ivanti

Relazione Sulla Sicurezza Informatica Del Lavoro Da Casa In Remoto

2020

Panoramica

Le soluzioni Secure Access consentono alle aziende di continuare a operare rendendo sicuro il remote computing e collegando persone e dispositivi a data center e applicazioni cloud, anche nelle circostanze più imprevedibili.

Quando l'impatto del Coronavirus (COVID-19) si è intensificato trasformandosi in pandemia, l'Organizzazione Mondiale della Sanità ha raccomandato ai cittadini di lavorare da casa e di evitare l'uso dei trasporti pubblici e degli uffici come misura precauzionale volta a mitigare la diffusione e il rischio di infezione.

All'inizio del 2020, i funzionari governativi e locali di tutto il mondo hanno iniziato a raccomandare e a richiedere ai cittadini di mettersi in sicurezza, cessando il lavoro in sede di tutte le attività ad eccezione di quelle essenziali. Le aziende hanno posto in atto azioni immediate per espandere e agevolare le possibilità di lavoro in remoto da casa (WFH).

Oltre al potenziale impatto sulla produttività degli utenti, questo spostamento emergenziale del luogo di lavoro e la rapida esigenza di capacità di lavoro a distanza hanno minacciato l'infrastruttura IT, la continuità aziendale e la sicurezza delle informazioni.

La presente Relazione sul lavoro da casa in remoto 2020, sponsorizzata da Pulse Secure e realizzata da Cybersecurity Insiders, offre una prospettiva approfondita sulle modalità di transizione dei lavoratori e delle risorse da parte delle imprese e mette in luce le sfide di sicurezza informatica WFH, le criticità, le strategie e gli esiti previsti. Il sondaggio, condotto nel maggio del 2020, ha intervistato oltre 400 responsabili della sicurezza IT, professionisti e aziende di varie dimensioni in diversi settori. Il sondaggio ha evidenziato che l'84% delle aziende si aspetta un lavoro a distanza più diffuso e permanente e quasi un terzo prevede di aumentare nel prossimo futuro il budget destinato a garantire un accesso sicuro.

Tra i risultati chiave figurano:

- Oltre il triplo di incremento nell'espansione della capacità degli utenti WFH con oltre il 75% delle organizzazioni che offrono una copertura pari a quasi il 100%
- Il 33% delle aziende non erano sufficientemente preparate ad un accesso remoto sicuro di emergenza
- Il 54% accelererà il passaggio di più flussi di lavoro e app al cloud
- Il 38% delle organizzazioni ha sperimentato aumenti di produttività e altri benefici
- L'84% preannuncia programmi WFH più ampi e permanenti
- Più della metà prevede di aumentare un budget per l'accesso sicuro nei prossimi dodici mesi (oltre aprile 2020)
- Il 66% si aspetta un aumento delle minacce alla sicurezza WFH e il 63% prevede che il lavoro a distanza possa esporre a
- rischi di conformità
- Malware, phishing, accesso non autorizzato di utenti e dispositivi e sistemi senza patch sono stati percepiti come i maggiori vettori di attacco WFH
- Anti-virus/malware, firewall, VPN SSL, autenticazione a più fattori e backup sono state le soluzioni più utilizzate per garantire sicurezza WFH/resilienza aziendale

Ringraziamo sentitamente Pulse Secure per aver sostenuto questo importante progetto di ricerca.

Ci auguriamo che troverete questa relazione istruttiva e utile nel proseguimento degli sforzi volti a proteggere i vostri

investimenti IT, garantire la continuità aziendale e salvaguardare i vostri dipendenti.

Grazie,

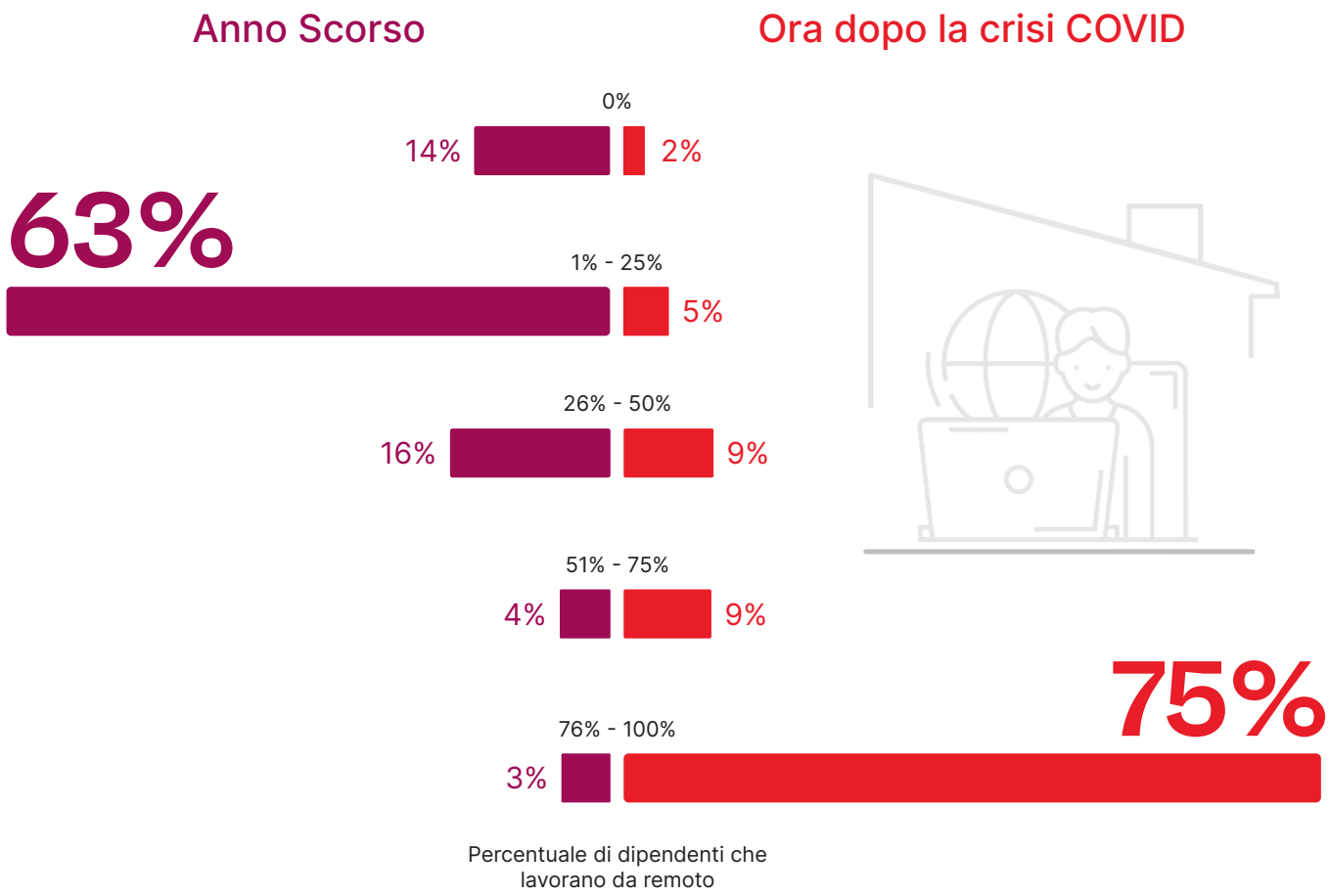
Holger Schulze

CEO e fondatore
Cybersecurity Insiders

Incremento Esplosivo Della Forza Lavoro Da Remoto

L'indagine rivela un massiccio spostamento verso ambienti di lavoro remoti e domestici a causa della pandemia COVID-19. Mentre prima della crisi una maggioranza del 63% delle organizzazioni registrava un quarto dei dipendenti che lavoravano in ambienti remoti/domestici, una clamorosa percentuale di tre quarti delle stesse organizzazioni riferisce che oltre il 75% della propria forza lavoro attualmente lavora da casa.

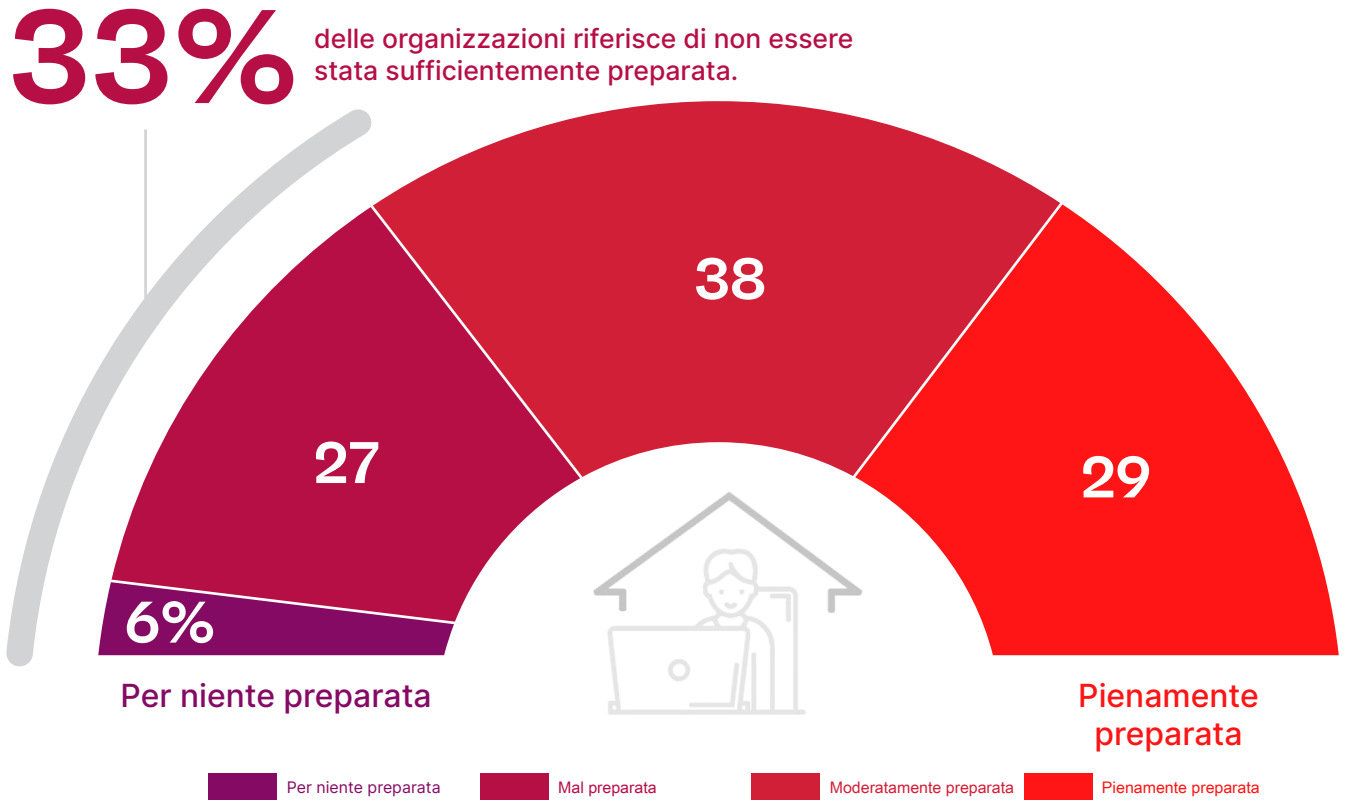
Quale percentuale della vostra forza lavoro lavorava da remoto/da casa l'ANNO SCORSO rispetto ad ORA in periodo di crisi COVID?



Prepararsi Al Lavoro Da Remoto

Un terzo delle organizzazioni riferisce di non essere stata sufficientemente preparata al rapido passaggio dagli scenari di lavoro on-premises a quelli remoti.

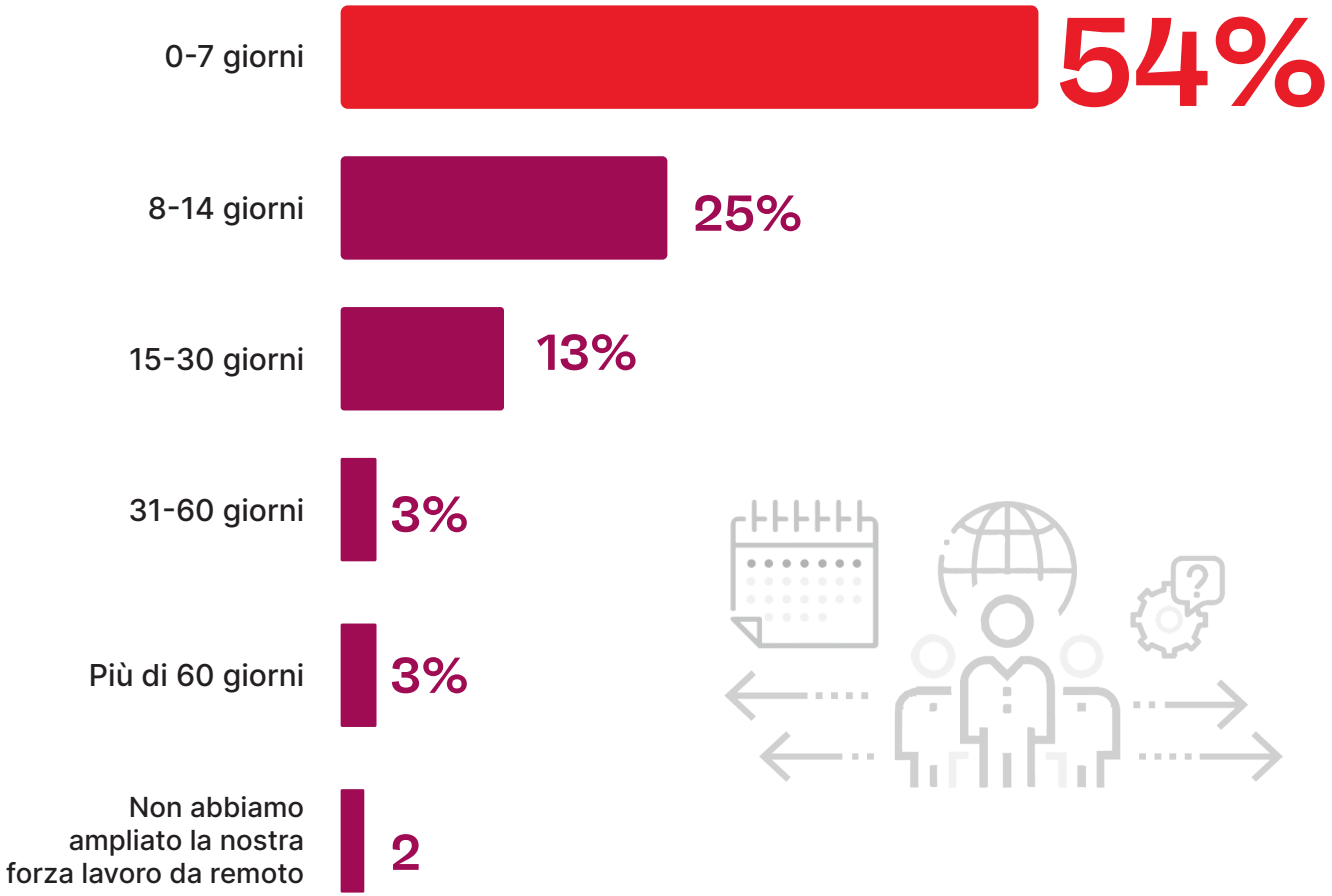
Prima della pandemia di COVID-19, in che misura la vostra organizzazione era preparata con un piano di business continuity/disaster recovery che prevedesse un rapido passaggio dalla forza lavoro on- premises a quella remota?



Giorni Necessari Per Ampliare La Capacità Da Remoto

La maggioranza delle organizzazioni (54%) dichiara di aver ampliato con successo la capacità di supportare pienamente l'ampliamento della forza lavoro in sette giorni o meno.

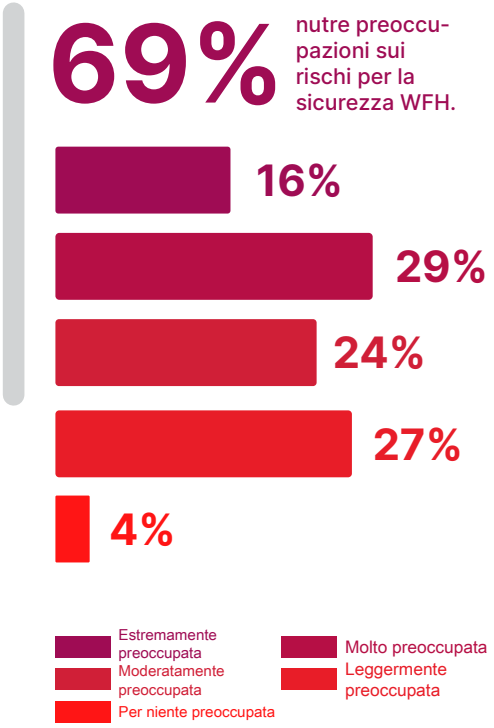
Quanti giorni sono occorsi alla vostra organizzazione per ampliare la capacità di supportare pienamente la forza lavoro da remoto recentemente ampliata?



Percezione Della Sicurezza Del Lavoro Da Remoto

Nonostante il 79% delle organizzazioni ritenga di essersi preparata adeguatamente alla sicurezza WFH, due terzi delle organizzazioni coinvolte in questo sondaggio (69%) nutrono preoccupazioni sui rischi per la sicurezza legati agli utenti che lavorano da casa.

In che misura siete preoccupati rispetto ai rischi per la sicurezza introdotti dagli utenti che lavorano da casa e in che misura la vostra organizzazione era preparata per il passaggio al lavoro a distanza dal punto di vista della sicurezza?



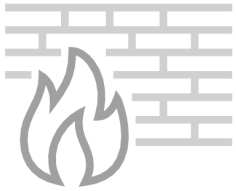
Controlli Di Sicurezza In Atto

I principali controlli di sicurezza in atto per proteggere il lavoro da remoto/da casa sono rappresentati da soluzioni anti-virus/anti-malware (77%), firewall (77%), reti private virtuali (66%) e autenticazione a più fattori (66%).

Quali sono i controlli di sicurezza che attualmente implementate per proteggere gli scenari di lavoro remoto-ufficio domestico?

77%

Anti-virus/ anti-malware



77%

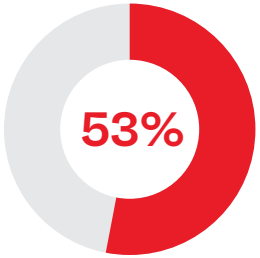
Firewall

66%

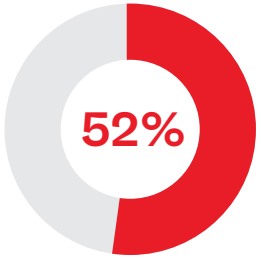
Rete privata virtuale
(VPN/SSL-VPN)

66%

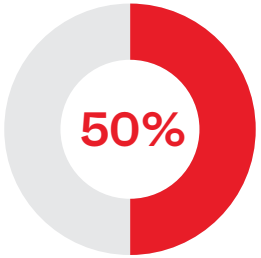
Autenticazione a più fattori
(MFA)



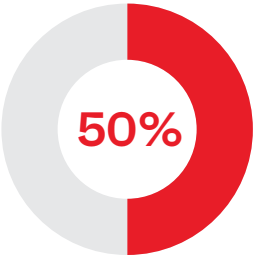
Backup e recupero



Gestione password



Crittografia file



Sicurezza degli endpoint
(EDR)

Anti-phishing 47% | Single sign-on 45% | Conformità endpoint 34% | Mobile Device Management (MDM) 34% | Web Application Firewall (WAF) 29% | Virtual Desktop Infrastructure (VDI) 26% | Load balancing/Application Delivery Controller (ADC) 24% | Web proxy/web filtering 23% | Cloud DLP 18% | Cloud Access Security Brokers (CASB) 16% | User and Entity Behavior Monitoring (UEBA) 11% | Software-Defined Perimeter (SDP) 10% | Zero Trust Network Access (ZTNA) 8% | Altro 3%

Sfide Chiave Per La Sicurezza

Nell'elenco delle sfide chiave per la sicurezza che le organizzazioni che stanno incrementando la propria forza lavoro da remoto devono affrontare, la consapevolezza degli utenti è al primo posto (59%). Seguono l'accesso da reti domestiche o pubbliche non sicure (56%) e l'uso di dispositivi personali (43%).

Quale ritenete sia la maggiore sfida per la sicurezza della vostra organizzazione per quanto riguarda la crescita della forza lavoro da remoto?

59%

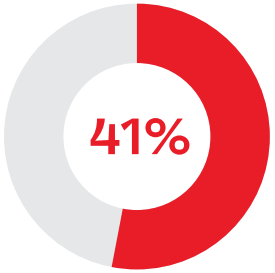
Consapevolezza e formazione dell'utente

56%

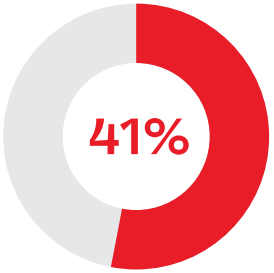
Sicurezza della rete WiFi domestica/pubblica

43%

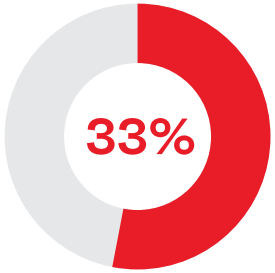
Uso di dispositivi personali/BYOD



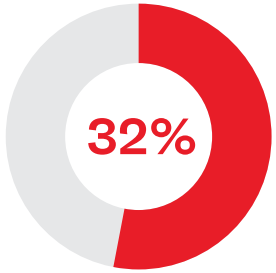
Uscita di dati sensibili



Aumento dei rischi per la sicurezza



Mancanza di visibilità



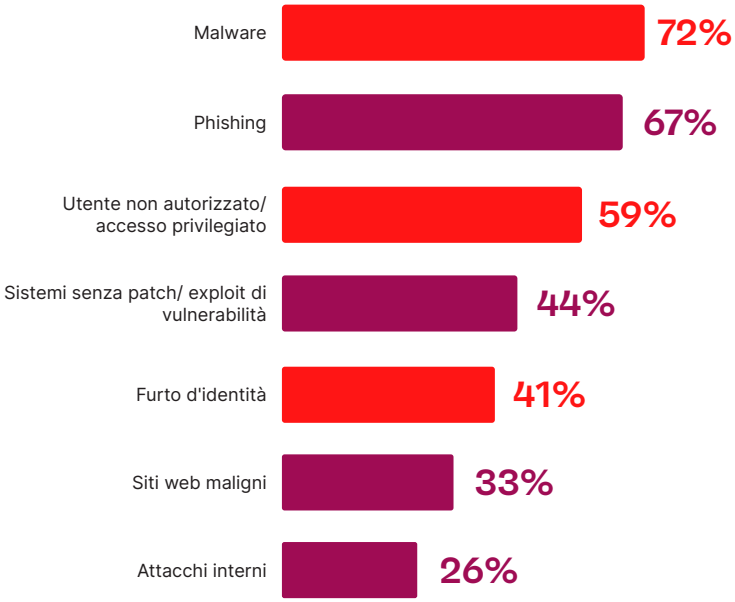
Costi extra di soluzioni per la sicurezza

Disponibilità/esperienza utente 30% | Aggiunta di capacità 24% | Uso non autorizzato di applicazioni cloud 21% | Lacune di responsabilità/controllo 21% | Nessuna 5% | Altro 2%

Vettori Di Attacco

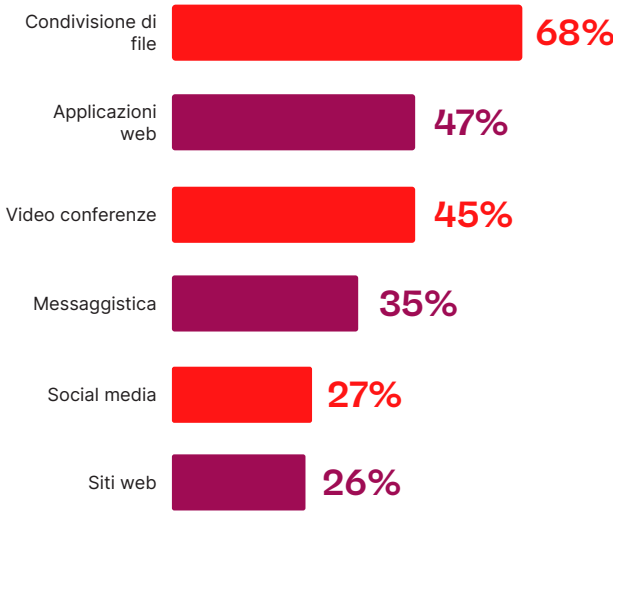
Malware, phishing, accesso non autorizzato di utenti/dispositivi e sistemi senza patch sono stati indicati come i principali vettori di attacco dovuti ai dipendenti che lavorano da casa. Tra le applicazioni che contribuiscono alla produttività e alla collaborazione, le maggiori preoccupazioni nutrite dalle organizzazioni in materia di sicurezza riguardano la condivisione di file (68%), le applicazioni web (47%), le videoconferenze (45%) e la messaggistica (35%).

Quali sono i vettori specifici di minacce che vi preoccupano maggiormente dipendenti che lavorano da casa?



Altro 5%

Quali applicazioni di lavoro utilizzate dai lavoratori a maggiormente sicurezza? distanza vi dal punto preoccupano vista della



Altro 2%

Livello Di Sicurezza Del Lavoro Da Remoto

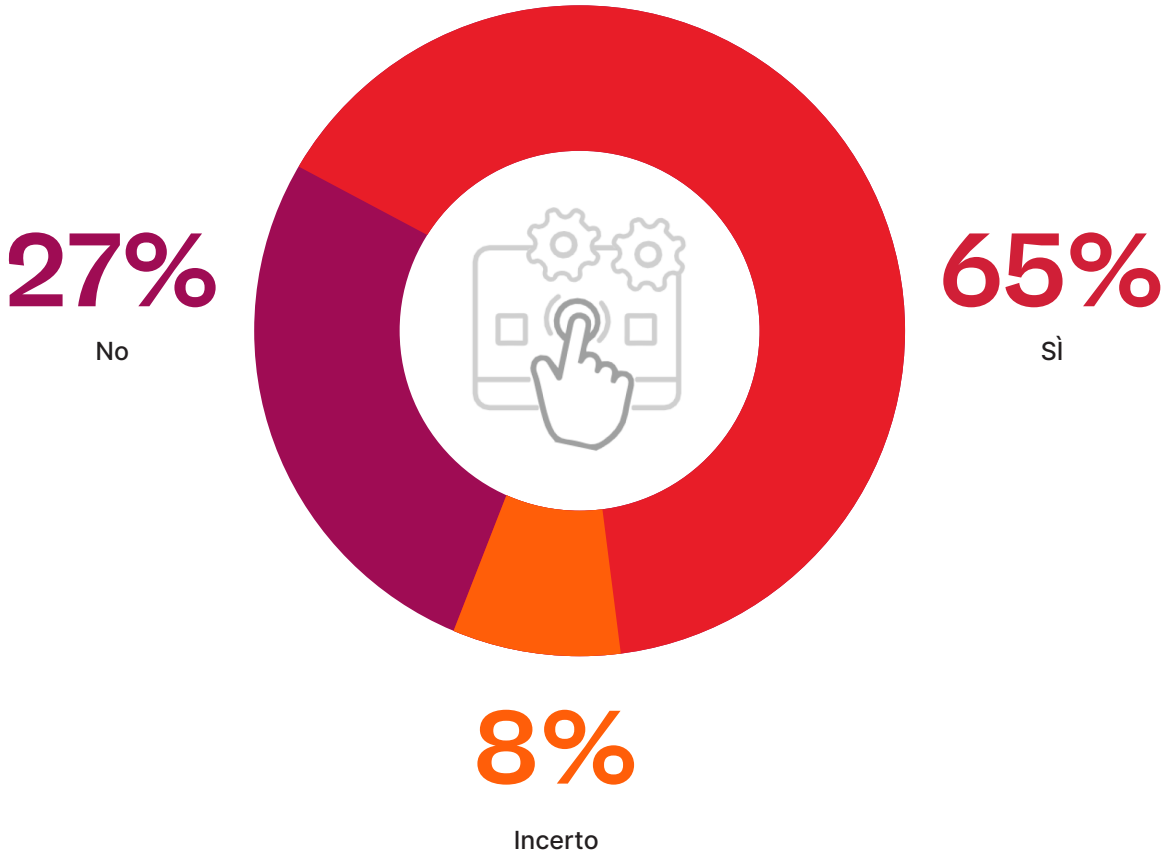
Una maggioranza del 78% conferma di applicare lo stesso livello di controlli di sicurezza per tutti i ruoli che accedono da remoto.

Applicate lo stesso livello di controlli di sicurezza e di gestione dei dati per tutti i ruoli dell'azienda che accedono da remoto?

Accesso Da Dispositivi Personali

Quasi tre quarti delle organizzazioni hanno autorizzato l'accesso da dispositivi personali e non gestiti per supportare il lavoro da casa, mentre almeno il 27% vede questo scenario come un rischio significativo per la sicurezza.

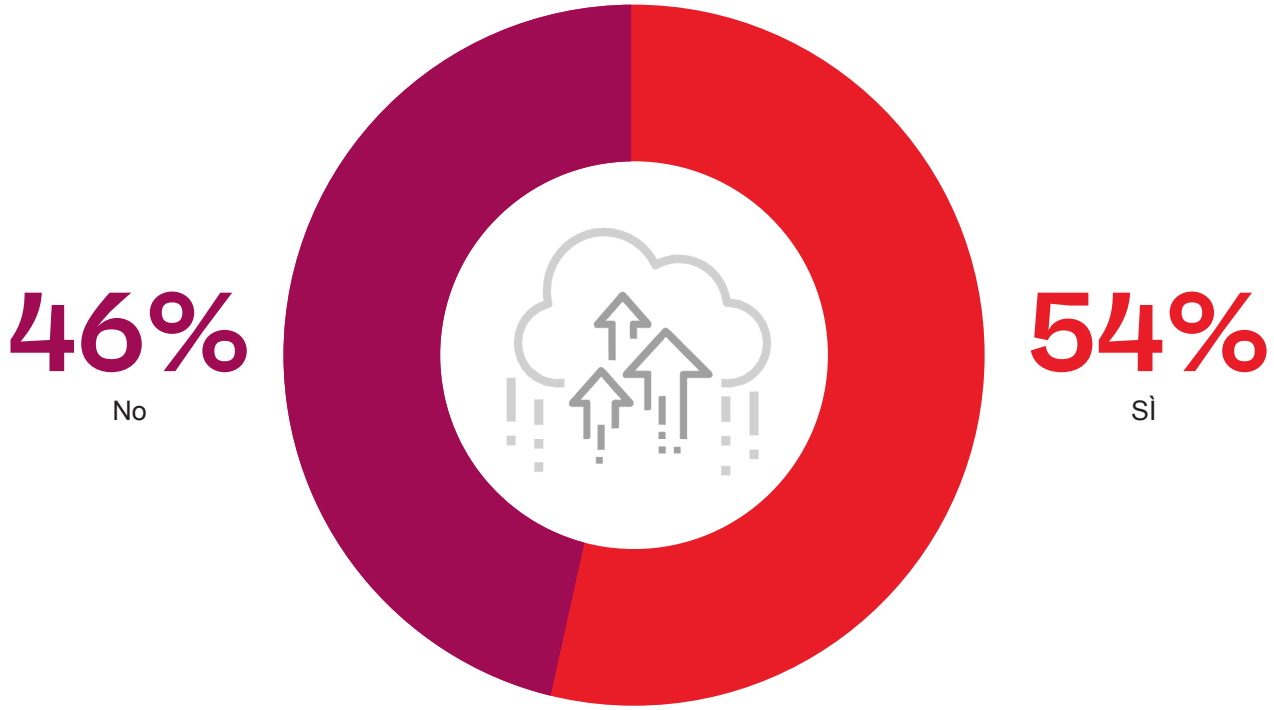
I dipendenti sono in grado di accedere alle applicazioni gestite da dispositivi personali e non gestiti?



Migrazione Al Cloud

Una maggioranza del 54% conferma che la pandemia di COVID ha accelerato la migrazione dei flussi di lavoro alle app basate sul cloud.

Il COVID ha accelerato la migrazione di ulteriori flussi di lavoro o applicazioni degli utenti verso applicazioni basate sul cloud?



Remote Security Risk

Organizations are most concerned with protection of sensitive data, especially when accessed by unmanaged endpoints (46%), followed by added exposure to malware (34%).

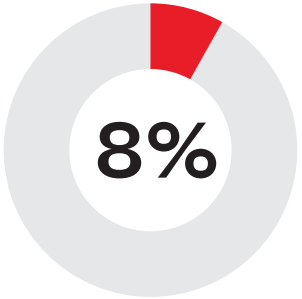
What is the primary risk you're concerned with as your users connect remotely?

46%

Protezione dei miei dati, soprattutto quando l'accesso avviene da endpoint non gestiti

34%

Esposizione a malware, phishing o altri exploit



Garantire la conformità dei miei utenti regolamentati

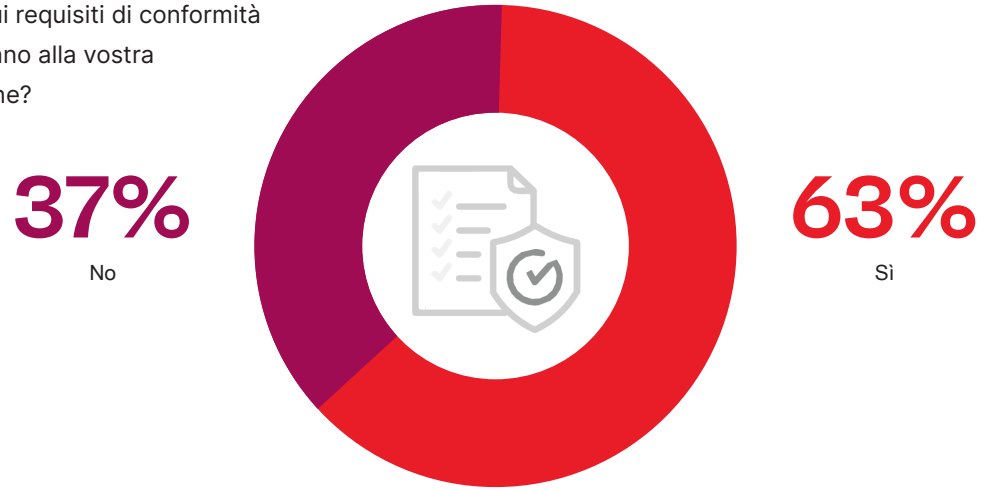
Audit e supervisione dei dipendenti che svolgono Il lavoro da risorse non gestite

Altro 4%

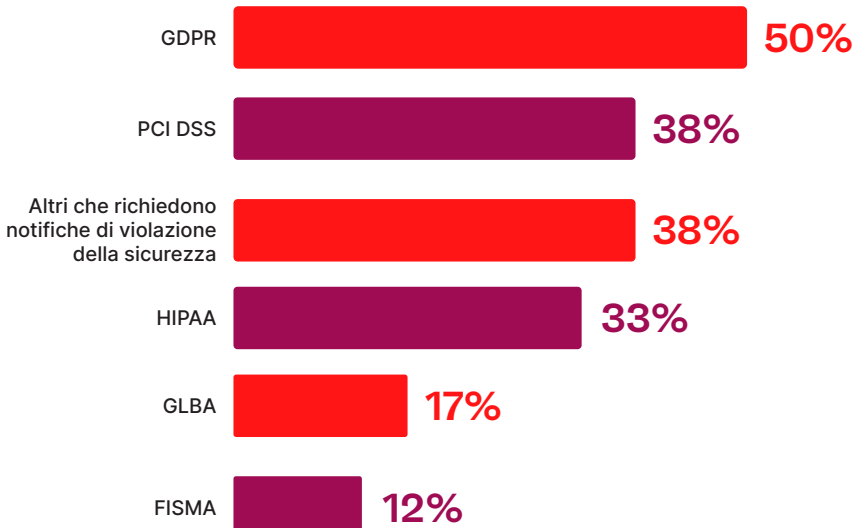
Impatto Sulla Conformità

Due terzi delle organizzazioni ritengono che gli ambienti di lavoro a distanza abbiano un impatto sulla rispettiva condizione di conformità.

Il lavoro a distanza potrebbe avere un impatto sui requisiti di conformità che si applicano alla vostra organizzazione?



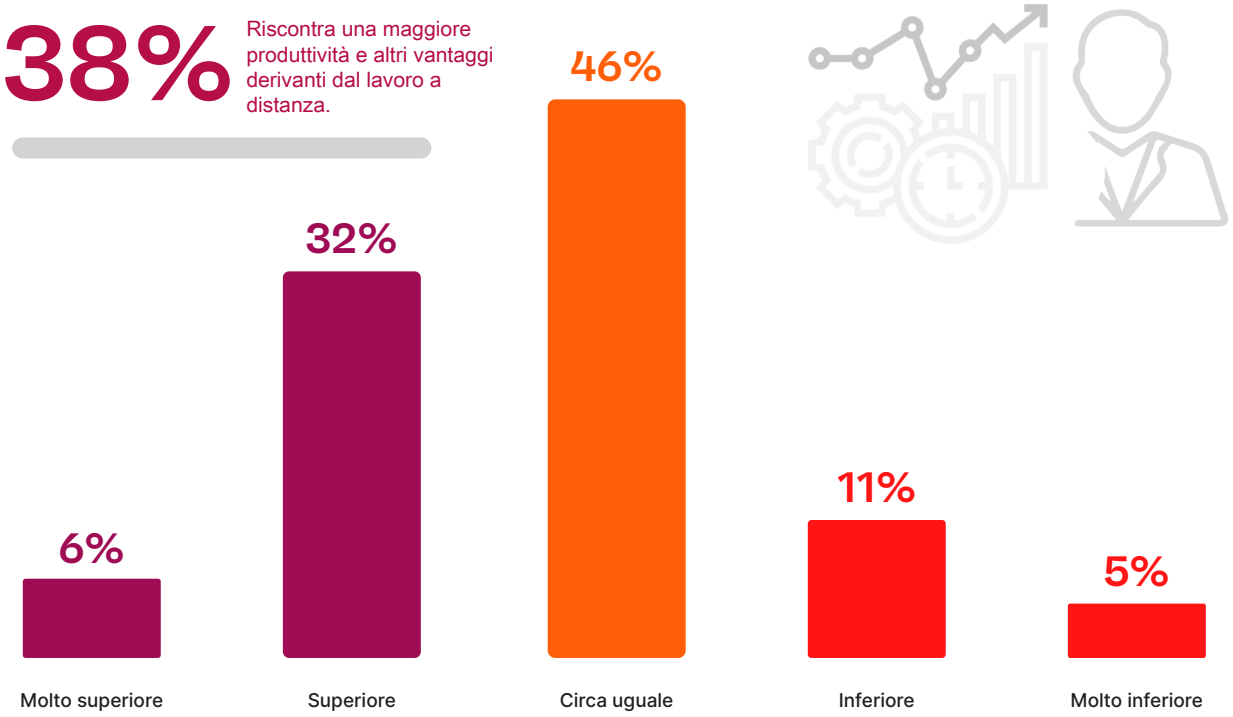
If so, which ones?



Effetti Sulla Produttività

Il 38% delle organizzazioni ha dichiarato di assistere a una maggiore produttività e ad altri vantaggi derivanti dal lavoro a distanza. Solo il 16% riscontra una minore produttività.

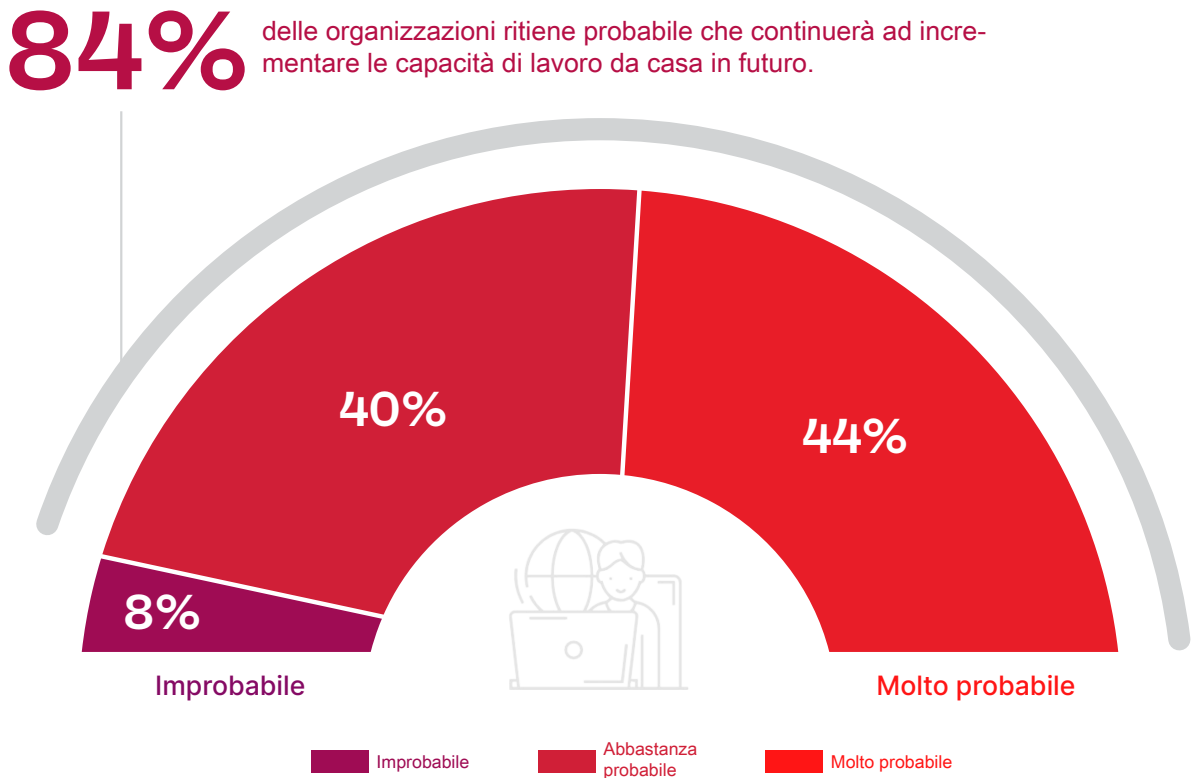
La vostra organizzazione riscontra una maggiore produttività e altri vantaggi derivanti dal lavoro a distanza?



Il Lavoro Da Remoto

Una maggioranza dell'84% delle organizzazioni ritiene probabile (44% molto probabile) che continuerà ad incrementare le capacità di lavoro da casa in futuro, grazie all'aumento della produttività e ad altri vantaggi per l'azienda.

Prevedete di continuare a sostenere un aumento delle capacità di lavoro da casa in futuro (grazie all'aumento della produttività e ad altri vantaggi per l'azienda)?

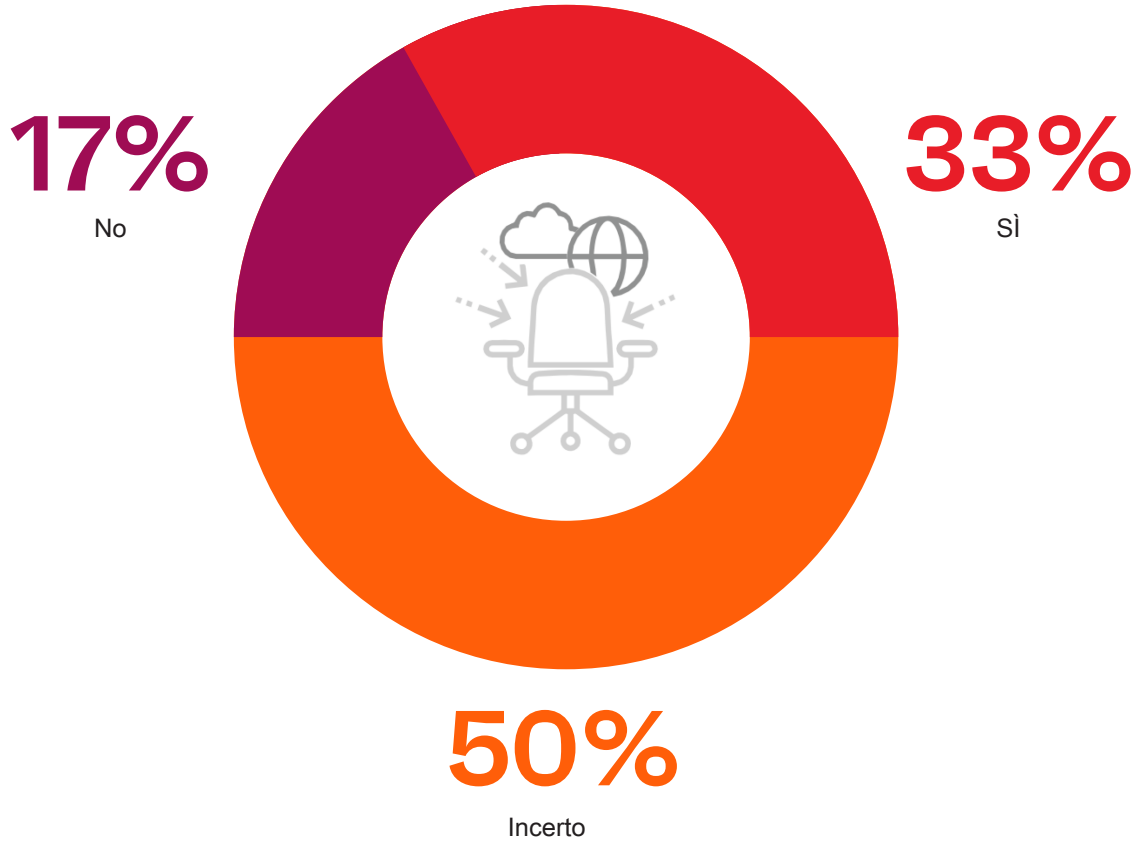


Incerto 8%

Rendere Permanente Il Lavoro Da Remoto

Un terzo delle organizzazioni sta pensando di rendere alcune posizioni remote in via permanente una volta terminata la crisi COVID.

La vostra organizzazione sta pensando di rendere remote in via permanente alcune posizioni (che prima erano in sede) al termine della crisi COVID?

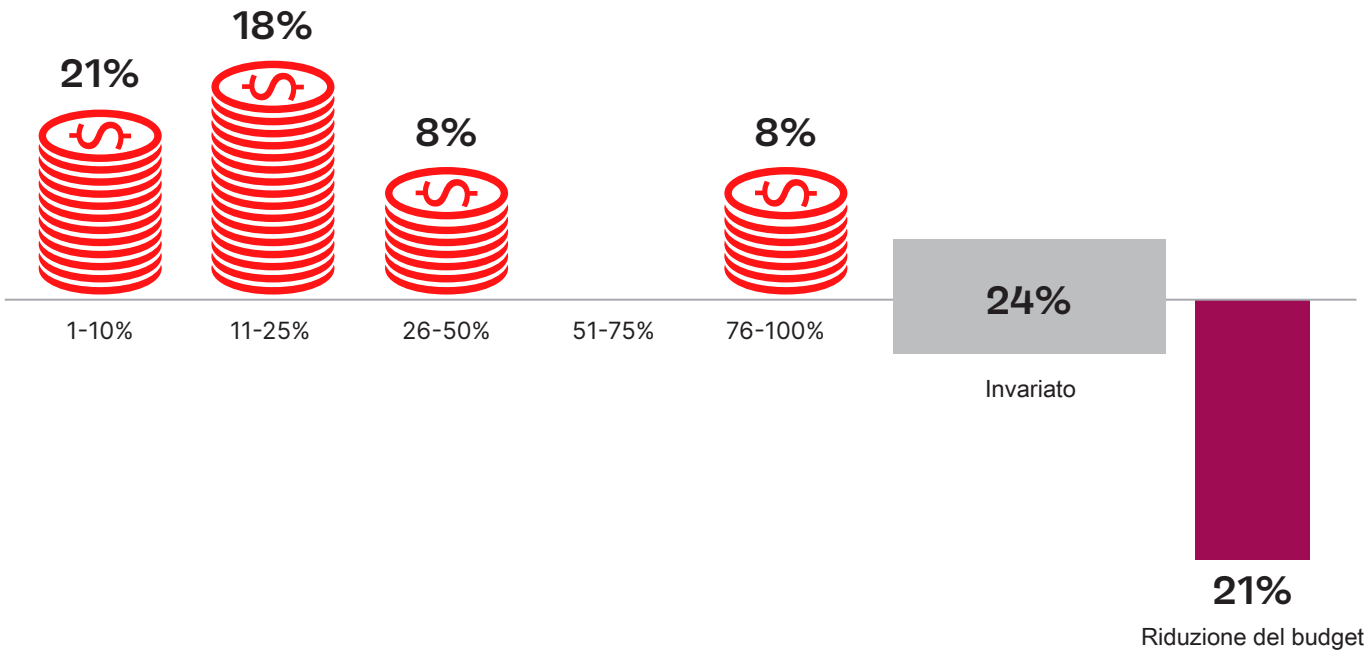


Tendenze Dei Budget

La maggioranza (55%) delle organizzazioni prevede che i budget destinati alla sicurezza della forza lavoro in remoto cresceranno nei prossimi 12 mesi (dopo aprile 2020). Per un quarto degli intervistati, i budget per la sicurezza rimarranno invariati e solo il 21% prevede una riduzione dei budget.

In che misura il vostro budget per i controlli di sicurezza del lavoro da remoto è destinato a crescere nei prossimi 12 mesi?

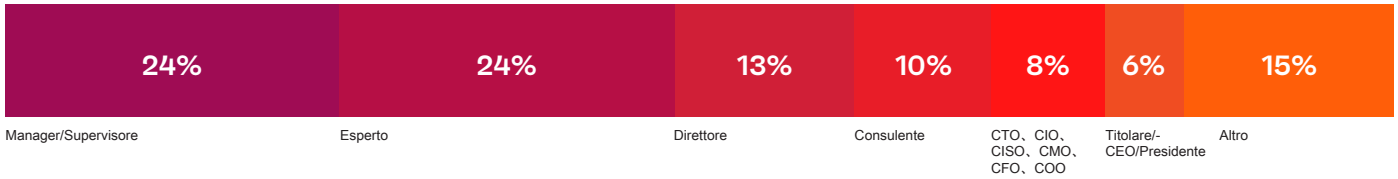
55% prevede che i budget per la sicurezza della forza lavoro da remoto aumenteranno nei prossimi 12 mesi.



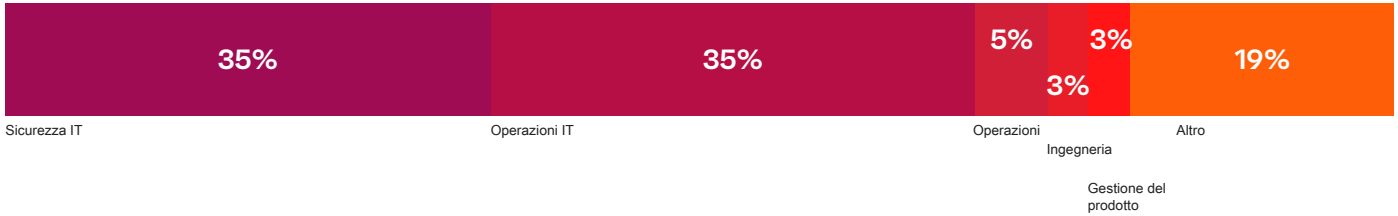
Metodologia E Demografia

Il presente report si basa sui risultati di un approfondito sondaggio online condotto nel maggio 2020, che ha coinvolto 413 professionisti dell'IT e della sicurezza informatica negli Stati Uniti, volto a individuare le ultime tendenze adottate dalle aziende, le sfide, le lacune e le preferenze delle soluzioni per le forze lavoro da remoto, alla luce della pandemia di COVID-19 del 2020. Gli intervistati spaziano dai dirigenti tecnici ai professionisti della sicurezza IT e rappresentano uno spaccato equilibrato di organizzazioni di varie dimensioni in più settori.

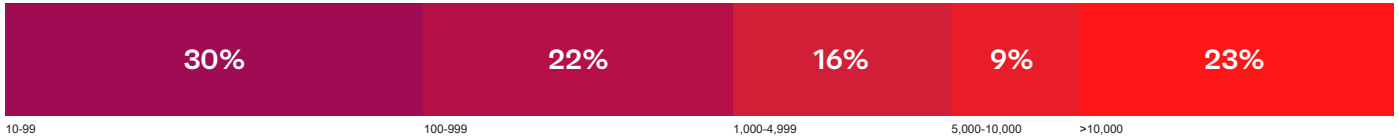
Livello Di Carriera



Reparto



Dimensioni Dell'azienda



Industria

Pulse Secure
Acquired by Ivanti

Pulse Secure offre soluzioni di accesso sicuro semplici e complete, basate su software, destinate a persone, dispositivi, beni e servizi e volte a migliorare la visibilità, la protezione e la produttività dei nostri clienti. Le nostre suite integrano in modo unico l'accesso al cloud, ai dispositivi mobili, alle applicazioni e alla rete per attivare l'IT ibrido in un mondo Zero Trust. Oltre 23.000 imprese e fornitori di servizi di ogni settore verticale si affidano a Pulse Secure per consentire alla propria forza lavoro mobile di accedere in modo sicuro ad applicazioni e informazioni nei data center e nel cloud, garantendo al contempo la conformità aziendale.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com