ivanti

Rapport Sur La Cybers Curit Du Work-From-Home (WFH)

2020

Présentation

Les solutions d'accès sécurisé (Secure Access) assurent le bon fonctionnement des entreprises car elles garantissent la sécurité de l'informatique distante, et connectent les personnes et les périphériques aux applications du centre de données et du Cloud, même dans les circonstances les plus imprévisibles.

Lorsque l'impact du Coronavirus (COVID-19) s'est intensifié et que c'est devenu une pandémie, l'Organisation mondiale de la santé a suggéré que tout le monde travaille depuis son domicile, afin d'éviter les transports publics et les environnements de bureau, en vue de limiter la propagation du virus et les risques d'infection.

Début 2020, les gouvernements et les administrations locales du monde entier ont commencé à conseiller, voire à imposer, aux gens de s'isoler et d'éviter le travail sur site, sauf pour les entreprises essentielles. Les entreprises ont immédiatement réagi pour étendre et faciliter le télétravail depuis le domicile (WFH).

Outre l'impact potentiel sur la productivité des utilisateurs, ce changement de lieu de travail et ce besoin immédiat de fonctions de télétravail ont mis en danger l'infrastructure IT, la continuité des activités et la sécurité des informations.

Le présent rapport 2020 sur le télétravail depuis le domicile (Work From Home), sponsorisé par Pulse Secure et produit par Cybersecurity Insiders, examine en détail la façon dont les entreprises ont assuré la transition de leurs collaborateurs et de leurs ressources, et montre les problèmes de cybersécurité, les inquiétudes, les stratégies et les résultats espérés du télétravail depuis le domicile (WFH). Cette enquête a été menée en mai 2020 auprès de plus de 400 décideurs de la sécurité IT, techniciens et entreprises de tailles diverses dans plusieurs secteurs d'activité. Cette enquête a montré que

84 % des entreprises prévoient que le télétravail va s'étendre et devenir plus permanent, et près d'un tiers prévoient d'augmenter leur budget pour sécuriser les accès à court terme.

Principaux résultats de l'enquête :

- Plus de 3 fois davantage d'expansion des capacités d'utilisateurs en télétravail depuis le domicile (WFH), avec près de 100 % du personnel pour plus de 75 % des entreprises
- 33 % des entreprises n'étaient pas assez préparées à l'urgence de l'accès distant sécurisé
- 54 % vont basculer davantage de workflows et d'applis dans le Cloud
- 38 % des entreprises ont constaté des gains de productivité et d'autres avantages
- 84 % prévoient des programmes de télétravail (WFH) plus larges et plus permanents
- Plus de la moitié prévoient d'augmenter leur budget de sécurisation des accès dans les 12 prochains mois (après avril 2020)
- 66 % prévoient une augmentation des menaces de sécurité liées au télétravail (WFH) et 63 % prévoient que le télétravail (WFH) va poser des problèmes de conformité
- Le malware, l'hameçonnage, l'accès des utilisateurs et périphériques non autorisés, et les systèmes sans correctifs sont considérés comme les principaux vecteurs d'attaque du télétravail (WFH)
- L'antivirus/malware, le pare-feu, le VPN SSL, l'authentification multifacteur (MFA) et la sauvegarde sont les principales solutions employées pour garantir la sécurité du télétravail et la résilience des entreprises

Merci beaucoup à Pulse Secure pour son soutien à cet important projet de recherche.

Nous espérons que les informations de ce rapport vous intéresseront et vous seront utiles pour continuer à protéger vos investissements IT, à assurer la continuité des activités et à préserver vos collaborateurs.

Merci,

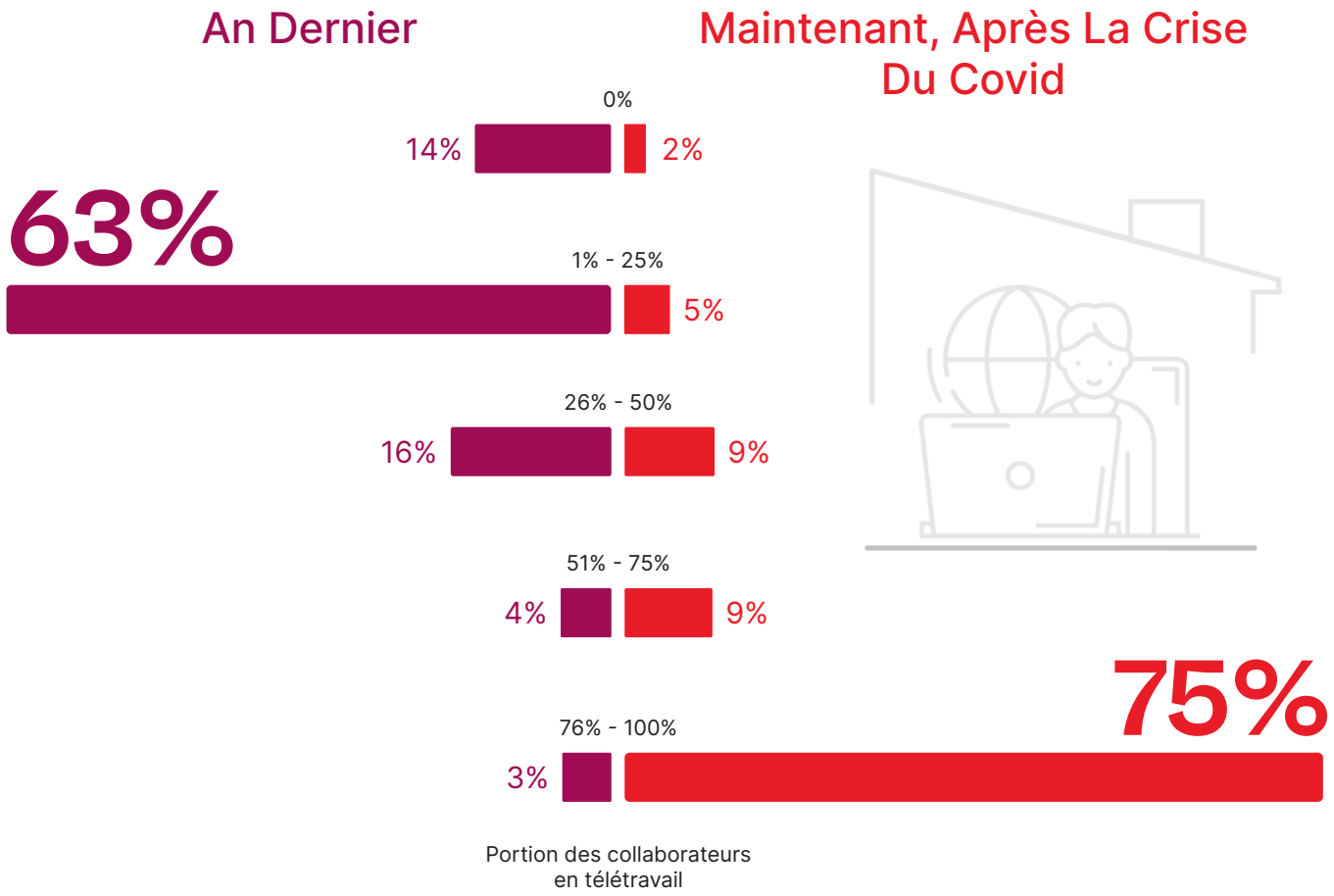
Holger Schulze

CEO and Founder
Cybersecurity Insiders

Explosion Du Nombre De Collaborateurs En Télétravail

L'enquête révèle un passage massif à un environnement de travail distant, au domicile, en raison de la pandémie de COVID-19. Même si la majorité des entreprises (63 %) avaient déjà jusqu'à un quart de leurs collaborateurs en télétravail (depuis le domicile ou ailleurs) avant la crise, trois quarts de ces entreprises, et c'est énorme, signalent que plus de 75 % de leur personnel travaille désormais depuis le domicile.

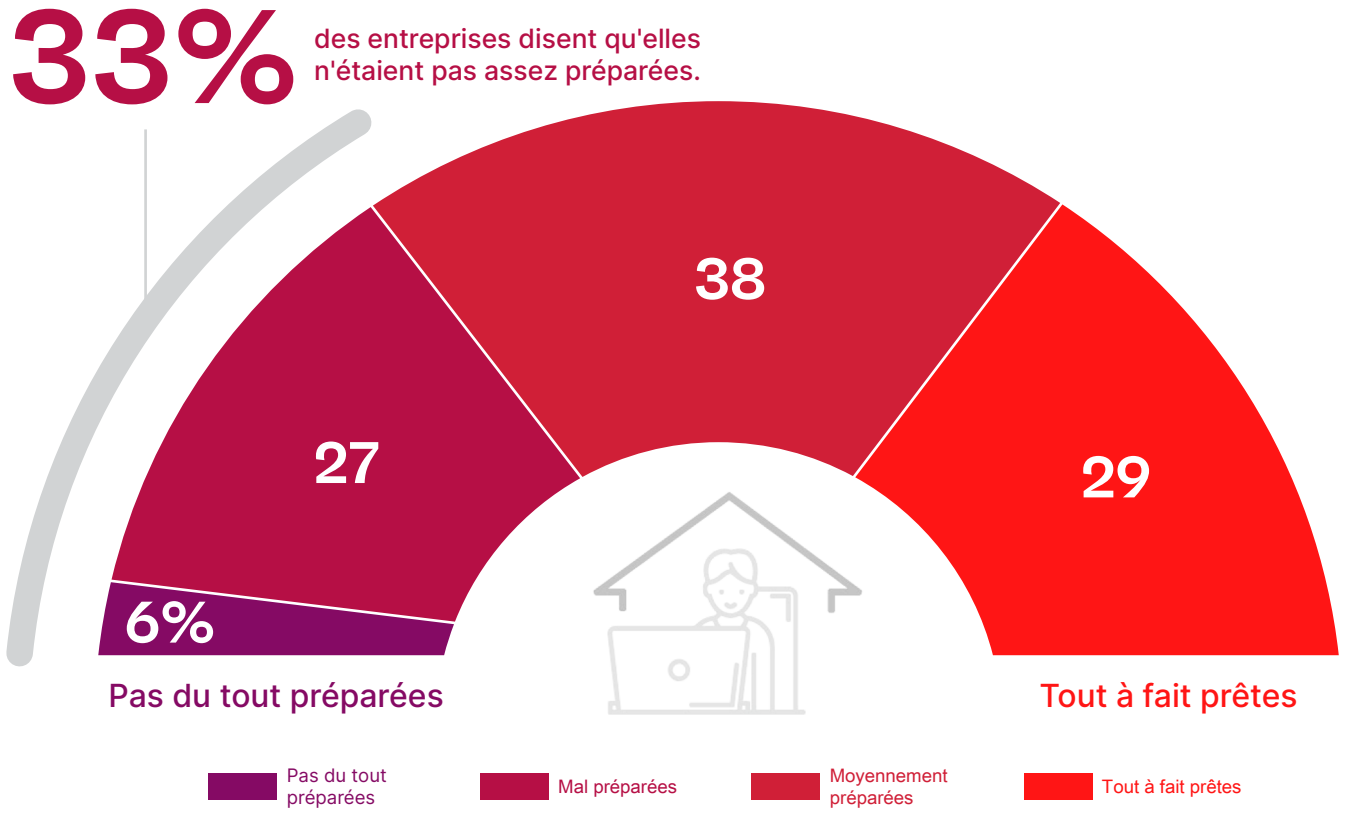
Quel pourcentage de votre personnel travaillait à distance/à son domicile l'AN DERNIER, par rapport à la situation MAINTENANT avec la crise du COVID ?



Préparation Au Télétravail

Un tiers des entreprises admettent qu'elles n'étaient pas assez préparées au passage rapide du travail sur site au télétravail.

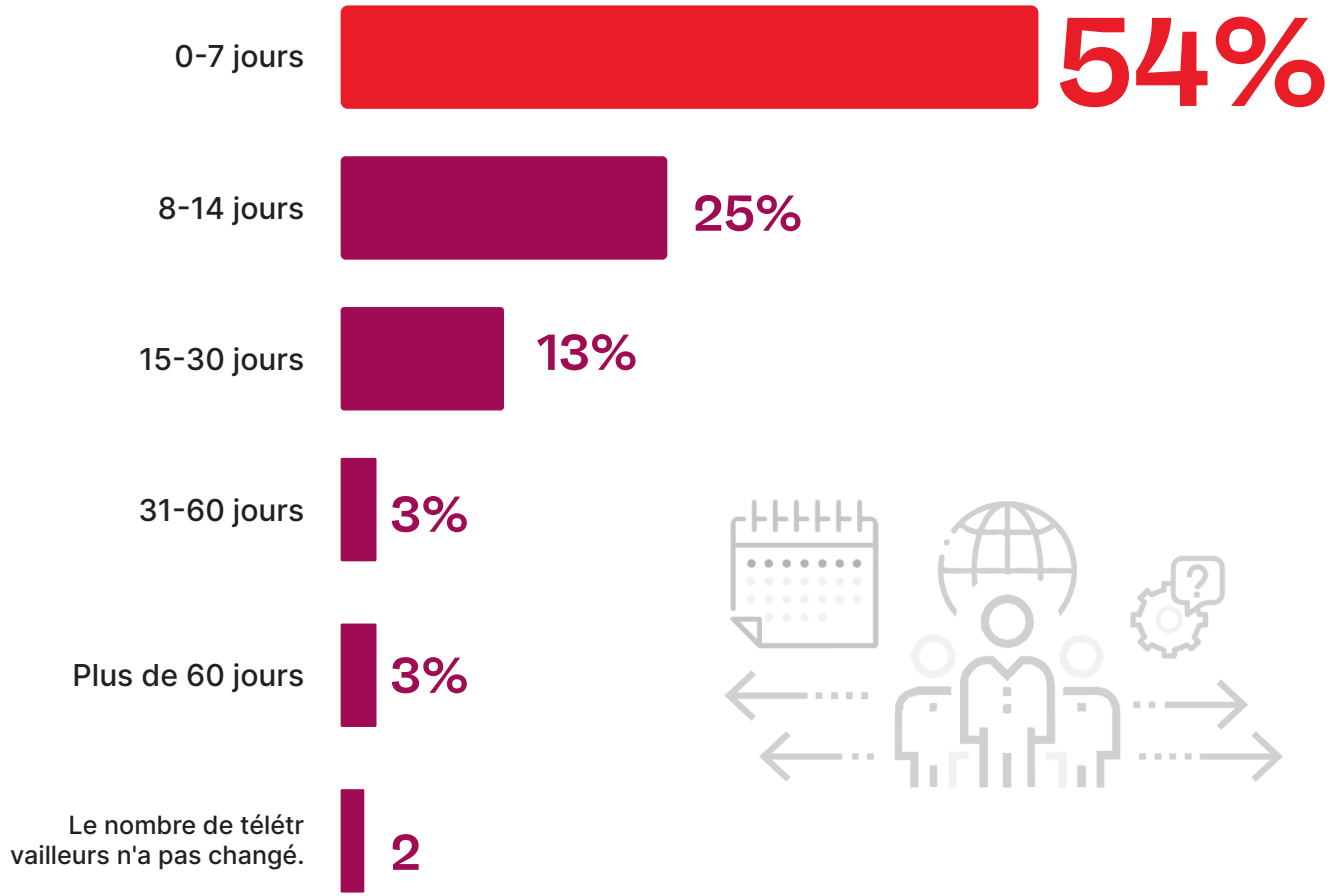
Avant la pandémie de COVID-19, quel était le niveau de préparation de votre entreprise, avec un plan de continuité des activités/reprise après sinistre impliquant un passage rapide du travail sur site au télétravail ?



Nombre De Jours Requis Pour Augmenter Les Capacités De Télétravail

La majorité des entreprises (54 %) disent qu'elles ont réussi à augmenter leurs capacités pour prendre totalement en charge les collaborateurs en télétravail supplémentaires en sept jours maximum.

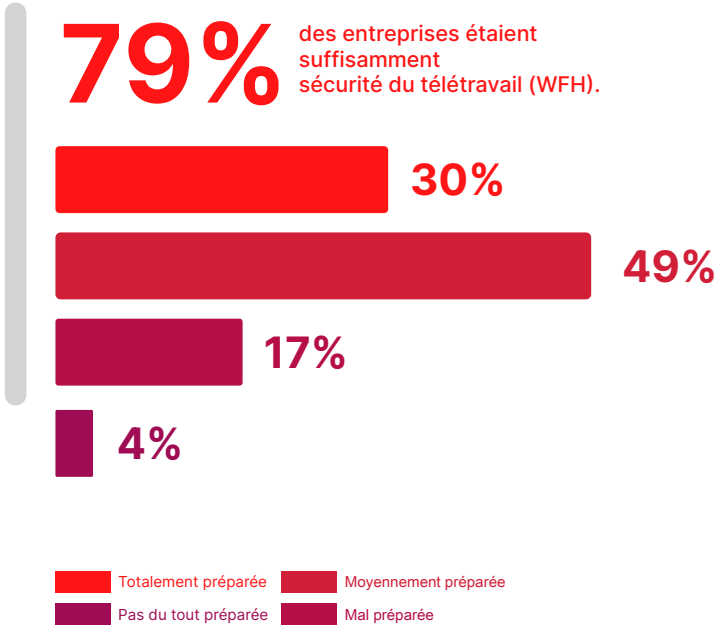
Combien a-t-il fallu de jours à votre entreprise pour étendre ses capacités afin de totalement prendre en charge l'augmentation

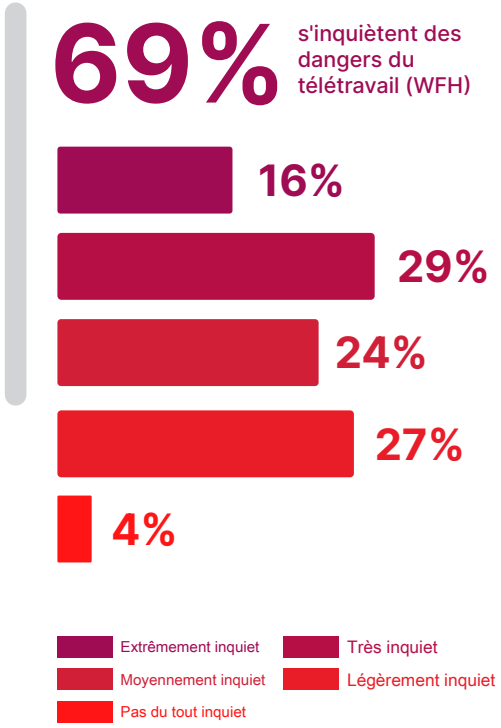


Perception De La Sécurité Du Télétravail

Bien que 79 % des entreprises considèrent qu'elles étaient suffisamment préparées à la sécurité du télétravail depuis le domicile (WFH), deux tiers des entreprises interrogées (69 %) s'inquiètent des risques pour la sécurité lorsque les collaborateurs travaillent chez eux.

Êtes-vous inquiet des risques de sécurité introduits par les collaborateurs travaillant à domicile, et à quel point votre entreprise était-elle prête au passage au télétravail, du point de vue de la sécurité ?





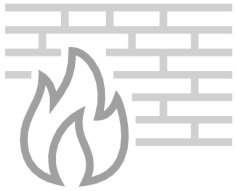
Contrôles De Sécurité En Place

Les principaux contrôles de sécurité mis en place pour protéger le télétravail/le travail au domicile (WFH) sont les solutions antivirus/ antimalware (77 %), les pare-feux (77 %), les réseaux privés virtuels (66 %) et l'authentification multifacteur (66 %).

Quels contrôles de sécurité sont actuellement déployés pour sécuriser vos collaborateurs qui travaillent à domicile ?

77%

Antivirus /antimalware



77%

Pare-feux

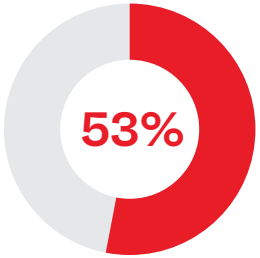
66%

Réseau privé virtuel
(VPN/SSL-VPN)

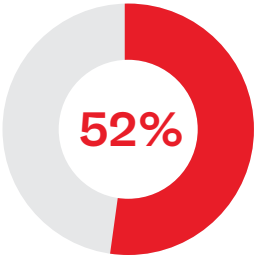
66%

Authentification multifacteur
(MFA)

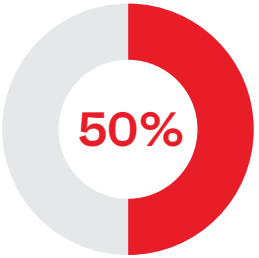
Antihameçonnage 47 % | Connexion avec identification unique (SSO) 45 % | Conformité du poste client 34 % | Gestion des périphériques mobiles (MDM) 34 % | Pare-feu d'application Web (WAF) 29 % | Infrastructure de postes de travail virtuels (VDI) 26 % | Équilibrage de charge/Contrôle de distribution des applications (ADC) 24 % | Proxy Web/Filtrage Web 23 % | Prévention des pertes de données (DLP) dans le Cloud 18 % | Brokers de sécurité d'accès au Cloud (CASB) 16 % | Analyse du comportement des utilisateurs et des entités (UEBA) 11 % | Périmètre défini par logiciel (SDP) 10 % | Accès réseau Zero Trust (ZTNA) 8 % | Autre 3 %



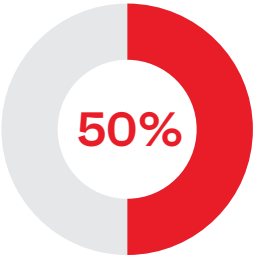
Sauvegarde et récupération



Gestion des mots de passe



Cryptage des fichiers



Sécurité du poste client
(EDR)

Principaux Problèmes De Sécurité

Le manque d'information des utilisateurs est le plus sévère (59 %) des problèmes de sécurité que rencontrent les entreprises qui augmentent le nombre de leurs collaborateurs en télétravail. Viennent ensuite l'accès via des réseaux privés ou des réseaux publics non sécurisés (56 %), et l'utilisation de périphériques personnels (43 %).

D'après vous, quel est le plus gros problème de sécurité pour votre entreprise lorsqu'il faut augmenter le nombre des collaborateurs en télétravail ?

59%

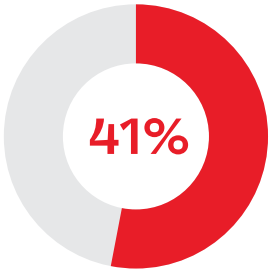
Information et éducation des utilisateurs

56%

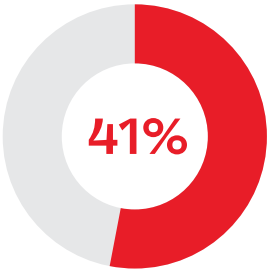
Sécurité des réseaux privés/Wi-Fi publics

43%

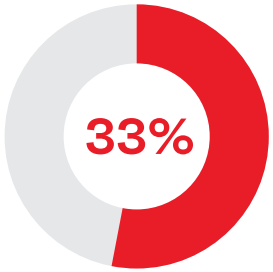
Utilisation de périphériques personnels/BYOD



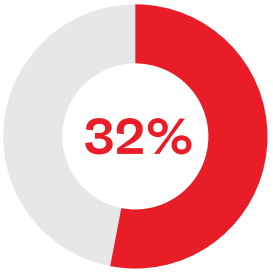
Données sensibles qui quittent le périmètre



Augmentation des risques pour la sécurité



Manque de visibilité



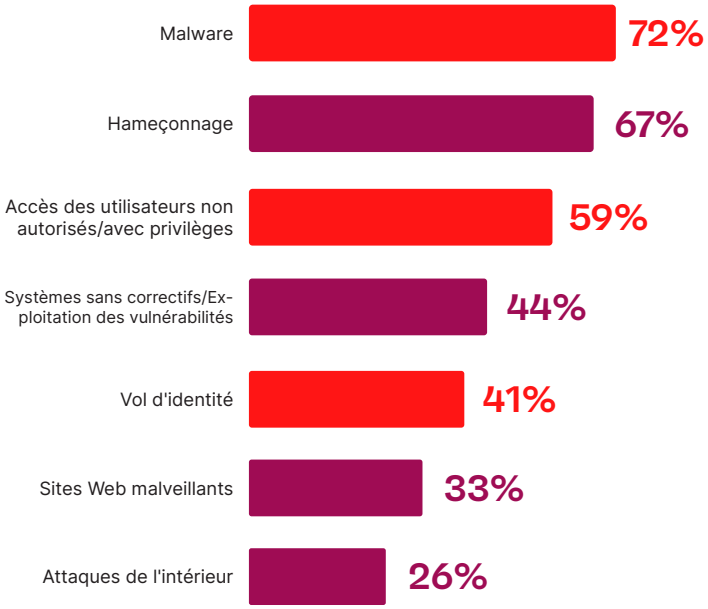
Coût supplémentaire des solutions de sécurité

Disponibilité/Expérience utilisateur 30 % | Ajout de capacité 24 % | Utilisation non autorisée d'applis de Cloud 21 % | Responsabilisation/Fréquence des audits 21 % | Aucun 5 % | Autre 2 %

Amplification Des Vecteurs D'attaque

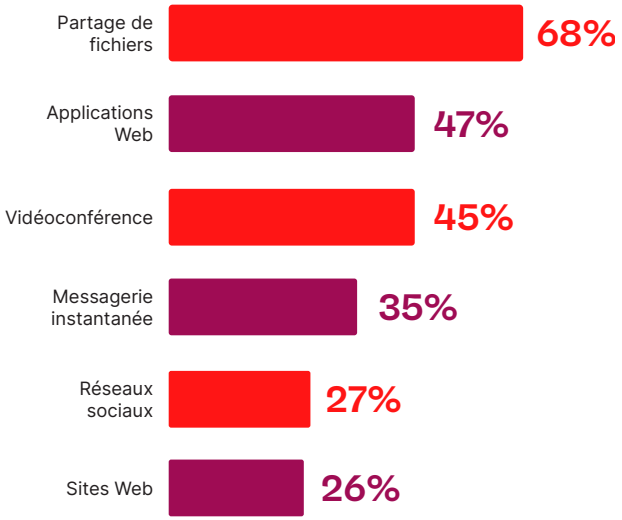
Le malware, l'hameçonnage, l'accès des utilisateurs/périphériques non autorisés et les systèmes sans correctifs ont été identifiés comme les principaux vecteurs d'attaques liés au fait que les collaborateurs travaillent depuis leur domicile. Parmi les applications qui contribuent à la productivité et à la collaboration, les entreprises s'inquiètent surtout de la sécurité du partage de fichiers (68 %), des applications Web (47 %), de la vidéoconférence (45 %) et de la messagerie instantanée (35 %).

Quels sont les vecteurs de menace spécifiques qui vous inquiètent particulièrement lorsque vos collaborateurs travaillent à leur domicile ?



Autre 5%

Quelles sont les applications utilisées par les télétravailleurs dont la sécurité vous préoccupe le plus ?



Autre 2%

Niveau De Sécurité Du Télétravail

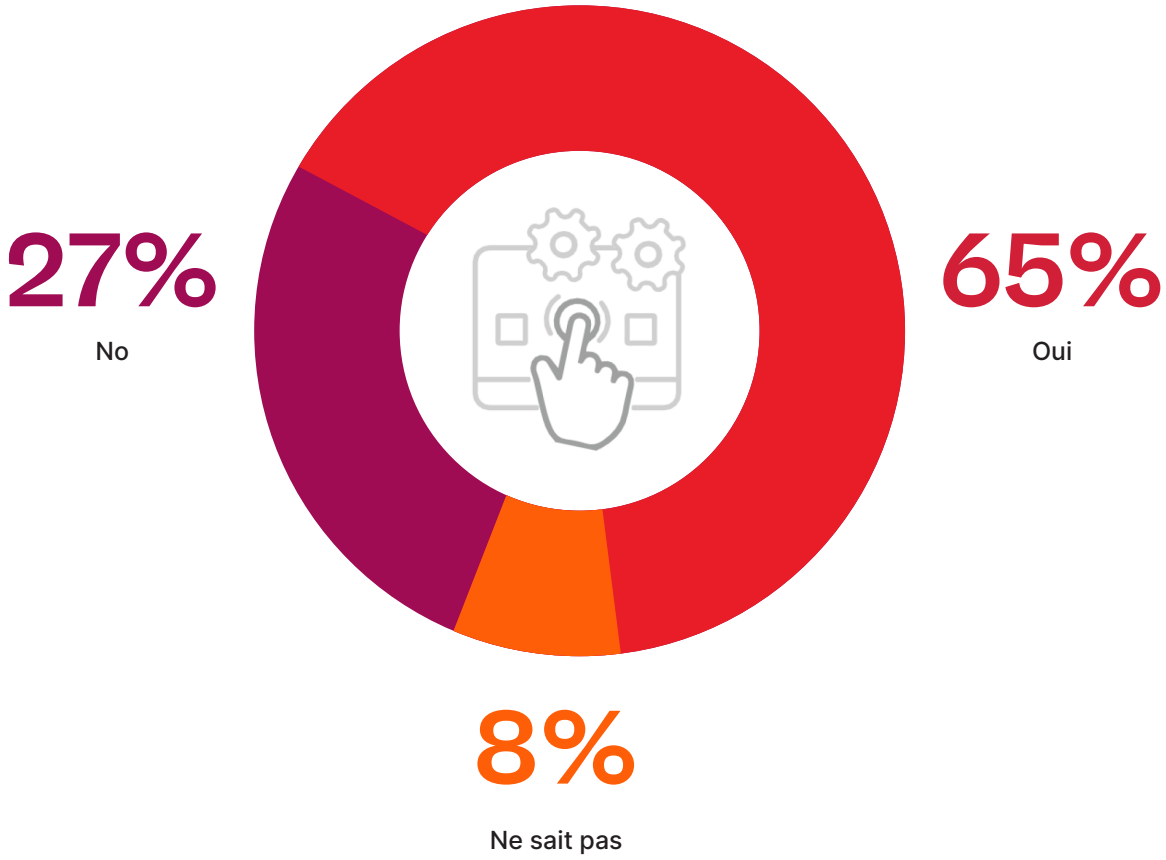
La majorité des entreprises (78 %) confirment qu'elles appliquent le même niveau de contrôles de sécurité à tous les rôles qui accèdent aux ressources à distance.

Appliquez-vous le même niveau de contrôles de sécurité et de gestion des données à tous les rôles de votre entreprise pour l'accès à distance ?

Accès Depuis Des Périphériques Personnels

Près de trois quarts des entreprises autorisent l'accès depuis des périphériques personnels non gérés pour prendre en charge le travail depuis le domicile (WFH), alors qu'au moins 27 % considèrent que cette situation représente un vrai danger pour la sécurité.

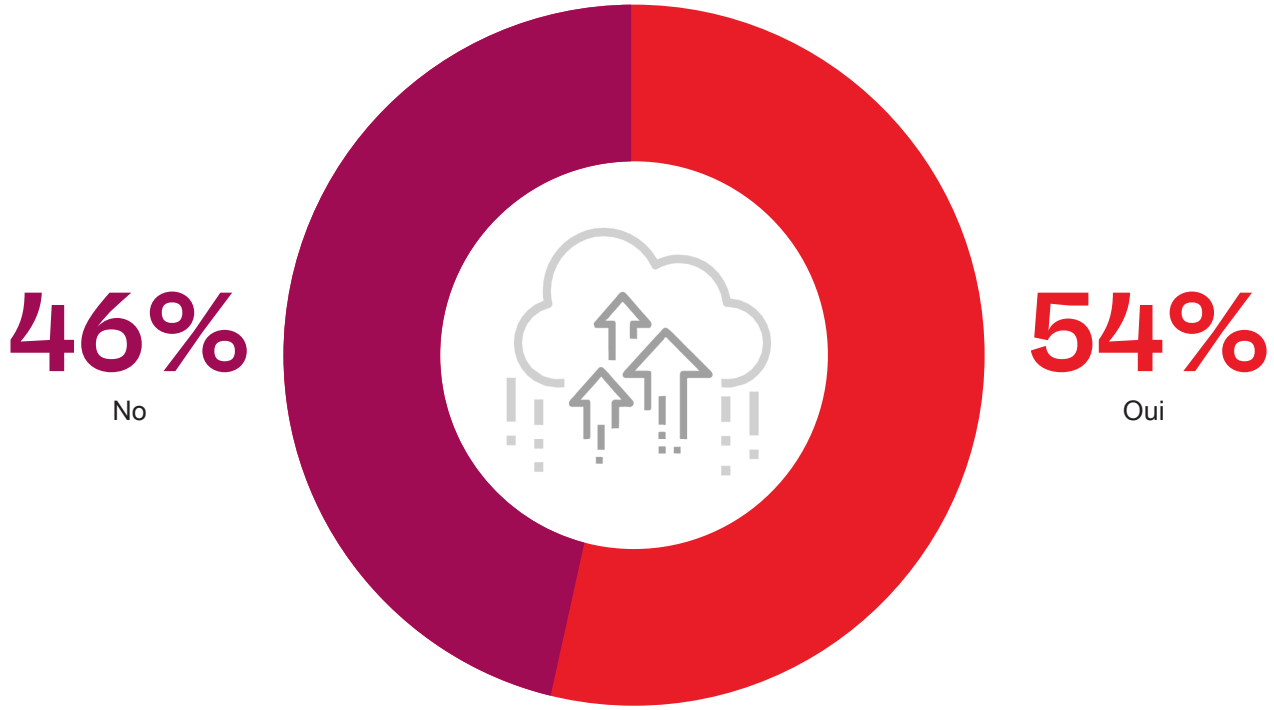
Vos collaborateurs peuvent-ils accéder aux applications gérées depuis des périphériques personnels non gérés ?



Migrationvers Le Cloud

Une majorité d'entreprises (54 %) disent que la pandémie de COVID a accéléré la migration des workflows vers des applis de Cloud.

Le COVID a-t-il accéléré la migration de workflows utilisateur ou d'applications supplémentaires vers des applications de Cloud ?



Dangers Du Télétravail Pour La Sécurité

Les entreprises se préoccupent surtout de la protection des données sensibles, surtout lorsqu'on y accède à l'aide de postes client non gérés (46%), et de l'exposition plus important aux malwares (34%).

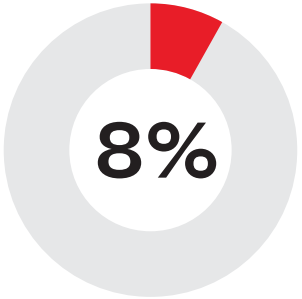
Quel est le principal danger qui vous inquiète lorsque vos utilisateurs se connectent à distance ?

46%

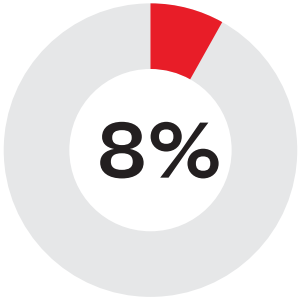
Protection de mes données, surtout en cas d'accès sur un poste client non géré

34%

Exposition au malware, à l'hameçonnage ou à d'autres attaques



Garantie de conformité de mes utilisateurs soumis à des régulations



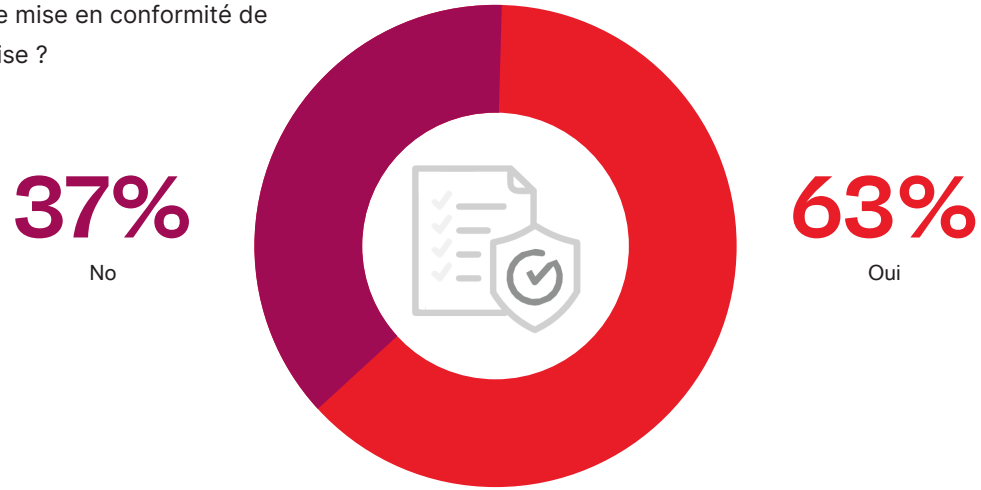
Audit et supervision des collaborateurs qui travaillent depuis des ressources non gérées

Autre 4%

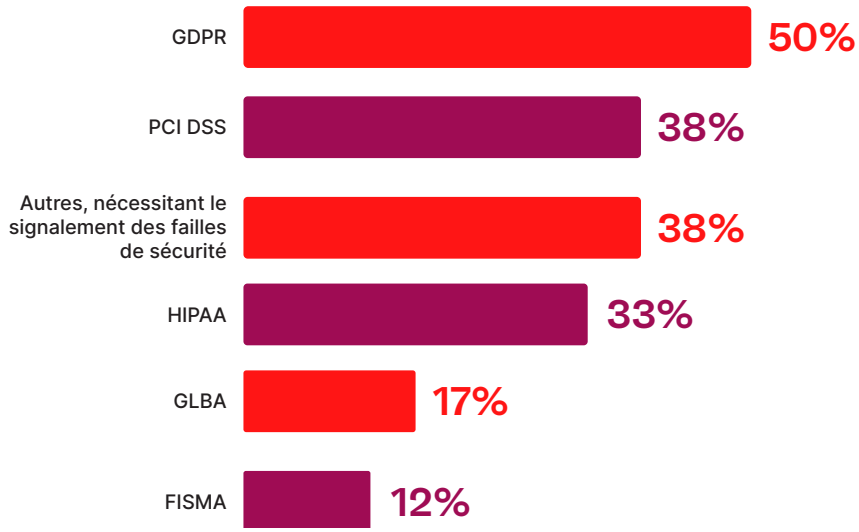
Impact Sur La Conformité

Deux tiers des entreprises considèrent que les environnements de télétravail ont un impact sur leur état de sécurisation.

Le télétravail peut-il impacter les obligations de mise en conformité de votre entreprise ?



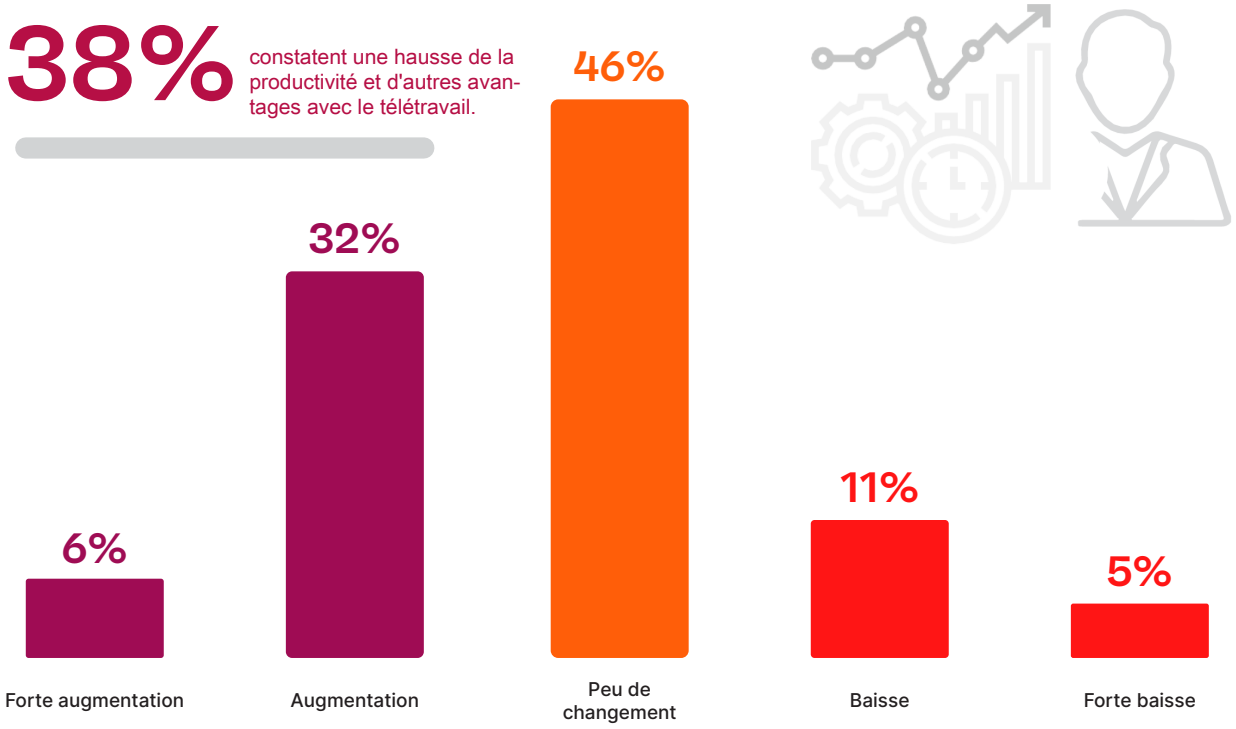
Si oui, lesquelles ?



Effets Sur La Productivité

38 % des entreprises disent avoir constaté une hausse de la productivité et d'autres avantages avec le télétravail. Seulement 16 % constatent une baisse de productivité.

Votre entreprise constate-t-elle une hausse de la productivité et d'autres avantages avec le télétravail ?

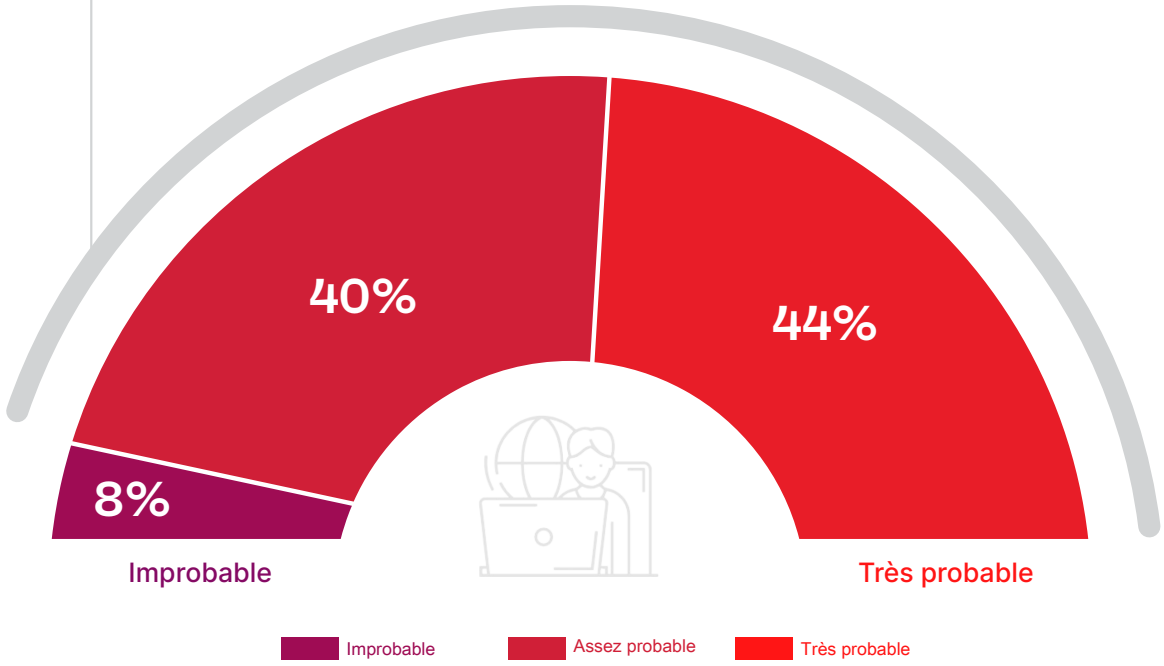


Le Futur Du Télétravail

Une majorité d'entreprises, soit 84 %, considèrent qu'il est probable (44 % disent même très probable) qu'elles continueront à augmenter leurs capacités de télétravail depuis le domicile (WFH) à l'avenir, pour tirer parti de la hausse de productivité et des autres avantages pour l'entreprise.

Pensez-vous continuer à prendre en charge l'augmentation des capacités de travail depuis le domicile à l'avenir (en raison de la hausse de productivité et des autres avantages pour l'entreprise) ?

84% des entreprises considèrent qu'il est probable qu'elles continu- eront à augmenter leurs capacités de télétravail depuis le domicile (WFH) à l'avenir.

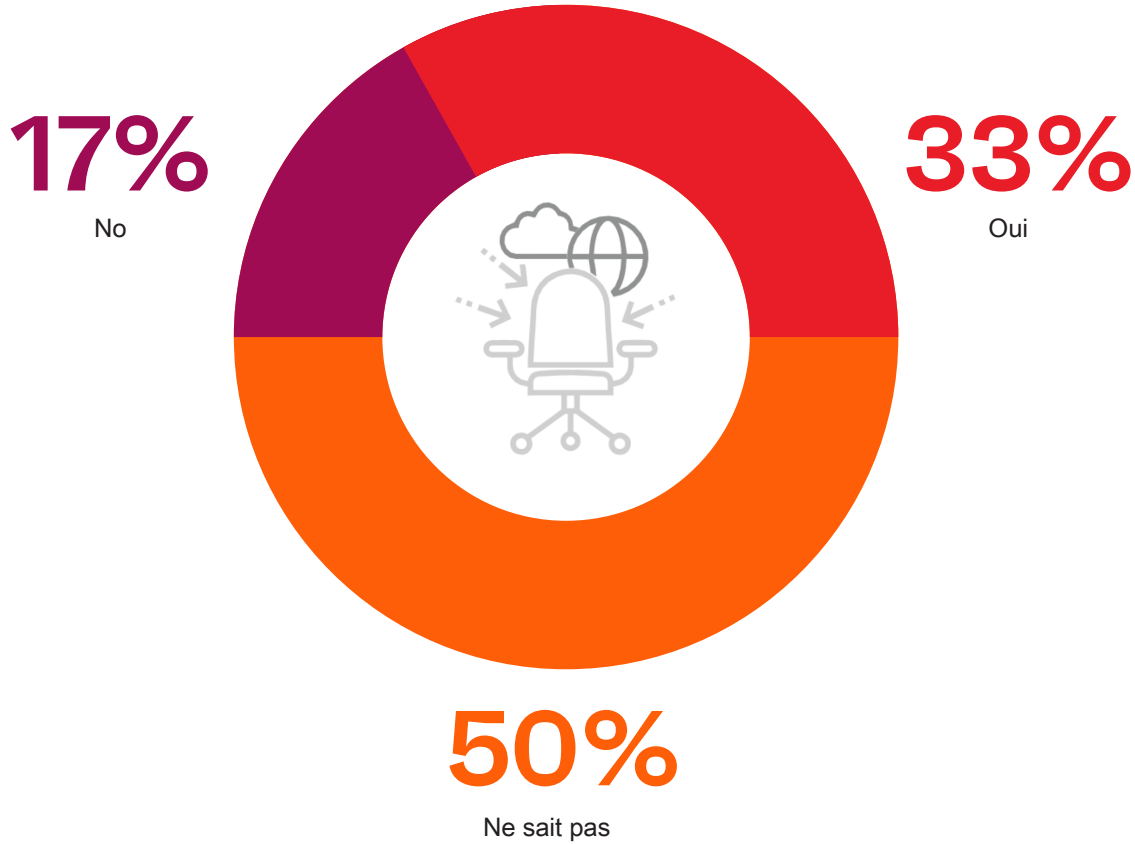


Ne sait pas 8 %

Rendre Le Télétravail

Un tiers des entreprises envisagent de convertir définitivement certains postes au télétravail, même après la crise du COVID.

Votre entreprise envisage-t-elle de convertir définitivement certains postes au télétravail (alors que ces personnes travaillaient sur site) une fois la crise du COVID terminée ?

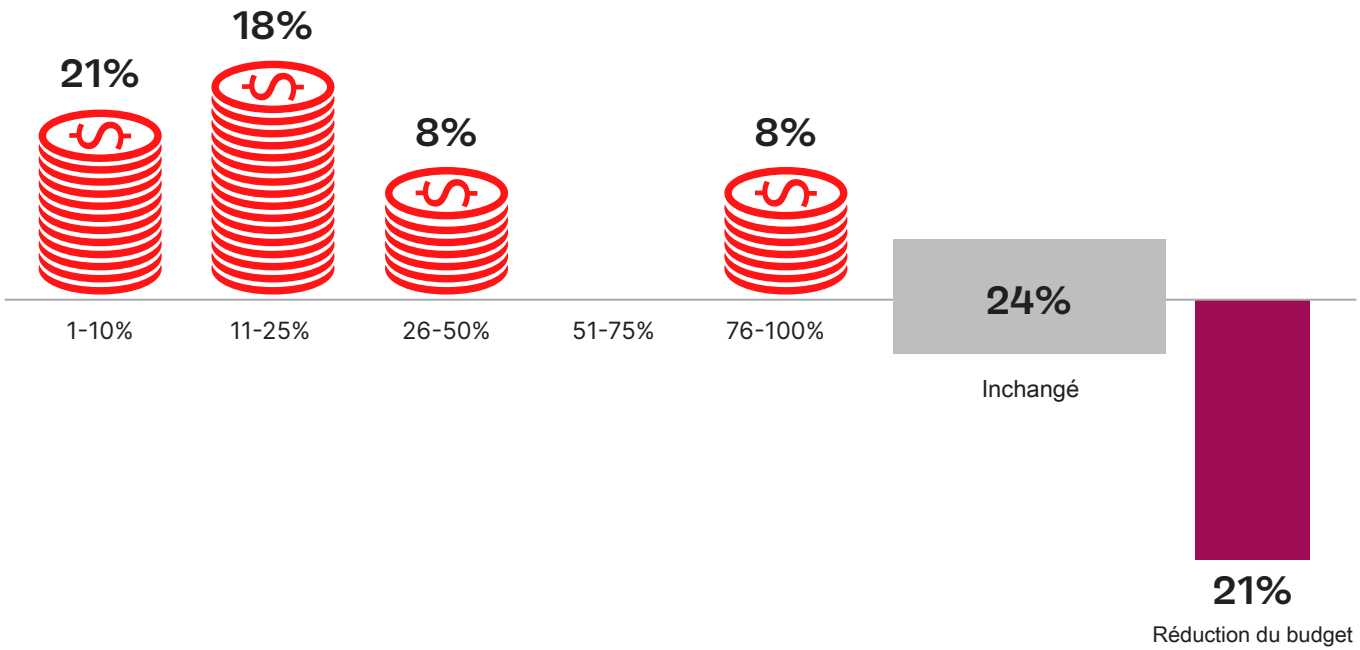


Tendances Budgétaires

La majorité (55 %) des entreprises prévoient que le budget de sécurisation des collaborateurs en télétravail va augmenter au cours de l'année à venir (après avril 2020). Pour un quart des personnes interrogées, ce budget de sécurité ne va pas changer et 21 % seulement prévoient une baisse des budgets.

Comment votre budget de contrôle de la sécurité du télétravail va-t-il évoluer ces 12 prochains mois ?

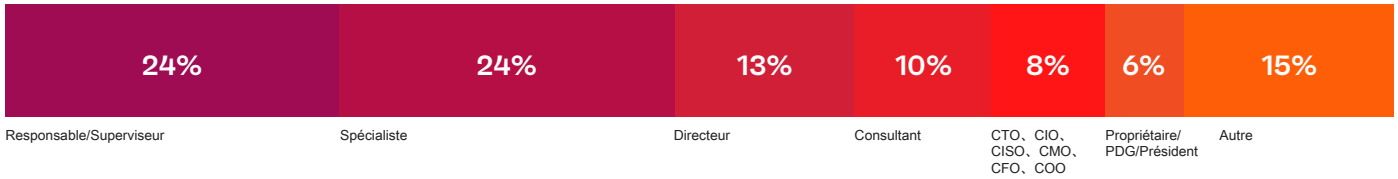
55% prévoient que le budget de sécurisation des collaborateurs en télétravail va augmenter au cours de l'année à venir.



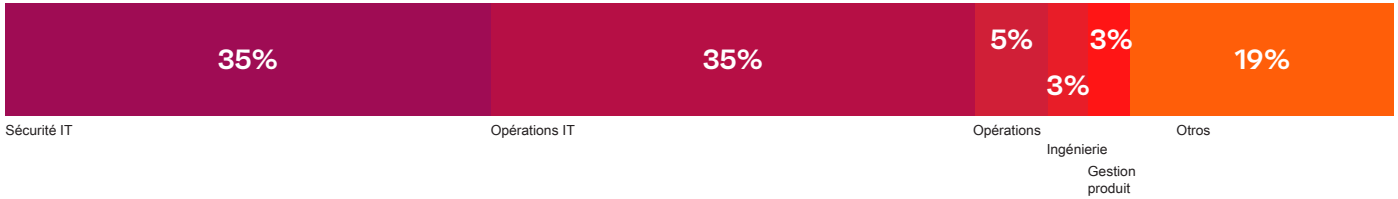
Méthodologie Et Personnes Interrogées

Ce rapport repose sur les résultats d'une enquête en ligne complète portant sur 413 professionnels de l'IT et de la cybersécurité aux États-Unis, menée en janvier 2020 pour connaître les dernières tendances d'adoption, les difficultés, les manques et les solutions préférées des entreprises en matière de sécurité des télétravailleurs avec la pandémie de COVID-19 en 2020. Nous avons interrogé divers acteurs, des responsables techniques aux techniciens de sécurité IT, pour constituer un panel représentatif d'entreprises de toutes tailles dans plusieurs secteurs d'activité.

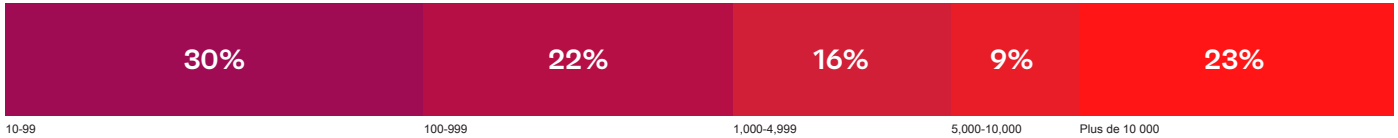
Postes



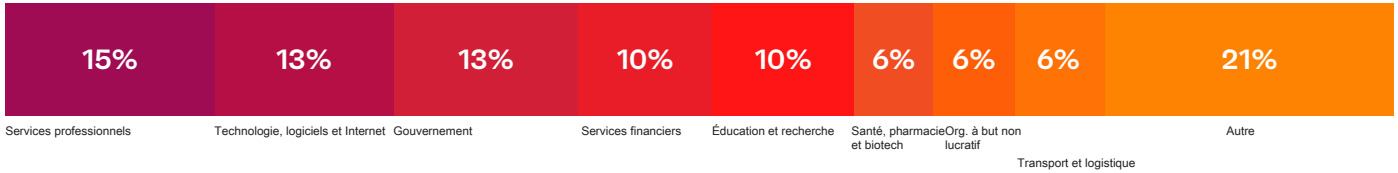
Département



Taille De L'entreprise



Secteur D'activité



Pulse Secure
Acquired by Ivanti

Pulse Secure fournit des solutions d'accès sécurisé (Secure Access) avec des logiciels très complets, destinés aux personnes, aux périphériques, aux objets et aux services. Elles améliorent la visibilité, la protection et la productivité de nos clients. Nos suites intègrent de façon unique des outils de Cloud, de mobilité, des applications et des outils d'accès réseau pour donner des moyens à l' IT hybride dans un univers Zero Trust (Confiance zéro). Plus de 23 000 entreprises et fournisseurs de services, dans tous les marchés verticaux, font confiance à Pulse Secure pour donner à leurs collaborateurs mobiles les moyens d'accéder en toute sécurité aux applications et aux informations du centre de données et du Cloud, tout en garantissant la conformité de l'entreprise. Pour en savoir plus, visitez le site www.pulsesecure.net

ivanti

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