Sécurité des modèles de travail hybrides : état des lieux 2021

Sommaire

4 Introduction : les modèles de travail hybrides prennent forme

5 À propos de l'enquête

6 Les chiffres marquants

7 Les entreprises anticipent une pérennisation des modèles de travail hybrides

8 Pour beaucoup, la pandémie a redéfini les priorités de la transformation informatique

9 La sécurité en tête des défis à relever

10 Les trois stratégies d'évolution des accès réseau et de la sécurité

12 La sécurité, un enjeu souvent relégué au second plan

14 Contournement des mesures de sécurité du télétravail, symptôme d'une protection défaillante

16 La sécurité redevient un enjeu prioritaire

17 Impact du contournement des mesures de sécurité

18 Perspectives des dirigeants et des professionnels des réseaux et de la sécurité

20 Établissement d'un modèle de travail optimal

22 Conclusion

Présenté par :

Prisma Access de Palo Alto Networks est la plateforme de sécurité cloud la plus complète du marché : elle regroupe dans un même service intégré plus de produits spécialisés que toute autre solution concurrente. Partie intégrante de notre solution SASE (Secure Access Service Edge), Prisma Access transforme la sécurité réseau pour faciliter la mise en place de modèles de travail hybrides sécurisés dans les entreprises. Contrairement aux plateformes concurrentes, Prisma Access protège l'ensemble du trafic applicatif grâce à des fonctions complètes de sécurité de pointe, tout en garantissant aux utilisateurs des expériences irrépro-chables au travers d'engagements SLA leaders.

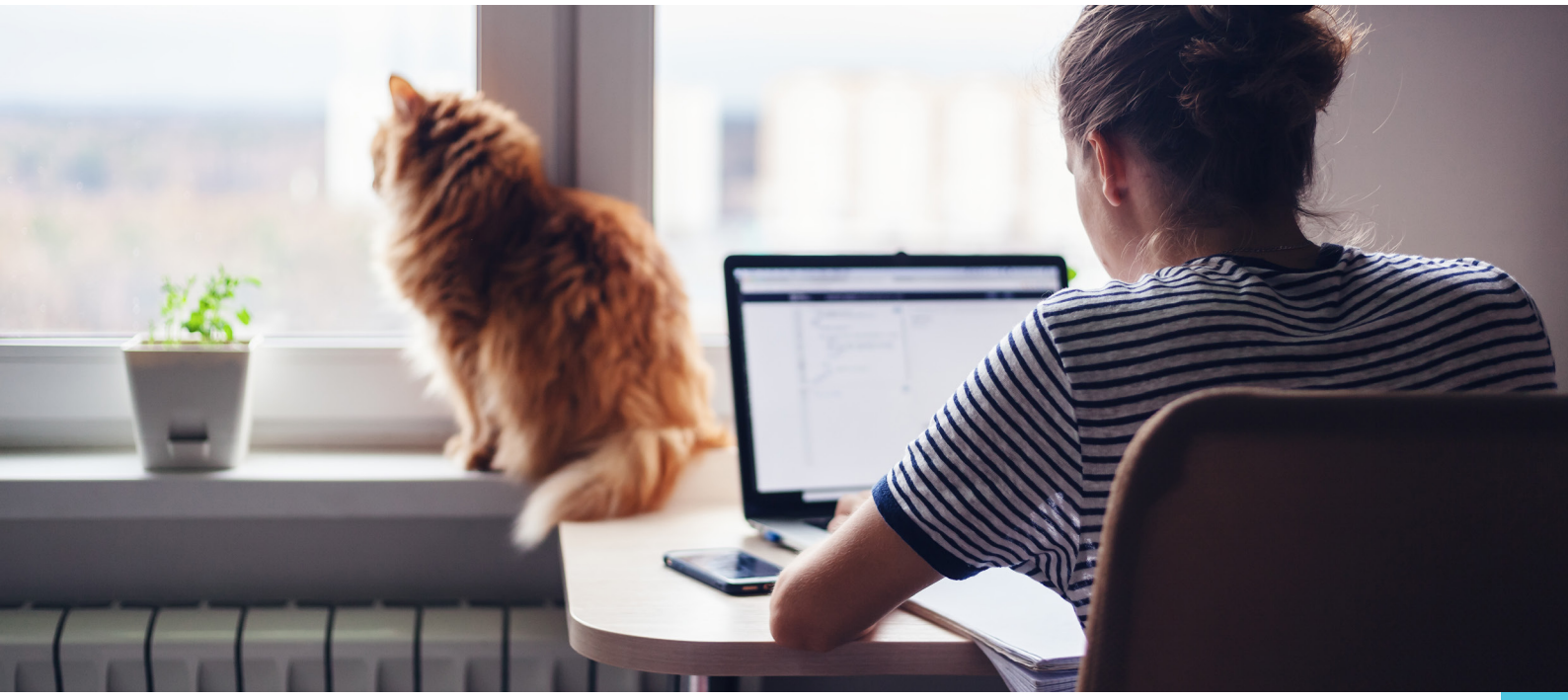
Pour en savoir plus, suivez @PrismaAccess sur Twitter ou rendez-vous sur https://www.paloaltonetworks.com/prisma/access

Introduction : Les modèles de travail hybrides prennent forme

Du jour au lendemain, la pandémie de COVID-19 a contraint les entreprises à réinventer leur modèle de travail, la plupart optant pour le télétravail partout où cela était possible. Pour répondre à cette nécessité immédiate, les entreprises ont dû s'adapter rapidement, en capitalisant sur leurs technologies existantes ou en adoptant de nouvelles solutions pour garantir la productivité de leurs utilisateurs distants.

Aujourd'hui, malgré la levée des restrictions sanitaires un peu partout dans le monde, un nouveau modèle de travail hybride est clairement en train de prendre forme. D'après l'enquête internationale sur le télétravail « Global Work-from-Home Experience Survey », la demande est forte. Selon cette étude, 76 % des salariés dans le monde veulent conserver la possibilité de travailler à domicile au moins à temps partiel[1]. Gartner corrobore cette tendance : « En 2022, 25 % des travailleurs dits « du savoir » dans le monde choisiront leur domicile comme lieu d'exercice principal de leur activité, tandis que 45 % d'entre eux seront en télétravail deux à trois jours par semaine[2]. »

Les entreprises cherchent désormais à faire évoluer leurs réseaux et leurs architectures de sécurité pour maintenir la productivité de leur modèle de travail hybride sur le long terme, tout en limitant le risque de compromission de sécurité. Car lors du basculement dans l'urgence d'une forte population de salariés pendant la pandémie, elles ont pris conscience des fortes lacunes de leurs systèmes existants, totalement inadaptés à une montée en charge rapide et à l'application d'une sécurité homogène sur tous les lieux de travail. À l'heure où elles planchent sur leurs stratégies de travail hybrides à long terme, les entreprises transforment leurs infrastructures réseau et de sécurité pour permettre un accès 24h/7j aux ressources de l'entreprise et offrir une expérience utilisateur sécurisée et cohérente.



À propos de l'enquête

Objectifs

Pour mieux comprendre comment les entreprises s'adaptent au modèle de travail hybride engendré par la pandémie mondiale, Palo Alto Networks a mené l'une des études les plus exhaustives sur le sujet sous l'angle de la sécurité. Intitulée « Sécurité des modèles de travail hybrides : état des lieux 2021 », cette étude visait plusieurs objectifs :

Déterminer les types de technologies et d'outils employés par les entreprises pour sous-tendre les pratiques de télétravail

Évaluer l'impact de la sécurité des accès distants sur la mise en place du télétravail dans les entreprises

Démontrer l'intérêt d'investir dans des architectures réseau et de sécurité unifiées pour offrir un environnement de télétravail sûr et efficace

Méthodologie

Les analystes ont interrogé 3 000 personnes exerçant dans les domaines de la sécurité de l'information, des opérations réseau et du développement applicatif. L'enquête a été menée par ONR, cabinet d'études indépendant, pour le compte de Palo Alto Networks.

L'échantillon des personnes interrogées est distribué comme suit :

1 250

dans la zone Amériques

1 000

en Europe (Royaume-Uni compris)

750

en Asie-Pacifique

Cette population était composée de cadres-dirigeants dans des fonctions technologiques (direction et vice-présidence) et de professionnels rattachés à des équipes réseau, opérations et sécurité, tous dotés de bonnes connaissances sur l'architecture réseau et de sécurité de leur entreprise.

Les chiffres marquants

De nombreuses entreprises ont eu des difficultés à gérer les accès distants et les problèmes de sécurité découlant des modèles de travail hybrides pendant la pandémie.

ont eu du mal à assurer la sécurité des accès distants nécessaires aux environnements de télétravail

De nombreux dirigeants craignent que des raccourcis n'aient été pris et que la sécurité de leur entreprise pourrait en pâtir.

48 %

des entreprises admettent avoir abaissé le niveau de sécurité ou augmenté le risque par un assouplissement des politiques de sécurité et une indulgence envers les télétravailleurs dont elles n'auraient pas fait preuve en temps normal

35 %

des personnes interrogées admettent que leurs télétravailleurs ont sciemment contourné ou désactivé les mesures de sécurité des accès à distance.

53 %

des entreprises ayant priorisé l'accès distant aux dépens de la sécurité s'exposent désormais aux risques générés par les infractions non détectées à la politique d'usage acceptable et l'emploi d'applications non approuvées

Les entreprises se projettent sur des solutions hybrides sécurisées pour leurs salariés.

des personnes interrogées envisagent une solution hybride combinant télétravail et présentiel

des entreprises prévoient que leurs fonctions de sécurité seront majoritairement ou totalement dans le cloud ces 24 prochains mois

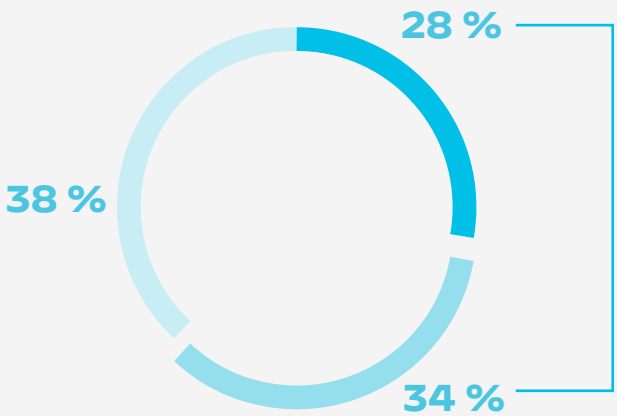
Les entreprises anticipent une pérennisation des modèles de travail hybrides

Alors que les entreprises réfléchissent à leur stratégie de travail hybride pour l'après-pandémie, elles doivent prendre en compte de nombreux critères : opérations, infrastructure technologique, actifs immobiliers, productivité du personnel, satisfaction des salariés et culture de l'entreprise.

Au moment de l'enquête, plus des deux-tiers des entreprises ont indiqué qu'entre 25 et 75 % de leurs effectifs étaient en télétravail, soit un taux comparable à celui enregistré en pleine pandémie. Certes, une partie des salariés a repris le chemin de l'entreprise, mais l'environnement actuel reste globalement similaire à celui qu'il était au plus fort de la crise sanitaire, c'est-à-dire dominé par le télétravail.

Certaines entreprises sont en train d'évaluer le rapport optimal entre télétravail et présentiel. Mais à l'échelle mondiale, les entreprises prévoient globalement de maintenir le télétravail plus ou moins au taux actuel. Pour 44 % d'entre elles, plus de la moitié des effectifs devrait être en télétravail sur un horizon à 12 mois. Dans ce contexte, 62 % des entreprises déclarent avoir entamé l'optimisation de leur modèle de travail hybride, tandis que 94 % envisagent l'hybridation, sous une forme ou sous une autre, dans les 12 prochains mois.

Projections de télétravail sur les 12 prochains mois



62 %

des personnes interrogées envisagent d'opter pour une solution hybride télétravail/présentiel

Maintien du même taux de télétravail
Baisse du taux de télétravail
Hausse du taux de télétravail

Une des entreprises sondées ne s'y trompe pas : « On ne peut tout simplement pas envisager un retour complet au présentiel en 2022. Le changement serait trop radical. Tous les systèmes sont là, et on a bien progressé dans ce domaine. Par conséquent, le télétravail formera une composante incontournable de la planification. »

Pour beaucoup, la pandémie a redéfini les priorités de la transformation informatique

Avant la pandémie, beaucoup d'entreprises étaient en plein chantier de transformation numérique, dont certains pans concernaient la migration vers le cloud et la modernisation de leur infrastructure pour mieux sous-tendre les nouvelles pratiques de télétravail. La soudaineté de la pandémie a donné un sérieux coup d'accélérateur à ces projets. Du jour au lendemain, les priorités des équipes informatiques se sont recentrées sur le télétravail. D'après notre enquête, 67 % des entreprises ont simultanément renforcé la capacité de leur architecture d'accès distant existante et déployé de nouvelles technologies pour faire évoluer leur infrastructure. Beaucoup ont d'abord seulement augmenté la capacité de leur architecture actuelle dans une perspective de court terme, mais 64 % prévoient de changer leur architecture d'accès distant au cours des 24 prochains mois.

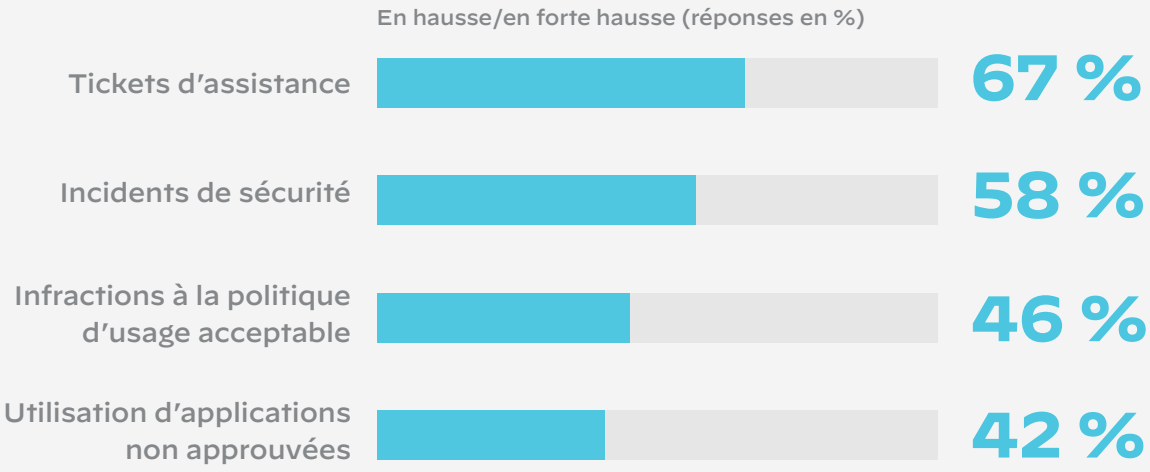
« Notre plan stratégique, la migration vers le cloud, reste un projet phare à longue échéance. Il faut juste revoir le calendrier, car nous avons réaffecté certains budgets d'investissement pour couvrir les besoins immédiats en accès distant. »

La sécurité en tête des défis à relever

D'après notre enquête, au milieu de l'année 2021, la plupart des entreprises étaient satisfaites de leur réseau et avaient résolu les problèmes initiaux liés aux performances et à l'efficacité des outils de collaboration. Même si la majorité des entreprises ont stabilisé leur réseau et leur accès distant, un quart à un tiers des personnes interrogées éprouve toujours des difficultés à offrir une expérience utilisateur satisfaisante et homogène.

Les entreprises sont toujours aux prises avec d'importantes difficultés, la sécurité arrivant en tête de liste pour 51 % des sondés. La qualité de service et la complexité technique suivent de près avec respectivement 48 % et 47 %. D'après les participants à notre enquête, le passage au télétravail en pleine crise de COVID-19 s'est traduit par une forte hausse de certaines activités : tickets d'assistance, incidents de sécurité, infractions à la politique d'usage acceptable et utilisation d'applications non approuvées.

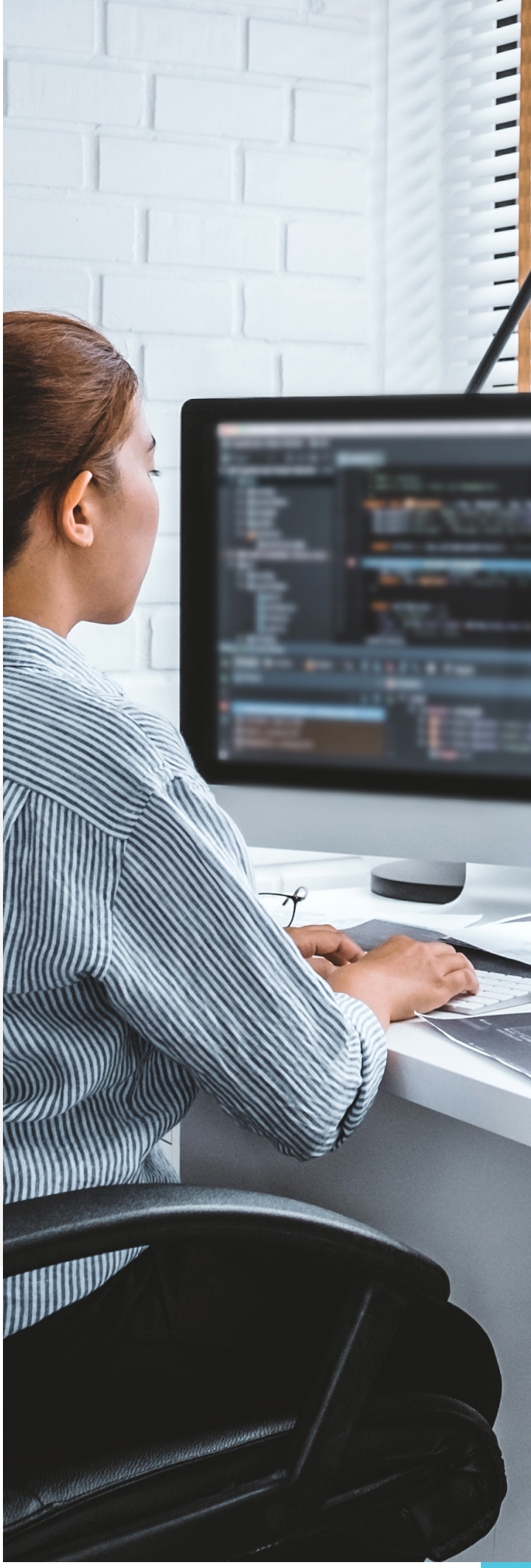
Impacts de la COVID-19 et du passage au télétravail constatés sur votre réseau



Par ailleurs, le télétravail a compliqué les processus de résolution des problèmes. Comme le souligne une des personnes interrogées, « on ne peut pas aller voir un collègue pour lui communiquer son problème et repartir une fois le problème résolu. »

Les trois stratégies d'évolution des accès réseau et de la sécurité

Dans un contexte d'extrême incertitude et de forte pression budgétaire, notamment au début de la pandémie, les entreprises hésitaient à investir dans des solutions de long terme. La majorité d'entre elles déclarent avoir eu du mal à fournir à la fois des accès distants plus performants et une meilleure sécurité en télétravail (respectivement 59 % et 61 %), et à avoir investi là où elles estimaient les besoins les plus pressants.



59 %

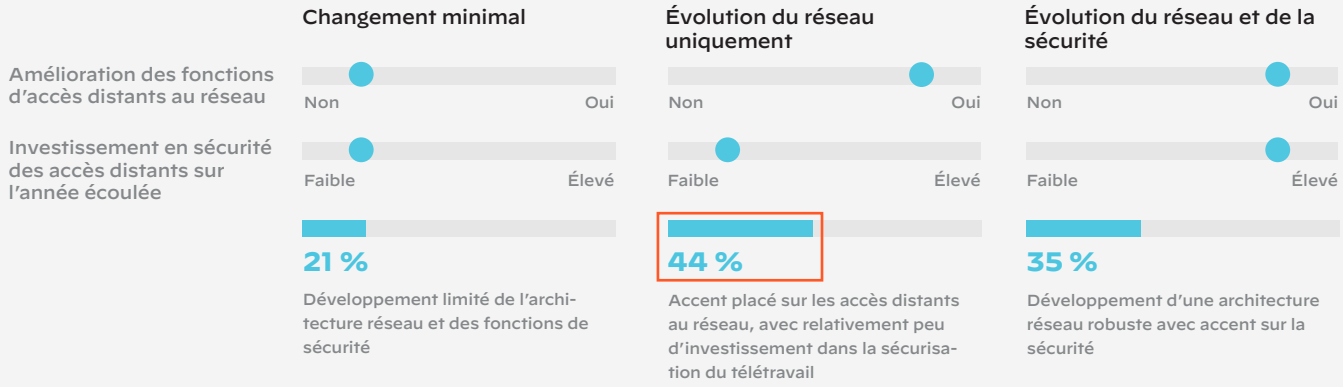
des entreprises ont éprouvé des difficultés à mettre en place les aménagements de télétravail nécessaires en réaction à la COVID-19

61 %

des entreprises ont eu du mal à sécuriser les accès distants nécessaires à leurs télétravailleurs

Trois grandes approches du développement de fonctions réseau et de sécurité se sont alors dessinées :

- **Changement minimal :** 21 % des entreprises ont très peu modifié leur architecture réseau et leurs fonctions de sécurité.
- **Évolution du réseau uniquement :** 44 % des entreprises (proportion la plus élevée) ont réaffecté leurs budgets technologiques à l'amélioration des accès distants, mais en investissant relativement peu dans l'aspect sécurité du télétravail.
- **Évolution du réseau et de la sécurité :** 35 % des entreprises ont adopté une approche plus équilibrée en développant des capacités plus robustes d'accès distant au réseau en parallèle au renforcement de la sécurité.



Maintenant que les modèles de travail hybrides sont entrés dans les habitudes, les entreprises ayant opté pour un minimum de changement commencent à repérer des fissures dans leur architecture réseau. Pour 48 % des sondés dans cette situation, leur réseau n'est pas en capacité de répondre aux demandes actuelles en télétravail et leur modèle de réseau distant n'est pas soutenable en l'état. À l'inverse, ce sentiment n'est partagé que par 21 % des entreprises ayant fait évoluer leur réseau et 14 % de celles qui ont amélioré à la fois leur réseau et leurs fonctions de sécurité à distance.

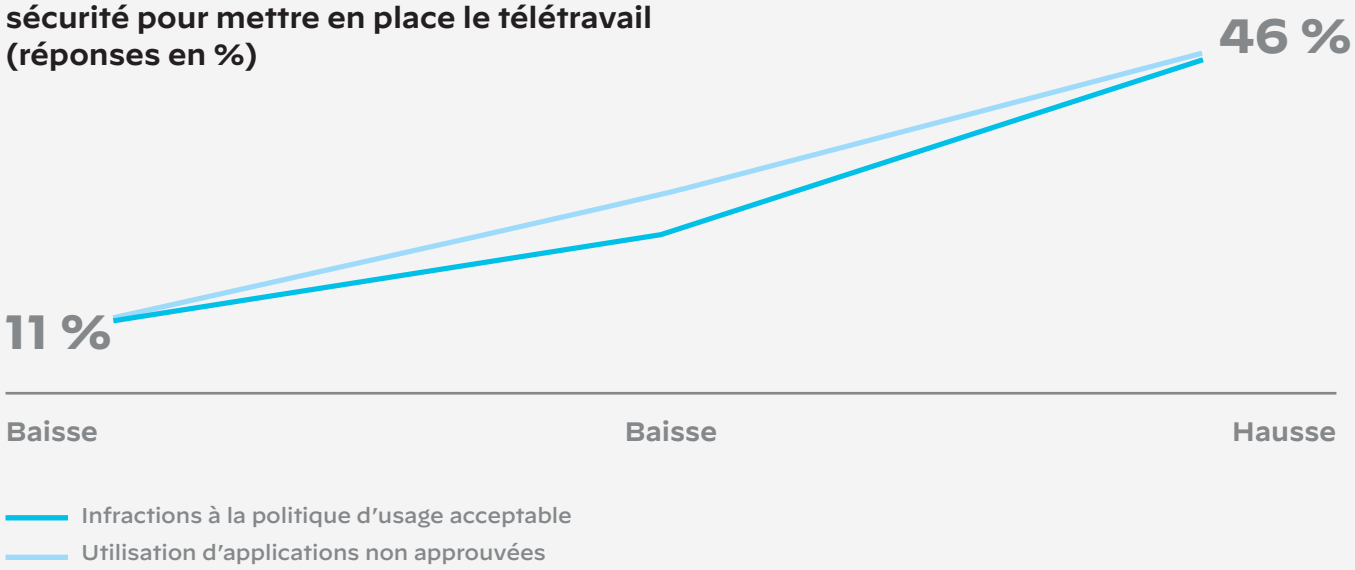
« Quand on a basculé en télétravail initialement, on ignorait si cette situation allait durer une semaine ou un mois. Il était donc difficile de prendre des décisions pertinentes à long terme, car on ne savait pas si les gens allaient revenir au bureau en masse une fois la crise passée. »

La sécurité, un enjeu souvent relégué au second plan

Les données indiquent également que près de la moitié des personnes interrogées ont concentré leurs efforts sur leur architecture réseau dans une optique d'amélioration des accès distants, mais sans prêter suffisamment attention au renforcement de la sécurité.

Dans ce domaine, l'expansion des accès distants pour les télétravailleurs n'a pas été sans conséquences. En passant au télétravail, 48 % des entreprises admettent avoir soit abaissé le niveau de sécurité, soit augmenté le risque par un assouplissement des politiques de sécurité et une indulgence envers les télétravailleurs dont elles n'auraient pas fait preuve en temps normal.

Entreprises ayant assoupli leurs politiques de sécurité pour mettre en place le télétravail (réponses en %)



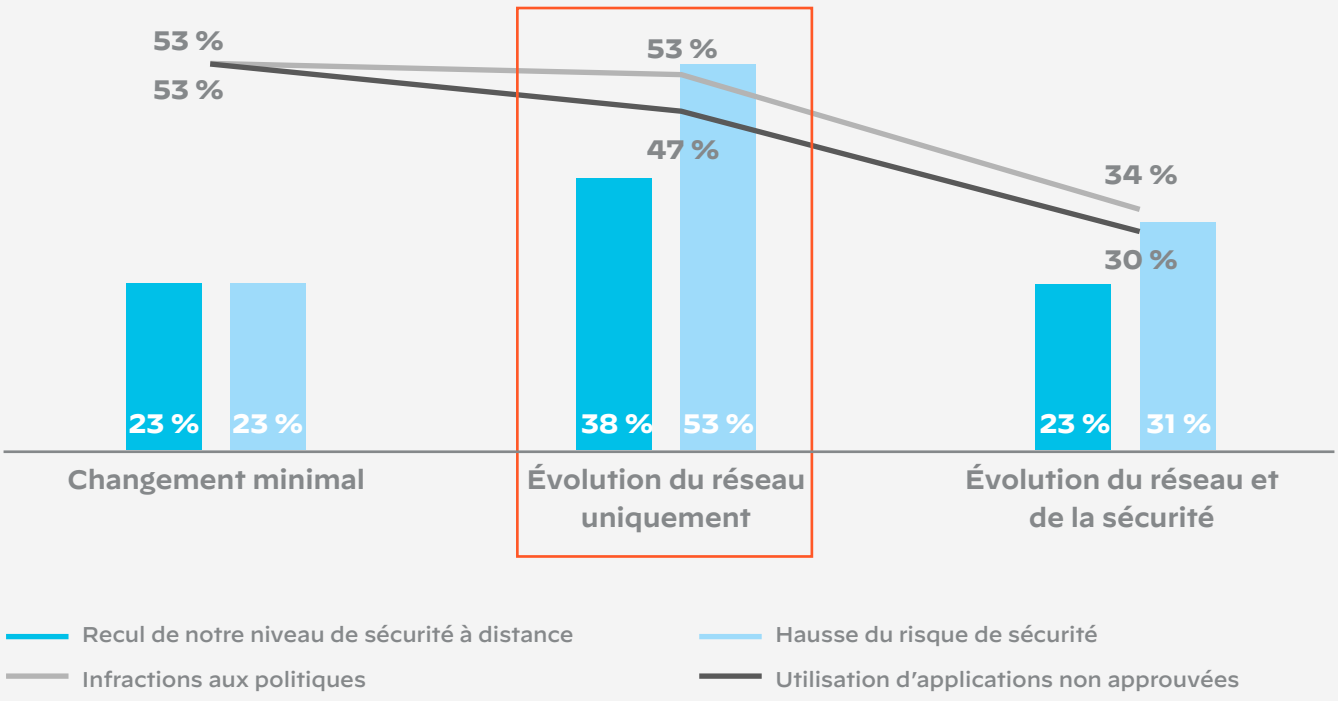
Le télétravail introduit de nouvelles problématiques de sécurité

Pendant qu'elles adaptaient leurs accès distants, beaucoup d'entreprises ont fait l'impasse sur les contrôles, procédures et politiques de sécurité formels pour le télétravail. Comme le résume une des personnes interrogées : « Nous n'avions pas vraiment établi une posture de sécurité claire pour le télétravail. À mesure que ce dernier s'est développé, l'écart de sécurité s'est creusé. Le télétravail est une tout autre affaire par rapport à des opérations classiques sur site. »

Les raisons de ces carences sont multiples : budgets restreints, manque de temps et de ressources, et nécessité de passer rapidement au télétravail en réaction à la pandémie, avec pour résultat un assouplissement des restrictions de sécurité. Plus de la moitié des entreprises (53 %) ayant priorisé les accès distants aux dépens de la sécurité s'exposent désormais à un risque réel généré par les infractions non détectées à la politique d'usage acceptable et l'emploi d'applications non approuvées. Curieusement, celles qui s'étaient limitées à un changement minimal de leurs accès distants ont constaté une hausse de 23 % des incidents de sécurité. Leur sécurité a donc également faibli, mais dans une moindre mesure.

Impact de la COVID-19 et du passage au télétravail sur différents aspects des réseaux d'entreprise

D'accord/tout à fait d'accord (réponses en %)



Comme on l'a vu par le passé, lorsque les mesures de sécurité deviennent trop contraignantes (ralentissement des systèmes, baisse de productivité et dégradation de l'expérience utilisateur), les salariés redoublent d'imagination pour trouver des moyens de les contourner. Le télétravail et l'essor des applications cloud n'ont fait que faciliter ce type de comportement. La hausse du télétravail s'est traduite par une sécurité de plus en plus pesante, mais aussi davantage de possibilités de la contourner.

Il est néanmoins important de noter que la plupart des entreprises étaient pleinement conscientes des risques de sécurité qu'elles couraient. D'autre part, nombre d'entre elles se trouvaient dans une situation où il leur était difficile d'engager les investissements nécessaires pour consolider leurs défenses. Faute d'indicateurs de performance (KPI) fiables, elles manquaient d'arguments pour justifier des investissements dans leur sécurité.

Contournement des mesures de sécurité du télétravail, symptôme d'une protection défaillante

Au total, 35 % des personnes interrogées admettent que leurs salariés ont contourné ou désactivé sciemment les mesures de sécurité mises en place pour les accès distants, avec des conséquences variées en termes de gravité.

Quels sont les principaux déterminants de ces comportements à risque ? D'abord, le passage précipité au télétravail dicté par la pandémie a introduit des facteurs incitant au contournement des mesures de sécurité à distance. Ces facteurs n'avaient souvent rien de nouveau, mais beaucoup d'entre eux n'avaient pas été précisément cernés ou constatés à grande échelle avant la pandémie.

Le surcroît de complexité, l'assouplissement des politiques de sécurité et une relative improvisation sont autant de facteurs ayant contribué à cette situation. Du côté des utilisateurs, le contournement des mesures de sécurité s'est produit sous la forme d'applications non approuvées (le « Shadow IT ») et du BYOD (Bring Your Own Device), une pratique selon laquelle les salariés utilisent leurs appareils personnels à des fins professionnelles et non les appareils fournis par l'entreprise.

Malheureusement, les entreprises qui n'ont pas fait de la sécurité leur priorité avant la pandémie continuent d'en faire les frais. Celles qui recensent aujourd'hui des taux élevés de contournement de la sécurité des accès à distance sont les mêmes qui ont relégué la sécurité au second plan au moment d'étendre leur infrastructure d'accès distant en réponse à la généralisation du télétravail. Les taux élevés de contournement de la sécurité sont principalement dus à des outils de collaboration inadéquats, une augmentation de l'usage des appareils personnels sans contrôles ou politiques de sécurité adaptés, et l'utilisation d'applications non approuvées. Beaucoup d'entreprises n'ont pas anticipé les conséquences de leur imprévoyance en matière de sécurité, tant elles étaient accaparées par le passage au télétravail.

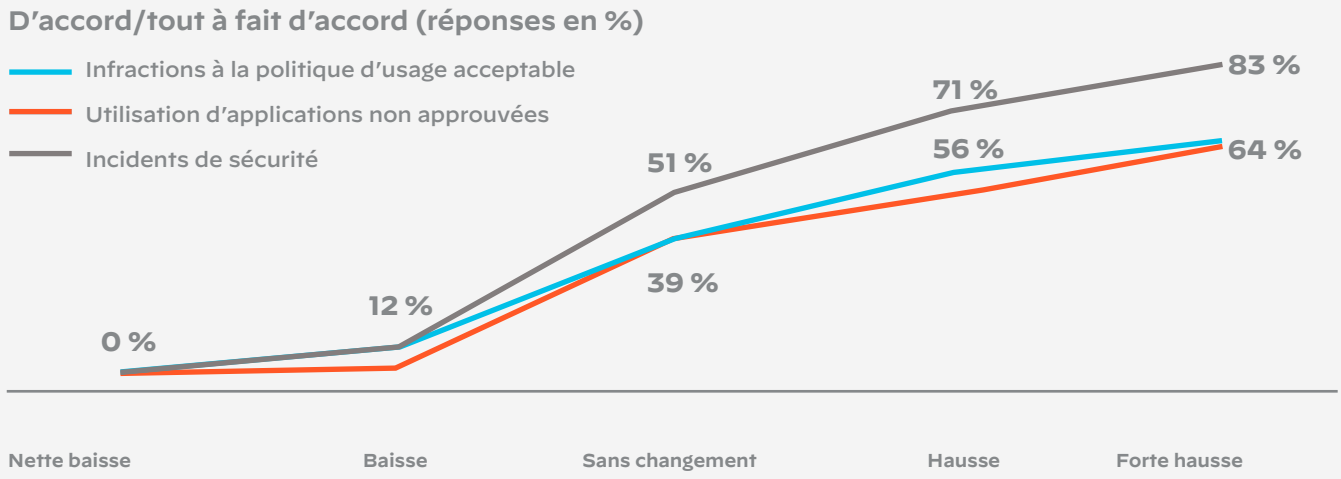
Comportements à risque des télétravailleurs

- Utilisation des appareils personnels à des fins professionnelles (BYOD)
- Chargement de données d'entreprise vers des applications ou services cloud non approuvés
- Contournement des contrôles de sécurité
- Connexion à des réseaux non sécurisés à domicile ou en déplacement
- Manque de formation et de sensibilisation à la cybersécurité
- Non-signalement des actes de phishing et autres menaces
- Transmission de fichiers confidentiels par e-mail
- Défaut de mise à jour de sécurité des appareils

Les résultats de l'enquête vont dans ce sens :

- Les entreprises dépourvues d'outils efficaces de collaboration à distance déclarent que leurs utilisateurs sont **plus de huit fois plus enclins** à esquiver les mesures de sécurité en place. Les salariés soit utilisent leur propre méthode de contournement, soit recourent à des applications non approuvées qu'ils jugent plus efficaces pour collaborer, avec dans les deux cas une augmentation des risques de sécurité.
- Au pic de la pandémie, beaucoup d'entreprises ont assoupli leurs politiques BYOD. Notre enquête indique que 60 % des entreprises ont étendu l'usage du BYOD pour que leurs collaborateurs puissent travailler depuis chez eux. Ce faisant, elles ont **multiplié par plus de huit** le risque que leurs utilisateurs ignorent, contournent ou désactivent les fonctions de sécurité par rapport à celles ayant restreint le BYOD.
- Le boom du BYOD a aussi multiplié les problèmes de sécurité : utilisation d'applications non approuvées, infractions à la politique d'usage acceptable mais aussi, et surtout, augmentation des incidents de sécurité. Parmi les entreprises où le BYOD s'est fortement répandu, 83 % ont constaté une hausse des incidents de sécurité et de l'utilisation d'applications non approuvées, tandis que 64 % ont observé une recrudescence des infractions à la politique d'usage acceptable. Au début de la crise sanitaire, les entreprises se doutaient probablement que le BYOD allait entraîner une augmentation des problèmes de sécurité, mais certainement pas dans de telles proportions.

Usages BYOD depuis la crise de COVID-19



« Nos technologies de sécurité n'étaient pas prévues pour fournir de la visibilité sur ce volume d'accès distants, car la majorité des collaborateurs travaillaient [auparavant] uniquement en présentiel. Elles étaient axées sur la visibilité des accès sur site, pas au niveau des accès distants. »

La sécurité redevient un enjeu prioritaire

Les entreprises commencent à entrevoir les carences de leur stratégie de sécurité des accès à distance, basée sur des solutions spécialisées pour 59 % des personnes interrogées. Dans 49 % des cas, cet assemblage hétéroclite de solutions non intégrées crée des angles morts qui nuisent à leur capacité à prioriser les risques et à neutraliser les menaces.

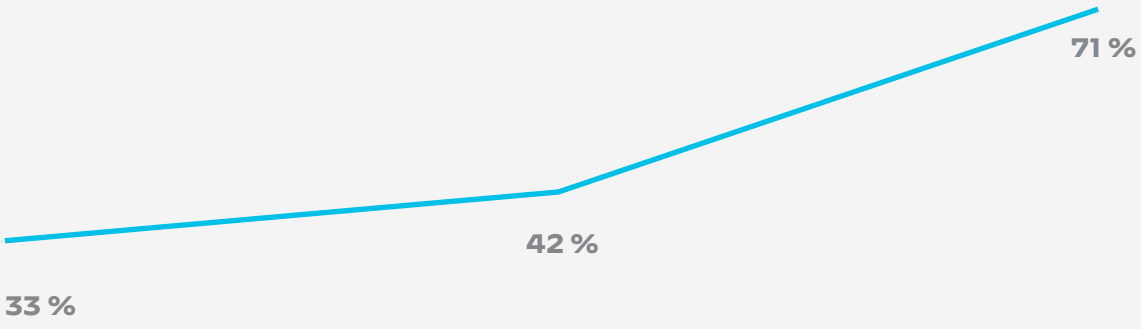
Maintenant que l'urgence du passage au télétravail est retombée dans la plupart des régions du monde, les entreprises se recentrent sur le développement de solutions de travail hybrides sur le long terme. Selon 74 % d'entre elles, une seule et même solution de sécurité complète des accès à distance améliorerait leur posture de sécurité. Par ailleurs, les responsables sécurité et les décideurs sont de plus en plus favorables à une sécurité en mode cloud.

Basculement vers une sécurité en mode cloud

Côté proactivité, 67 % des entreprises ont pris des mesures en pleine pandémie pour mieux protéger leurs télétravailleurs : 41 % ont migré certaines fonctions de sécurité vers le cloud tandis que 26 % ont consolidé leur dispositif de sécurité sur site comme mesure temporaire.

Les perspectives semblent néanmoins encourageantes : 71 % des personnes interrogées prévoient de migrer l'essentiel ou la totalité de leurs fonctions de sécurité vers le cloud au cours des 24 prochains mois. Cette tendance marquée favorise l'essor des modèles de travail hybrides. La mobilité des collaborateurs étant désormais une réalité dans la vie des entreprises, les technologies de sécurité dans le cloud sont essentielles pour promouvoir la collaboration, quel que soit le lieu de travail des utilisateurs.

Entreprises dont la sécurité est principalement ou entièrement dans le cloud (réponses en %)



Impact du contournement des dispositifs de sécurité

Au-delà des problèmes de sécurité abordés plus haut, le contournement des mesures de sécurité remet en cause la viabilité des architectures réseau des entreprises et empêche les modèles de travail hybrides de tenir toutes leurs promesses. D'après notre enquête, c'est une préoccupation majeure pour les entreprises où le contournement de la sécurité est élevé par rapport à celles où ce taux est moyen. Par rapport aux entreprises à taux de contournement moyen ou faible, les entreprises à taux élevé :

- Sont presque quatre fois plus nombreuses à exprimer des réserves quant à la capacité de leur réseau existant à répondre aux demandes actuelles.
- Sont plus de quatre fois plus nombreuses à estimer que leur architecture d'accès à distance n'est pas pérenne.

Au-delà des conséquences sur le réseau et la sécurité, les entreprises où le taux de contournement est élevé reconnaissent que la situation a eu des répercussions négatives sur le télétravail.

- Elles sont en effet plus de deux fois plus enclines à considérer que le contournement de la sécurité a nui à la productivité du personnel.
- Leur perception de la satisfaction des collaborateurs est globalement inférieure, avec 60 % pour cette catégorie, contre respectivement 80 % et 70 % dans les entreprises à taux de contournement faible et moyen.

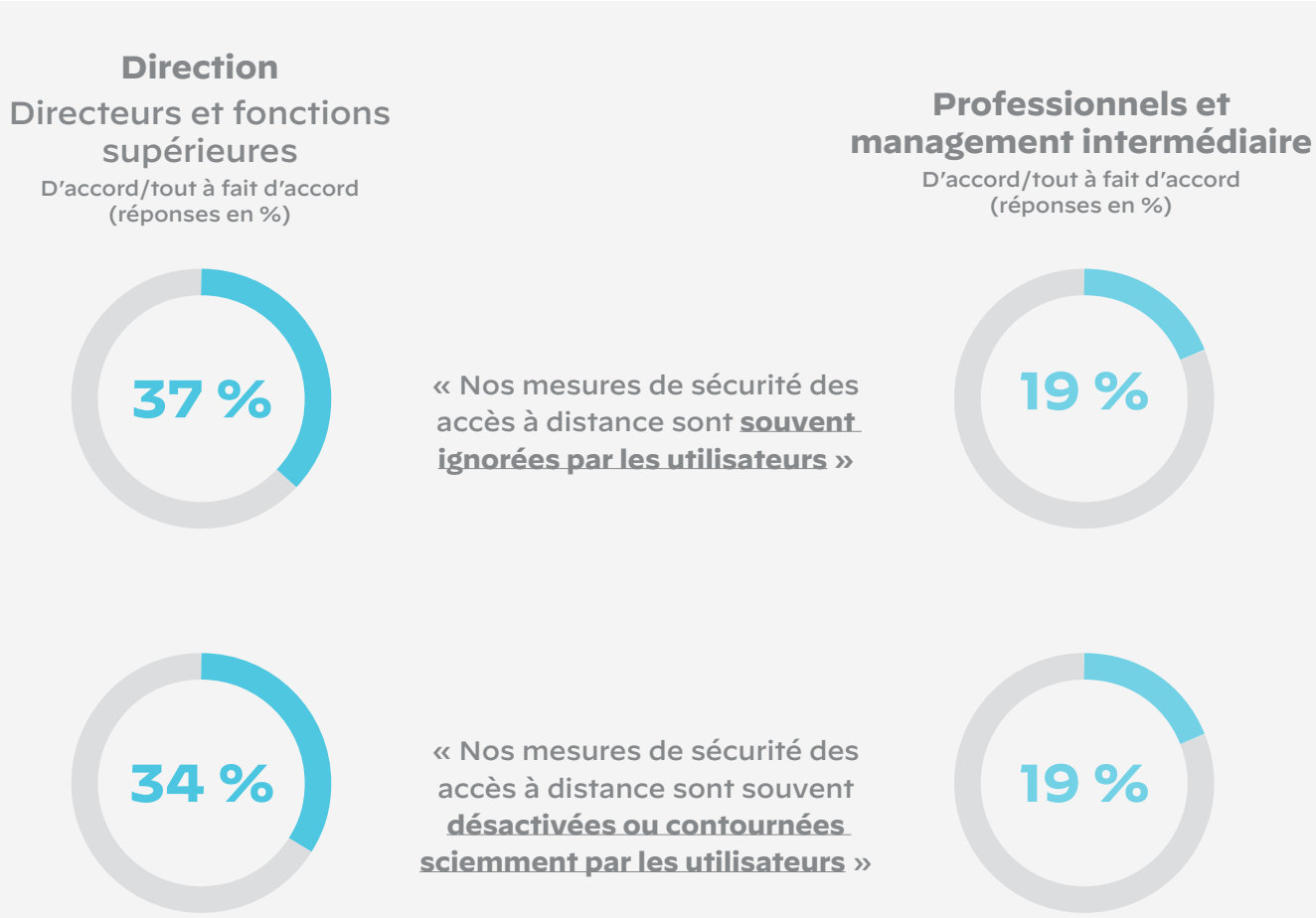
Perspectives des dirigeants et des professionnels des réseaux et de la sécurité

Au sujet du modèle de travail hybride, la cadres-dirigeants (membres du Comex et vice-présidents) et les professionnels des réseaux ou de la sécurité (y compris management intermédiaire) ne s'accordent pas complètement sur les problématiques du modèle de travail hybride que leur entreprise doit affronter. Notre enquête indique que ces deux catégories ont une vision positive de l'expérience utilisateur pour les accès distants, ce malgré les problèmes rapportés par les usagers eux-mêmes : connectivité médiocre à leur domicile ou encore manque de connaissances et de formation sur les outils de collaboration, les technologies d'accès à distance et les politiques de sécurité en télétravail. Environ 70 % des dirigeants et des professionnels pensent que les utilisateurs bénéficient d'un accès fluide et transparent à toutes les applications, quel que soit leur lieu de travail, et que leur entreprise assure une connectivité continue et fiable.

Sur la question de la stabilité des réseaux distants de l'entreprise, les avis divergent : les cadres-dirigeants sont bien plus préoccupés par ce point que les professionnels réseaux/sécurité. Ainsi, 43 % des cadres-dirigeants, contre seulement 13 % des professionnels, admettent que leur architecture actuelle d'accès distant ne peut pas prendre en charge les demandes de travail hybride et/ou qu'elle n'est pas pérenne. Plus de la moitié des cadres-dirigeants interrogés (53 %) n'ont pas entièrement confiance en leurs outils de collaboration, tandis qu'un peu moins d'un tiers des professionnels (30 %) partagent ce sentiment.

Pourquoi cet écart ? Par rapport aux décideurs et aux utilisateurs, il est possible que les professionnels de première ligne tendent à surestimer ou à exprimer une vision biaisée de la qualité et de l'efficacité des solutions qu'ils gèrent. Les professionnels ont aussi une expérience pratique des outils et de l'environnement, qui leur permet de mieux comprendre l'architecture d'accès distant et ses limites par rapport à la perception que peuvent en avoir les dirigeants et les utilisateurs.

Il se peut également que les inquiétudes de la direction à propos de ses réseaux distants soient alimentées par les craintes découlant du contournement des fonctions de sécurité. Pour plus de 30 % des dirigeants, les salariés ignorent, contournent ou désactivent les mesures de sécurité, alors que 19 % des professionnels réseau/sécurité partagent cet avis. Ces derniers ne perçoivent peut-être pas toute l'ampleur du phénomène à l'échelle de l'entreprise.



La migration de la sécurité vers une approche SASE (Secure Access Service Edge) dans le cloud est un autre sujet où direction et professionnels expriment des avis divergents. Une grande majorité des professionnels réseau/sécurité considère que le passage à la sécurité dans le cloud est porteur de valeur, tandis que 27 % des dirigeants ne sont pas encore à l'aise avec cette idée.

Établissement d'un modèle de travail optimal

Au sortir de la crise de COVID, il apparaît clairement que la plupart des entreprises dans le monde s'orientent vers un modèle de travail hybride. Les résultats de l'enquête montrent que la majorité des entreprises ayant investi dans l'évolution de leur sécurité et de leurs réseaux distants visent un modèle de travail hybride à plus de 50 %. Celles qui se sont limitées à des changements minimaux ou à la seule question des accès à distance se sentent moins en confiance et envisagent un modèle de travail hybride pour moins de 50 % de leurs collaborateurs.

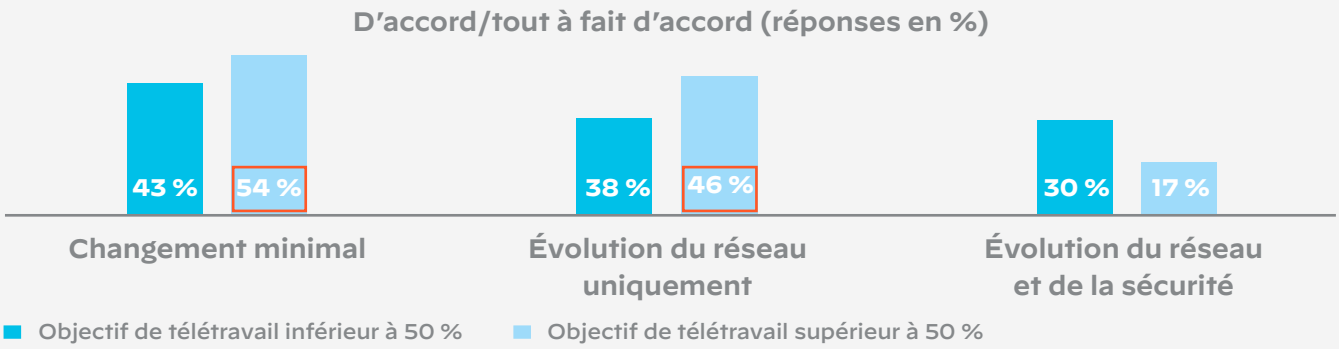
De leur côté, les salariés semblent clairement apprécier le télétravail : 71 % des entreprises signalent une hausse de la satisfaction des collaborateurs depuis l'instauration de ces aménagements. Face à cet engouement, il n'est pas surprenant que la majorité des entreprises cherche à maintenir un modèle de travail hybride. Seules 15 % d'entre elles indiquent qu'elles tenteront de revenir à la situation d'avant-COVID, et 6 % qu'elles seront complètement de retour en présentiel d'ici l'année prochaine. À l'inverse, on constate que 44 % des entreprises prévoient de conserver plus de la moitié de leurs effectifs en télétravail l'année prochaine, et presque toutes comptent mettre en place un environnement de travail hybride.

Un message clair émerge de l'enquête : les entreprises visant un taux de travail hybride élevé (plus de 50 %) doivent ériger la sécurité au rang de leurs priorités pour réduire les actes de contournement des mesures de sécurité distante. Plusieurs chiffres corroborent cette affirmation, plus particulièrement pour les entreprises ayant limité les changements au minimum et celles qui se sont cantonnées au réseau, reléguant la sécurité au second plan :

- Comme indiqué plus haut, plus de la moitié des cadres-dirigeants interrogés n'ont pas pleinement confiance en leurs outils de collaboration, contre environ un cinquième des professionnels réseau/sécurité.
- Les entreprises ayant limité les changements au minimum ou à la seule évolution de leur réseau indiquent avoir du mal à assurer une collaboration efficace et productive des équipes, avec respectivement 54 % et 46 %. À l'inverse, seules 17 % des entreprises ayant fait évoluer à la fois leur réseau et leur sécurité connaissent ce problème.

Stratégies d'adaptation du réseau et de la sécurité

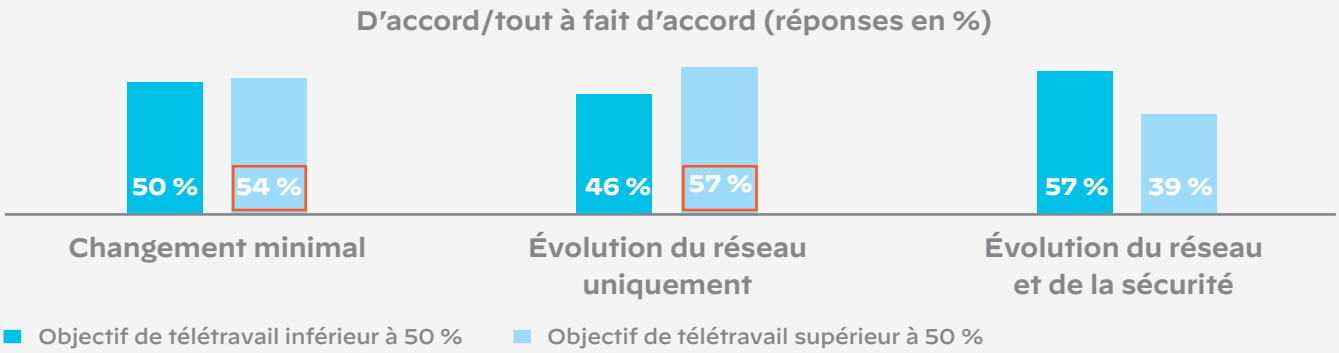
« Les outils de collaboration de mon entreprise ne permettent pas à nos télétravailleurs d'échanger et de collaborer efficacement avec leurs collègues »



- Pour plus de 53 % des entreprises ayant limité les changements au minimum et 57 % des entreprises s'étant cantonnées au seul réseau, les problèmes de visibilité découlant de l'exploitation de solutions non intégrées représentent une préoccupation majeure.

Stratégies d'adaptation du réseau et de la sécurité

« Je pense que le nombre de solutions spécialisées que nous utilisons pour sécuriser nos télétravailleurs crée des angles morts qui nuisent à notre capacité à prioriser les risques et à prévenir les menaces. »



Conclusion

Au sortir de la crise sanitaire, le concept de travail hybride s'est enraciné dans les mentalités. Reste à savoir dans quelle mesure les entreprises envisagent de pérenniser ce modèle de travail et comment elles s'y préparent.

Les résultats de notre enquête indiquent que les entreprises qui envisagent d'abaisser la proportion de télétravailleurs parviennent à s'en sortir pour le moment. En revanche, celles qui souhaitent accroître leur capacité de travail hybride doivent affronter plusieurs problèmes de taille : fort taux de contournement des mesures de sécurité, inefficacité des outils de collaboration à distance et manque de visibilité sur l'environnement de l'entreprise dans son ensemble.

Plus des trois quarts des entreprises reconnaissent que la connectivité réseau est indispensable à la satisfaction des salariés, et elles mettent les bouchées doubles dans ce domaine. Pour 81 % des cadres-dirigeants, l'architecture d'accès distant est une priorité. Ils notent par ailleurs que le maintien d'une sécurité exhaustive et de la qualité de service représentent à la fois leurs plus grands défis et leurs objectifs premiers. En conséquence, ils augmentent les investissements dans les architectures de sécurité distante et migrent vers une sécurité en mode cloud.

En évoluant des infrastructures conventionnelles d'accès distant vers des solutions cloud, les entreprises peuvent absorber les besoins actuels et émergents de leurs télétravailleurs, avec en plus de nets avantages par rapport aux architectures classiques :

- Visibilité sur le réseau, les applications et le trafic des utilisateurs où qu'ils soient : sur site, chez eux ou en déplacement
- Contrôle des accès et des partages par les utilisateurs et les applications
- Sécurité sur la totalité de l'infrastructure réseau, des applications, des services et des utilisateurs pour une neutralisation rapide de toutes les menaces et vulnérabilités
- Déploiement simplifié pour un raccordement facile de nouveaux sites distants et télétravailleurs au réseau, sans matériel ni détachement d'un technicien sur site

Hausse des investissements dans la sécurité des accès distants

Au cours des 12 prochains mois, les entreprises envisagent d'augmenter leurs investissements dans la sécurité des accès distants : 54 % des entreprises interrogées prévoient ainsi de dépenser plus de 5 millions de dollars dans ce domaine, contre 31 % l'an passé.

Pour en savoir plus sur le cabinet d'études qui a mené l'enquête de terrain et effectué des analyses approfondies, rendez-vous sur https://www.onrcx.com/.

1. https://globalworkplaceanalytics.com/global-work-from-home-experience-survey
2. https://www.gartner.com/smarterwithgartner/making-hybrid-work-more-permanent-set-some-ground-rules/


En savoir plus
Découvrez comment Palo Alto Networks peut vous accompagner sur la voie d'un modèle de travail hybride productif et sécurisé.
paloalto NETWORKS
PRISMA ACCESS
BY PALO ALTO NETWORKS