TeamViewer

LIVRE BLANC

Télétravail au-delà de 2020

Surmonter les défis informatiques de la technologie existante grâce à l'accès et à la gestion à distance

Table des matières

Introduction :
La situation du télétravail

Certains considèrent le concept du télétravail comme un avantage. En fait, l'idée de travailler ailleurs qu'au bureau est, depuis presque 50 ans, de plus en plus populaire.

1970s

En 1973, alors qu'il travaillait à distance sur un projet pour la NASA, le physicien Jack Nilles a inventé le terme « télétravail ». Son succès en tant que télétravailleur l'a amené à proposer que le travail devrait être transféré aux travailleurs au lieu de forcer les travailleurs à se rendre au travail.

1990s

Le gouvernement fédéral américain a commencé à proposer un nombre limité de postes de télétravail dans les années 1990, et la Loi sur l'amélioration du télétravail a été adopté par le Congrès et promulgué en 2010, afin de rendre le télétravail universellement sûr et efficace pour les travailleurs fédéraux.

2000s

En raison de la prolifération des cyberattaques malveillantes au début des années 2000, les entreprises ou quiconque souhaitant des connexions Internet plus sécurisées se sont tournés vers les réseaux privés virtuels (VPN).

2010s

Dans les années 2010, le télétravail s'est développé avec l'amélioration de la technologie et avec l'allongement des trajets domicile-travail. Selon « The Remote Work Report », publié par GitLab et sur la base d'enquêtes réalisées entre le 30 janvier 2020 et le 10 février 2020 — avant le début du boom du télétravail induit par la pandémie — sur 3 000 professionnels adultes qui travaillaient à distance ou avaient la possibilité de travailler à distance, « 42 pour cent des personnes à 100 pour cent à distance ont déclaré travailler à distance depuis plus de 5 ans. 28 % déclarent travailler à distance depuis 3 à 5 ans. 19 % déclarent travailler à distance depuis 1 à 2 ans. Et 11 % ont déclaré travailler à distance depuis moins d'un an. »[1]

COVID-19

La pandémie de COVID-19 a provoqué l'expansion la plus rapide du télétravail de l'histoire. Étant donné que les communautés et les nations ne se sont pas déplacées, le télétravail est devenu un mode opératoire standard. Même les entreprises avec les politiques strictes « sans travail à domicile » ont dû adopter le télétravail - au moins à titre temporaire.

La croyance répandue selon laquelle plus d'employés travailleront à distance une fois la pandémie entièrement maîtrisée qu'avant son apparition est influencée par de nombreux facteurs comme :

- De nombreuses personnes préféreraient travailler pour une entreprise qui leur permet de travailler à domicile, à temps plein ou à temps partiel
- Les entreprises y voient des opportunités de diminution de leur loyer en réduisant la superficie de leurs bureaux
- L'abondance de ciel bleu clair et des voies navigables propres pendant les périodes de quarantaine ont démontré aux organisations qu'encourager les employés à travailler à domicile est l'un des moyens les plus simples et les plus efficaces de réduire leur empreinte carbone

43% **des travailleurs à temps plein souhaiteraient travailler à distance plus souvent[2]**

74% **des directeurs financiers ont l'intention de transférer en permanence certains employés vers le télétravail[3]**

25%-30% **de la main-d'œuvre devraient travailler à domicile plusieurs jours par semaine d'ici la fin de 2021[4]**

Les organisations croient fortement en l'avenir du télétravail, et agissent en conséquence. En septembre 2020, le Washington Post a rapporté que la fonction « Responsable du télétravail » est un nouveau titre de poste prisé. Selon l'article, Facebook a publié l'ouverture d'un poste de « Directeur, télétravail » et d'autres organisations emboîtent le pas.[5]

Les réactions à la récente flambée du télétravail nous révèlent que travailler ailleurs que dans un bureau centralisé est fait pour durer.

Le nouveau défi du phénomène actuel du télétravail est que l'avenir de nombreuses petites et moyennes entreprises (PME) dépendra grandement de la manière dont leurs responsables informatiques et les MSP déploieront et prendront en charge la technologie qui permet à cinq ou 1 000 télétravailleurs de rester productifs sans risques inhérents de problèmes techniques, de goulots d'étranglement de connectivité ou de failles de sécurité.

Exigences clés pour la configuration d'une main-d'œuvre à distance

Options du modèle de télétravail

Pour les entreprises, la mise en œuvre du télétravail n'est pas un scénario universel convenant à tous. Voici trois modèles populaires en pratique aujourd'hui.

01

Télétravail à 100 %
L'entreprise n'a pas de bureau. Les employés sont plutôt des nomades numériques, travaillant de n'importe où dans le monde, se rencontrant et collaborant en ligne.

02

Hybride à distance
Il peut s'agir de combinaison d'employés travaillant au bureau à temps plein, d'employés travaillant à domicile à temps plein ou d'employés partageant leur temps entre la maison et le travail.

03

Équipe de travail fractionnée ou rotative
La moitié des employés viennent au bureau certains jours, tandis que l'autre moitié vient les autres jours. Les travailleurs se déplacent moins fréquemment et les ressources du bureau sont moins sollicitées.

La cohésion de l'entreprise et les liens sociaux sont maintenus en permettant aux équipes de se voir et de travailler les unes avec les autres en personne. Cette option est devenue populaire auprès des organisations qui souhaitent conserver la culture de bureau intacte tout en étant à l'écoute des travailleurs qui préfèrent travailler à distance. Dans certains cas, les équipes rotatives ont rendu possible le partage des bureaux et des ressources, ce qui a réduit les besoins en espace de bureau et les coûts de location.

Aucune donnée ne permet d'affirmer que l'un de ces modèles est bon ou mauvais. Les entreprises peuvent consulter des experts et étudier les résultats d'autres entreprises, mais finalement, chaque organisation doit décider par elle-même et s'adapter si nécessaire pour obtenir les meilleurs résultats.

Outils nécessaires

Quel que soit le modèle choisi, chaque environnement de télétravail nécessite des outils qui permettent au service informatique de fournir :

Connectivité sécurisée pour que le télétravail puisse être effectué depuis n'importe où, tout en protégeant les données d'entreprise

Assistance à distance pour résoudre les problèmes de logiciels et installer les mises à jour et les mises à niveau sans avoir à envoyer un technicien sur le site distant ou à demander à l'employé d'apporter ou d'expédier du matériel au bureau

Surveillance à distance pour permettre une assistance et une maintenance proactive des appareils et pour alerter le service informatique des problèmes potentiels avant qu'ils ne deviennent des problèmes graves

Gestion des actifs à distance pour que le service informatique puisse voir et gérer chaque appareil géré par l'entreprise dans un seul tableau de bord

Protection contre les logiciels malveillants pour protéger chaque appareil contre les logiciels malveillants, tels que les virus, les attaques de phishing, les ransomwares, les logiciels espions, les rootkits, etc.

Mise à jour corrective pour corriger les vulnérabilités logicielles de manière proactive et mettre à jour les applications avant qu'elles ne deviennent des points d'entrée pour les cyberattaques

Sauvegarde de données afin que les fichiers de l'entreprise sur les appareils distants soient automatiquement sauvegardés dans le cloud, disponibles pour une restauration à distance dans le cadre d'un plan de reprise après sinistre, que ce soit sur le même terminal ou sur un terminal différent si l'appareil d'origine n'est plus disponible

Outils de vidéoconférence et de collaboration, afin que les employés puissent travailler ensemble et se rencontrer n'importe où, quel que soit leur emplacement

Grâce à ces outils, les télétravailleurs n'ont pas à apporter leurs appareils aux techniciens informatiques pour obtenir une assistance ou des services, et les techniciens informatiques n'ont pas à se déplacer vers les appareils pour les protéger et les surveiller. Mais sans connectivité sécurisée, tous ces outils et appareils utilisés sont à risque.

Deux questions à se poser lors de l'évaluation de vos options

Lors de la planification de votre infrastructure de télétravail, il est important de vous poser dès le début les deux questions suivantes, car les réponses vous aideront à évaluer les solutions disponibles.

Êtes-vous prêt à fournir des ordinateurs et des téléphones portables à vos employés pour qu'ils puissent exercer leurs activités, ou attendez-vous à ce qu'ils (ou demandez-leur) utilisent leurs appareils personnels pour le travail ?

Chaque appareil qui se connecte à votre réseau doit être protégé. Cela se complique si les appareils appartiennent à des employés, car vous ne souhaitez certainement pas que les documents commerciaux confidentiels soient enregistrés localement sur des appareils personnels.

Quelle est l'importance de l'évolutivité pour votre environnement de télétravail ?

L'évolutivité constitue une préoccupation pour toute entreprise qui souhaite se développer. À mesure qu'une PME grandit, la mise à l'échelle implique de rendre la technologie et l'assistance disponibles à plus de personnes. Une technologie qui peut facilement évoluer vous permet d'ajouter plus d'utilisateurs sans engager de dépenses d'infrastructure supplémentaires ni devoir effectuer des mises à niveau logicielles coûteuses. Bien que certains coûts soient inévitables, vous ne devriez pas avoir à reconstruire votre infrastructure informatique à mesure que votre entreprise poursuit son expansion.

Les technologies peuvent évoluer négativement de diverses manières. Certaines technologies, comme le VPN, n'ont jamais été conçues pour évoluer. Souvent, les entreprises décident d'acheter un VPN parce qu'elles en ont entendu parler et parce que les coûts initiaux semblent raisonnables.

Par contre, le VPN n'a jamais été conçu pour permettre à l'ensemble de votre personnel de se connecter à distance à votre serveur pendant une journée toute entière. Ainsi, même si votre effectif n'augmente pas, la bande passante de votre VPN doit augmenter pour fonctionner à une capacité supérieure. Cela signifiera probablement qu'il vous faudra investir dans un nouveau matériel et des logiciels mis à niveau, ce qui entraînera des coûts supplémentaires.

Et lorsque votre entreprise grandit, les coûts supplémentaires des nouvelles mises à niveau du matériel et des logiciels seront à nouveau nécessaires.

Connectivité sécurisée : La différence entre l'accès à distance et le VPN

Le service informatique doit fournir une connectivité permettant aux télétravailleurs d'être aussi productifs qu'au bureau. Il doit aussi permettre aux techniciens de fournir une assistance à distance et protéger les sessions à distance des pirates, des logiciels malveillants et d'autres menaces.

Alors que le VPN est la solution de statu quo pour permettre aux employés d'accéder aux systèmes d'entreprise, l'augmentation rapide du nombre de télétravailleur causée par la pandémie de coronavirus a révélé plusieurs inconvénients du VPN en tant que protocole de tunneling. Avec le VPN, un tunnel virtuel connecte le télétravailleur à un serveur. Voici les problèmes qui peuvent survenir lorsque les utilisateurs téléchargent des fichiers du serveur sur leur propre ordinateur et apportent des modifications aux documents localement avant de les enregistrer sur le serveur :

Goulots d'étranglement
Comme un tunnel que vous traversez avec votre voiture, le VPN se remplit de trafic alors que de plus en plus d'utilisateurs tentent d'accéder à votre réseau d'entreprise. Lorsque seulement quelques employés travaillent à distance, cela ne représente généralement pas un problème. Mais lorsque des centaines de travailleurs d'une entreprise essaient d'accéder au serveur en même temps, les goulots d'étranglement ralentissent le trafic à une exploration et peuvent même pour certains bloquer la connexion au serveur. Quand cela se produit, les télétravailleurs sont frustrés et ne sont pas productifs.

Sécurité
Une fois que les télétravailleurs téléchargent des documents du serveur vers leurs appareils personnels, rien ne les empêche d'enregistrer des fichiers sur ces appareils. En fonction de l'employé et de son niveau d'accès au réseau, il existe un risque de vol des documents de valeur par des employés qui ne respectent pas l'éthique. De plus, les VPN s'arrêtent parfois sans raison apparente, laissant la connexion entre le serveur et l'appareil non sécurisée. Pour cette raison, certains utilisateurs de VPN installent la fonctionnalité kill switch qui permet d'arrêter immédiatement la connexion entre l'ordinateur local et le serveur si le VPN s'arrête.

Puissance de traitement
Les employés qui travaillent sur des ordinateurs de bureau puissants dans leur lieu de travail seront limités aux logiciels de l'ordinateur qu'ils utilisent à distance et à la puissance de traitement que cet ordinateur permet. Par exemple, certaines équipes utilisent des programmes de CAO sur leur bureau. Leur ordinateur à la maison ne possède pas de carte graphique avancée pour prendre en charge les logiciels de CAO, ce qui signifie qu'ils ne peuvent pas travailler sur des projets depuis chez eux.

Les fonctions d'accès à distance fonctionnent d'une manière complètement différente. Premièrement, il n'y a pas de tunnel. Les télétravailleurs se connectent directement à leur bureau professionnel. Une fois à distance, ils voient une image inversée de ce qui se passe sur leur ordinateur de bureau et le font fonctionner comme s'ils étaient en personne sur leur lieu de travail. Contrairement au VPN, l'accès à distance fonctionne différemment dans les trois domaines problématiques évoqués ci-dessus :

Goulots d'étranglement
Il n'y en a pas. Le seul transfert entre les machines est l'image inversée, nécessitant une bande passante négligeable.

Sécurité
Chaque session ainsi que tous les transferts de fichiers sont protégés par un cryptage de bout en bout. Les employés travaillant à distance peuvent accéder aux applications de bureau et travailler en toute sécurité avec d'énormes fichiers sur l'ordinateur hôte dont le téléchargement ou le transfert prendrait autrement des heures.

Puissance de traitement
Il n'est pas nécessaire que l'appareil local soit puissant, car il fonctionne simplement comme un miroir de l'appareil distant ou du bureau, avec la souris, le moniteur et le clavier locaux servant de moyen de partage d'écran et de contrôle de l'appareil distant.

De plus, le VPN est coûteux — surtout si vous avez besoin de le mettre à l'échelle pour plus d'utilisateurs. Le temps entre l'installation et le déploiement pour le VPN est de plusieurs semaines, tandis que l'accès à distance peut être configuré et utilisé en quelques minutes. Le VPN nécessite également une installation et une configuration approfondies, mais doit aussi être compatible avec votre routeur. À l'opposé, les solutions d'accès à distance basées sur le cloud ne nécessitent pas d'installation, de configuration ou de maintenance approfondies. Tout est fait dans le cloud par le fournisseur.

Le VPN est tout simplement une technologie obsolète dont le succès appartient au passé, comme le souligne Paul Martini dans Security Boulevard : « C'est certain, les jours du VPN sont limités. La pandémie de coronavirus s'est peut-être solidifiée et accélérée ces jours-là, conduisant finalement à la mort du VPN. »[5] Contrairement au VPN, l'accès à distance est à l'épreuve du temps et évolue facilement, en fonction de la croissance rapide de l'entreprise.

Accès à distance contre le VPN

Caracteristiques	Accès à distance L'accès à distance avec TeamViewer vous permet de vous connecter à un dispositif cible, tel qu'un ordinateur, un smartphone ou une tablette. Les seules données transférées sont une image de ce qui est affiché sur l'écran du dispositif cible. Les utilisateurs peuvent prendre le contrôle de la souris et du clavier ou de l'écran tactile cibles pour faire fonctionner les appareils, et peuvent utiliser toutes les applications et fichiers comme s'ils étaient en personne sur leur lieu de travail.	Réseau privé virtuel (VPN) Un VPN ou réseau privé virtuel, vous permet d'envoyer et de recevoir des données par un tunnel entre deux appareils. Toutes les données sont transférées par l'intermédiaire du serveur VPN vers l'appareil local de cet utilisateur, ce qui entraine un risque de perte et/ou de vol. Cela vous permet de vous connecter à un réseau d'entreprise et d'accéder aux ressources derrière un pare-feu. Toute la puissance de traitement dépend de l'appareil local de l'utilisateur.
Cela permet au service informatique de fournir une assistance à distance et aux utilisateurs de recevoir une assistance à distance sur leurs appareils	✓	✗
Accès aux postes de travail	✓	✗
Transferts de fichiers à distance	✓	✓
Contrôle de l'appareil à distance	✓	✗
Accès aux appareils sans surveillance	✓	✗
À distance dans le réseau d'entreprise	✓	✓
Coûts de configuration et de maintenance	Ø	$$$
Évolutivité instantanée	✓	✗

Comprendre la surveillance et la gestion à distance

Permettre aux employés de travailler efficacement de n'importe où et à tout moment augmente leur rendement potentiel, leur productivité et leur valeur globale pour l'organisation. La prise en charge, la gestion et le maintien de la visibilité de tous les périphériques réseau et distants connectés représentent un effort massif pour le service informatique, même s'il ne s'agit que d'une poignée de périphériques.

Le seul moyen efficace pour le service informatique de prendre en charge, surveiller, mettre à jour et patcher tous les périphériques - à la fois émis par l'entreprise et le BYOD - est de le faire à distance et autant que possible, automatiquement. Autrement, les techniciens perdent du temps à passer d'un appareil physique à un autre, à réagir aux problèmes qui peuvent empêcher les gens de travailler.

Importance de la sécurité

Sans la mise en œuvre de mesures de sécurité strictes, les appareils distants sont menacés, qu'ils soient fournis par l'entreprise ou appartenant aux employés.

D'après une enquête menée auprès de 411 professionnels de l'informatique et de la sécurité par Check Point, **71 pour cent des professionnels de la sécurité ont remarqué une augmentation des menaces de sécurité ou des attaques depuis le début de l'épidémie de coronavirus.** Les attaques de logiciels malveillants (28 %) et de ransomwares (19 %) ont considérablement augmenté.[6] Les types de menaces liées aux coronavirus comprenaient :

55%

des e-mails de phishing concernent des nouvelles et des remèdes sur le coronavirus

32%

de sites Web malveillants offrent des conseils ou des remèdes contre le COVID-19

Les logiciels malveillants, le phishing et les sites Web malveillants peuvent tous entraîner des failles de sécurité pouvant entraîner le vol de données. Que faire si un employé de votre entreprise travaillant sur VPN a téléchargé une base de données clients de votre serveur vers son ordinateur, et que cet ordinateur a été piraté et la base de données volée en raison d'une sécurité insuffisante ?

Vous êtes tout à coup confronté à une situation où votre entreprise a violé la confidentialité de chaque client de cette liste, car elle n'a pas gardé la liste sécurisée. Les mesures que vous prenez après la violation de données, y compris la notification aux clients, l'indemnisation des pertes subies et la prise de mesures correctives pour éviter que cela ne se reproduise, peuvent déterminer le statut futur de la marque, de la réputation et des finances de votre entreprise.

Il ne s'agit là que d'un exemple montrant l'importance de protéger tous les appareils distants contre tous les types de cyberattaques. C'est aussi la raison pour laquelle une solution de surveillance et de gestion à distance n'est pas complète sauf si elle inclut la possibilité de gérer à distance la sécurité et les tâches de maintenance informatique, telles que le déploiement de la protection contre les logiciels malveillants, la correction des vulnérabilités, la mise à jour des logiciels et la sauvegarde des fichiers.

Lors du choix de solutions pour l'accès à distance, l'assistance à distance, la surveillance à distance et la gestion à distance, la sécurité doit être la priorité absolue. Sans sécurité, la vitesse de votre connexion n'a pas d'importance.

Solutions d'(RMM)accès et de support à distance TeamViewer, solutions de surveillance et de gestion à distance

La prise en charge des appareils distants et des appareils réseau est essentielle à tout modèle de travail à distance.

Les solutions d'accès et de support à distance TeamViewer ainsi que les solutions de surveillance et de gestion à distance TeamViewer fournissent tout ce dont vous avez besoin pour prendre en charge les télétravailleurs, le tout dans une console de gestion centralisée — tout par un seul fournisseur.

Avec les solutions de surveillance et de gestion à distance TeamViewer, commencez avec seulement cinq terminaux et évoluez autant que vous le souhaitez sans dépasser la solution.

Caractéristiques clés

Accès à distance
Connectez-vous en toute sécurité à un appareil Windows ou macOS et prenez-en le contrôle comme si vous y étiez, sans avoir besoin de VPN.

Support à distance
À distance sur les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles* pour analyser et résoudre les problèmes, modifier les paramètres et effectuer des mises à jour.

** Nécessite l'AddOn de prise en charge pour les appareils mobiles TeamViewer*

Surveillance des périphériques à distance
Soyez proactif au lieu d'être réactif en identifiant les problèmes de périphérique avant qu'ils ne surviennent. Cela vous permettra de résoudre les problèmes potentiels avant qu'ils ne s'aggravent.

Surveillance des périphériques réseau
Obtenez de la visibilité dans la disponibilité, l'état et les problèmes des périphériques réseau tels que les routeurs, les imprimantes, etc.

Gestion des actifs
Affichez et gérez tous les actifs informatiques depuis un tableau de bord unique.

Gestion des correctifs
Détectez automatiquement et corriger les vulnérabilités des logiciels et des systèmes d'exploitation tiers obsolètes.

Protection des terminaux
Assurez-vous que tous les périphériques soient protégés contre les logiciels malveillants, les virus, les chevaux de Troie, les logiciels espions, les rootkits, les ransomwares et plus encore avec **la protection antivirus certifiée VB100.**

Sauvegarde
Évitez la perte de données en sauvegardant automatiquement les fichiers des terminaux vers le cloud, disponibles à tout moment pour la reprise après sinistre à distance.

Évolutivité
Ajoutez autant d'utilisateurs d'accès à distance que nécessaire et à tout moment, aucune mise à niveau matérielle ou logicielle n'étant requise. Avec RMM, commencez à surveiller et à gérer seulement cinq appareils, et ajoutez des centaines ou des milliers à mesure que votre entreprise se développe.

Sécurité

Une sécurité de niveau industriel est intégrée à TeamViewer.

- **Cryptage AES 256 bits de bout en bout**, chaque session est donc protégée
- **Authentification à deux facteurs** pour empêcher les utilisateurs non autorisés, même si un appareil est perdu ou volé
- **Conforme GDPR**
- **Les certifications comprennent :**
  - SOC2
  - HIPAA/HITECH
  - ISO/IEC 27001
  - ISO 9001:2015
  - Solution antivirus certifiée VB100 pour la protection des terminaux
- **La surveillance du centre de données 24h/24 et 7j/7** garantit une disponibilité du réseau 24h/24
- **Signature de code DigiCert** pour vérifier que le code est authentique et n'a pas été falsifié
- **Protection contre l'attaque par force brute** pour empêcher les pirates informatiques d'entrer
- **Un écran** noir maintient votre appareil au bureau verrouillé avec un écran noir, pour que personne ne puisse voir le travail que vous faites ou bien accéder à l'appareil

Conclusion

Alors que le boom du télétravail en 2020 a été forcé par la pandémie mondiale, les analystes commerciaux et les bulletins d'information indiquent qu'une part considérable de la main-d'œuvre continuera à travailler à distance. Cela signifie que les défis auxquels sont confrontés les services informatiques et les MSP pour déployer des espaces de travail distants qui sont abordables, rapides, sécurisés et évolutifs tout en permettant aux employés de travailler de manière productive - sur n'importe quel appareil, à tout moment et n'importe où - resteront.

En parallèle, le service informatique est confronté au défi de prendre en charge des appareils de tous formats, fabricants et systèmes d'exploitation, y compris les appareils appartenant aux employés. Les applications qui permettent au service informatique de surveiller et de gérer à distance tous les périphériques améliorent la productivité et l'efficacité informatiques.

La combinaison d'accès et de support à distance TeamViewer, solutions de surveillance et de gestion à distance TeamViewer répond à toutes les exigences de travail à distance dans une plate-forme intégrée. Vous pouvez ainsi consolider vos outils informatiques et travailler avec un seul fournisseur. Le résultat ? Cela permet aux télétravailleurs de travailler de manière sécurisée et productive de n'importe où et à tout moment sur n'importe quel appareil. Par ailleurs, le service informatique peut gérer et réparer à distance les appareils n'importe où en temps réel avec une visibilité complète sur l'état opérationnel de votre infrastructure informatique dans une seule console de gestion. La cerise sur le gâteau ? Le service informatique peut automatiser les tâches de routine, y compris l'application de correctifs, la surveillance et la sauvegarde des périphériques, sans avoir à basculer entre les différentes applications. Cela se traduit par des flux de travail plus efficaces et par moins de temps d'arrêt pour votre organisation.

Étapes suivantes :

Découvrez comment Remote Access and Support de TeamViewer fonctionne avec TeamViewer Remote Management grâce à une démonstration et un essai gratuit.

Demandez une démo gratuite | Demandez un essai gratuit

Ressources

En savoir plus sur l'accès et le support à distance TeamViewer

En savoir plus sur les solutions de surveillance et de gestion à distance TeamViewer (RMM)

TeamViewer

Références

1) GitLab (2020) : Rapport sur le travail à distance,
https://page.gitlab.com/rs/194-VVC-221/images/the-remote-work-report-by-gitlab.pdf

2) getabstract (Avril 2020) : Enquête nationale, une majorité d'employés américains souhaitent que le télétravail subsiste,
https://journal.getabstract.com/wp-content/uploads/2020/04/ga_remote_survey_2020_compressed.pdf

3) Gartner (Avril 2020) : Directeur financier de Gartner, Une enquête révèle que 74 % ont l'intention de transférer définitivement certains employés vers le télétravail,
gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-

4) GlobalWorkplaceAnalytics.com (Avril 2020) : Travail-à-domicile après Covid-19—Nos prévisions,
https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

5) Washington Post (Septembre 2020) : Nouveau titre de poste prisé durant la pandémie : « Responsable du télétravail »,
https://www.washingtonpost.com/business/2020/09/09/head-of-remote-work-jobs/

6) Security Boulevard (Mai, 2020) : La pandémie de coronavirus et la mort du VPN,
https://securityboulevard.com/2020/03/the-coronavirus-pandemic-and-the-death-of-the-vpn/

7) Security Boulevard (Mai 2020) : Les différentes façons dont vos employés peuvent être piratés lorsqu'ils travaillent à domicile et comment réagir,
https://securityboulevard.com/2020/05/the-many-ways-your-employees-can-get-hacked-while-working-from-home-and-how-to-respond/

À propos de TeamViewer

En tant que plateforme de connectivité à distance parmi les leaders mondiaux, TeamViewer garantit la connexion de tous les utilisateurs, sur tous types d'appareils, partout et à tout moment. TeamViewer offre un accès, une assistance et un contrôle à distance, ainsi que des possibilités de collaboration pour les points de terminaison en ligne de toute sorte et aide les entreprises de toute taille à exploiter pleinement leur potentiel numérique. TeamViewer est activé sur environ 2 milliards d'appareils. Près de 45 millions d'appareils sont en ligne simultanément. Fondée en 2005 à Göppingen, en Allemagne, TeamViewer est une société publique cotée à la Bourse de Francfort et qui emploie près de 800 personnes dans des bureaux répartis en Europe, aux États-Unis et en Asie-Pacifique.

www.teamviewer.com