN legacy e gli ambienti non segmentati possono creare le condizioni ideali per subire attacchi informatici durante le operazioni di fusione e acquisizione.

Per mitigare questi rischi durante le operazioni di fusione e acquisizione, le organizzazioni devono dare priorità alla due diligence nel campo della sicurezza informatica, imporre l'accesso con privilegi minimi e implementare la segmentazione. A differenza dei modelli di accesso basati sulle VPN, lo zero trust impedisce agli ambienti IT che vengono consolidati di ereditare autorizzazioni di accesso eccessive, riducendo di fatto il rischio di movimento laterale e l'escalation dei privilegi. Sostituendo le VPN e le difese basate sul perimetro con controlli degli accessi basati sull'identità che convalidano ogni richiesta, le organizzazioni sono in grado di proteggere sia gli ambienti IT legacy sia quelli appena integrati.

Quanto è preoccupata l'organizzazione per la potenziale vulnerabilità ad attacchi alla sicurezza informatica a seguito di operazioni di fusione e acquisizione?

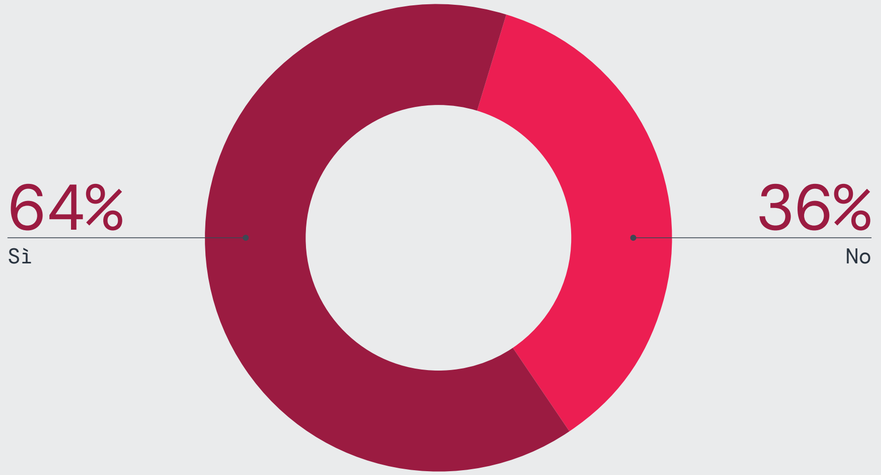


Figura 8: le aziende temono attacchi informatici a seguito di operazioni di fusione e acquisizione

©2025 Zscaler, Inc. Tutti i diritti riservati.

Accesso VPN di terze parti: una backdoor per gli aggressori

L'accesso da parte di utenti terzi è emerso come una delle porte d'ingresso più vulnerabili, che gli aggressori possono sfruttare con facilità. Per loro natura, le VPN tradizionali sono progettate per concedere un ampio accesso alla rete una volta completata l'autenticazione, estendendo questo privilegio a fornitori e partner esterni. Questa pratica genera punti ciechi che gli aggressori non esitano a colpire. Questi ultimi possono quindi sfruttare credenziali rubate o deboli, errori di configurazione e vulnerabilità non corrette per dirottare le connessioni attendibili. Con il 93% degli intervistati che esprime serie preoccupazioni riguardo alle vulnerabilità di tipo backdoor, l'accesso di terze parti rappresenta una bomba a orologeria per le aziende che si affidano a modelli di accesso statici basati sull'attendibilità.

Questa preoccupazione è ben fondata. Nell'agosto del 2024, Enterprise Financial Group (EFG) ha subito una grave violazione dei dati che ha visto l'esposizione delle informazioni personali di quasi 20.000 clienti. Questa violazione è stata ricondotta alle vulnerabilità di una VPN di terze parti utilizzata da EFG, che gli aggressori hanno sfruttato per infiltrarsi nella rete e accedere ai dati sensibili. Questo incidente evidenzia il modo in cui le VPN di terze parti creano lacune nella sicurezza che gli aggressori possono sfruttare come punti di accesso alle reti aziendali.

Le organizzazioni dovrebbero iniziare a verificare l'accesso VPN di terze parti e applicare controlli più rigorosi delle policy, come l'accesso a tempo limitato, l'ispezione del traffico end-to-end (dal dispositivo all'applicazione) e l'autenticazione adattiva. Il passaggio a un modello zero trust consentirà l'applicazione di un accesso specifico per singola applicazione, garantendo che i partner esterni dispongano solo dell'accesso minimo necessario. Inoltre, il monitoraggio continuo e le policy basate sul rischio consentono di mitigare significativamente le vulnerabilità associate alle terze parti.

Qual è il grado di preoccupazione dell'organizzazione riguardo all'eventualità che utenti terzi possano agire da potenziali backdoor per attacchi alla rete attraverso l'accesso VPN?

93% teme che gli utenti terzi possano essere causa di potenziali\rbackdoor nella loro rete attraverso l'accesso VPN

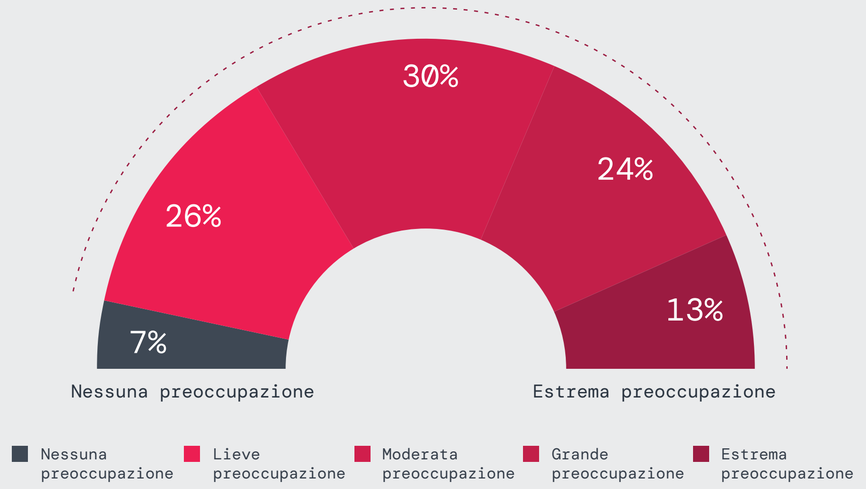


Figura 9: le aziende temono che l'accesso VPN di terze parti possa facilitare gli attacchi informatici.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Criticità e lacune nelle misure di protezione legacy

Gli strumenti tradizionali lasciano le applicazioni private esposte

Proteggere le applicazioni private da minacce web sempre più sofisticate, come ransomware, furto delle credenziali e abuso delle API, è diventata una priorità critica per le aziende moderne. Eppure, molte organizzazioni continuano ad affidarsi a strumenti obsoleti, che risultano inadeguati per contrastare l'attuale panorama di minacce.

Secondo l'indagine, firewall (84%), firewall per applicazioni web (WAF, 58%) e VPN (43%) continuano a essere le principali misure di difesa impiegate dalle organizzazioni per proteggersi dagli attacchi web. Tuttavia, gli aggressori riescono ad aggirare con sempre più facilità queste soluzioni, sfruttando dispositivi non aggiornati, configurazioni scadenti e debolezze intrinseche nei modelli di sicurezza basati sul perimetro, a dimostrazione che queste difese obsolete non sono più in grado di rispondere efficacemente alle minacce moderne.

Le recenti violazioni evidenziano le carenze delle difese basate sul perimetro. Nell'agosto del 2024 alcuni hacker cinesi, nello specifico un gruppo soprannominato Salt Typhoon, si sono infiltrati in importanti aziende di telecomunicazioni statunitensi, tra cui AT&T e Verizon, sfruttando le vulnerabilità presenti in dispositivi di rete e router non aggiornati. Questo attacco ha compromesso i metadati sensibili di oltre 1 milione di utenti, dimostrando la facilità con cui aggressori sofisticati riescono ad aggirare le misure di sicurezza tradizionali come firewall e VPN.

L'unica soluzione per proteggere efficacemente le applicazioni private è quella di andare oltre le difese perimetrali obsolete e adottare modelli di accesso zero trust. Le architetture zero trust eliminano la dipendenza dalla sicurezza basata sulla rete, consentendo agli utenti di connettersi direttamente alle applicazioni secondo rigide policy di accesso granulare e con privilegi minimiQuesto approccio blocca i tentativi di accesso non autorizzati e previene movimento laterale, dirottamento di sessione e furto di credenziali, tattiche comunemente utilizzate dagli aggressori per aggirare le difese perimetrali tradizionali.

Quali prodotti vengono utilizzati per proteggere le applicazioni private dagli attacchi provenienti dal web?

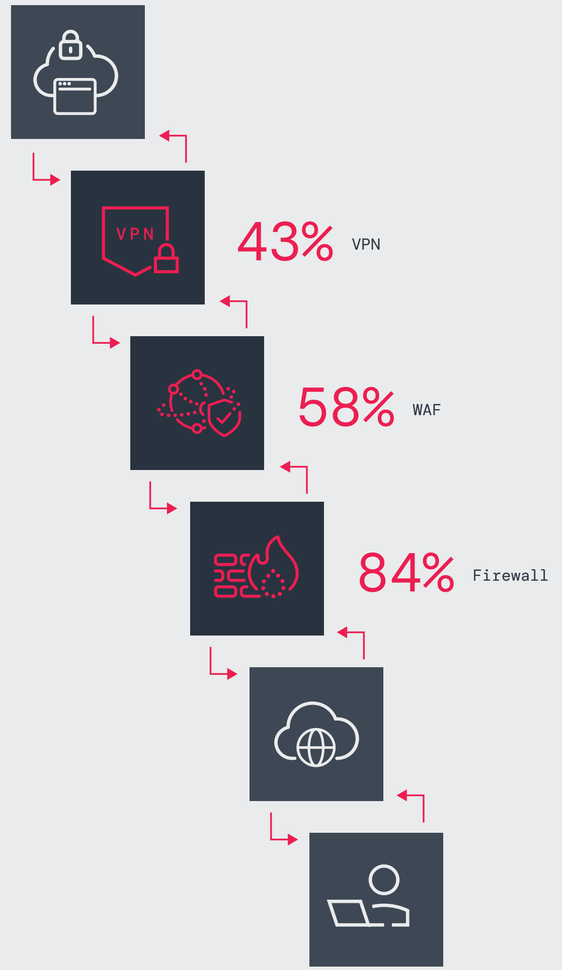


Figura 10: prodotti di sicurezza utilizzati dalle aziende per difendere le applicazioni private dalle minacce basate sul web.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Implementazione del NAC negli ambienti VPN: una protezione limitata

Il 54% delle organizzazioni intervistate dichiara di utilizzare NAC per proteggere l'accesso tramite VPN alle risorse private. Questo tipo di distribuzione non è comunque in grado di bloccare integralmente le violazioni e gli exploit comunemente associati alle vulnerabilità delle VPN, ed è quindi incapace di affrontare i rischi intrinseci dei modelli di attendibilità basati sulla rete.

Le soluzioni NAC eseguono controlli sul profilo di sicurezza dei dispositivi, l'autenticazione e la segmentazione della rete. Non sono però in grado di rispondere ai principali problemi di sicurezza delle VPN, ovvero autorizzazioni di accesso eccessive, rischi legati al movimento laterale e attendibilità implicita.

Le recenti violazioni dimostrano che, anche quando si adotta una soluzione NAC, le vulnerabilità delle VPN restano una debolezza critica. Nel novembre del 2023, il Dipartimento dell'Energia degli Stati Uniti ha confermato un grave incidente di sicurezza che ha coinvolto credenziali VPN compromesse, le quali hanno consentito agli aggressori di aggirare i controlli di accesso e di infiltrarsi nei sistemi interni sensibili. Gli aggressori sono quindi in grado di sfruttare direttamente le debolezze della VPN tramite credenziali rubate, vulnerabilità non corrette o dirottamento delle sessioni, rendendo il NAC una forma di difesa incompleta se il modello di attendibilità sottostante rimane invariato.

L'organizzazione utilizza un NAC (Network Access Control) tra la VPN e le risorse private?

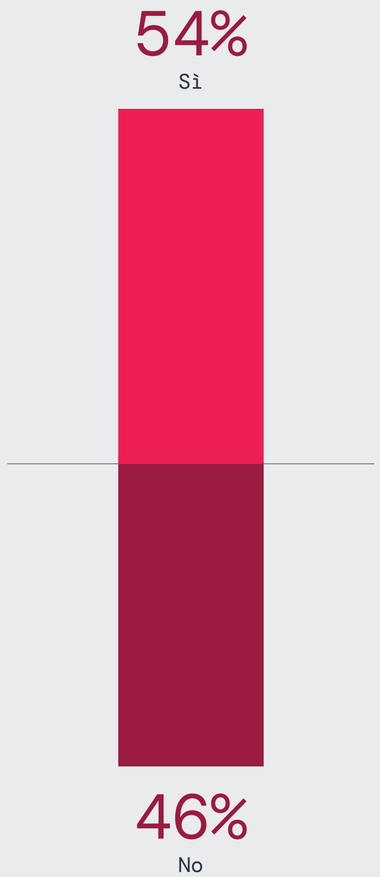


Figura 11: percentuale di aziende che utilizzano una soluzione NAC tra le VPN e le proprie risorse private.



Per superare i limiti delle architetture NAC e VPN legacy, le organizzazioni devono adottare un modello di sicurezza zero trust. Lo zero trust elimina l'attendibilità generalizzata sulla rete consentendo agli utenti di connettersi direttamente ad applicazioni specifiche secondo policy che vengono costantemente convalidate e che prendono in considerazione l'identità, il profilo di sicurezza del dispositivo e il contesto. Lo zero trust non solo blocca l'accesso non autorizzato, ma anche il movimento laterale, ostacolando gli aggressori prima che possano aumentare i propri privilegi o esfiltrare dati.

©2025 Zscaler, Inc. Tutti i diritti riservati.

I problemi della VPN negli ambiti della gestione e dell’esperienza utente

I problemi prestazionali della VPN: utenti frustrati e sovraccarico dell’IT

Le VPN non rappresentano solo un problema di sicurezza, ma anche una delle principali fonti di insoddisfazione degli utenti. Le prestazioni scadenti delle VPN sono sempre più oggetto di lamentele da parte degli utenti e, oltre ad avere un impatto negativo sulla produttività, causano un incremento del carico di lavoro per i team IT.

La lentezza della connessione è la lamentela più comune (23%), a sottolineare la reputazione delle VPN in termini di latenza, congestione e prestazioni scadenti quando si accede alle applicazioni cloud da casa. Anche le difficoltà legate all’autenticazione continuano a rappresentare un problema critico: il 20% degli intervistati segnala procedure di accesso complesse, mentre il 17% riscontra difficoltà nell’accedere alle applicazioni per via di errori di autenticazione.

Questi problemi nelle prestazioni interrompono le operazioni aziendali quotidiane, riducono la produttività e trasformano l’assistenza IT in un collo di bottiglia, in quanto i team si trovano a dover rispondere a frequenti richieste di risoluzione dei problemi, una situazione esacerbata dalla crescente complessità degli ambienti di lavoro da remoto e ibridi.

La sostituzione delle VPN con lo ZTNA (Zero Trust Network Access) non solo elimina la congestione della larghezza di banda, ma migliora anche considerevolmente l’esperienza degli utenti finali, consentendo connessioni dirette, sicure e senza latenza alle applicazioni. A differenza delle VPN, che instradano tutto il traffico attraverso un gateway centrale e creano colli di bottiglia nelle prestazioni, lo ZTNA consente un accesso diretto e sicuro alle applicazioni senza ridurre le prestazioni. Adottando controlli dell’accesso basati sull’identità, la verifica continua e la sicurezza fornita dal cloud, le organizzazioni riescono a eliminare le comuni frustrazioni legate all’uso delle VPN, ad aumentare la produttività della forza lavoro e ad alleggerire la pressione sui team IT derivante dalla gestione e dal supporto di infrastrutture VPN poco flessibili.

Qual è la lamentela che viene segnalata più frequentemente dagli utenti che accedono alle applicazioni tramite VPN?

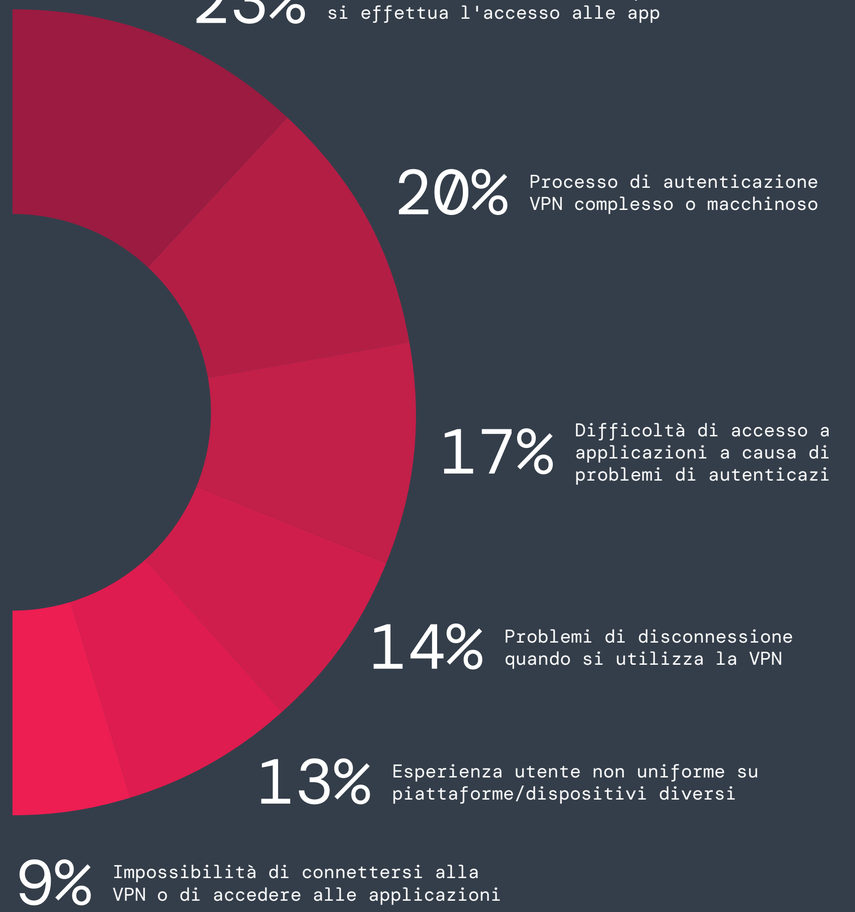


Figura 12: le lamentele più comuni segnalate dagli utenti delle VPN.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Gestire le VPN: sovraccarico per i team IT e vulnerabilità che aumentano l'esposizione

Le VPN stanno sovraccaricando i team IT con vulnerabilità di sicurezza persistenti, richieste di manutenzione che richiedono un elevato impiego di risorse e modelli di accesso obsoleti che non sono più in linea con le attuali esigenze degli ambienti aziendali incentrati sul cloud. La preoccupazione principale di questi team (52%) è data dalle lacune nella sicurezza che possono sfociare in incidenti di sicurezza, evidenziando i rischi costanti legati al furto delle credenziali, agli exploit dei software senza patch e agli aggressori che sfruttano l'accesso VPN per innescare un movimento laterale incontrollato. Tutto ciò evidenzia il motivo per cui le VPN vengono ormai percepite come soluzioni vulnerabili e cariche di rischi.

Le VPN rappresentano ormai un onere per i team IT, non solo dal punto di vista finanziario, ma anche operativo; il 41% degli intervistati ha infatti evidenziato i costi esorbitanti relativi alla manutenzione di queste soluzioni. Proteggere queste infrastrutture obsolete richiede un ciclo incessante di operazioni per l'applicazione delle patch, la risoluzione dei problemi e il monitoraggio dei log, e questo lascia i team senza risorse e impedisce loro di concentrarsi sulle attività di maggior valore.

Un'altra lacuna critica, citata dal 35% degli intervistati, è l'incapacità delle VPN di applicare controlli granulari dell'accesso. Invece di garantire un accesso preciso e basato sull'identità ad applicazioni specifiche, le VPN spesso forniscono una connettività estesa e senza restrizioni alla rete, intensificando drasticamente il rischio di minacce interne e movimento laterale da parte degli aggressori. Inoltre, il 26% cita i costi operativi di gestione legati ai concentratori VPN e ad altri dispositivi, a dimostrazione di quanto sia complesso eseguire la manutenzione di dispositivi hardware, tunnel di rete e gateway di accesso per consentire la connettività da remoto. Queste complessità risultano particolarmente insostenibili in un'epoca in cui gli ambienti di lavoro da remoto e nativi del cloud richiedono soluzioni più agili e scalabili.

Quali sono le preoccupazioni più comuni del team di sicurezza/IT in relazione al supporto delle VPN?

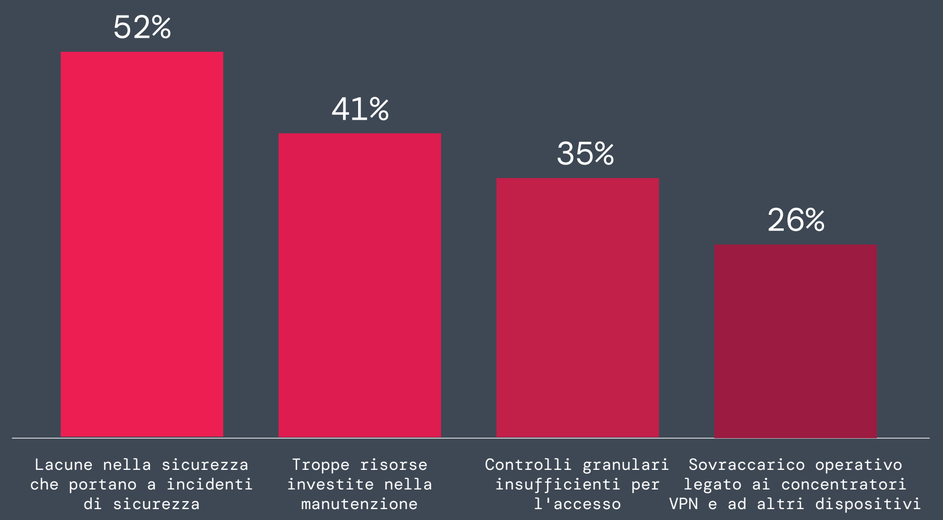


Figura 13: le principali preoccupazioni dei team IT e di sicurezza in relazione al supporto delle VPN.

Per affrontare queste sfide, le organizzazioni dovrebbero passare dall'accesso VPN basato sulla rete a un modello zero trust fornito sul cloud in grado di eliminare l'attendibilità implicita, ridurre le superfici di attacco e semplificare le operazioni IT. L'adozione dello zero trust riduce i costi operativi delle VPN, semplifica la gestione dell'accesso e riduce al minimo i rischi per la sicurezza su larga scala. I team IT vengono sollevati dal peso delle attività di manutenzione continua, e possono così concentrarsi su iniziative proattive di sicurezza e offrire un'esperienza utente più veloce e fluida.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Il peso della gestione delle VPN

La gestione dell'infrastruttura VPN continua a mettere a dura prova i team IT, e le preoccupazioni principali riguardano l'affidabilità, le prestazioni e i costi di manutenzione. La risoluzione dei problemi di connettività e stabilità delle VPN rimane la criticità principale, citata dal 54% degli intervistati. I team IT devono lottare incessantemente per mantenere l'uptime costante delle VPN, con interruzioni di connessione che causano problematiche diffuse che riducono la produttività, compromettono la sicurezza e frustrano i dipendenti.

Bilanciare le prestazioni della VPN e l'esperienza utente rimane una sfida molto significativa (50%), in quanto le VPN spesso generano latenza, disconnessioni e velocità incoerenti, in particolare negli ambienti cloud-first. Inoltre, il 47% dei professionisti IT individua nella continua necessità di applicare patch e nei costi per le risorse due dei principali fattori critici, mettendo in luce quanto sia complesso mitigare le vulnerabilità persistenti e le esigenze di manutenzione che caratterizzano i sistemi datati.

Queste sfide hanno avuto un ruolo in diverse violazioni di alto profilo. Da dicembre del 2023 fino all'inizio del 2024, diverse agenzie governative sono state prese di mira da attacchi diretti alle VPN. I ritardi nell'applicazione di patch per una vulnerabilità ampiamente nota hanno consentito agli aggressori di sfruttare software VPN obsoleti per ottenere un accesso non autorizzato alla rete. Questo evidenzia l'inadeguatezza dei cicli reattivi di applicazione delle patch, anche nelle organizzazioni dotate di team IT dedicati, e dimostra che le difese VPN inefficienti espongono i settori critici a minacce in continua evoluzione.

Dato che l'infrastruttura VPN richiede un ingente volume di risorse IT per la risoluzione dei problemi di connettività, l'applicazione delle patch di sicurezza e l'ottimizzazione delle prestazioni, le organizzazioni si trovano a doverne rivalutare la fattibilità a lungo termine. Sostituendo i concentratori VPN e le apparecchiature di rete come firewall e NAC con un'architettura nativa del cloud, i team IT possono eliminare i colli di bottiglia nell'infrastruttura, ridurre i cicli per l'applicazione delle patch ed evitare la risoluzione manuale dei problemi di connessione.

L'accesso basato su policy e con privilegi minimi garantisce che gli utenti si colleghino solo alle applicazioni autorizzate, senza l'onere di dover gestire complesse regole dei firewall o policy di segmentazione della rete. Passando a un modello zero trust fornito sul cloud, le aziende saranno in grado di azzerare i colli di bottiglia delle VPN, garantendo al contempo un accesso fluido e basato su policy alle applicazioni, senza tutto il carico di lavoro legato alla gestione dell'infrastruttura di rete, all'applicazione delle patch per i software o all'ottimizzazione della scalabilità.

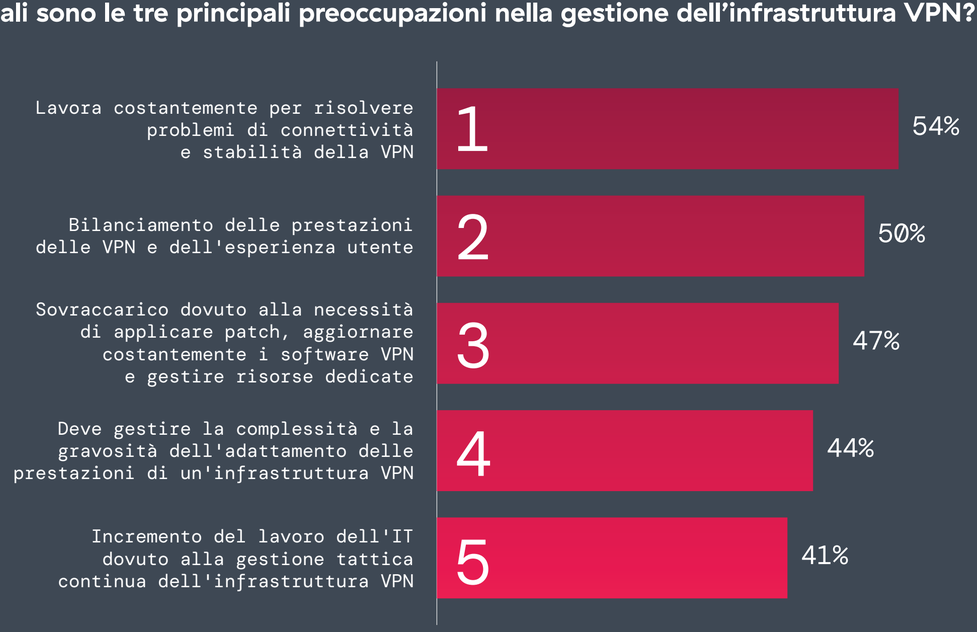


Figura 14: le principali preoccupazioni dei team IT che devono gestire un'infrastruttura VPN.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Controlli di accesso VPN troppo blandi: una falla critica nella sicurezza

La causa principale di molti dei rischi legati alle VPN risiede nel modo in cui le VPN definiscono l'accesso. Invece di fornire un accesso preciso e specifico a una data applicazione, molte organizzazioni continuano a concedere un accesso diffuso alla rete e ad affidarsi a modelli basati sull'attendibilità implicita, lasciando esposti i sistemi critici.

I risultati dell'indagine rivelano che il 52% delle organizzazioni dipende ancora da modelli di accesso obsoleti, come regole statiche dei firewall di rete (28%) o l'accesso aperto agli utenti autenticati (24%). Questi controlli consentono agli aggressori di muoversi facilmente all'interno delle reti senza essere scoperti, di aumentare i propri privilegi ed esfiltrare dati critici una volta ottenuto l'accesso.

Alcuni incidenti recenti sottolineano i pericoli che scaturiscono da un accesso così esteso. All'inizio del 2024, il Dipartimento degli Affari globali canadese (Global Affairs Canada, GAC) ha subito una grave violazione della sicurezza causata dalla compromissione di una VPN che veniva utilizzata dai dipendenti per accedere alla sede centrale di Ottawa. Gli aggressori hanno sfruttato le vulnerabilità della VPN per ottenere l'accesso non autorizzato alla rete, comportando la potenziale esposizione di informazioni sensibili. Questo evento ha dimostrato che un accesso illimitato e con privilegi eccessivi alla rete favorisce il movimento laterale e un'infiltrazione più profonda.

Per mitigare questi rischi, le organizzazioni dovrebbero eliminare l'attendibilità implicita e applicare controlli dell'accesso granulari e basati sull'identità. Passando da modelli di accesso basati sulla rete a una segmentazione diretta a livello di applicazione, si garantisce che un determinato utente possa raggiungere solo le risorse specifiche necessarie per il suo ruolo, riducendo drasticamente le superfici di attacco e impedendo il movimento laterale.

Come può essere definito l'accesso tramite VPN degli utenti alle applicazioni?

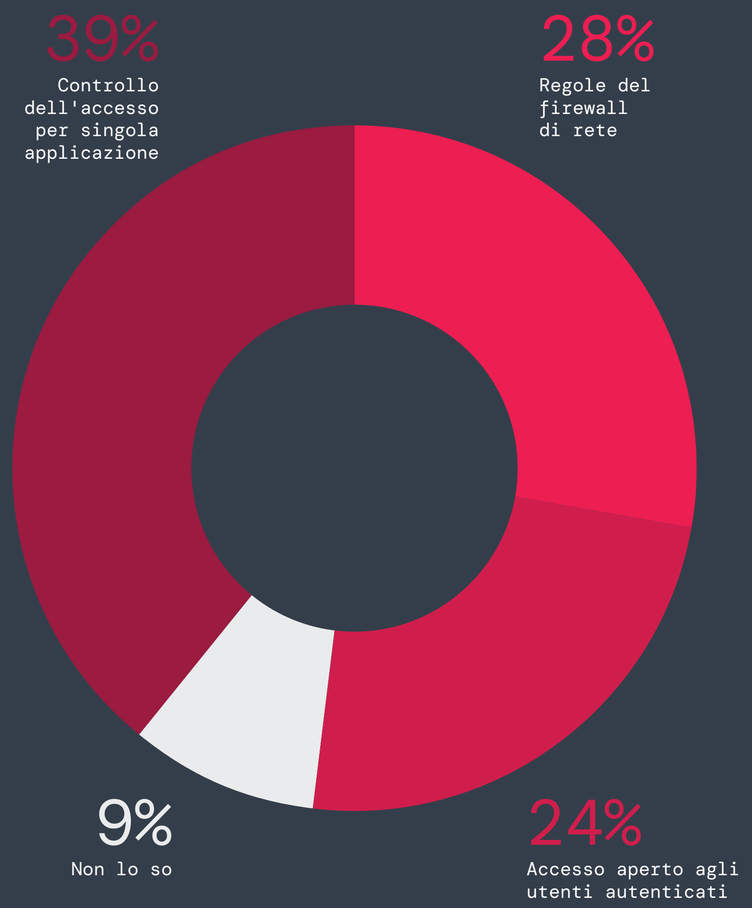


Figura 15: le modalità attraverso cui le aziende definiscono l'accesso VPN degli utenti alle applicazioni.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Sostituire la VPN: un passo verso l’accesso sicuro

Le crescenti vulnerabilità nella sicurezza, le sfide legate all’esperienza utente e gli elevati costi di manutenzione delle VPN stanno spingendo le organizzazioni ad accelerare la transizione verso moderne tecnologie di accesso sicuro, come lo ZTNA. Questo cambiamento rimarca la crescente consapevolezza dell’incapacità delle VPN di soddisfare le moderne esigenze in termini di operatività e sicurezza.

L’indagine conferma questa tendenza, con il 65% degli intervistati che afferma che le proprie organizzazioni stanno sostituendo o pianificano di sostituire le VPN entro il prossimo anno.

Dato che le organizzazioni stanno ormai abbandonando le VPN, è necessario dare priorità all’adozione di modelli di sicurezza forniti sul cloud in grado di garantire un accesso granulare a livello di applicazione, e non una connettività estesa alla rete. Lo ZTNA elimina i rischi delle VPN, assicurando che gli utenti possano accedere solo alle risorse di cui hanno bisogno sulla base dell’identità e del profilo di sicurezza, senza mai collocarli sulla rete aziendale. Questo approccio potenzia la sicurezza, riduce la complessità operativa e migliora l’esperienza utente, rendendo la sostituzione della VPN un passaggio urgente e necessario per le aziende moderne.

Quali sono i piani dell’organizzazione in relazione alla sostituzione del servizio VPN esistente?

65%

delle organizzazioni ha predisposto un piano per sostituire i propri servizi VPN esistenti

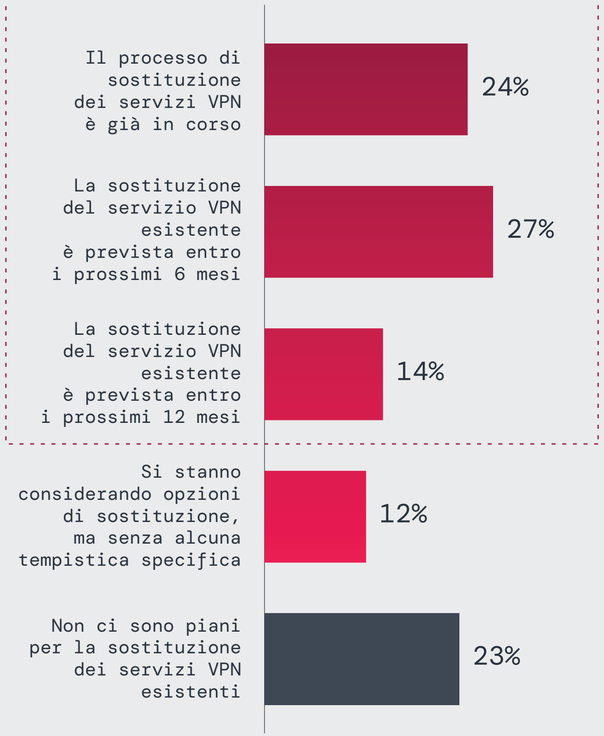
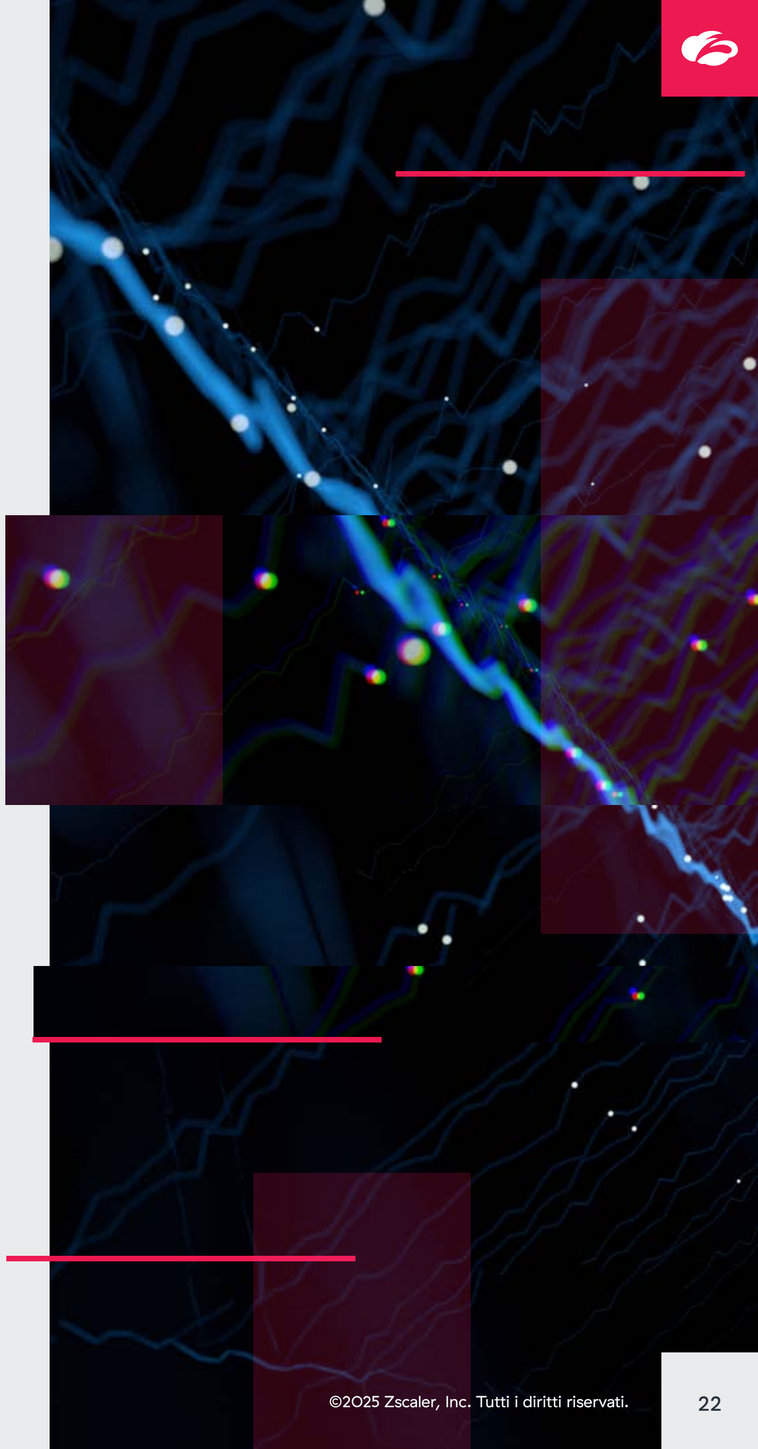


Figura 16: i piani delle aziende in relazione alla sostituzione dei servizi VPN esistenti.



©2025 Zscaler, Inc. Tutti i diritti riservati.

L’adozione dello zero trust

Lo zero trust sostituisce la VPN su larga scala

Con l’accelerazione della tendenza a sostituire le VPN, la maggioranza delle organizzazioni si sta orientando su architetture zero trust per abilitare controlli granulari dell’accesso, ridurre le superfici di attacco e migliorare la produttività degli utenti. I risultati dell’indagine sottolineano uno slancio verso questo nuovo approccio, con l’81% degli intervistati che prevede di adottare il modello zero trust entro l’anno. Tra essi, il 35% sta già implementando soluzioni zero trust, il 24% prevede il lancio entro sei mesi e il 22% ha in programma strategie di distribuzione per il prossimo anno; questi dati dimostrano che, nel settore della sicurezza informatica, lo zero trust è la strategia principale per sostituire le tecnologie di accesso legacy come le VPN.

Per adottare con successo il modello zero trust, è necessario un allineamento tra i team di sicurezza e le operazioni aziendali. Le organizzazioni dovrebbero condurre valutazioni dei rischi per identificare i punti di accesso più vulnerabili, che si tratti di accesso remoto, integrazioni di terze parti o applicazioni critiche, e dare di conseguenza la priorità all’implementazione dello zero trust. Sfruttare l’automazione per l’applicazione delle policy può accelerare la transizione, contribuendo al contempo a ridurre le spese amministrative.

Quali sono i piani dell’organizzazione in merito all’adozione di una strategia zero trust?

96% delle aziende ha già implementato, sta pianificando o ha investito in una strategia zero trust

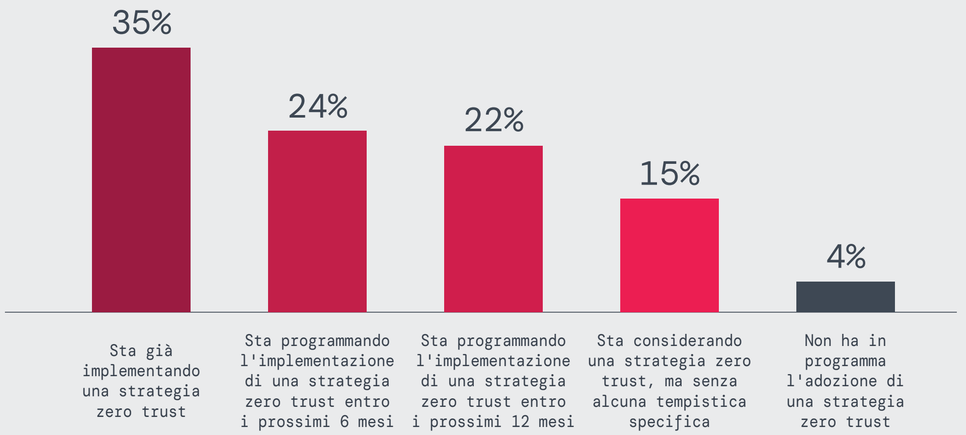


Figura 17: i piani delle aziende per l’implementazione di una strategia zero trust.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Priorità che portano a scegliere lo zero trust: il lavoro da remoto favorisce l'adozione

L'abbandono delle VPN tradizionali evidenzia una trasformazione molto significativa: le organizzazioni si stanno orientando verso architetture zero trust per colmare le lacune di sicurezza, semplificare le operazioni IT e soddisfare le esigenze di una forza lavoro decentralizzata che opera da remoto. In uno scenario caratterizzato da questa svolta strategica, lo zero trust emerge come la soluzione moderna per mitigare i rischi delle VPN e semplificare la gestione della sicurezza.

I risultati dell'indagine indicano che la protezione della forza lavoro da remoto è la principale motivazione alla base di questo cambiamento, con il 37% delle organizzazioni che si sta concentrando sul lavoro da remoto e il 28% sulla sicurezza della forza lavoro ibrida. Questa mossa riflette una tendenza a implementare modelli di sicurezza in grado di offrire un accesso diretto e specifico per singola applicazione, riducendo così le complessità associate alla gestione di più prodotti che caratterizzano le configurazioni VPN legacy.

L'implementazione di un framework zero trust non solo rafforza la sicurezza, ma riduce anche il carico operativo legato alla gestione di numerose soluzioni di sicurezza. Unificando le policy e i controlli di sicurezza in un sistema consolidato, le organizzazioni possono ridurre le spese amministrative e semplificare le operazioni. Ad esempio, una piattaforma zero trust che esegue più operazioni di applicazione delle policy in un'unica scansione può eliminare la necessità di concatenare diverse soluzioni, semplificando l'esperienza utente e consentendo al contempo di mantenere una sicurezza ottimale.

Per proteggere efficacemente la forza lavoro da remoto e ibrida con un'architettura zero trust, le organizzazioni dovrebbero concentrarsi sull'integrazione di misure di sicurezza in grado di ridurre al minimo la complessità. L'implementazione di una piattaforma zero trust unificata può consolidare diverse funzioni di sicurezza, riducendo la necessità di ricorrere a più prodotti specifici e semplificando di conseguenza la gestione. Questo approccio permette di potenziare la sicurezza e aumenta l'efficienza operativa, consentendo ai team IT di concentrarsi su iniziative strategiche, e non sulla gestione una matrice complessa di strumenti di sicurezza.

Qual è il principale caso d'uso che porta a implementare una soluzione zero trust?

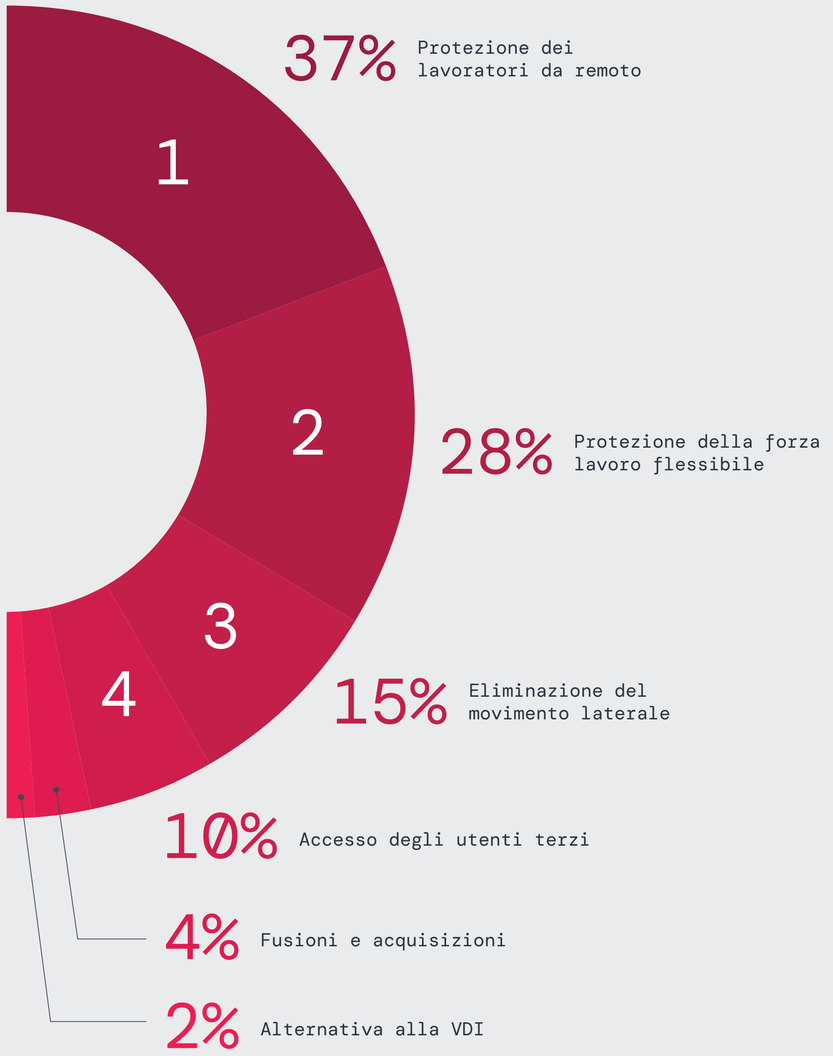


Figura 18: i principali casi d'uso che spingono le aziende a implementare soluzioni zero trust.

©2025 Zscaler, Inc. Tutti i diritti riservati.

I vantaggi principali della sostituzione delle VPN con il modello zero trust

L'adozione di soluzioni zero trust sta trasformando la sicurezza aziendale, offrendo vantaggi di vasta portata che vanno oltre l'accesso sicuro, in particolare semplificando la gestione, migliorando le prestazioni e la scalabilità, riducendo drasticamente la superficie di attacco e aumentando l'efficienza delle risorse. Le aziende che sostituiscono i modelli VPN con lo zero trust non stanno semplicemente aggiornando i propri strumenti; stanno preparando l'intera strategia di accesso remoto per affrontare in sicurezza il futuro.

La stragrande maggioranza degli intervistati (76%) vede il miglioramento della sicurezza e della conformità come il principale vantaggio; lo zero trust elimina infatti l'accesso automatico alla rete e riduce l'esposizione ai ransomware, al furto delle credenziali e ai rischi di movimento laterale.

Per il 64% i vantaggi principali sono invece rappresentati dai miglioramenti nella semplicità di gestione, la scalabilità e l'esperienza utente; lo zero trust elimina infatti il peso della gestione dei concentratori VPN, dell'applicazione costante di patch e della risoluzione dei problemi di accesso.

Quasi la metà (45%) degli intervistati cita la sostituzione della VPN con una soluzione zero trust come un passo fondamentale verso la realizzazione di un'architettura zero trust completa. Al contempo, il 34% sottolinea l'incremento della scalabilità e della flessibilità che rendono lo zero trust una soluzione più efficace per proteggere la forza lavoro da remoto e ibrida. Ci sono anche altri vantaggi che si aggiungono al valore offerto dallo zero trust, come: il miglioramento dell'esperienza degli utenti finali (32%), le integrazioni ottimali tra sistemi IT e di sicurezza (28%) e la riduzione dei costi operativi attraverso il risparmio sulle risorse (18%). Nel complesso, questi vantaggi illustrano il motivo per cui le organizzazioni stanno rapidamente eliminando le VPN tradizionali a favore del modello zero trust.

ManpowerGroup, leader globale nelle soluzioni per la forza lavoro, offre un interessante caso di studio per l'accesso sicuro con lo zero trust. Di fronte al compito di supportare una corposa forza lavoro operante da remoto, l'organizzazione ha sostituito con successo la propria infrastruttura VPN legacy con una soluzione zero trust di Zscaler. Incredibilmente, in soli 18 giorni, ManpowerGroup è riuscita a estendere l'accesso sicuro alle applicazioni a oltre 30.000 utenti, garantendo una continuità operativa senza interruzioni e riducendo i ticket dell'assistenza di ben il 97%. Questa implementazione evidenzia la capacità di un'architettura zero trust di scalare rapidamente, semplificare le operazioni e produrre risultati misurabili in termini di produttività e sicurezza.

Se la VPN è stata sostituita con una soluzione zero trust, quali sono stati i principali vantaggi ottenuti?

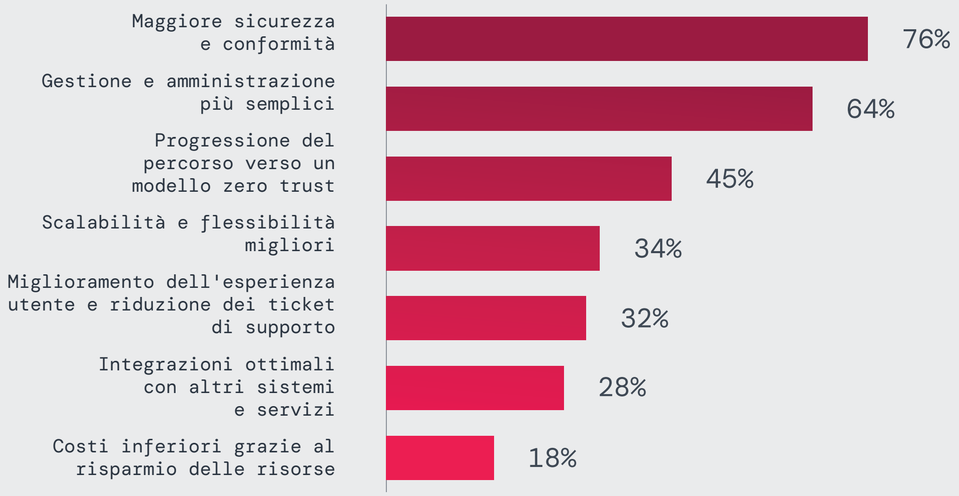


Figura 19: le aziende condividono i principali vantaggi di una soluzione zero trust rispetto alla soluzione VPN precedente.

L'adozione dello zero trust dovrebbe partire da cambiamenti a livello strategico che eliminino l'accesso alla rete tramite VPN a favore di connessioni dirette a livello di applicazione, per contrastare i rischi legati al movimento laterale. Le organizzazioni possono iniziare il processo di sostituzione del proprio modello di accesso legacy partendo dai casi d'uso più critici, come la protezione delle connessioni degli utenti da remoto e terzi, prima di implementare le funzionalità zero trust nell'intero ecosistema IT. L'automazione delle policy di accesso con un unico set di policy e l'integrazione della sicurezza basata sull'identità semplificheranno ulteriormente la gestione dello zero trust e consentiranno al contempo la scalabilità su sistemi distribuiti. Questi framework intelligenti permettono ai team IT di preservare il controllo in tempo reale sulla sicurezza senza sacrificare l'agilità o l'efficienza.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Le previsioni sui rischi delle VPN per il 2025

Le vulnerabilità critiche delle VPN continueranno a emergere

Il numero crescente di exploit delle VPN registrato negli ultimi anni subirà un'accelerazione nel 2025. Le tecnologie VPN rappresentano un obiettivo primario per gli aggressori, perché espongono le aziende a Internet e rendono le vulnerabilità facili da analizzare e sfruttare. Se da un lato le organizzazioni lottano per correggere in tempo i difetti delle VPN, dall'altro gli aggressori continueranno a individuare e sfruttare nuove vulnerabilità di elevata gravità, come dimostrato dalla violazione di Ivanti Pulse Secure a gennaio del 2025. Sia i ricercatori di sicurezza che i criminali informatici esaminano attivamente le infrastrutture VPN, rendendo inevitabile la divulgazione continua di nuove CVE critiche.

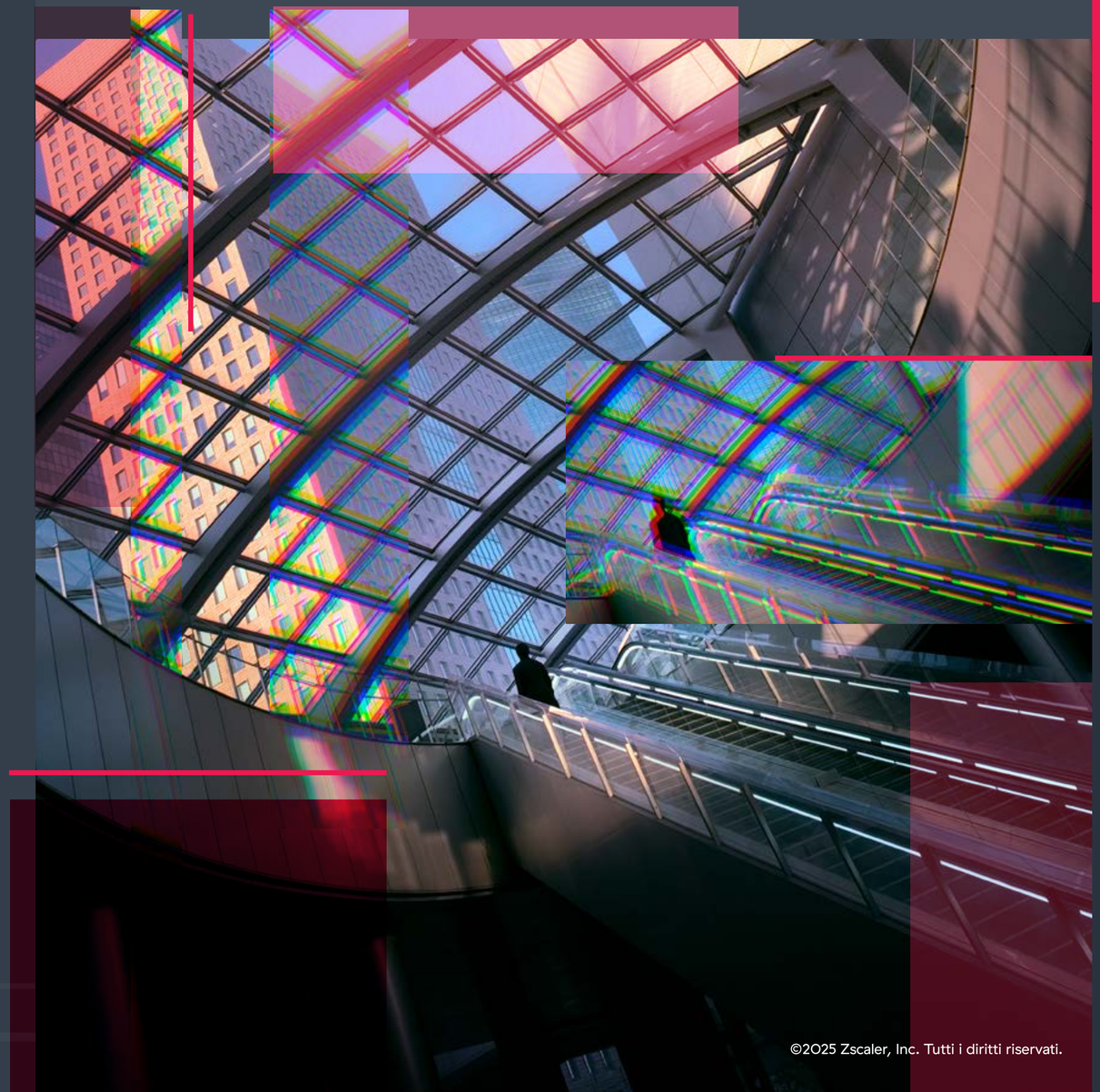
I gruppi ransomware intensificheranno gli exploit delle VPN

Il 92% degli intervistati esprime preoccupazione per le vulnerabilità delle VPN senza patch, e gli aggressori continueranno a sfruttare le falle delle VPN, note e 0-day, come principale metodo per ottenere l'accesso iniziale. I gruppi Ransomware as a service (RaaS) eseguono frequentemente la scansione delle VPN esposte con vulnerabilità non corrette, e questo consente loro di distribuire ransomware prima che i team IT siano in condizione di rispondere.

La campagna ransomware di gennaio del 2025 rivolta alle organizzazioni sanitarie statunitensi dimostra come le falle nella sicurezza delle VPN offrano agli aggressori un accesso diretto a sistemi sensibili. Man mano che questi attacchi diventano sempre più automatizzati, la necessità di passare alla sicurezza zero trust diventerà ancora più urgente.

Il movimento laterale tramite VPN porterà ad attacchi ancora più distruttivi

Una delle tecniche più efficaci utilizzate dai criminali informatici o dagli hacker supportati da Stati nazionali è quella di sfruttare l'ampio accesso offerto dalle VPN per muoversi lateralmente, incrementare i propri privilegi ed esfiltrare i dati. Con il 71% delle organizzazioni che esprime preoccupazione per questo rischio, la segmentazione della rete viene spesso vista come la soluzione definitiva, ma la sua complessità ne rende difficile l'implementazione. Molte organizzazioni non dispongono del personale qualificato per gestirla in modo efficace, e questo si traduce in progetti che richiedono mesi per essere completati o che si bloccano completamente. Per attenuare queste sfide le aziende dovrebbero adottare la segmentazione zero trust, che impone un controllo rigoroso dell'accesso alle applicazioni in base al principio dei privilegi minimi eliminando i percorsi che favoriscono il movimento laterale, senza dover ricorrere alla segmentazione tradizionale della rete.



©2025 Zscaler, Inc. Tutti i diritti riservati.

L’accesso tramite VPN di terze parti rimarrà un vettore di minacce critico

Anche se il 93% degli intervistati esprime preoccupazione per le vulnerabilità delle VPN associate a terze parti, gli aggressori continueranno a prendere di mira i punti di accesso esterni più deboli. Le credenziali di terze parti rubate e gli accessi VPN non configurati correttamente restano tra i principali punti deboli sfruttati dai criminali informatici. La violazione di Enterprise Financial Group (EFG) nel 2024 ha dimostrato che gli aggressori sfruttano le connessioni VPN di terze parti per infiltrarsi negli ambienti aziendali. Molte organizzazioni non hanno visibilità sulle autorizzazioni di accesso delle terze parti, e questo rende difficile applicare le policy di sicurezza. Per mitigare questi rischi, le imprese devono passare a un framework zero trust che consenta di implementare un controllo rigoroso degli accessi in base al principio dei privilegi minimi e la verifica continua di tutte le connessioni esterne.

Gli exploit delle VPN basati sull’AI aumenteranno

L’aumento degli attacchi informatici basati sull’AI avrà un impatto senza precedenti sulla sicurezza delle VPN. Gli aggressori sfrutteranno sempre più frequentemente l’AI per la ricognizione automatizzata, il password spraying intelligente e lo sviluppo rapido di exploit, e questo consentirà loro di compromettere le credenziali VPN su larga scala. Le tecniche di elusione basate sull’AI renderanno ancora più difficile rilevare le intrusioni derivanti dalle VPN prima che si verifichino danni significativi. Al contempo, le soluzioni di sicurezza VPN basate sull’AI potrebbero introdurre lacune di sicurezza impreviste, aprendo la strada a nuovi vettori di attacco utilizzabili dai criminali informatici. Con l’aumento delle minacce basate sull’AI, le organizzazioni devono adottare misure di sicurezza proattive, come la verifica continua dell’identità e i controlli dell’accesso zero trust.

Le violazioni più gravi legate alle VPN faranno notizia

A seguito di numerose violazioni di alto profilo avvenute nel 2024, le organizzazioni saranno sottoposte alla pressione sempre maggiore di divulgare gli incidenti informatici associati alle VPN. Con le nuove normative della SEC che impongono la trasparenza sui rischi per la sicurezza informatica, le organizzazioni che subiscono attacchi VPN si troveranno ad affrontare controlli normativi molto più rigorosi, danni alla reputazione e potenziali sanzioni finanziarie. Dato che le VPN continueranno a essere il principale punto di ingresso per gli attacchi, le organizzazioni saranno costrette a riconsiderare i modelli di accesso legacy accelerando il passaggio alla sicurezza zero trust.

Gli investimenti nello zero trust aumenteranno con il declino delle VPN

Con il 65% delle organizzazioni che ha già sostituito o pianifica di sostituire le proprie VPN entro un anno, si sta registrando un’accelerazione degli investimenti nella sicurezza zero trust, che è destinata a ridefinire il campo dell’accesso remoto. I requisiti normativi e gli obblighi di assicurazione informatica stanno spingendo le organizzazioni a guardare oltre le VPN, in quanto le soluzioni legacy non sono in grado di soddisfare i requisiti di sicurezza, scalabilità e conformità. L’adozione dello zero trust non solo offre una mitigazione del rischio informatico, ma consente anche di eliminare gli elevati costi di manutenzione di concentratori VPN, apparecchiature di rete e continui cicli di applicazione delle patch. Ecco perché le VPN vengono sempre più spesso considerate soluzioni obsolete, con l’intero settore che si sta muovendo verso modelli di sicurezza zero trust.



Queste previsioni evidenziano un consenso crescente: le organizzazioni che ritardano ad adottare lo zero trust risulteranno altamente vulnerabili all’incremento degli exploit delle VPN. Il futuro dell’accesso sicuro dipende dalla mitigazione proattiva dei rischi, non dall’applicazione reattiva delle patch: è giunto il momento di guardare oltre le VPN.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Le best practice per l'accesso sicuro

Mitigazione dei rischi delle VPN e rafforzamento della sicurezza zero trust

1. **Eliminare l'accesso basato sulla rete per ridurre al minimo la superficie di attacco**
   È fondamentale impedire agli aggressori di sfruttare i punti di ingresso alla rete esposti eliminando gradualmente le VPN e l'accesso basato sulla rete a favore di una connettività diretta e specifica per singola applicazione. I dati dell'indagine mostrano che il 54% delle organizzazioni cita i rischi per la sicurezza come la principale criticità delle VPN, rimarcando la necessità di rimuovere le dipendenze da queste tecnologie e i modelli di sicurezza basati su firewall, che espongono le aziende agli attacchi.

2. **Bloccare la compromissione iniziale attraverso la prevenzione delle minacce inline**
   Ispeziona tutto il traffico cifrato e non cifrato inline per bloccare exploit 0-day, malware e payload dei ransomware prima che raggiungano gli utenti. Con il 92% delle organizzazioni che teme che i ransomware possano prendere di mira le vulnerabilità delle VPN, l'ispezione del traffico in tempo reale e il blocco basato su policy sono essenziali. Un modello di sicurezza nativo del cloud elimina la necessità di ricorrere a firewall on-premise e riduce la superficie di attacco.

3. **Rafforzare l'autenticazione e implementare una strategia di sicurezza basata sull'identità**
   Implementa un modello di autenticazione a più fattori (MFA) resistente al phishing, che preveda ad esempio credenziali FIDO2, dati biometrici o token hardware per verificare l'accesso degli utenti. Evita i metodi di autenticazione legacy, come l'MFA basata su SMS e le notifiche push, modalità spesso aggirate dagli aggressori, e integra una strategia di sicurezza basata sull'identità con la verifica continua, invece di affidarti all'autenticazione singola.

4. **Applicare l'accesso con privilegi minimi e basato sul contesto implementando un approccio ZTNA**
   Sostituisci l'accesso VPN esteso con lo ZTNA (Zero Trust Network Access), per garantire che gli utenti si connettano solo alle applicazioni autorizzate, mai alla rete stessa, e implementa controlli granulari di accesso just-in-time (JIT) basati su identità, profilo di sicurezza del dispositivo e analisi del rischio in tempo reale che garantiscano l'accesso solo a ciò di cui gli utenti hanno bisogno, quando ne hanno bisogno.

5. **Eliminare il movimento laterale con la segmentazione zero trust**
   Gli utenti devono essere collegati direttamente alle applicazioni, non alla rete, per impedire agli aggressori di spostarsi tra i sistemi una volta ottenuto l'accesso iniziale. La segmentazione zero trust e la microsegmentazione basata sull'identità garantiscono che, anche se un utente viene compromesso, un aggressore non riesca a passare ad altre risorse o ad aumentare i propri privilegi. Lo ZTNA elimina i tunnel VPN che favoriscono il movimento laterale.

6. **Proteggere l'accesso esterno e di terze parti con controlli basati sull'identità**
   Implementa l'accesso con privilegi minimi per terze parti, fornitori e collaboratori, applicando rigorosi controlli di sessione, controlli dello stato dei dispositivi e monitoraggio continuo. La sostituzione dell'accesso di terze parti basato su VPN con lo ZTNA riduce significativamente l'esposizione al rischio derivante dalla compromissione delle credenziali dei fornitori; si tratta di un vantaggio molto rilevante, dato che il 93% delle organizzazioni esprime preoccupazione per i rischi che delle VPN associati a terze parti.



©2025 Zscaler, Inc. Tutti i diritti riservati.

7. **Migliorare la protezione dei dati implementando policy zero trust integrate**
Implementa controlli inline per prevenire la perdita dei dati (DLP) e soluzioni CASB (Cloud Access Security Broker) per ispezionare, cifrare e impedire in tempo reale la movimentazione non autorizzata dei dati. Un framework di sicurezza zero trust garantisce il controllo e l'ispezione di tutto traffico utente, anche nelle applicazioni SaaS e negli ambienti cloud.

8. **Implementare un'infrastruttura di sicurezza basata sull'AI e il monitoraggio continuo**
Impiega l'analisi in tempo reale basate sull'AI, la tecnologia di deception e il rilevamento comportamentale automatizzato per bloccare le minacce prima che causino danni più gravi. Le soluzioni ZTNA forniscono un punteggio di rischio in tempo reale per impedire agli account compromessi di accedere alle applicazioni sensibili. La ricerca proattiva e quotidiana delle minacce, insieme a controlli dell'accesso basati sul rischio, contribuiscono a ridurre drasticamente l'impatto delle violazioni.

9. **Valutare e adattare costantemente la sicurezza**
Esegui valutazioni automatizzate del rischio, test di penetrazione e simulazioni degli attacchi per adattare dinamicamente le policy di sicurezza zero trust.
Gli errori di configurazione della sicurezza e la mancanza di controlli adeguati sono aspetti importanti che possono sfociare in gravi violazioni; per questo motivo, le misure automatizzate e basate sulle policy sono fondamentali per ridurre l'errore umano.

10. **Eliminare l'infrastruttura VPN e automatizzare l'applicazione delle policy di sicurezza**
Elimina la necessità di ricorrere a concentratori VPN e di gestire regole dei firewall ed elenchi manuali di controllo degli accessi adottando un modello zero trust fornito sul cloud. Lo ZTNA consente di implementare policy di sicurezza dinamiche che si adattano in tempo reale alle variazioni nella conformità, agli aggiornamenti normativi e alle minacce informatiche in continua evoluzione, senza configurazioni manuali o dipendenze hardware.

Implementando queste strategie, le organizzazioni possono eliminare i rischi per la sicurezza legati alle VPN con un framework di sicurezza zero trust resiliente che garantisce una verifica continua, un accesso con privilegi minimi e la mitigazione proattiva delle minacce.



©2025 Zscaler, Inc. Tutti i diritti riservati.

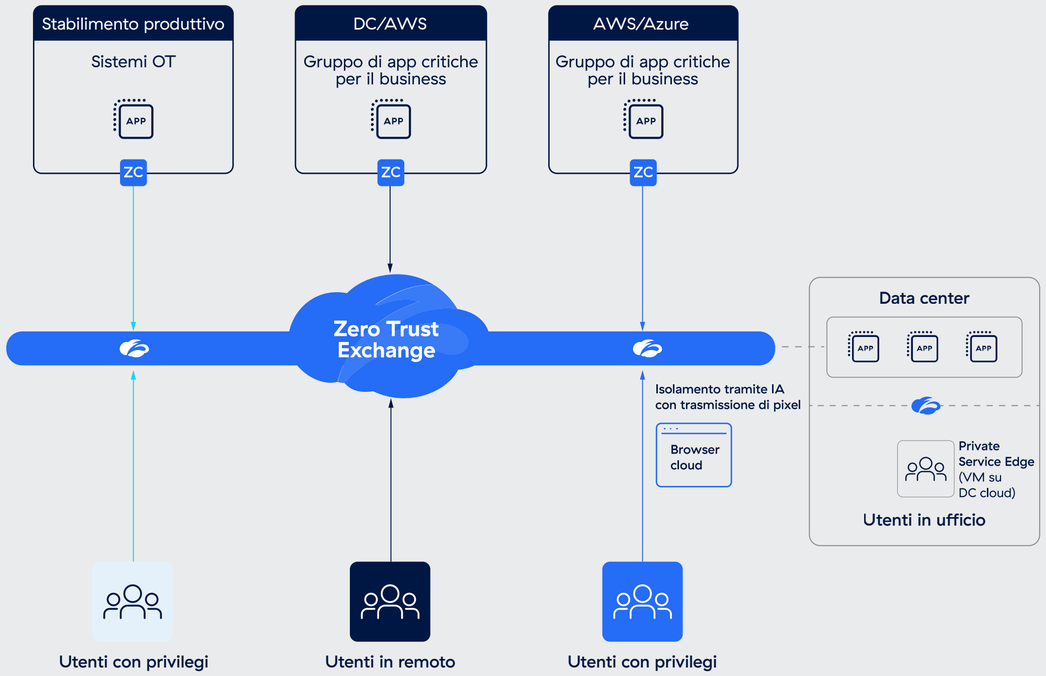
In che modo Zscaler rivoluziona l'accesso sicuro

Le VPN e i firewall tradizionali estendono notevolmente la superficie di attacco di un'organizzazione, perché collegano gli utenti direttamente alla rete. Un accesso così generalizzato consente agli aggressori di sfruttare le vulnerabilità, ottenere l'accesso e muoversi lateralmente all'interno dell'ambiente in estrema facilità. Con le minacce che continuano a evolversi e il lavoro ibrido che sta diventando la norma, affidarsi a queste tecnologie obsolete pone rischi critici per la sicurezza, che richiedono soluzioni più sicure e adattabili per essere mitigati.

Zscaler Private Access™ (ZPA) offre un'alternativa sicura e scalabile alle soluzioni di accesso remoto legacy come le VPN. In quanto soluzione nativa del cloud, ZPA fornisce un accesso zero trust a tutti gli utenti, offrendo una connettività diretta alle applicazioni private. Per ridurre al minimo la superficie di attacco, le applicazioni vengono protette dalla piattaforma Zscaler Zero Trust Exchange™, in modo da eliminare il movimento laterale attraverso la segmentazione utente–applicazione basata sull'AI e proteggere dalle minacce più sofisticate grazie all'ispezione integrata del traffico e alla tutela di applicazioni e dati.

La distribuzione di ZPA richiede poche ore e consente di sostituire le VPN e gli strumenti di accesso remoto legacy con una piattaforma zero trust olistica e nativa del cloud. Grazie al supporto del security cloud più grande del mondo, ZPA offre agli utenti una connettività veloce, affidabile e a bassa latenza a livello globale. La sua architettura nativa del cloud garantisce una scalabilità elastica, rispondendo in modo ottimale alle esigenze dei nuovi modelli di lavoro ibridi e distribuiti in diverse aree geografiche.

Con ZPA, le aziende possono adottare una forza lavoro ibrida e cloud–first in totale sicurezza, con la certezza che le risorse siano protette, gli utenti produttivi e le operazioni IT pronte per far fronte al futuro.



©2025 Zscaler, Inc. Tutti i diritti riservati.



I principali vantaggi di Zscaler Private Access (ZPA)

Riduzione della superficie di attacco per proteggere dagli attacchi ransomware

Le vulnerabilità delle VPN espongono le organizzazioni agli utenti malintenzionati, sottoponendole al rischio di subire attacchi ransomware e furti di credenziali. ZPA elimina questo rischio nascondendo tutte le applicazioni dietro a Zero Trust Exchange e concedendo agli utenti un accesso diretto e zero trust solo alle applicazioni autorizzate. Impedendo agli utenti non autorizzati, tra cui fornitori e collaboratori terzi, di rilevare le applicazioni e di muoversi lateralmente, ZPA offre una protezione avanzata dagli attacchi ransomware. La nostra soluzione consente l'accesso remoto sicuro a tutte le applicazioni, comprese le app private, le applicazioni connesse alla rete come le soluzioni VoIP e le app server-to-client. Inoltre, ZPA riduce al minimo l'impatto delle interruzioni offrendo una soluzione completa di continuità operativa e aiuta le organizzazioni a soddisfare rigorosi requisiti di conformità.

Eliminazione del movimento laterale delle minacce

ZPA instaura un modello di accesso basato sui privilegi minimi, connettendo gli utenti direttamente ad applicazioni specifiche e impedendo l'accesso alle altre app presenti sulla rete. Fornisce informazioni visive sull'accesso utente-applicazione e sulle policy applicate, contribuendo a migliorare la visibilità e il controllo.

La segmentazione basata sull'AI di ZPA genera automaticamente raccomandazioni per i segmenti e le policy delle app, semplificando l'implementazione e garantendo al contempo la massima scalabilità e una sicurezza avanzata.

Massima visibilità e analisi granulari

ZPA offre una visibilità dettagliata e in tempo reale sull'utilizzo delle applicazioni, sul comportamento degli utenti e sui modelli di accesso. I team IT possono utilizzare questi dati per monitorare, verificare e identificare rapidamente le potenziali minacce, migliorando il profilo di sicurezza complessivo. Questo può inoltre contribuire a garantire la conformità alle normative.

Implementazione di un accesso clientless per mitigare le vulnerabilità associate alle terze parti

ZPA Clientless Access semplifica l'accesso delle terze parti consentendo a collaboratori e partner di connettersi in modo sicuro alle applicazioni tramite qualsiasi browser, senza bisogno di un client. Inoltre, isola i dispositivi non gestiti dalla rete aziendale, protegge i dati sensibili e si integra con Google Chrome Enterprise Browser per potenziare la sicurezza quando si impiegano dispositivi personali. Questo approccio moderno abbatte i costi, mitiga i rischi associati all'accesso delle terze parti ed elimina la dipendenza dalla gestione di soluzioni VDI legacy.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Previeni la compromissione delle app private

ZPA riduce al minimo il rischio legato alla compromissione delle app private e alla perdita dei dati con un'ispezione end-to-end inline e completa del traffico delle app private. Le sue avanzate funzionalità di prevenzione della perdita dei dati garantiscono la massima protezione delle informazioni sensibili, bloccando al contempo l'accesso non autorizzato. Nascondendo le applicazioni dalla rete Internet pubblica e consentendo connessioni sicure tra utenti e app in base ai principi dello zero trust, ZPA riduce la superficie di attacco, impedisce il movimento laterale e protegge dalle violazioni, contribuendo così a migliorare il profilo di sicurezza complessivo.

Semplificazione della gestione delle policy e accelerazione della distribuzione

ZPA snellisce le operazioni IT semplificando l'implementazione dell'accesso remoto, la gestione delle policy e la segmentazione utente-app. Le attività che in precedenza richiedevano molto tempo, come l'onboarding degli utenti, l'applicazione delle patch e gli aggiornamenti, ora possono essere completate in pochi minuti, riducendo notevolmente il carico di lavoro dell'IT. Grazie alla gestione centralizzata e alle raccomandazioni automatizzate sulle policy, ZPA consente ai team IT di migliorare l'efficienza, ridurre al minimo la complessità e concentrarsi sulle iniziative strategiche, anziché sulle operazioni di routine.

Applicazione del controllo degli accessi basato sul profilo di sicurezza

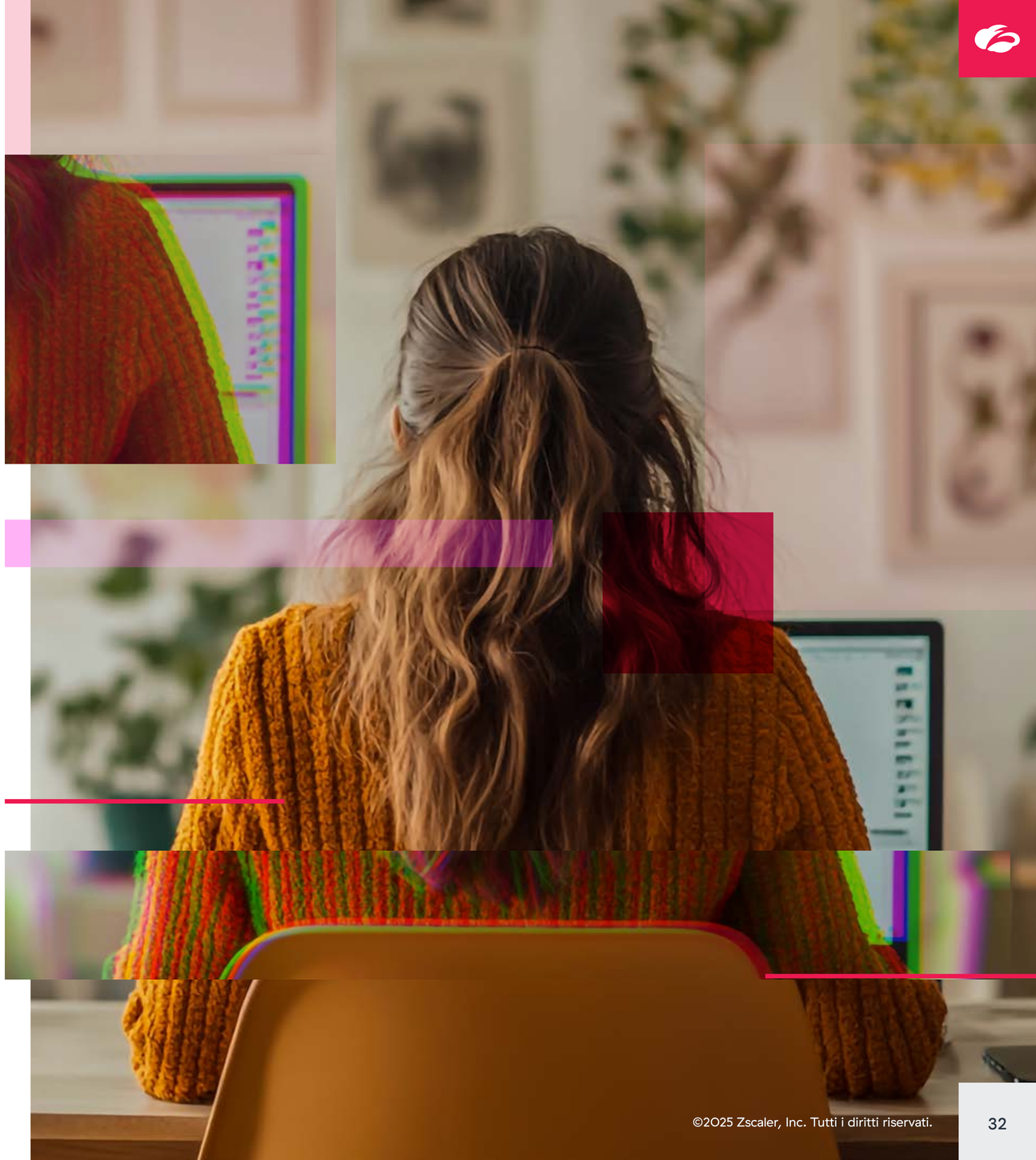
ZPA si integra con gli strumenti di valutazione del profilo di sicurezza degli endpoint per verificare il livello di sicurezza dei dispositivi degli utenti prima di concedere l'accesso. In questo modo, è possibile garantire che solo i dispositivi conformi possano connettersi, riducendo i rischi derivanti dai dispositivi non gestiti o compromessi.

Offri agli utenti esperienze di livello superiore

ZPA garantisce esperienze utente ottimali offrendo una connettività rapida, fluida e sicura alle applicazioni aziendali critiche. A differenza delle VPN, che indirizzano il traffico attraverso un data center centralizzato, ZPA consente connessioni dirette tra utenti e applicazioni tramite Zero Trust Exchange. Questo riduce drasticamente la latenza e migliora le prestazioni delle applicazioni, indipendentemente dal fatto che gli utenti siano in sede, in remoto o in movimento. Riducendo al minimo gli accessi multipli e la dipendenza da software basati su client, ZPA semplifica l'accesso e incrementa la produttività. Inoltre, le funzionalità di monitoraggio proattivo di ZPA agevolano la risoluzione dei problemi, garantendo un accesso senza interruzioni e di alta qualità a tutti gli utenti.

Abbatti il costo totale di proprietà (TCO)

ZPA riduce significativamente il costo totale di proprietà, eliminando la necessità di ricorrere all'impiego di svariati prodotti non integrati, come VPN, firewall, NAC e concentratori VPN. Basata su un'architettura zero trust nativa del cloud, la soluzione ZPA consente di eliminare i costi infrastrutturali relativi al supporto dell'hardware, alla manutenzione, alle riparazioni e agli aggiornamenti. La gestione semplificata e l'applicazione automatizzata delle policy abbattono anche i costi operativi, consentendo ai team IT di risparmiare tempo e risorse ed elevando al contempo sicurezza e scalabilità.



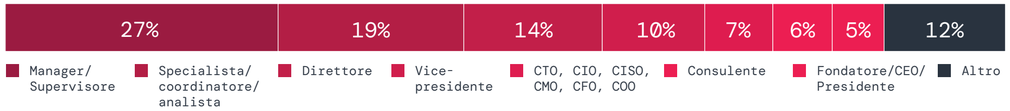
©2025 Zscaler, Inc. Tutti i diritti riservati.



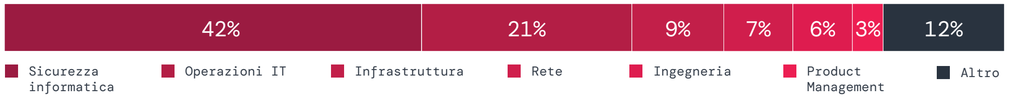
Metodologia e dati demografici

Questo report si basa su un'indagine approfondita condotta all'inizio del 2025 su 632 professionisti IT e della sicurezza informatica, e ha esaminato i rischi associati alla sicurezza delle VPN, le tendenze relative ai modelli di accesso adottati dalle aziende e l'adozione delle architetture zero trust. Tra gli intervistati ci sono dirigenti, professionisti della sicurezza informatica e responsabili delle infrastrutture di rete operanti in vari settori. I risultati di questo report restituiscono una prospettiva supportata dai dati che delinea il declino delle VPN e il passaggio allo zero trust, offrendo spunti utili per le organizzazioni che intendono modernizzare le proprie strategie per la sicurezza dell'accesso.

Livello carriera



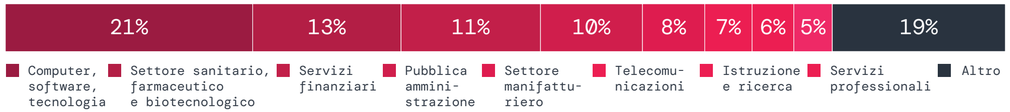
Reparto



Dimensioni dell'azienda



Settore



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

Informazioni su ThreatLabz

ThreatLabz è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti è responsabile della ricerca di nuove minacce e della protezione costante delle migliaia di aziende che utilizzano la piattaforma globale di Zscaler. Oltre alla ricerca sui malware e all'analisi del loro comportamento, i membri del team si occupano delle attività di ricerca e sviluppo di nuovi prototipi per la protezione contro le minacce avanzate sulla piattaforma Zscaler. Inoltre, conducono regolarmente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler siano in linea con gli standard di conformità. Sul suo portale, ThreatLabz pubblica regolarmente analisi approfondite sulle minacce nuove ed emergenti: **research.zscaler.com**.

Informazioni su Cybersecurity Insiders

CYBERSECURITY INSIDERS: LA TUA FONTE AFFIDABILE DI INFORMAZIONI SULLA SICUREZZA INFORMATICA BASATE SUI DATI

Cybersecurity Insiders fornisce informazioni utili corroborate dai dati e convalide indipendenti, consentendo ai responsabili della sicurezza informatica di prendere decisioni strategiche e ben ponderate. Basandoci su oltre un decennio di ricerca con una rete globale che conta oltre 600.000 professionisti della sicurezza informatica, forniamo informazioni concrete che aiutano i leader a orientarsi tra minacce in continua evoluzione, valutare le nuove tecnologie e definire strategie lungimiranti con una maggiore sicurezza.

Per i fornitori di soluzioni di sicurezza informatica, trasformiamo i dati delle ricerche in risultati concreti, consolidandone la credibilità, la fruibilità e l'attendibilità attraverso formati di grande impatto, come report di mercato basati sui dati e webinar che contribuiscono a delineare una leadership di pensiero, linee guida per i CISO che illustrano le best practice, recensioni dei prodotti che valutano le soluzioni, articoli pratici che istruiscono gli acquirenti e riconoscimenti che elevano la reputazione dei marchi.

Combinando questi contenuti con la distribuzione integrata, aiutiamo i marchi a consolidare la fiducia dei loro clienti, ad aumentare la consapevolezza e a stimolare la domanda nel mercato altamente competitivo della sicurezza informatica.

Per saperne di più: **cybersecurity-insiders.com**



Holger Schulze,
CEO e Fondatore
di Cybersecurity Insiders

©2025 Zscaler, Inc. Tutti i diritti riservati.



zscaler™ | Zero Trust Everywhere

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **www.zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

© 2025 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su **zscaler.com/it/legal/trademarks** sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi titolari.

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

