2021

Cybersecurity
INSIDERS

IL RISCHIO CORRELATO ALLA VPN

RESOCONTO

INDICE

PANORAMICA

Per quasi 30 anni, le VPN (Virtual Private Networks) sono state il mezzo principale per fornire l'accesso alla rete aziendale agli utenti in remoto. Oggi, il mondo si è trasformato digitalmente, lo zero trust è diventato un must e le applicazioni si sono spostate al di fuori del perimetro tradizionale, rivoluzionando la realtà del passato.

"La VPN aziendale è una tecnologia ormai datata, con le organizzazioni che si spostano sempre più verso servizi basati sul cloud.[...] Tuttavia, per effetto della pandemia globale causata dal coronavirus, le aziende si stanno rendendo conto che devono cambiare radicalmente il loro modo di lavorare".

Rob Smith, Senior Director Analyst, Gartner.

Le tecnologie VPN, un tempo il cuore dell'accesso remoto, sono diventate una fonte di rischio che ha portato le organizzazioni a rivedere la propria strategia di accesso a lungo termine, nonché l'utilizzo della VPN stessa. L'incremento a livello mondiale del lavoro da remoto, dovuto alla pandemia di COVID-19, ha portato a un aumento dell'uso delle VPN e, conseguentemente, ad un incremento della superficie di attacco cui sono soggette le imprese. Gli attori delle minacce stanno prendendo di mira le VPN, come viene evidenziato negli innumerevoli nuovi articoli sugli attacchi che le sfruttano e dalle quasi 500 vulnerabilità note della VPN elencate nel database CVE.

Questo Resoconto sul Rischio correlato alla VPN del 2021 e' stato creato intervistando 357 professionisti della sicurezza informatica e fornisce informazioni sull'attuale ambiente ad accesso remoto, sullo stato della VPN all'interno dell'azienda, sull'aumento delle vulnerabilità della VPN e sul ruolo che verrà ricoperto in futuro dall'approccio zero trust per consentire l'accesso alle app.

RISULTATI CHIAVE:

- **Il 93%** delle aziende sta sfruttando i servizi VPN, sebbene il 94% sia consapevole del fatto che i criminali informatici stanno prendendo di mira le VPN per ottenere l'accesso alle risorse di rete.
- **Il 72%** delle organizzazioni teme che la VPN possa compromettere la capacità dell'IT di preservare la sicurezza dei propri ambienti.
- **Il 67%** delle imprese sta prendendo in considerazione un'alternativa ad accesso remoto in sostituzione della VPN tradizionale.
- Attualmente, **il 72%** delle aziende sta dando priorità all'adozione di un modello zero trust, mentre il 59% ha accelerato i propri sforzi, per via dell'attenzione rivolta al lavoro da remoto.

Un ringraziamento particolare va a Zscaler per aver supportato questo importante progetto di ricerca.

Ci auguriamo che questo resoconto possa rivelarsi utile e informativo nel supportare il proseguimento degli sforzi per proteggere gli ambienti IT.

Grazie,

Holger Schulze

Holger Schulze
CEO e Fondatore
Cybersecurity Insiders

Cybersecurity
INSIDERS

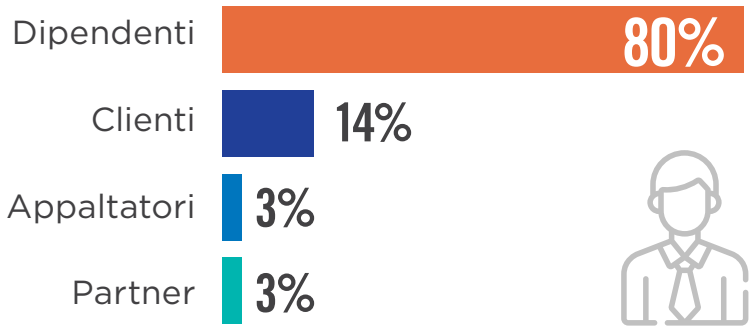
AMBIENTE AD ACCESSO REMOTO

ACCESSO SICURO PER CHI, COSA...

Per creare un piano di supporto al lavoro da remoto nel mondo moderno, i team di sicurezza IT devono prendere in considerazione alcuni fattori: chi accede alle proprie applicazioni, da quali dispositivi e da dove? Di seguito, verrà riportato ciò che è stato riscontrato attraverso il nostro sondaggio.

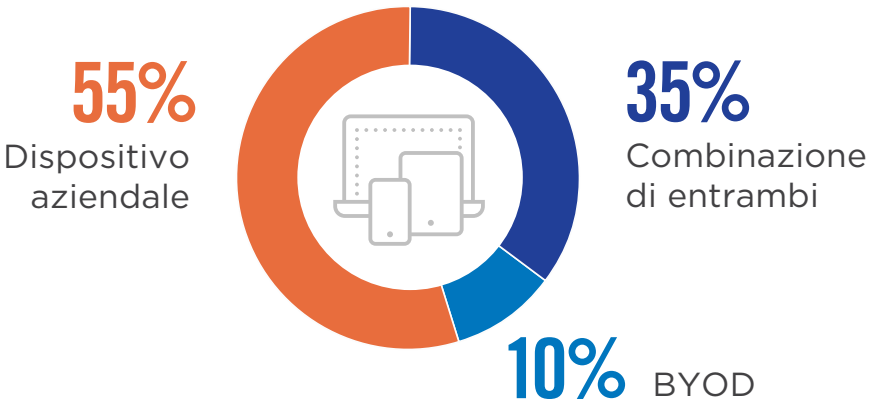
CHI: quando si tratta di richiedere un accesso sicuro alle app aziendali, i dipendenti hanno la priorità, come del resto è prevedibile. **Per l'80% delle organizzazioni, consentire ai dipendenti di accedere costituisce la loro priorità principale**, seguiti dai clienti (14%), dai partner e dagli appaltatori (3% ciascuno).

Quando si richiede l'accesso sicuro alle applicazioni aziendali, quale gruppo ha la priorità?



COSA: quando viene chiesto quali tipi di dispositivi vengono utilizzati dai lavoratori da remoto per connettersi alle risorse aziendali e alle app, il **45% delle organizzazioni segnala di consentire l'uso di dispositivi BYOD/personali.** L'impossibilità di applicare misure di sicurezza su tali dispositivi BYOD rende molto più complesso garantire la sicurezza dei dispositivi e il controllo dell'accesso, soprattutto in ambienti di lavoro da remoto.

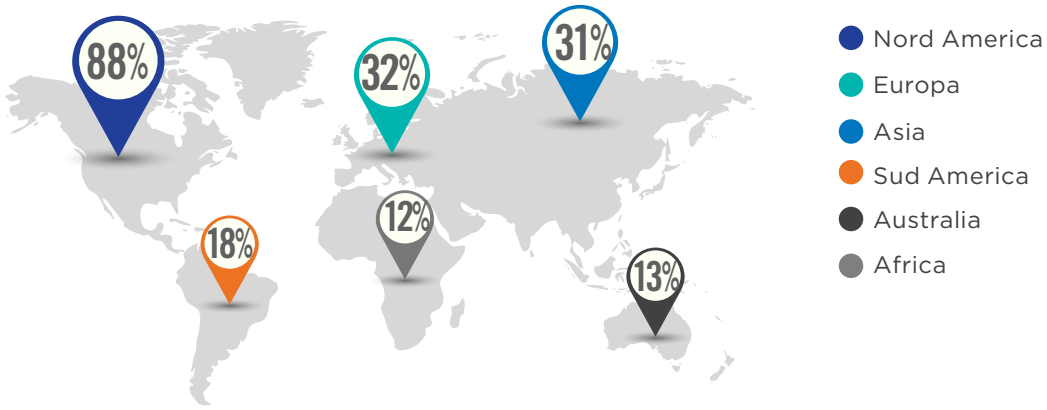
Quali dispositivi utilizzano i dipendenti per connettersi alle risorse e alle applicazioni aziendali?



... E DOVE

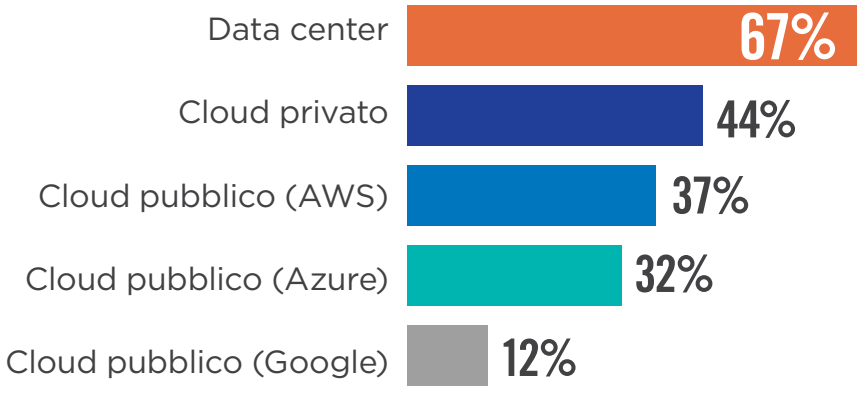
DOVE: le organizzazioni che hanno partecipato al nostro sondaggio riportano che **l'88% ha dipendenti da remoto si connettono dal Nord America, il 32% dall'Europa e il 31% dall'Asia.** Con utenti distribuiti in diverse aree geografiche, il supporto alla sicurezza del lavoro da remoto può diventare una sfida ancora più complessa, in quanto le diverse regioni adottano differenti standard in termini di sicurezza, disponibilità, policy di conformità, ecc.

Da dove si connettono i dipendenti da remoto?



Inoltre, questo sondaggio ha rilevato che **le applicazioni private delle aziende sono, in genere, in esecuzione nei data center (67%), seguiti dal cloud privato (44%) e quindi dai cloud pubblici (37% AWS/32% Azure/12% Google Cloud Platform)**. Con le organizzazioni che continuano ad adottare una strategia multi-cloud, garantire una sicurezza uniforme in tutti gli ambienti diventa sempre più complesso.

Attualmente, dove vengono eseguite le applicazioni private?



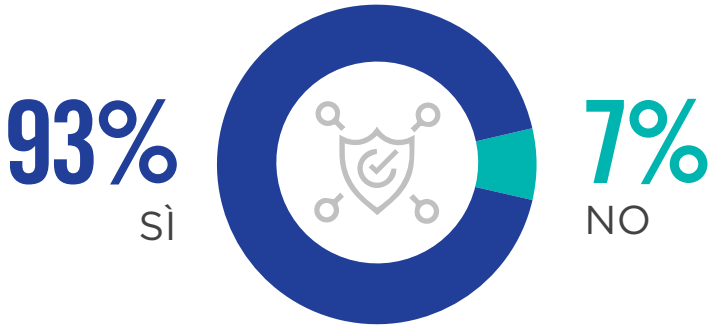
Altro 4%

STATO DELLA VPN

UTILIZZO DELLA VPN E NUMERO DI GATEWAY

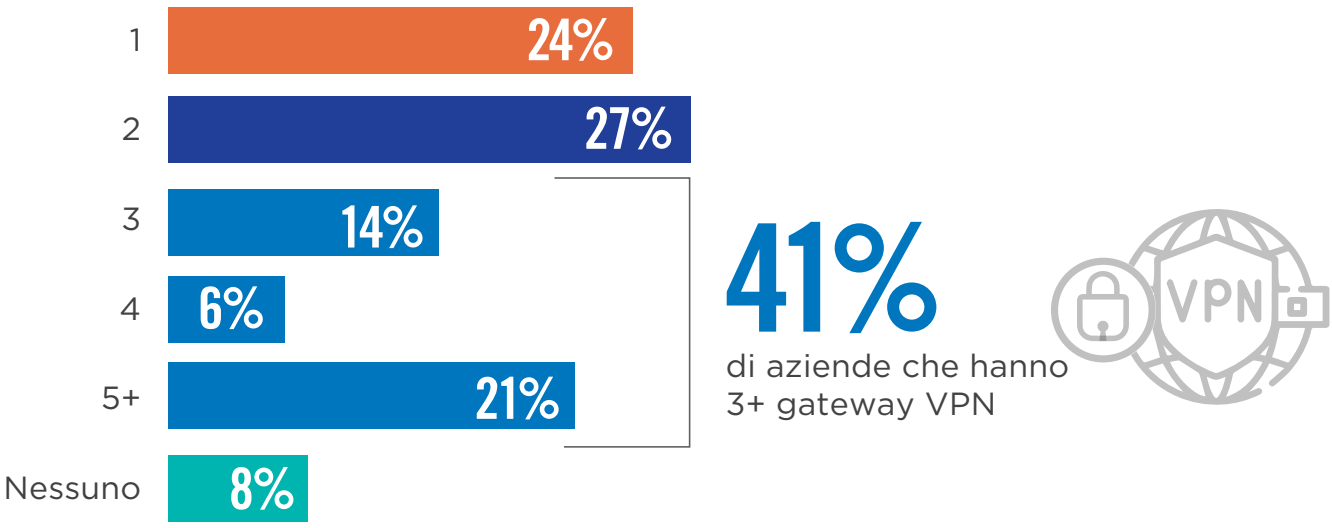
L'adozione dell'accesso remoto è notevolmente aumentata, per via degli eventi imprevisti che si sono verificati durante il 2020. Sebbene il nostro sondaggio abbia rilevato che **la stragrande maggioranza delle organizzazioni stia attualmente sfruttando un servizio VPN per un accesso remoto sicuro (93%)**, abbiamo voluto approfondire in modo più dettagliato lo stato effettivo della VPN e come il 2020 abbia influito sull'accesso remoto.

Attualmente, l'organizzazione sta utilizzando un servizio VPN?



Quando agli intervistati viene chiesto quanti gateway VPN in entrata hanno a livello globale, **il 41% delle organizzazioni dichiara di avere più di 3 gateway VPN, con la metà di queste aziende che segnalano di averne più di 5.** Ogni gateway richiede uno stack di apparecchi di applicazione, tra cui VPN (RAS), firewall interno, bilanciatore del carico interno, bilanciatore di carico globale, DDoS, firewall esterno, ecc. Più elevato è il numero di gateway di un'organizzazione, più costoso sarà garantire la sicurezza dell'accesso remoto e più complicato sarà per l'IT amministrare e gestire ogni stack in ingresso.

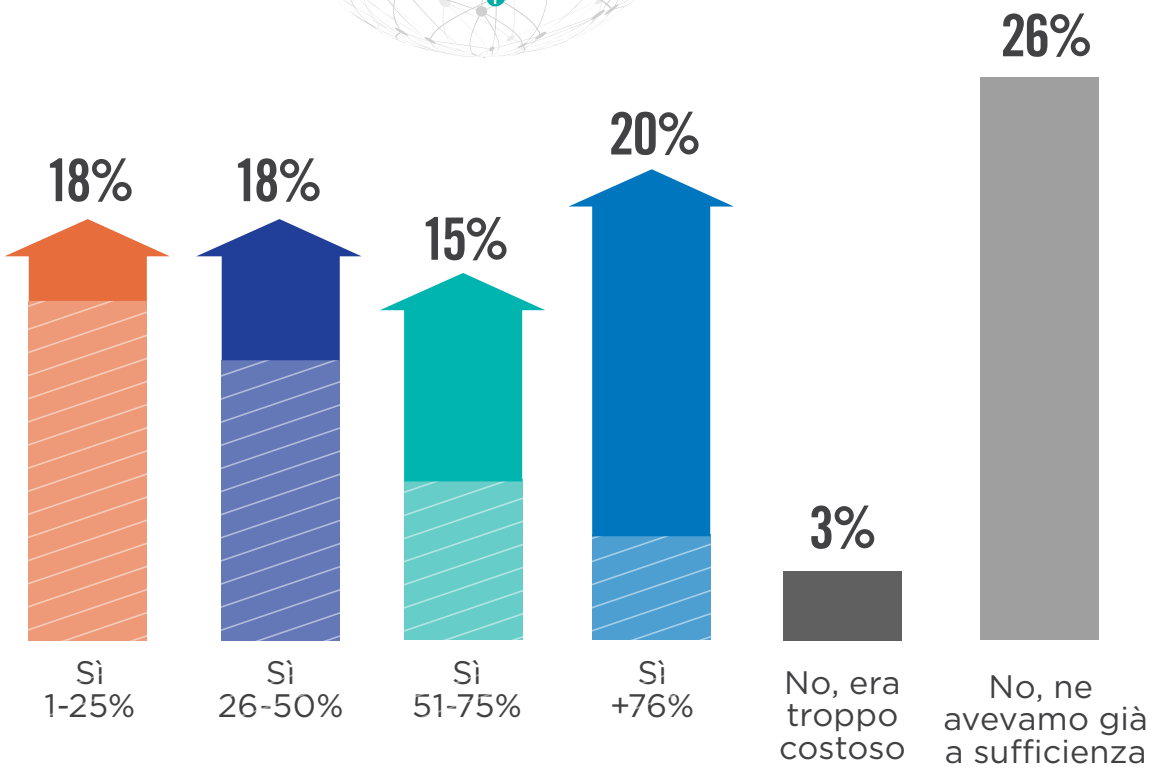
Quanti sono i diversi gateway VPN in entrata adottati da un organizzazione a livello globale?



CAPACITÀ DELLA VPN E SCALABILITÀ

La pandemia di COVID-19 ha conseguentemente creato un aumento dei dipendenti da remoto, con **il 71% delle aziende che ha dichiarato di aver dovuto necessariamente aumentare la capacità delle VPN. Tra le aziende che hanno richiesto una larghezza di banda aggiuntiva, un terzo di esse ha aumentato la capacità delle VPN di oltre il 50%**. Al contrario, il 26% delle aziende ha segnalato che non è stato necessario scalare le VPN durante la pandemia di COVID-19. Ciò potrebbe indicare che queste organizzazioni disponevano di capacità inutilizzata sino alla pandemia e che quindi stavano sostenendo costi eccessivi per la loro VPN.

Durante la pandemia COVID-19, l'organizzazione ha visto crescere la capacità della VPN? Se sì, in che percentuale?



LE PRINCIPALI SFIDE DELLA VPN

Sebbene molte organizzazioni si siano affidate alla VPN per un accesso remoto sicuro come risposta alla forza lavoro sempre più mobile, tale scelta porta con sé delle insidie. **Quando viene chiesto di classificare le sfide più significative che le organizzazioni si trovano ad affrontare in relazione alla propria soluzione di accesso remoto, al primo posto vi è la mancanza di visibilità sulle attività degli utenti, seguita dall'elevato costo dell'infrastruttura di sicurezza.**

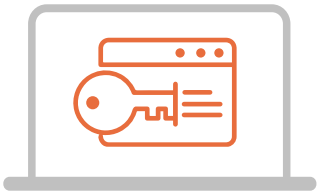
Qual è la sfida più gravosa che l'organizzazione si trova ad affrontare in relazione alla soluzione di accesso remoto attualmente in uso?

24%

Mancanza di visibilità sull'attività svolta dall'utente

23%

Costi elevati legati a dispositivi di sicurezza/ infrastruttura

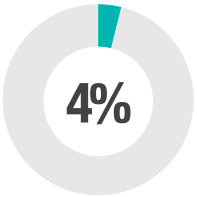


19%

Richiede di consentire ai dipendenti e a terze parti l'accesso alla rete aziendale

Scarsa esperienza utente a causa del backhauling del traffico verso i gateway VPN

Complessità della gestione dell'accesso remoto esistente negli ambienti cloud pubblici



Impossibilità di scalare per soddisfare la domanda degli utenti

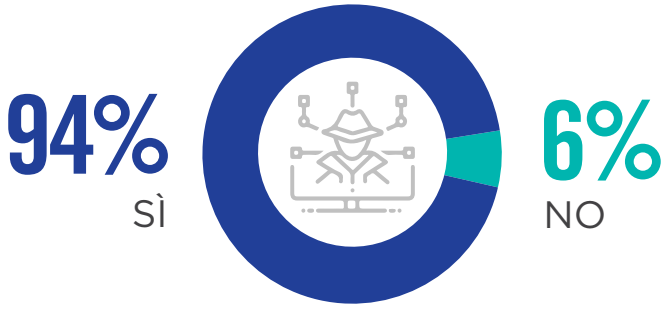
Con gli utenti che non si connettono più localmente dall'ufficio, l'IT perde il controllo su una notevole quantità delle loro attività, il che lascia molti nell'impossibilità di sapere a cosa stiano accedendo gli utenti. Inoltre, poiché le aziende hanno dovuto scalare la propria VPN a causa dell'aumento dell'accesso remoto, l'elevato costo degli apparecchi di applicazione e dell'infrastruttura ha intaccato i bilanci dell'IT.

VULNERABILITÀ E RISCHI DELLA VPN

AUMENTO DELLE MINACCE LEGATE ALLA VPN

L'aumento del lavoro da remoto ha portato anche a un picco della popolarità degli attacchi mirati alle VPN fra i criminali informatici che cercano di ottenere l'accesso non autorizzato alle risorse di rete esposte a Internet. In realtà, **il 94% delle aziende sa che le proprie VPN sono vulnerabili agli attacchi informatici e che vengono sfruttate per le aggressioni,** ma continua comunque a impiegare questa tecnologia, nonostante sia consapevole del rischio associato.

Le organizzazioni sono consapevoli che i criminali informatici stanno prendendo di mira le VPN per ottenere l'accesso alle risorse di rete tramite attacchi sotto forma di "exploit" come quelli di codice remoto, server Windows, ransomware e attacchi di ingegneria sociale?



Quando alle organizzazioni vengono richieste informazioni sugli attacchi basati su Internet, **le stesse concordano sul fatto che ingegneria sociale (75%), ransomware (74%) e malware (60%) sono i vettori di attacco più critici**. Come abbiamo visto in passato, basta un solo dispositivo infetto o delle credenziali rubate per mettere a rischio l'intera rete, motivo per cui i criminali informatici sfruttano in modo specifico gli utenti che accedono alle VPN.

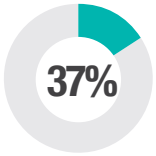
Quali sono gli attacchi basati su Internet che preoccupano maggiormente l'organizzazione?

75%
Ingegneria sociale

74%
Ransomware

60%
Malware

Exploit di codice remoto



Attacchi DDoS

Altro 4%

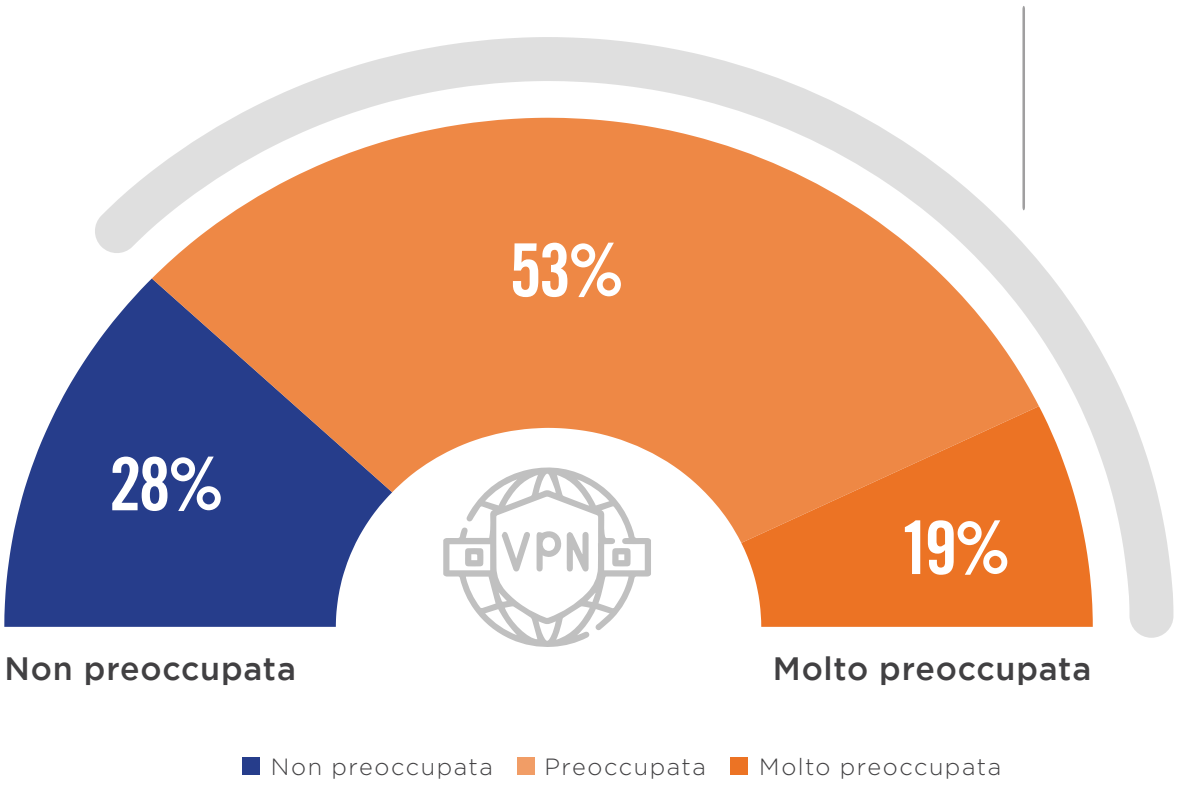
PREOCCUPAZIONI LEGATE ALLA SICUREZZA DELLA VPN

Le aziende per il 72% affermano di essere preoccupate del fatto che la VPN possa mettere a repentaglio la capacità di preservare la sicurezza dei propri ambienti IT. La domanda rivolta a tutti coloro che operano nell'IT è quindi: se la soluzione di accesso remoto sicuro non fornisce il livello di sicurezza desiderato, è necessario modificare la strategia di accesso remoto?

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

72%

teme che la VPN possa compromettere la capacità di preservare la sicurezza dell'ambiente.



ALTERNATIVE ALLA VPN

Con quasi tre aziende su quattro preoccupate per ciò che concerne la sicurezza della VPN, **la maggior parte delle organizzazioni (67%) sta prendendo in considerazione delle alternative di accesso remoto in sostituzione alla VPN tradizionale.**

Alla luce delle vulnerabilità e dei rischi correlati alla VPN, il 2021 sembra dettare la fine dell'epoca della VPN e l'inizio di una nuova era verso l'adozione di una strategia zero trust.

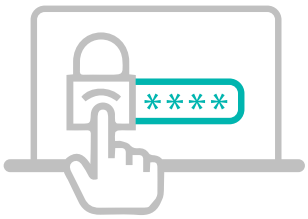
L'organizzazione ha considerato delle alternative di accesso remoto per sostituire la VPN tradizionale?

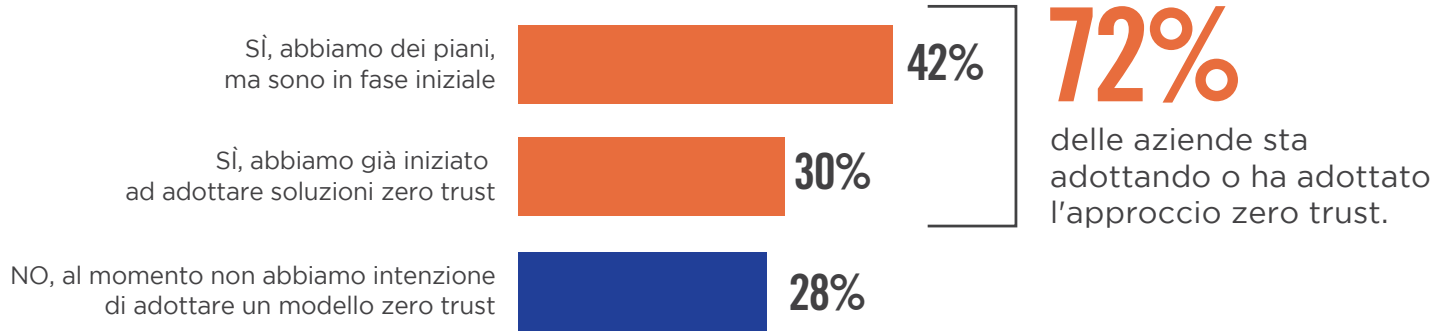
IL FUTURO DELL'ACCESSO REMOTO

ACCELERAZIONE DELL'ADOZIONE DELL'APPROCCIO ZERO TRUST

L'adozione di una strategia zero trust, tramite Zero Trust Network Access (ZTNA) e/o Zero Trust Architectures (ZTA), ha visto una rapida ascesa negli ultimi anni. Con l'aumento dei lavoratori mobili, **l'adozione dello zero trust è diventata una priorità per molte organizzazioni, con il 72% delle aziende che conferma i propri piani di adozione di un modello zero trust.**

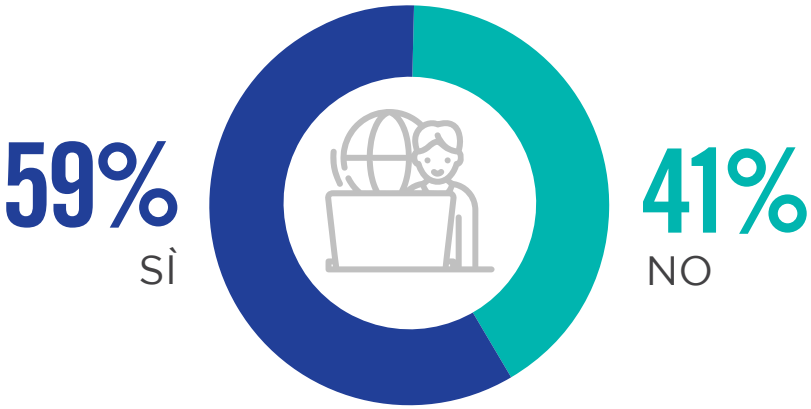
L'adozione di un modello di trust zero è una priorità per l'organizzazione?





non solo le organizzazioni stanno dando la massima priorità all'approccio zero trust, ma **il 59% delle aziende sta accelerando anche i progetti zero trust per un'implementazione più rapida della tecnologia all'interno dell'organizzazione.**

L'attenzione rivolta al lavoro da remoto ha accelerato la priorità dei progetti zero trust dell'organizzazione?



L'ACCESSO REMOTO
FA UN PASSO VERSO IL FUTURO

Il passaggio all'approccio zero trust e al lavoro da qualsiasi luogo hanno rappresentato un catalizzatore per cambiare il modo in cui le organizzazioni proteggono l'accesso remoto. Quando alle organizzazioni vengono richieste informazioni in merito alle proprie prospettive in termini di accesso remoto, il **77% ritiene che la propria forza lavoro futura sarà ibrida**, con una maggiore flessibilità nel consentire agli utenti di lavorare da remoto o in ufficio.

Nella corsa verso il 2022, l'organizzazione come considera l'accesso remoto?

77%

I dipendenti hanno maggiore flessibilità per lavorare in remoto durante la settimana

15%

Oggi, i dipendenti operano completamente da remoto

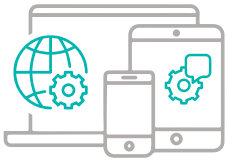
8%

I dipendenti sono tornati a lavorare esclusivamente dall'ufficio

PUNTI CHIAVE DA RICORDARE

Sebbene la VPN abbia goduto della massima notorietà per 30 anni, l'aumento degli attacchi mirati alle VPN, congiuntamente alla costante transizione verso la mobilità e il cloud, ha reso le organizzazioni consapevoli della necessità di cambiare la propria strategia di accesso remoto sicuro, optando per un approccio basato su principi dello zero trust.

In conclusione, ecco i punti chiave da ricordare:



Con la diffusione del lavoro da remoto, gli utenti sono ovunque, accedono alle app da qualsiasi dispositivo e alle applicazioni presenti sia nel data center che nel cloud.

Le VPN sono sempre più pericolose, poiché gli attacchi basati su ingegneria sociale, ransomware e malware continuano a progredire, esponendo le aziende a maggiori rischi.

Le imprese sono preoccupate per il livello di sicurezza delle VPN e stanno cercando di adottare un approccio di accesso remoto più moderno, vale a dire un modello zero trust.

La maggior parte delle organizzazioni ha dato priorità a dei piani per adottare una strategia zero trust. Con molte aziende pronte a dare spazio a una forza lavoro ibrida e a concedere maggiore flessibilità sul posto di lavoro, l'adozione dell'approccio zero trust diventa fondamentale.

La VPN sta esponendo l'organizzazione a dei rischi?

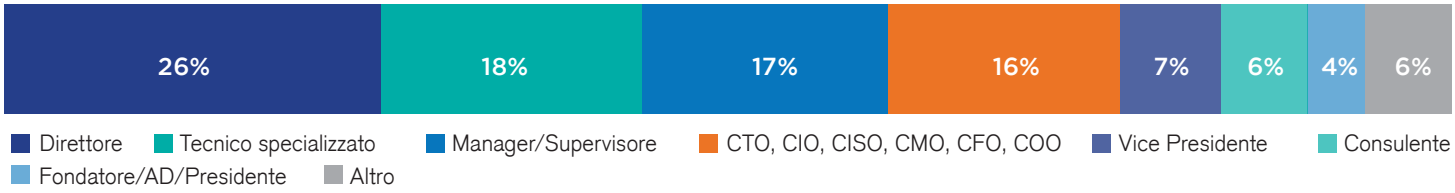
È possibile ricevere una valutazione gratuita dei rischi e scoprire qual è la propria superficie d'attacco della rete, prima che siano gli aggressori a scoprilo.

SCOPRI L'ENTITÀ DELLA TUA SUPERFICIE DI ATTACCO

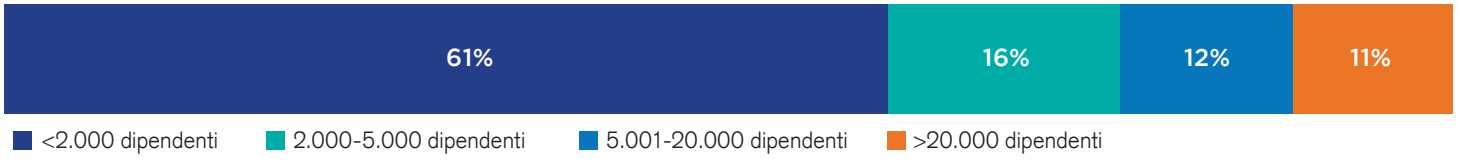
METODOLOGIA E DATI DEMOGRAFICI

Questo resoconto si basa sui risultati di un sondaggio online completo effettuato su 357 professionisti dell'IT e della sicurezza informatica e condotto a gennaio 2021 per identificare le ultime tendenze, le sfide, le lacune e le preferenze relative ai rischi legati alla VPN. Gli intervistati spaziano dai dirigenti tecnici ai professionisti della sicurezza IT, rappresentando quindi uno spaccato bilanciato di organizzazioni di varie dimensioni, operanti in più settori.

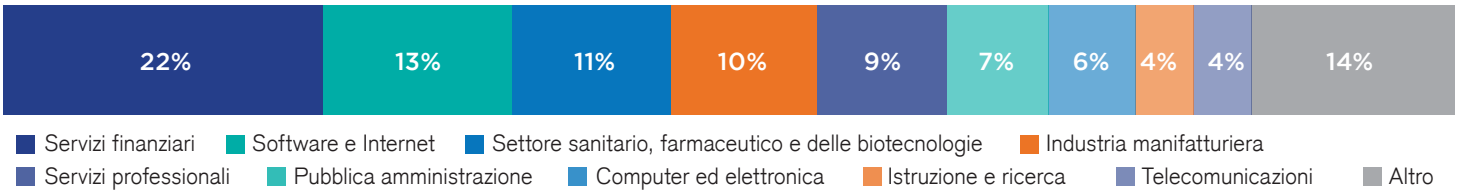
POSIZIONE RICOPERTA



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. La soluzione Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni indipendentemente dalla posizione in cui si trovino e da dove si connettano. Distribuita in più di 150 data center a livello globale, la soluzione Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security in linea del mondo. Scopri di più visitando zscaler.com o seguici su Twitter @zscaler.

zscaler.com