Report del 2024 di Zscaler ThreatLabz sui rischi delle VPN

Cybersecurity INSIDERS

Esplora le principali tendenze relative alla sicurezza, ai rischi e all'esperienza utente che si ottengono con le VPN, mentre l'adozione dello zero trust è sempre più diffusa.

Contenuti

Panoramica

L'odierno ambiente di lavoro distribuito e incentrato sul cloud ha portato a un cambiamento nei metodi di accesso dalle tradizionali reti private virtuali (VPN) a strutture di sicurezza più robuste, come lo Zero Trust. Tradizionalmente, le VPN fornivano funzionalità di accesso remoto essenziali per connettere utenti o interi uffici. Tuttavia, la crescente sofisticazione delle minacce informatiche e l'espansione della forza lavoro da remoto e delle tecnologie cloud hanno messo in luce le significative vulnerabilità nelle VPN. A causa della loro architettura legacy, le VPN garantiscono un accesso alla rete eccessivamente ampio una volta verificate le credenziali, aumentando significativamente il rischio di attacchi informatici in caso di compromissione delle credenziali.

Vari recenti exploit di alto profilo delle apparecchiature VPN hanno evidenziato vulnerabilità critiche (in particolare CVE-2023-46805, CVE-2024-21887 e CVE-2024-21893) che colpiscono settori essenziali, inclusa la difesa statunitense. Queste vulnerabilità consentono agli aggressori di aggirare l'autenticazione, eseguire comandi con privilegi elevati e mantenere la persistenza dopo il ripristino del dispositivo. In risposta, la Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti ha emesso una direttiva di emergenza alle agenzie federali affinché disconnettano immediatamente i dispositivi VPN interessati a causa dei sostanziali rischi per la sicurezza.

Attraverso l'ordine esecutivo 14028, il governo degli Stati Uniti impone l'adozione di architetture zero trust per migliorare la sicurezza informatica e abbandonare le VPN tradizionali. Questa direttiva, che fa parte di una strategia globale per rafforzare la sicurezza informatica nazionale, incarica le agenzie federali di implementare lo zero trust per la verifica ogni richiesta di accesso indipendentemente dall'origine. L'Office of Management and Budget (OMB) sostiene ulteriormente questa iniziativa con una dettagliata strategia zero trust a livello federale, sottolineando la necessità di un passaggio dalla fiducia implicita basata su VPN all'interno dei perimetri di rete alla verifica continua di tutte le richieste di accesso. Queste direttive e raccomandazioni mostrano che la comunità della sicurezza informatica è d'accordo sulla difesa più solida fornita dallo zero trust contro le complesse minacce informatiche in evoluzione, una necessità sottolineata dalle recenti vulnerabilità e dagli exploit legati alle VPN tradizionali.

Di conseguenza, le organizzazioni stanno rapidamente adottando modelli zero trust, i quali non si basano sull'assegnazione della fiducia intrinseca a utenti o dispositivi all'interno o all'esterno del perimetro di rete, ma richiedono una verifica granulare per ogni richiesta di accesso. Questo approccio è particolarmente efficace nel prevenire il movimento laterale all'interno delle reti, un exploit che gli aggressori spesso utilizzano per incrementare il proprio livello di intrusione dopo aver ottenuto l'accesso iniziale.

Basato su un sondaggio che ha coinvolto 647 professionisti IT e della cybersecurity, questo report analizza le molteplici sfide legate alla sicurezza e all'esperienza utente che si ottengono con la VPN; oltre a mostrare la complessità della gestione degli accessi mette in luce anche le vulnerabilità ai diversi tipi di attacchi informatici e il relativo potenziale di compromissione del profilo di sicurezza generale delle organizzazioni. Il report delinea inoltre modelli di sicurezza più avanzati, in particolare quello dello Zero Trust, che si è saldamente affermato come un framework solido e a prova di futuro per proteggere e accelerare la trasformazione digitale.

Siamo grati a Zscaler per aver contribuito a questo sondaggio sui rischi VPN. La loro esperienza nelle soluzioni Zero Trust e di accesso sicuro ha arricchito significativamente i nostri risultati. Siamo certi che gli spunti offerti da questo report consentiranno ai professionisti dell'IT e della sicurezza informatica di poter affrontare al meglio il loro percorso verso la sicurezza zero trust.

Grazie,
Holger Schulze, fondatore di Cybersecurity Insiders

"Nell'ultimo anno, numerose vulnerabilità critiche delle VPN sono servite da punti di ingresso efficaci per attacchi contro grandi aziende ed enti federali. Considerando questi avvenimenti ripetuti, le aziende devono essere consapevoli che gli aggressori sfrutteranno sempre più queste risorse datate esposte a Internet (tramite apparecchiature fisiche e virtuali) che consentono loro di spostarsi facilmente lateralmente attraverso le tradizionali reti piatte. È essenziale quindi passare a un'architettura Zero Trust in grado di ridurre significativamente la superficie di attacco con l'eliminazione delle tecnologie datate come VPN e firewall, l'applicazione di controlli di sicurezza coerenti con l'ispezione TLS e la limitazione del raggio di aggressione con la segmentazione e la deception, prevenendo così violazioni dannose".

— DEEPEN DESAI, CHIEF SECURITY OFFICER DI ZSCALER

Risultati principali

Gli attacchi alle VPN sono in aumento.

Il 56% delle organizzazioni ha subito uno o più attacchi informatici legati alle VPN nell'ultimo anno, un dato in aumento rispetto al 45% dell'anno precedente; questo evidenzia la crescente frequenza e sofisticazione di questi attacchi.

La stragrande maggioranza delle aziende sta passando alla Zero Trust.

il 78% delle organizzazioni prevede di implementare strategie Zero Trust nei prossimi dodici mesi. Nel frattempo, il 62% delle aziende concorda sul fatto che le VPN sono agli antipodi dello zero trust.

La maggior parte delle persone ha dubbi sulla sicurezza delle VPN.

Il 91% degli intervistati ha espresso preoccupazione riguardo alla possibile compromissione, a causa delle VPN, del proprio ambiente di sicurezza IT, in seguito alle recenti violazioni che hanno messo in evidenza i rischi derivanti dal mantenimento di infrastrutture VPN obsolete o prive di patch.

Le VPN non possono competere con ransomware, malware e DDoS.

Gli intervistati hanno identificato ransomware (42%), malware (35%) e attacchi DDoS (30%) come le principali minacce che sfruttano le vulnerabilità delle VPN, sottolineando la portata dei rischi che le organizzazioni devono affrontare a causa delle debolezze intrinseche delle tradizionali architetture VPN.

Il rischio di movimento laterale non può essere ignorato.

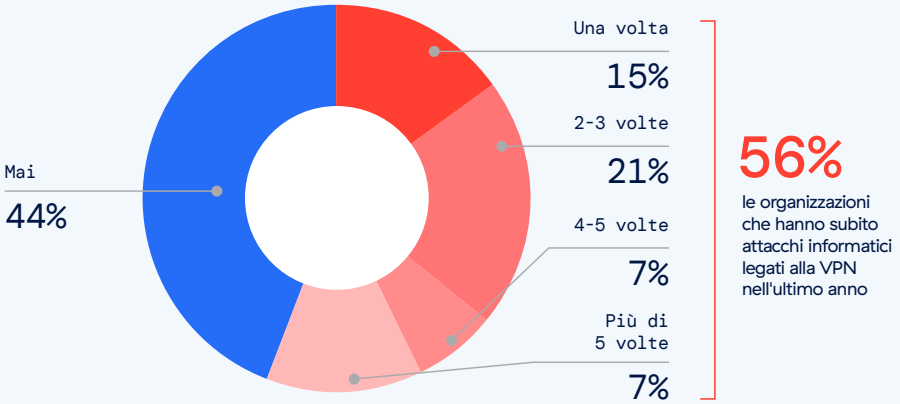
Il 53% delle aziende violate tramite vulnerabilità VPN afferma che gli autori delle minacce si sono mossi lateralmente, dimostrando fallimenti di contenimento nel punto iniziale di compromissione che sottolineano i rischi delle reti tradizionali e piatte.

Problemi di sicurezza con le VPN

Attacchi alle VPN in aumento

La frequenza e la gravità degli attacchi che sfruttano le vulnerabilità delle VPN evidenziano l'inefficacia delle misure di sicurezza informatica convenzionali e sottolineano i rischi persistenti posti dall'esposizione della rete. Il nostro sondaggio rivela che, nell'ultimo anno, il 56% delle organizzazioni ha subito attacchi informatici che hanno sfruttato le vulnerabilità della VPN, un aumento significativo rispetto al 45% dell'anno precedente. Inoltre, il 41% delle organizzazioni ha riferito di aver subito due o più attacchi legati alla VPN, indicando gravi lacune nella sicurezza.

Negli ultimi 12 mesi, quante volte la tua organizzazione ha subito un attacco che ha sfruttato le vulnerabilità di sicurezza presenti nei server VPN?

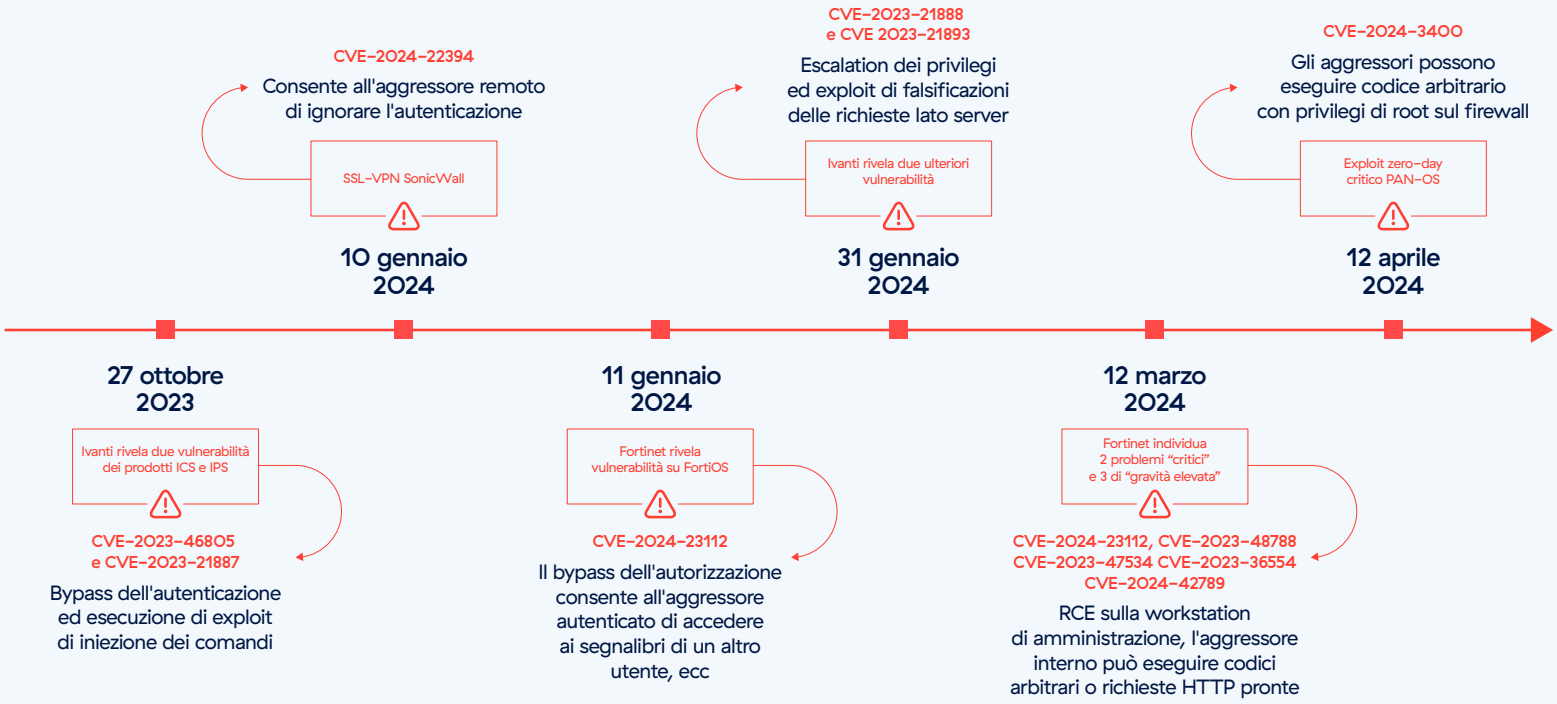


Le tendenze recenti confermano che gli attacchi alle VPN stanno diventando non solo più frequenti, ma anche più sofisticati. Ad esempio, sono sempre di più i casi di ransomware che, sfruttando i difetti delle VPN, in particolare in seguito a vulnerabilità divulgate pubblicamente, ne sottolineano le debolezze inerenti. Queste vulnerabilità offrono agli aggressori facili punti di ingresso per infiltrarsi nelle reti e facilitare il movimento laterale, portando a sostanziali violazioni dei dati e interruzioni operative.

Le principali vulnerabilità della VPN riscontrate nell'ultimo anno

Considerando la recente serie di CVE di elevata gravità che influiscono sui prodotti VPN, non sorprende che le aziende segnalino sempre più attacchi che sfruttano questo tipo di vulnerabilità. Naturalmente, nessun singolo fornitore o particolare tecnologia può essere immune dalle vulnerabilità del software. Nel caso della VPN, ogni CVE può rappresentare un punto cieco nella sicurezza dell'azienda: una testa di ponte che consente agli aggressori di compromettere una risorsa VPN, stabilire la persistenza, spostarsi lateralmente attraverso la rete e rubare dati. Poiché le CVE delle VPN continuano a essere rese note a questo ritmo, rappresenteranno un rischio persistente per le aziende che utilizzano questa tecnologia per la connettività remota.

Una serie di recenti CVE evidenzia un difetto di architettura



Come affrontare i problemi di sicurezza delle VPN

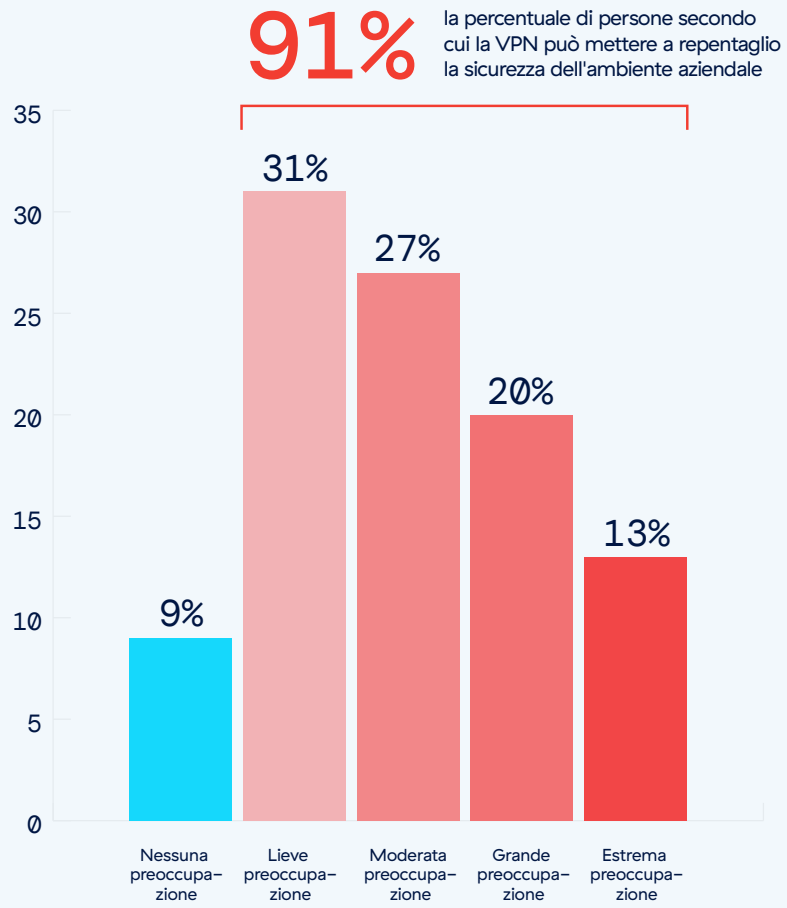
I risultati del sondaggio riflettono una grande preoccupazione riguardo alle VPN che possono compromettere gli ambienti di sicurezza, in linea con le tendenze attuali e l'aumento delle vulnerabilità nelle tecnologie VPN. La stragrande maggioranza degli intervistati (il 91%, in aumento rispetto all'88% nel 2023) esprime preoccupazione per le VPN, che sono considerate rischiose per la sicurezza IT; questo dimostra una maggiore consapevolezza tra le organizzazioni riguardo i rischi legati alle VPN.

Questa preoccupazione è giustificata dai recenti exploit che hanno preso di mira le VPN Ivanti, in cui gli aggressori hanno sfruttato gravi vulnerabilità per penetrare nelle reti ed esfiltrare dati sensibili. Questi incidenti, che coinvolgono vulnerabilità come CVE-2024-21888 e CVE-2024-21893, evidenziano i rischi legati al mantenimento e alla protezione di infrastrutture VPN obsolete o prive di patch. Inoltre, l'architettura intrinseca delle VPN pone notevoli rischi per la sicurezza nell'odierno panorama digitale senza perimetro. Man mano che le aziende adottano sempre più servizi cloud, e con l'evoluzione dei modelli di lavoro remoto, le VPN devono affrontare nuove sfide di sicurezza, tra cui la gestione dei diritti di accesso e la protezione di una superficie di attacco in espansione.

Queste vulnerabilità e limitazioni architetturali sottolineano un cambiamento fondamentale di percezione nei confronti delle VPN, che si allinea alle tendenze più ampie della sicurezza informatica secondo cui è necessario adottare framework più dinamici e resilienti come lo zero trust.

Le organizzazioni lungimiranti passano alle architetture zero trust per ottenere un controllo più granulare e ridurre significativamente la superficie di attacco non attribuendo mai una fiducia implicita, sia all'interno che all'esterno del perimetro di rete. L'adozione di tale strategia è utile per affrontare le vulnerabilità immediate delle VPN tradizionali ed è in linea con un approccio proattivo alla sicurezza informatica, una necessità importante per adattarsi al panorama delle minacce in evoluzione.

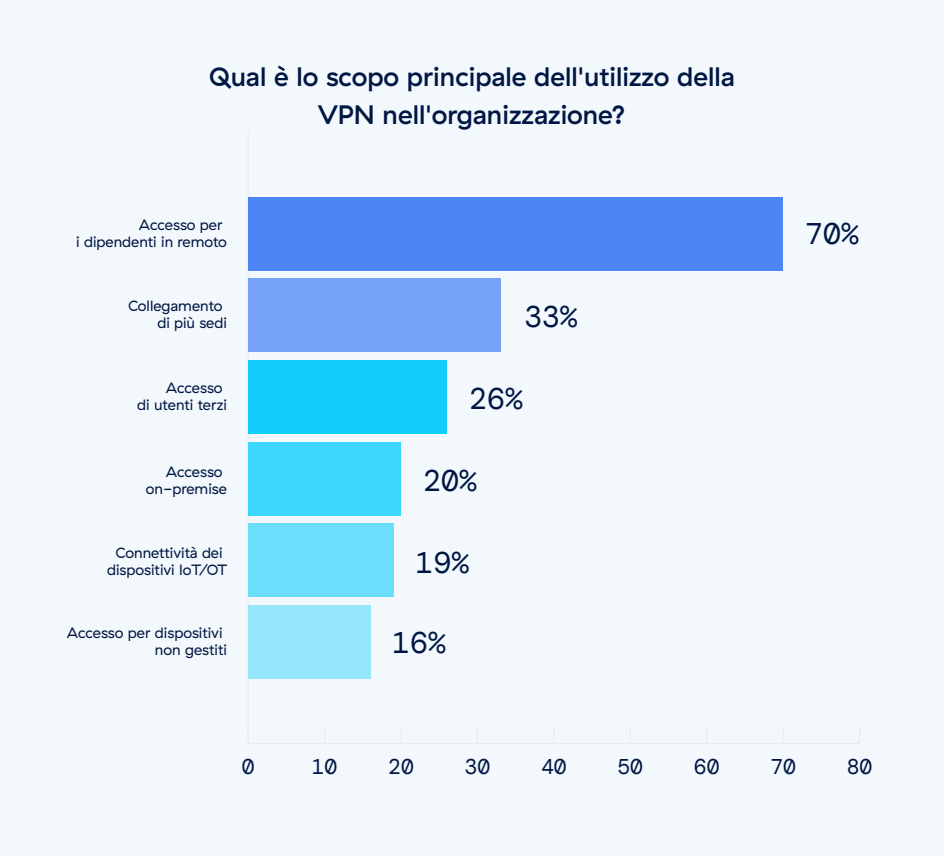
In che misura l'organizzazione è preoccupata del fatto che la VPN possa mettere a rischio la capacità di preservare la sicurezza dell'ambiente?



Gli scenari principali di accesso sicuro

Capire perché le organizzazioni utilizzano le VPN è essenziale, in quanto mette in luce il modo in cui le aziende danno priorità all'accesso sicuro. Rivela inoltre quali casi d'uso sono più esposti a rischi per la sicurezza indicando le aree che richiedono strategie più solide e innovative.

Un significativo 70% delle organizzazioni utilizza le VPN principalmente per tutelare l'accesso dei dipendenti in remoto. Questo utilizzo diffuso rende l'accesso da remoto un obiettivo primario per gli attacchi informatici. Il 33% utilizza le VPN per connettere più siti, con rischi sostanziali, perché queste connessioni possono fungere da vettori di attacchi informatici se non adeguatamente protette. Inoltre, il 26% delle organizzazioni ha ampliato l'accesso a terzi, e questo complica ulteriormente le cose a causa dei diversi atteggiamenti di sicurezza degli stakeholder esterni e della mancanza di controllo sulle policy di sicurezza. Infine, il 20% delle organizzazioni utilizza le VPN per l'accesso in sede e il 19% le utilizza per la connettività con dispositivi IoT/OT.



Le VPN non forniscono più una sicurezza adeguata nei critici casi di accesso di oggi. Queste tecnologie operano infatti su modelli di fiducia obsoleti che garantiscono un ampio accesso alla rete previa una semplice autenticazione dell'utente. Questo accesso ampio espone le organizzazioni a rischi significativi e consente ai potenziali aggressori di sfruttare un unico punto di ingresso per navigare ed estrarre dati sensibili attraverso la rete.

Gestione, prestazioni ed esperienza utente con le VPN

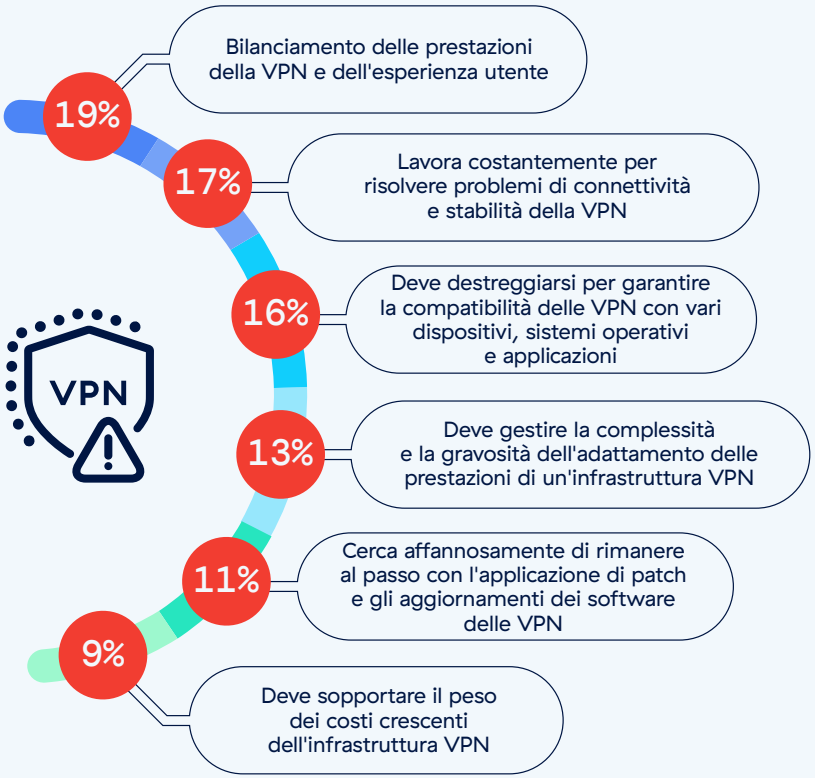
Sfide nella gestione delle VPN

Oltre ai rischi intrinseci per la sicurezza, la gestione delle infrastrutture VPN presenta sfide significative per i team IT poiché, per garantire l'affidabilità delle soluzioni di accesso, vi sono requisiti più stringenti negli ambienti di lavoro frammentati e incentrati sul cloud. La sfida gestionale principale per i professionisti IT è quella di trovare il giusto equilibrio tra le prestazioni della VPN e l'esperienza dell'utente (19%). Questo problema è cruciale, in quanto ha un impatto diretto sulla produttività: se la VPN rallenta la rete o si rivela troppo scomoda da utilizzare, può portare a una minore soddisfazione dei dipendenti e a processi aziendali lenti e inefficienti.

La seconda preoccupazione più comune, citata dal 17% degli intervistati, è la costante attività di risoluzione dei problemi di connettività e stabilità della VPN. Questi problemi non solo prendono molto tempo al personale IT, ma causano anche frustranti interruzioni per gli utenti. Altre sfide degne di nota includono la mancanza di compatibilità delle VPN con una varietà più ampia di dispositivi, sistemi operativi e applicazioni, ritenuta critica da circa il 16% dei professionisti IT. Inoltre, il 13% degli intervistati deve affrontare la complessità e l'intenso lavoro richiesto dall'aumento di portata dell'infrastruttura VPN, un problema critico quando le organizzazioni crescono e le loro esigenze aumentano in un contesto di grave carenza di professionisti qualificati della sicurezza informatica.

Queste informazioni sottolineano la necessità per le organizzazioni di esplorare alternative più agili, facili da usare e che richiedano meno risorse, come i modelli di accesso alla rete Zero Trust (ZTNA). Lo ZTNA offre un controllo più granulare, una maggiore scalabilità e una riduzione del carico di gestione; queste caratteristico lo rendono una scelta superiore rispetto alle tradizionali VPN nel dinamico panorama della sicurezza informatica di oggi.

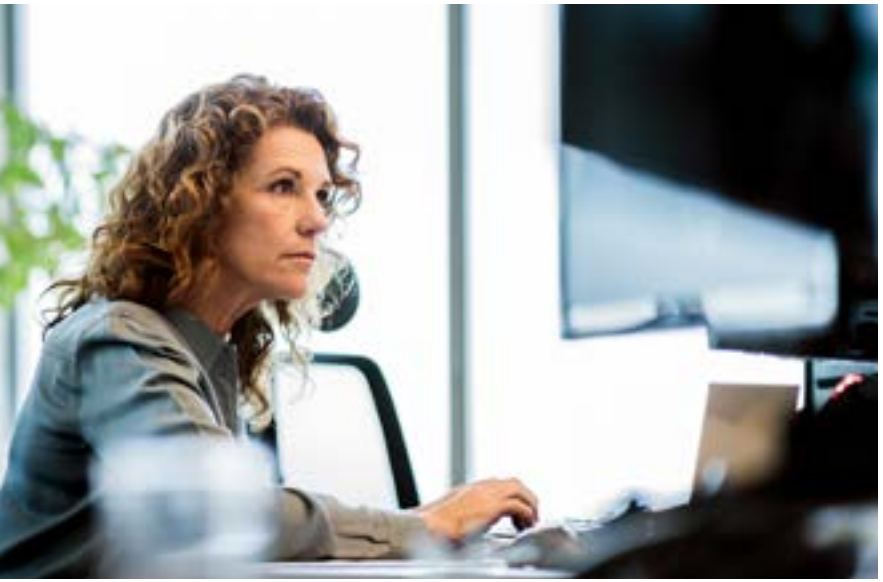
Qual è il principale problema riscontrato dall'organizzazione nella gestione dell'infrastruttura VPN?



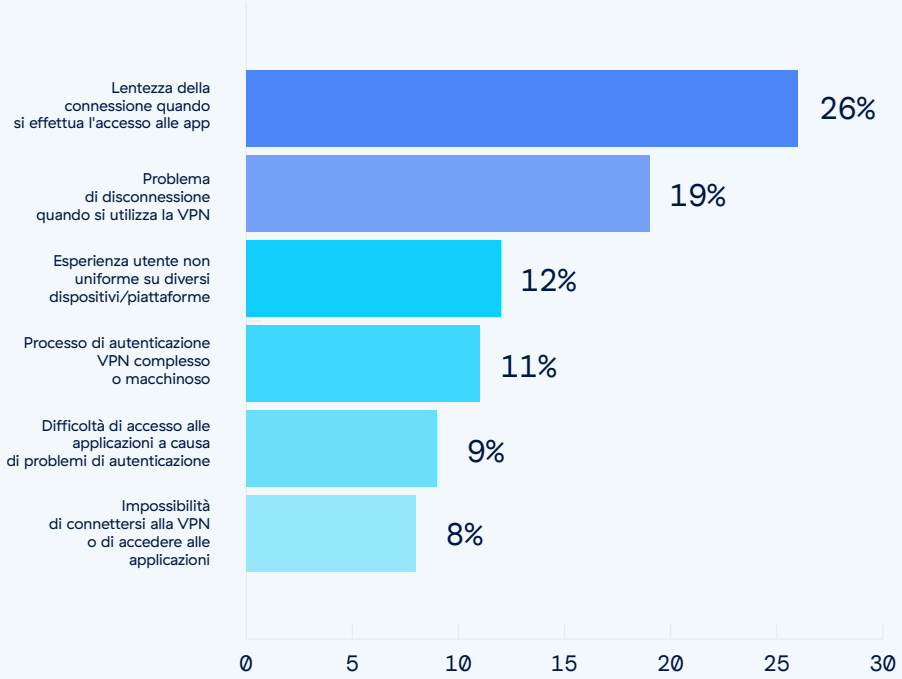
Sfide comuni per gli utenti delle VPN

La lamentela più frequente degli utenti delle VPN, come notato dal 26% degli intervistati, riguarda la bassa velocità di connessione. Questo evidenzia un problema critico di produttività e soddisfazione degli utenti, poiché la lentezza delle connessioni può ridurre significativamente l'efficienza delle attività di routine e l'accesso alle risorse basate su cloud, soprattutto per chi lavora da casa.

Le interruzioni della connessione VPN rappresentano il secondo problema più comune, citato dal 19% degli intervistati. Questo problema può interrompere le attività e le comunicazioni in corso, influenzando in modo significativo l'esperienza utente e la continuità operativa. Il problema derivante da esperienze utente incostanti tra diversi dispositivi e piattaforme, segnalato dal 12% degli utenti, indica la necessità di una maggiore uniformità delle prestazioni.

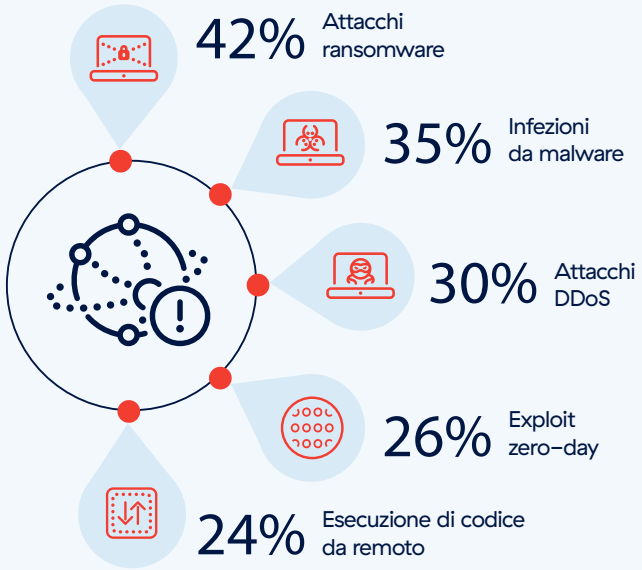


Qual è la lamentela che viene segnalata più frequentemente dagli utenti che accedono alle applicazioni tramite VPN?



Per affrontare queste preoccupazioni, le organizzazioni dovrebbero prendere in considerazione soluzioni di accesso alla rete che offrano maggiore stabilità e coerenza tra le varie piattaforme. L'implementazione di un'architettura zero trust può essere particolarmente efficace, poiché migliora la sicurezza senza introdurre colli di bottiglia nelle prestazioni. Le reti zero trust garantiscono che i problemi di connessione non compromettano la sicurezza e che il controllo degli accessi sia rigoroso e adattabile ai diversi ambienti d'uso.

Quali sono i tipi di attacchi informatici maggiormente in grado di sfruttare le vulnerabilità delle VPN dell'organizzazione?



Per contrastare queste vulnerabilità, le organizzazioni dovrebbero adottare misure di sicurezza proattive, come un modello zero trust. Lo zero trust impone severi controlli di accesso e una verifica continua di tutte le connessioni di rete, indipendentemente dalla loro origine. Questa strategia mitiga efficacemente i rischi posti da un'ampia gamma di attacchi che sfruttano i punti deboli della VPN, limitando il movimento laterale e rafforzando i controlli di accesso.

Exploit della vulnerabilità della VPN

La varietà di attacchi informatici che sfruttano i punti deboli delle VPN evidenzia la portata dei rischi che le organizzazioni devono affrontare. Secondo il 42% degli intervistati, la VPN è più suscettibile agli attacchi ransomware; questo ne evidenzia il significativo impatto e la frequenza degli eventi. Seguono le infezioni malware, segnalate dal 35% degli intervistati, e gli attacchi DDoS, riportati dal 30%, che possono compromettere la disponibilità, la riservatezza e l'integrità dei sistemi.

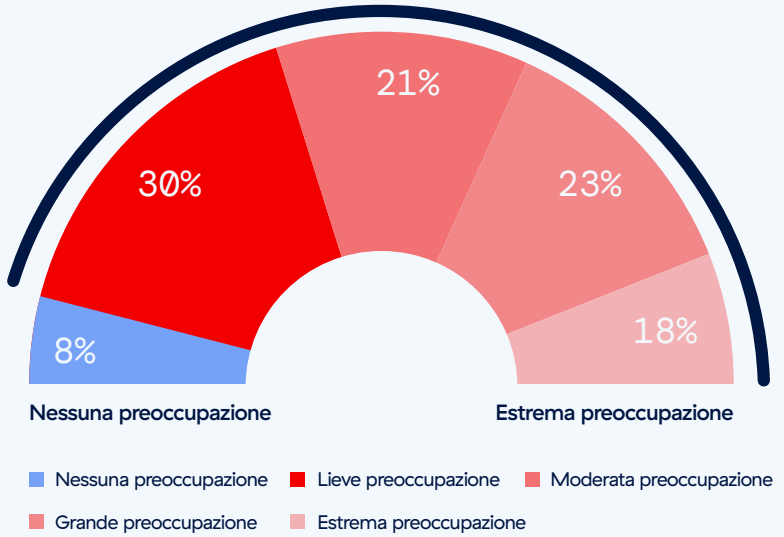
Rischio associati a terzi con le VPN

L'indagine sottolinea una significativa preoccupazione riguardo all'accesso VPN di terze parti come vulnerabilità della sicurezza della rete. Un notevole 92% degli intervistati esprime preoccupazione per questo rischio, segnando un leggero aumento rispetto al 90% del 2023. Questo crescente riconoscimento evidenzia l'accesso di terze parti come potenziale causa dell'apertura di un punto di ingresso per le minacce informatiche.

I nuovi approfondimenti sulle vulnerabilità e sulle violazioni delle VPN hanno ulteriormente convalidato queste preoccupazioni. Le VPN tradizionali in genere forniscono un accesso ampio alla rete successivamente alla verifica delle credenziali di accesso, e comportano rischi se le misure di sicurezza dei fornitori terzi vengono compromesse.

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

92% percentuale di persone che crede che gli utenti terzi possano causare potenziali backdoor nella loro rete attraverso l'accesso VPN



Le organizzazioni dovrebbero accelerare la transizione dalle VPN tradizionali alle architetture zero trust. Questo cambiamento implica l'implementazione di sistemi che verifichino rigorosamente le richieste di accesso in base all'identità e al contesto, limitando i fornitori terzi risorse specifiche essenziali per le loro attività.

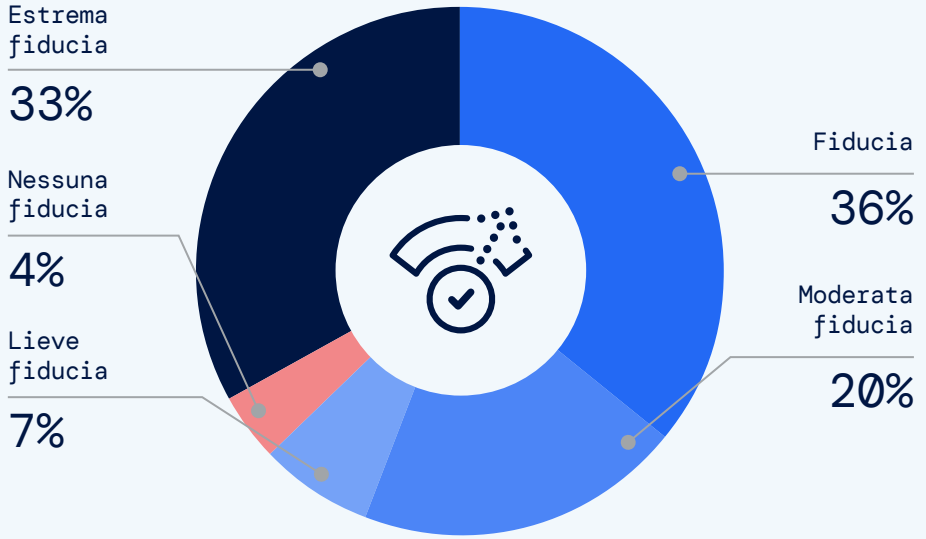
Problemi di sicurezza con l'infrastruttura VPN

Eccessiva fiducia nella sicurezza delle VPN

La recente ondata di violazioni delle VPN evidenzia una disconnessione tra la sicurezza percepita e il rischio reale. I recenti gravi exploit nei prodotti VPN ci fanno capire che anche le organizzazioni ben preparate potrebbero sottovalutare le capacità degli avversari informatici che sfruttano le vulnerabilità inerenti alla tecnologia VPN. Un significativo 69% degli intervistati ha citato di avere un'elevata fiducia nella capacità della propria organizzazione di gestire le vulnerabilità delle VPN, che potrebbe non essere completamente in linea con il panorama delle minacce in aumento, in cui abili aggressori sfruttano molto rapidamente anche i punti deboli più ridotti. L'eccessiva sicurezza può essere particolarmente rischiosa data la complessità e la persistenza dei recenti exploit delle VPN, come dimostrato dagli incidenti che coinvolgono gruppi supportati da stati e bande di criminali informatici che prendono di mira sistemi senza patch per periodi prolungati.

Le organizzazioni devono ricalibrare la propria posizione in materia di sicurezza incorporando rigorose valutazioni delle vulnerabilità, aggiornamenti frequenti e una formazione completa sulla consapevolezza in materia di questi temi. È consigliabile adottare un approccio di sicurezza a più livelli che non faccia eccessivo affidamento sulle VPN per una protezione completa. Questo approccio dovrebbe includere il monitoraggio avanzato, il rilevamento delle anomalie e l'integrazione dei principi zero trust.

Quanto credi nella capacità della tua organizzazione di rilevare e mitigare le vulnerabilità della VPN che la espongono ad attacchi di sicurezza informatica?



Vettori di attacco ransomware

L'indagine identifica chiaramente le vulnerabilità delle risorse esposte all'esterno come il potenziale vettore di attacco ransomware più preoccupante, rilevato dal 33% degli intervistati. Si tratta di un consenso diffuso sui rischi associati alle applicazioni web o ai servizi di rete esposti, che spesso rappresentano il primo punto di ingresso per gli attacchi ransomware.

Il furto dell'identità segue con il 26%, a sottolineare il ruolo svolto dalle credenziali compromesse nel consentire agli aggressori di aggirare le misure di sicurezza e ottenere l'accesso per distribuire payload ransomware. Le preoccupazioni circa le vulnerabilità nelle infrastrutture desktop virtuali (VDI) e gli attacchi da parte degli stati-nazione, rispettivamente al 14% e al 12%, evidenziano le diverse origini delle minacce ransomware da cui le organizzazioni devono difendersi. Scattered Spider (un gruppo di criminali informatici che utilizza sofisticate tattiche di ingegneria sociale, tra cui phishing, attacchi di autenticazione multifattore e scambio di SIM), preoccupa l'11% dei partecipanti.

Le organizzazioni dovrebbero migliorare le proprie difese e i protocolli di gestione dell'identità. L'implementazione di processi completi di gestione delle vulnerabilità e l'adozione di un modello di sicurezza zero trust possono ridurre efficacemente il rischio di attacchi ransomware negando l'accesso alle risorse di rete e la diffusione laterale.

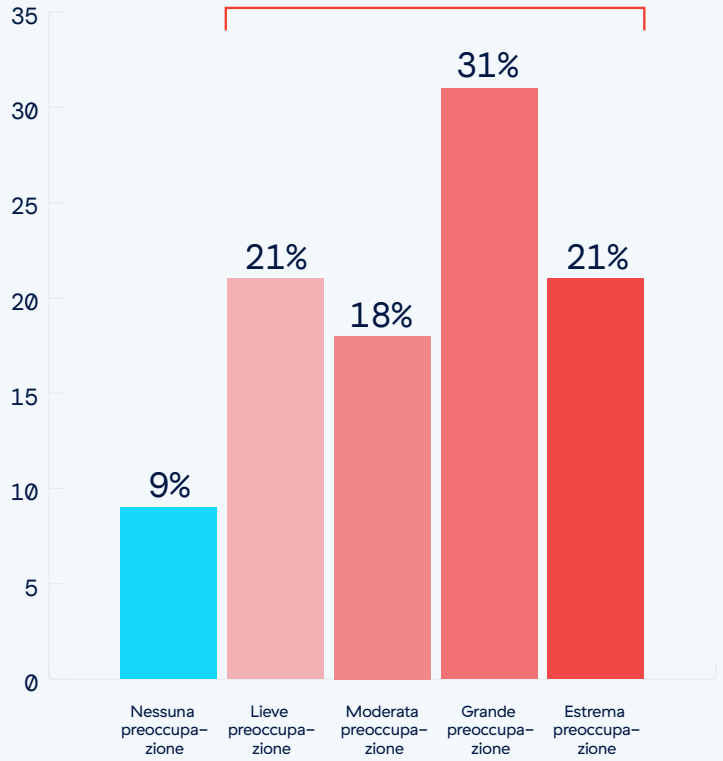
Preoccupazioni relative ai ransomware

I risultati del sondaggio mostrano che il 52% degli intervistati è molto o estremamente preoccupato per la minaccia dei ransomware a causa di vulnerabilità non risolte da patch. Si tratta di una preoccupazione giustificata, dal momento che le vulnerabilità senza patch rimangono un vettore di attacco primario per i ransomware. Alcune recenti analisi mostrano che una parte sostanziale degli attacchi ransomware sfrutta queste vulnerabilità e riesce ad avere un impatto particolarmente grave rispetto ad altri tipi di attacco.

I gruppi di ransomware stanno diventando sempre più sofisticati, e molti di essi utilizzano tattiche elaborate in grado di sfruttare rapidamente le vulnerabilità appena scoperte prima che le organizzazioni possano applicarvi le patch. Questo rapido ciclo di sfruttamento riduce notevolmente la finestra di risposta alle vulnerabilità critiche, evidenziando l'urgente necessità di misure di sicurezza avanzate che riducano la superficie di attacco.

Quanto ti preoccupa la possibilità di essere vittima di ransomware a causa di vulnerabilità senza patch?

91% percentuale di persone preoccupate della possibilità di essere vittime di ransomware a causa di vulnerabilità senza patch



Movimento laterale negli attacchi alle VPN

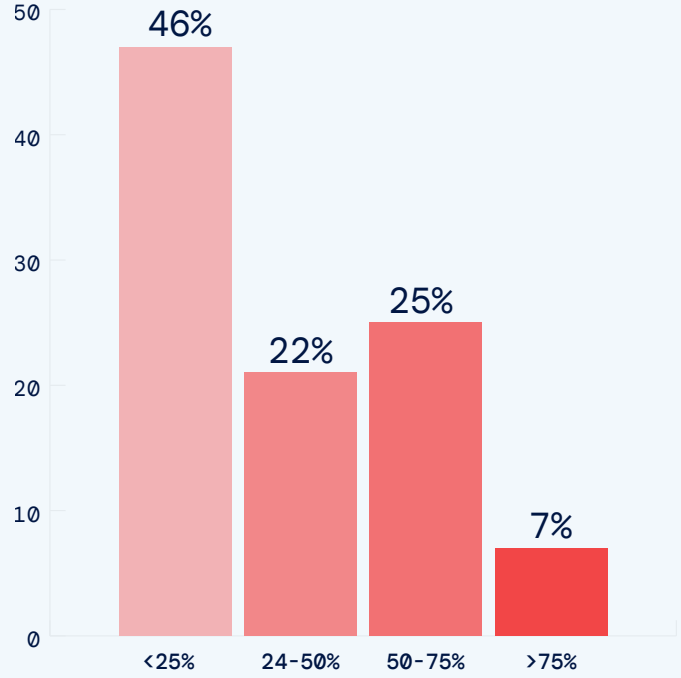
La maggior parte degli intervistati (53%) riferisce che oltre il 25% degli attacchi legati alle VPN ha incluso il movimento laterale, a dimostrazione del dei significativi fallimenti di contenimento nel punto iniziale di compromissione. Quasi un terzo (32%) ha riscontrato movimenti laterali in più della metà degli attacchi, indicando le principali sfide nella fase successiva alla violazione delle difese di rete.

Il movimento laterale rappresenta un rischio significativo con le VPN, perché gli aggressori possono ottenere un ampio accesso alla rete, simile a quello di un utente autenticato. Implementando questa tattica, gli utenti malintenzionati possono muoversi inosservati attraverso la rete e prendere di mira le aree sensibili.

In questo modo, le VPN possono aggravare i rischi ed espandere la portata di un attacco oltre il suo punto di ingresso iniziale. Per risolvere questo problema è necessaria una segmentazione rigorosa, idealmente facendo passare il traffico utente–applicazione tramite un'architettura Zero Trust e un monitoraggio continuo. Questo riduce sostanzialmente il raggio d'azione del movimento laterale, consentendo l'accesso granulare a un insieme più piccolo di applicazioni per ogni singolo utente, mentre il resto viene reso invisibile.

La crescente sofisticazione degli attacchi che sfruttano le vulnerabilità delle VPN sottolinea la necessità di uno spostamento verso un framework zero trust. Applicando severi controlli di accesso e verifiche continue, lo zero trust limita i movimenti laterali non autorizzati e migliora la sicurezza.

Di tutti gli attacchi subiti dalla tua organizzazione, quale percentuale ha sfrutta la diffusione laterale delle minacce dopo aver ottenuto l'accesso tramite VPN?

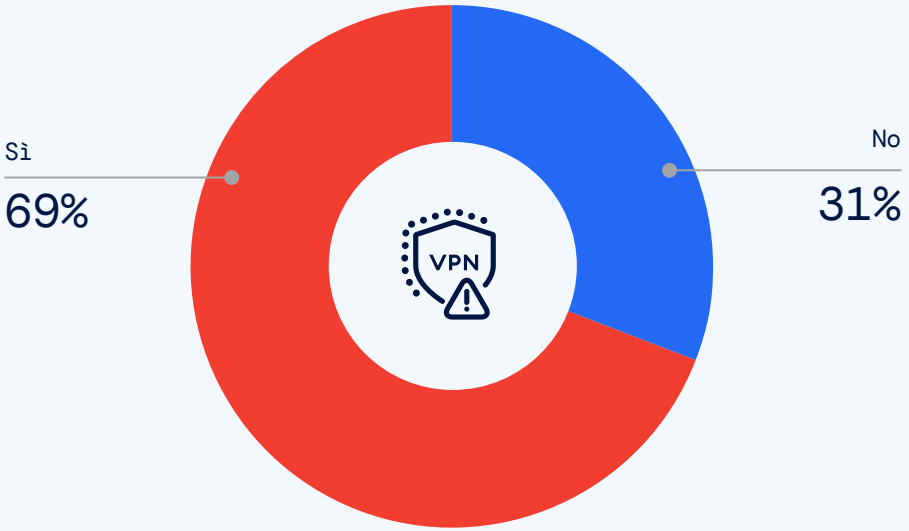


I problemi di sicurezza delle VPN Dopo fusioni e acquisizioni

Le preoccupazioni riguardo all'impatto di fusioni e acquisizioni sulle infrastrutture VPN esistenti mette in luce le potenziali vulnerabilità che derivano dai cambiamenti organizzativi e dall'integrazione di reti diverse.

Un rilevante 69% degli intervistati esprime preoccupazione di subire attacchi informatici in seguito a questo processo, un dato che rende evidente la diffusa preoccupazione per i rischi per la sicurezza associati a questi cambiamenti aziendali. Questo sentimento mostra chiaramente che le attività di fusione e acquisizione possono destabilizzare i framework di sicurezza esistenti aumentando l'esposizione alle minacce informatiche.

Ti preoccupa la possibilità di diventare vittima di un attacco successivo a una fusione o acquisizione con la tua attuale infrastruttura?



Per le aziende, i periodi di transizione derivanti da fusioni e acquisizioni si rivelano un'opportunità unica per eliminare gradualmente le tecnologie VPN antiquate e vulnerabili a favore di framework zero trust. Nello specifico, le architetture Zero Trust migliorano la sicurezza fornendo una segmentazione completa dell'ambiente tra utenti e applicazioni e tra diversi workload filiali e dispositivi, siano essi dispositivi gestiti, non gestiti, sistemi IoT o OT. Questo approccio rafforza in modo significativo la sicurezza durante e dopo la transizione, attraverso una verifica rigorosa di tutti gli utenti e i dispositivi, una segmentazione completa e un'applicazione rigorosa dei controlli di accesso a privilegi minimi.

Adozione aziendale dello Zero Trust

Progressi nell'adozione dello Zero Trust

L'indagine riflette una forte tendenza verso l'adozione di sistemi di sicurezza zero trust, che ne rende evidente il crescente riconoscimento per il miglioramento della sicurezza informatica delle organizzazioni. Un significativo 31% degli intervistati sta già implementando lo zero trust (rispetto al 27% nel 2023), un dato che testimonia la proattività delle aziende nella protezione delle risorse di rete.

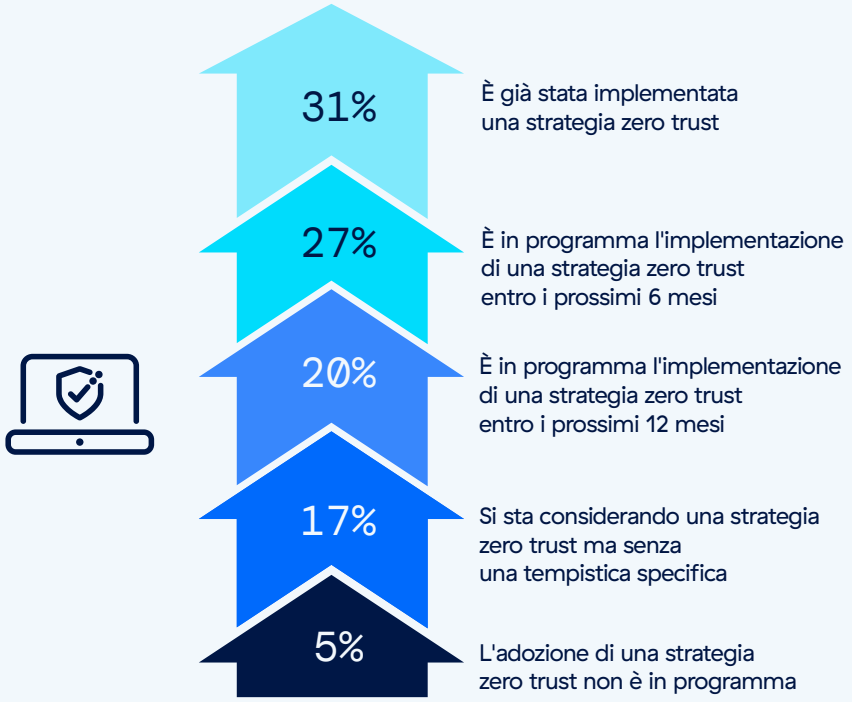
Inoltre, il 27% delle organizzazioni prevede di implementare una strategia zero trust entro i prossimi sei mesi (rispetto al 18% nel 2023), mentre un altro 20% delle organizzazioni prevede di effettuare il passaggio entro i prossimi 12 mesi; questi numeri dimostrano un impegno diffuso verso il passaggio a un approccio zero trust. In breve. più di tre quarti degli intervistati (78%) riconosce l'urgenza e i vantaggi della zero trust.

Tuttavia, il 17% degli intervistati sta ancora considerando una strategia zero trust senza una tempistica specifica (in calo rispetto al 23% nel 2023), evidenziando alcune esitazioni o potenziali sfide nella pianificazione o nell'avvio della transizione. Solo una piccola parte (5%) non segnala piani per l'adozione dello zero trust (in ribasso rispetto all'8% del 2023), forse a causa della mancanza di risorse.

Un'analisi per dimensione aziendale indica che le organizzazioni più grandi incluse nel nostro sondaggio, in particolare quelle con oltre 20.000 dipendenti, hanno maggiori probabilità di adottare strategie zero trust e di farlo con maggiore rapidità: il 33% le sta infatti già implementando. Al contrario, le aziende più piccole con 1.000–5.000 dipendenti mostrano un tasso di adozione leggermente inferiore, pari al 29%, suggerendo che la scala e la disponibilità delle risorse possono influenzare il ritmo e la portata del cambiamento.

Le organizzazioni ancora indecise o che intendono adottare lo zero trust dovrebbero iniziare a valutare il loro attuale livello di sicurezza e l'architettura di rete, per identificare esigenze specifiche e potenziali sfide

Quali sono i tuoi piani in merito all'adozione di una strategia zero trust nella tua organizzazione?

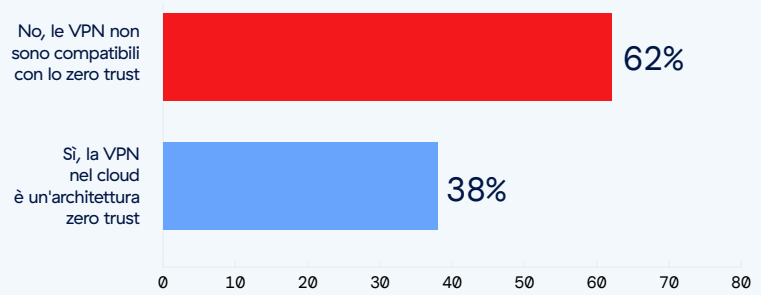


Non si ottiene una sicurezza Zero Trust con le VPN

I risultati del sondaggio riflettono un divario significativo nelle credenze sulla compatibilità delle VPN con i framework di sicurezza Zero Trust. La maggior parte (62%) crede che le VPN siano fondamentalmente "anti-zero trust", a conferma che le tradizionali architetture VPN non si allineano ai principi di questo approccio. Al contrario, il 38% degli intervistati ritiene che le VPN, in particolare le piattaforme basate su cloud, siano compatibili con le architetture zero trust.

Sebbene questa prospettiva possa derivare dal fatto che i fornitori di VPN affermano che le loro soluzioni basate su cloud sono in linea con i principi zero trust, è importante esaminare attentamente queste asserzioni. Il semplice hosting di un servizio VPN nel cloud, ad esempio, non conferisce automaticamente attributi zero trust. La sicurezza zero trust richiede molto più di un semplice ambiente di hosting sicuro; impone un passaggio fondamentale dalle difese basate sul perimetro a un modello in cui la sicurezza è dinamica, granulare e basata sul contesto.

Credi di poter ottenere la sicurezza Zero Trust con le VPN?



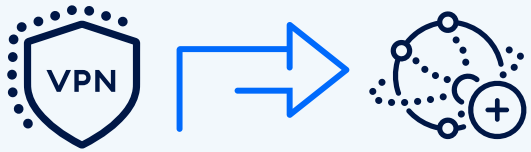
La vera sicurezza zero trust implica la convalida continua di tutti gli utenti e i dispositivi, l'applicazione dell'accesso a privilegi minimi e la segmentazione del traffico per impedire il movimento laterale, funzionalità che le VPN tradizionali, anche quelle basate su cloud, non forniscono. Le organizzazioni devono quindi verificare che qualsiasi VPN a cui viene associato il termine "zero trust" incorpori effettivamente questi principi fondamentali e non faccia solo promesse di marketing.

Passaggio dalla VPN all'accesso alla rete Zero Trust

I risultati del sondaggio mostrano che la maggior parte delle organizzazioni sta effettuando un cambiamento strategico, con il 53% degli intervistati che cita piani per sostituire le soluzioni VPN esistenti con soluzioni ZTNA nel prossimo futuro. Lo ZTNA offre un approccio più flessibile e sicuro grazie all'applicazione di policy basate sul contesto dell'utente, la posizione e la sicurezza del dispositivo, senza presumere l'affidabilità in base alla posizione della rete. Si tratta di un approccio in contrasto con le VPN tradizionali, che generalmente garantiscono un ampio accesso alla rete e generano vulnerabilità nella sicurezza.

Per il 53% delle organizzazioni che si stanno muovendo verso la ZTNA, è fondamentale garantire una transizione graduale e pianificare valutazioni complete del rischio, aggiornando le policy di accesso e istruendo gli utenti sui nuovi protocolli. Nel frattempo, il 47% che non ha ancora intenzione di cambiare dovrebbe valutare le attuali sfide in termini di sicurezza e considerare se la ZTNA potrebbe affrontarle in modo più efficace rispetto alla VPN.

La tua organizzazione ha in programma di sostituire la propria infrastruttura VPN esistente con una soluzione ZTNA (Zero Trust Network Access) nel prossimo futuro?



53%

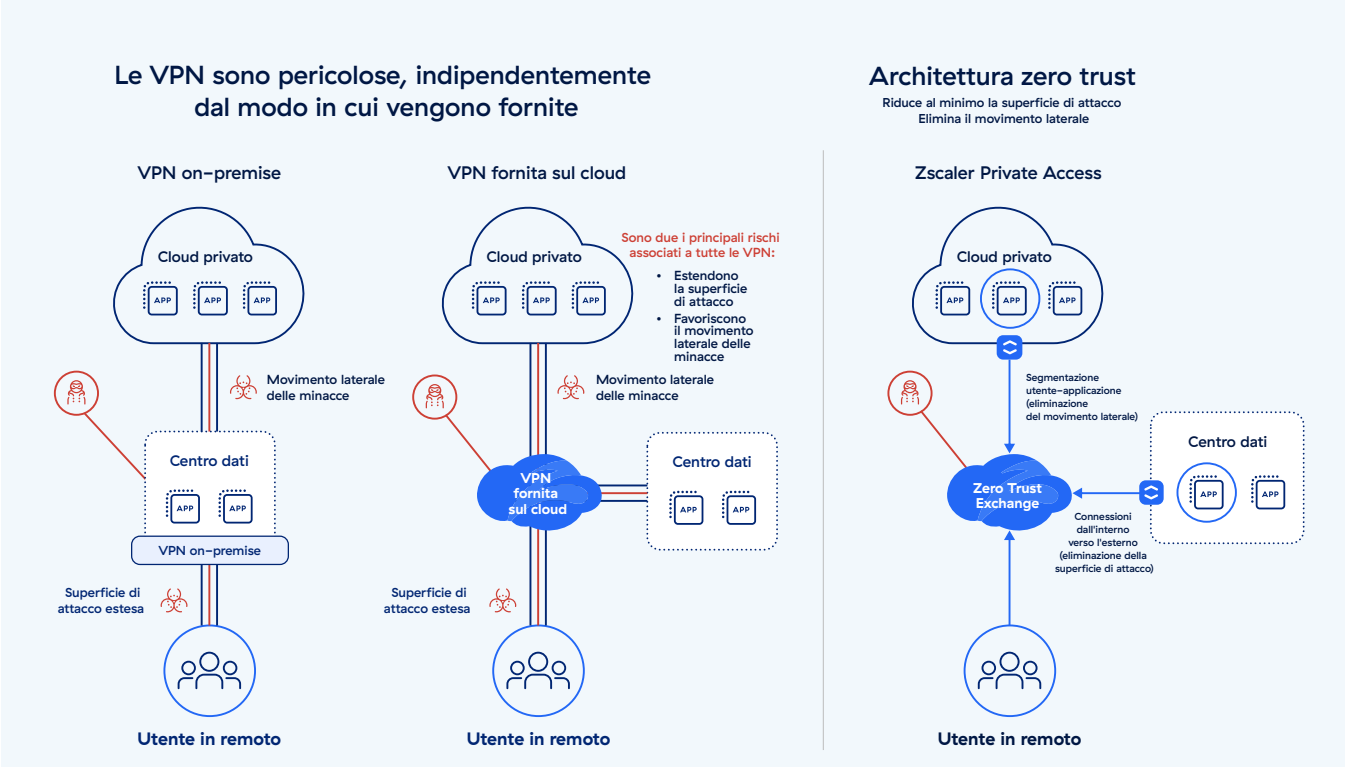
percentuale che ha in programma di sostituire la VPN con una soluzione ZTNA nel prossimo futuro

Perché lo Zero Trust è più sicuro di una VPN

Dal punto di vista dell'architettura, lo zero trust e lo ZTNA sono più sicuri delle VPN tradizionali per diversi motivi, principalmente grazie a un solido framework di sicurezza che non ripone mai intrinsecamente fiducia in nessuna singola connessione. Le architetture tradizionali basate su VPN sono soggette a un singolo punto di fallimento. Quando una VPN o un dispositivo viene compromesso (ad esempio tramite una nuova CVE), gli autori delle minacce possono sfruttare la fiducia di una rete piatta per ottenere l'accesso all'intera rete, spostarsi lateralmente, rubare dati e distribuire ransomware. Questo è il motivo per cui i professionisti della sicurezza sono sempre più preoccupati per i rischi di questi strumenti antiquati.

Le VPN locali e fornite sul cloud presentano vulnerabilità di sicurezza simili. Inoltre, le VPN introducono complessità, con conseguenti costi inutili e lunghe attività come il provisioning degli utenti, la gestione delle tabelle di routing, la risoluzione dei problemi di connettività, l'applicazione di patch, il monitoraggio e l'ottimizzazione delle prestazioni.

In un'architettura Zero Trust, nessuna singola connessione è mai considerata attendibile. Gli utenti si connettono direttamente alle applicazioni, mai alla rete sottostante. Inoltre, ogni connessione viene terminata automaticamente, indipendentemente dall'origine, prima di essere verificata da 7 livelli di controlli di sicurezza Zero Trust. L'architettura Zero Trust consente alle organizzazioni di segmentare in modo completo i propri ambienti con un accesso granulare: dagli utenti alle applicazioni, tra workload diversi, tra filiali e tra dispositivi, inclusi quelli IoT e OT.



I principali vantaggi e le differenze

Superficie di attacco significativamente ridotta
Un'architettura zero trust consente una connettività inside-out che nasconde risorse critiche, applicazioni, server e altro dalla rete Internet pubblica, eliminando al contempo la necessità di utilizzare risorse vulnerabili come VPN e firewall. Questo consente alle aziende di fornire una connettività ibrida alla propria forza lavoro, riducendo notevolmente la superficie di attacco. Al contrario, le architetture basate su VPN e firewall richiedono alle aziende di espandere la superficie di attacco per soddisfare una maggiore connettività.

Verifica continua
I modelli Zero Trust impongono una verifica continua delle credenziali e del livello di sicurezza prima di concedere l'accesso alle risorse, rendendo molto più difficile per le entità non autorizzate ottenere e mantenere l'accesso a informazioni e sistemi sensibili. Nel frattempo, con le VPN, l'utente o il dispositivo spesso ha ampie possibilità di arrivare alle risorse di rete, una volta ottenuto l'accesso.

Accesso con privilegi minimi
I principi zero trust applicano policy di accesso a privilegi minimi, garantendo che utenti e dispositivi abbiano accesso solo alle risorse di cui hanno bisogno per i loro ruoli specifici. Così facendo, riduce al minimo il rischio di minacce interne e movimento laterale all'interno di una rete, vulnerabilità comuni nelle configurazioni VPN.

Accesso granulare e segmentazione
Dividendo le risorse di rete in segmenti separati (tra utenti e app, tra workload e tra dispositivi) lo zero trust isola le potenziali violazioni in zone più piccole, riducendo notevolmente l'impatto di un attacco. Anche se le organizzazioni spesso tentano di segmentare i propri ambienti di rete, si tratta di un processo costoso e complesso dal punto di vista operativo che, in pratica, spesso rimane incompleto, richiede centinaia di regole firewall distinte ed espone aree di rete più ampie agli utenti autenticati.

Potenziamento della forza lavoro ibrida odierna
Lo Zero Trust consente di estendere facilmente e rapidamente agli utenti in remoto l'accesso alle applicazioni private, alla sede centrale, alle filiali e ai partner terzi.

Esperienza utente migliore e complessità ridotta
Lo zero trust migliora l'esperienza utente eliminando la necessità che tutto il traffico remoto venga instradato attraverso un punto di rete centrale, un comune collo di bottiglia nelle prestazioni con VPN. Questa architettura è in grado di gestire meglio i requisiti di scalabilità delle reti moderne che includono policy IoT e BYOD. Inoltre, lo zero trust riduce i costi di gestione automatizzando i controlli di sicurezza e semplificando l'applicazione delle policy sulla rete.

Questi vantaggi architetturali rendono lo zero trust un'alternativa convincente alle VPN tradizionali, in particolare nel panorama delle minacce sempre più sofisticate e distribuite di oggi. Alle organizzazioni che desiderano rafforzare le proprie difese di sicurezza informatica, l'adozione di un approccio zero trust fornisce un'infrastruttura di sicurezza più solida, flessibile e scalabile.

Le previsioni per il 2024 e oltre

1 Le gravi vulnerabilità e gli exploit VPN aumenteranno

Considerata la frequenza, la gravità e la portata delle vulnerabilità della VPN rivelate lo scorso anno, le aziende dovrebbero aspettarsi che questa tendenza continui. Gli autori delle minacce e i ricercatori sulla sicurezza sono consapevoli delle vulnerabilità presenti nei prodotti VPN. A loro volta, stanno attivamente cercando di trovarne altre, e nei prossimi mesi e anni potrebbero esserne individuate diverse.

2 Gli attacchi di alto profilo causati dalle VPN saranno al centro dell'attenzione

Secondo quanto anticipato nella nostra prima previsione, vedremo la violazione di organizzazioni più grandi a causa di vulnerabilità nelle VPN. In parte queste violazioni saranno causate dalle nuove linee guida normative della SEC, che impongono alle società pubbliche di divulgare dettagli sulle violazioni che hanno un impatto tangibile. Come abbiamo visto, gli autori delle minacce creano costantemente backdoor negli ambienti presi di mira quando si verificano vulnerabilità della VPN, in modo da sfruttarle in momenti successivi, anche dopo la risoluzione delle stesse. Nel corso dell'anno, molti di questi inizieranno a essere divulgati nei documenti pubblici della SEC e faranno notizia.

3 Un'impennata delle offerte VPN basate sull'intelligenza artificiale solleverà problemi di sicurezza e privacy

Con i continui progressi nell'intelligenza artificiale, le soluzioni VPN basate sull'AI invaderanno il mercato. Tuttavia, le imprese dovrebbero valutare queste offerte con cautela. Pur promettendo migliori prestazioni, l'integrazione dell'intelligenza artificiale amplificherà i rischi per la sicurezza e aumenterà le opportunità per gli aggressori di sfruttare le vulnerabilità delle VPN. Inoltre, un'analisi approfondita dei dati, che aumentano il rischio di esposizione di informazioni sensibili, farà nascere preoccupazioni per la privacy.

4 Gli attacchi di tipo password spray alle VPN continueranno a crescere

Gli aggressori troveranno sempre più modi per sfruttare una gestione debole delle password e profili di connessione VPN predefiniti non utilizzati attraverso attacchi di tipo spray password. In questi attacchi, gli autori delle minacce provano la stessa password su più account VPN finché non hanno successo, ottenendo così un accesso non autorizzato. Considerando le numerose recenti violazioni di alto profilo che hanno sfruttato efficacemente questa tecnica, le aziende dovrebbero aspettarsi che attacchi simili persistano.

5 La spesa aziendale si sposterà dalle VPN alla connettività Zero Trust

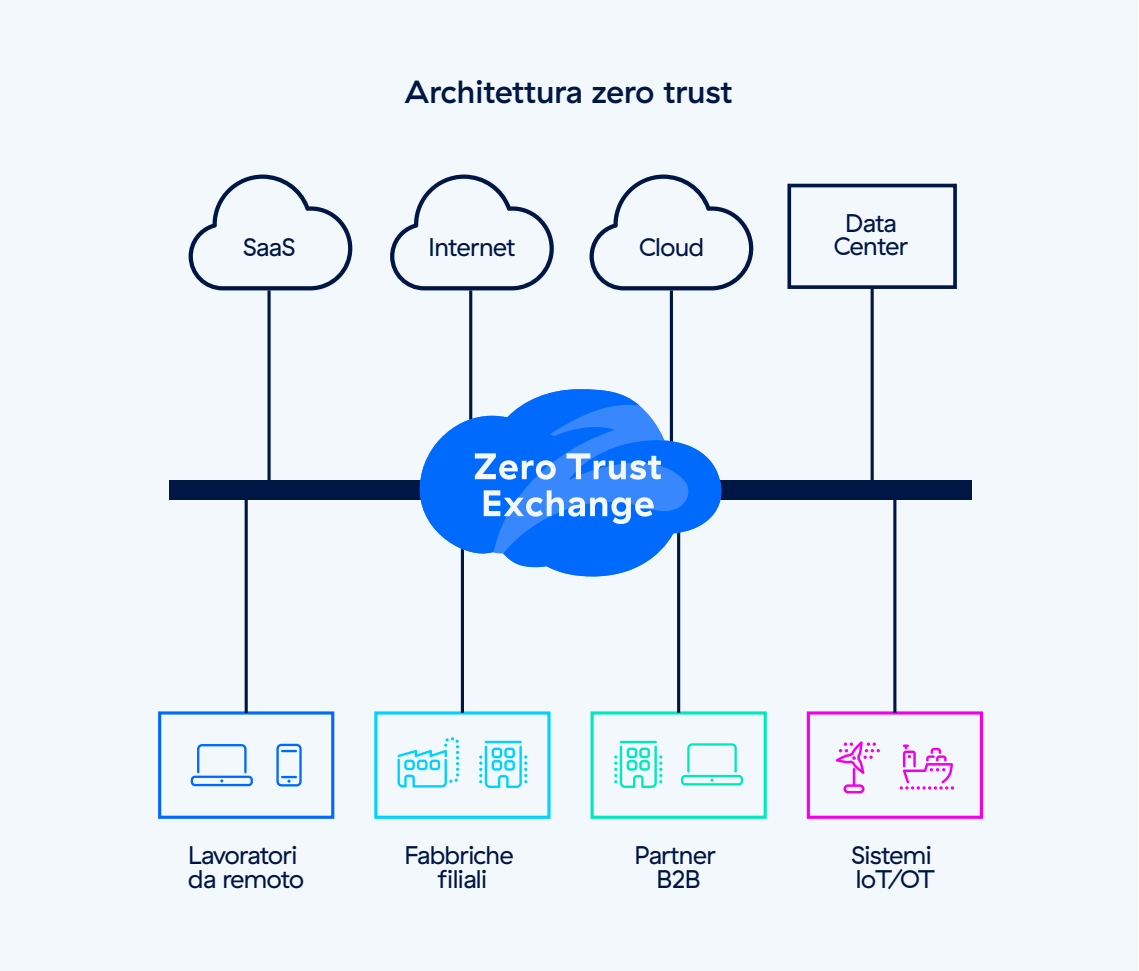
Sebbene la VPN consenta da tempo la connettività remota per le aziende, le costanti e crescenti sfide legate alla sicurezza della tecnologia renderanno più difficile giustificare la spesa a lungo termine. Man mano che le aziende consolideranno il consenso sullo zero trust come architettura preferita per la sicurezza e la connettività, i budget aziendali si sposteranno verso questo tipo di iniziative per proteggere la forza lavoro da remoto.

In che modo Zscaler consente la sostituzione della VPN e la trasformazione Zero Trust

I firewall tradizionali e le VPN generano una superficie di attacco molto estesa, che consente agli aggressori di vedere e sfruttare le risorse esposte. Mettendo gli utenti in rete e consentendo loro di accedere a qualsiasi applicazione ospitata, questi approcci datati offrono agli aggressori un facile accesso ai dati sensibili. Inoltre, in questo modo, fornire un accesso sicuro o condividere risorse con agenzie, fornitori e altre terze parti diventa un'operazione lunga e difficile. I costi e le complessità quindi aumentano, e non si può soddisfare la forza lavoro ibrida che caratterizza il mondo di oggi.

La piattaforma Zscaler Zero Trust Exchange™, il cloud di sicurezza inline più grande al mondo, connette in modo sicuro utenti, workload, dispositivi IoT/OT e partner B2B senza estendere l'accesso alla rete.

Zscaler Private Access™ (ZPA™), una parte essenziale di Zero Trust Exchange, fornisce accesso diretto alle applicazioni private nascoste dietro Zero Trust Exchange, riducendo al minimo la superficie di attacco e consentendo la segmentazione utente–applicazione 1:1, l'eliminazione del movimento laterale, la protezione delle applicazioni private e l'ispezione del traffico inline, bloccando al tempo stesso le minacce zero-day ed elevando il livello di sicurezza. In quanto servizio nativo del cloud, la distribuzione di ZPA può essere effettuata in poche ore per sostituire gli strumenti tradizionali di accesso remoto come VPN e VDI.



Zero Trust Networking

ZPA consente un accesso granulare e segmentato con connettività inside-out (dall'interno verso l'esterno) ad applicazioni e workload privati. Inoltre, ZPA include una serie completa di servizi di controllo degli accessi, come la segmentazione da utente ad app basata sull'intelligenza artificiale, con raccomandazioni automatizzate sulle policy di accesso degli utenti e la segmentazione di applicazioni e tra diversi workload, l'accesso remoto privilegiato, un servizio edge privato, l'accesso browser e altro.

Protezione dalle minacce informatiche

ZPA offre funzionalità avanzate di protezione informatica per proteggere la tua organizzazione, come la protezione delle applicazioni tramite l'ispezione di sicurezza inline per fermare gli attacchi più diffusi e le vulnerabilità zero-day, oltre a una tecnologia di deception che attira gli aggressori con applicazioni esca e facilita il rilevamento di minacce sofisticate.

Protezione dei dati

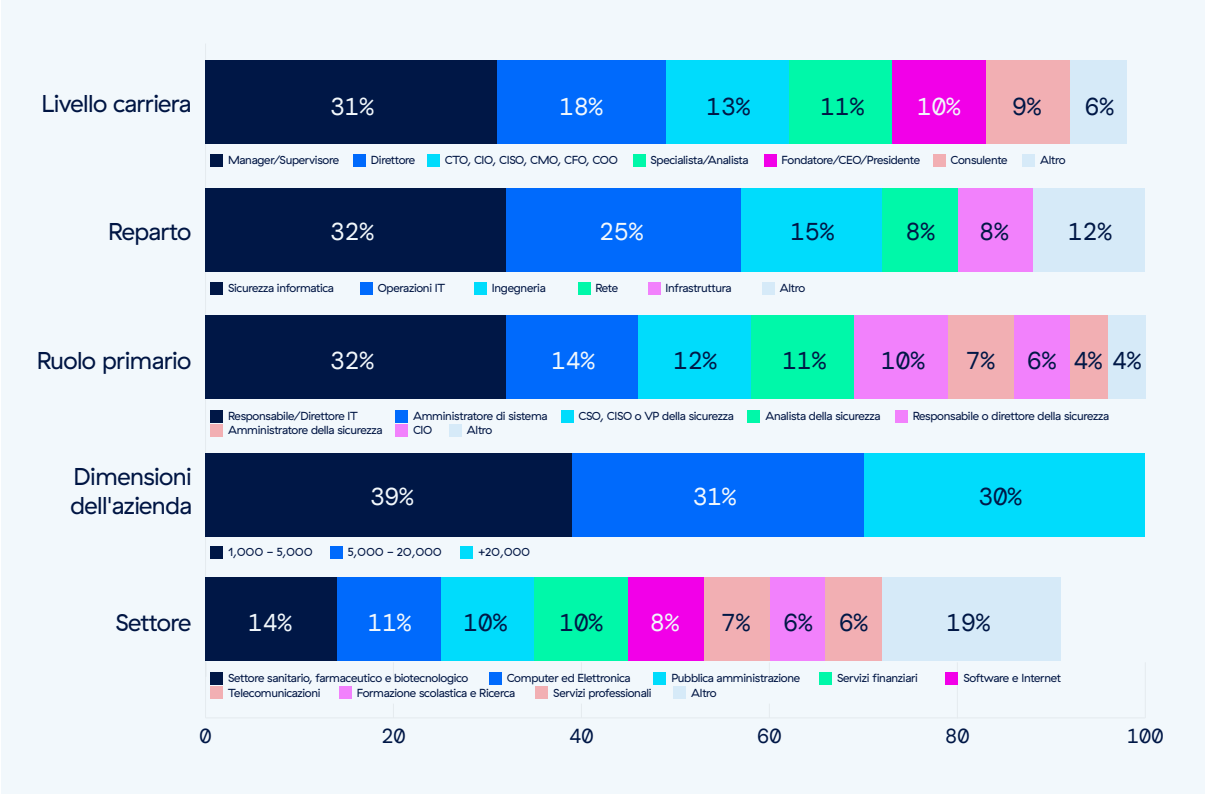
ZPA fornisce una protezione olistica e blocca la perdita di dati su tutti i canali con la prevenzione della perdita di dati web (DLP), la DLP per gli endpoint e l'isolamento del browser che previene la perdita di dati per gli utenti vulnerabili e gli endpoint BYOD.

Best practice per contrastare i rischi delle VPN

- **Ridurre al minimo la superficie di attacco:** fornisci accesso diretto alle applicazioni, garantendo che sia le applicazioni che gli utenti siano invisibili su Internet, impedendo efficacemente agli aggressori di scoprirli e sfruttarli per l'accesso iniziale.
- **Prevenire la compromissione iniziale:** è necessario ispezionare tutto il traffico inline per bloccare in automatico gli attacchi 0-day, i malware e le altre minacce sofisticate.
- **Bloccare l'accesso non autorizzato:** utilizza un'autenticazione sicura a più fattori (MFA) con password o token monouso, dati biometrici o credenziali FIDO2 per convalidare le richieste di accesso degli utenti. Al contrario, un'MFA debole utilizza spesso approcci che utilizzano domande per la reimpostazione della password.
- **Implementare l'accesso a privilegi minimi**: limita le autorizzazioni per utenti, traffico, sistemi e applicazioni utilizzando l'identità e il contesto, e garantisci che solo gli utenti autorizzati possano accedere a risorse approvate (con ulteriori controlli sicurezza in caso di compromissione dell'MFA o furto di credenziali).
- **Eliminare il movimento laterale:** collega gli utenti direttamente alle applicazioni, non alla rete, per limitare il raggio di azione di un potenziale incidente e mitigare il rischio di movimento laterale delle minacce.
- **Bloccare gli utenti compromessi e le minacce interne:** abilita l'ispezione e il monitoraggio inline per rilevare gli utenti compromessi con accesso alla rete, alle applicazioni private e ai dati.
- **Bloccare la perdita dei dati:** ispeziona i dati in movimento e quelli inattivi per fermare il furto attivo dei dati durante un attacco.
- **Distribuire misure di difesa attiva:** usa la tecnologia di deception basata sull'uso di esche ed esegui la caccia quotidiana alle minacce per sventare e bloccare attacchi in tempo reale.
- **Testare il profilo di sicurezza:** ottieni valutazioni periodiche e indipendenti sui rischi e guida le attività del purple team per identificare e colmare le lacune nel programma di sicurezza. È importante richiedere che i fornitori di servizi e i partner per la tecnologia facciano lo stesso e condividano i risultati di questi report con i team responsabili della sicurezza dell'azienda.

Metodologia e dati demografici

Questo report si basa sui risultati di un'approfondita indagine online a cui hanno partecipato 647 professionisti IT e di sicurezza informatica svolta ad aprile 2024. L'indagine è stata condotta con lo scopo di identificare le ultime tendenze relativamente alle soluzioni adottate dalle aziende, le sfide, le lacune e le soluzioni preferite in relazione ai rischi delle VPN. Gli intervistati vanno da dirigenti tecnici a professionisti della sicurezza IT, e rappresentano in modo bilanciato organizzazioni di varie dimensioni operanti in più settori.



Informazioni su Zscaler

Zscaler 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 nel mondo, 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.it.

Informazioni su ThreatLabz

ThreatLabz è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti di alto livello 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 comportamentale, i membri del team sono coinvolti nella ricerca e nello sviluppo di nuovi moduli prototipo per la protezione dalle minacce avanzate sulla piattaforma Zscaler. Inoltre, conducono costantemente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler siano sempre in linea con gli standard di conformità della sicurezza. ThreatLabz pubblica regolarmente analisi approfondite sulle minacce nuove ed emergenti sul suo portale: research.zscaler.com.

Informazioni su Cybersecurity Insiders

Cybersecurity Insiders riunisce oltre 600.000 professionisti della sicurezza informatica e fornitori di soluzioni tecnologiche di alto livello per facilitare la risoluzione intelligente dei problemi e la collaborazione nell'affrontare le attuali sfide più critiche della cybersecurity.

Il nostro approccio si concentra sulla creazione e la cura di contenuti esclusivi, volti a istruire e formare i professionisti della cybersecurity sulle ultime tendenze, soluzioni e best practice da seguire. Con studi di ricerca approfonditi, recensioni imparziali dei prodotti, guide pratiche, webinar coinvolgenti e articoli formativi, ci impegniamo a fornire risorse che rispondano in modo concreto alle complesse sfide esistenti nel panorama della sicurezza informatica.

Contattaci oggi stesso per scoprire il modo in cui Cybersecurity Insiders può aiutarti a emergere in un mercato altamente competitivo e ad accrescere la domanda, la visibilità e la presenza del marchio.

Inviaci un'e-mail a info@cybersecurity-insiders.com o visita cybersecurity-insiders.com.

Esplora il tuo mondo, in sicurezza.

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita di dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la piattaforma di cloud security inline più grande del mondo. Per saperne di più, visita il sito **www.zscaler.it**.

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