

Pourquoi Citrix Workspace est un meilleur choix que le VPN pour les télétravailleurs modernes



Jamais autant de personnes n'ont télétravaillé qu'aujourd'hui. Le VPN était traditionnellement la solution de sécurité de prédilection pour fournir un accès sécurisé aux systèmes et aux fichiers de l'entreprise. Mais les VPN sont complexes à gérer et ils introduisent des risques de sécurité au niveau du réseau. Ils offrent en outre une expérience médiocre aux utilisateurs et ne sont ni scalables, ni respectueux de la vie privée.

Le vieux modèle de sécurité dit de « paramètre de sécurité » des VPN classiques est maintenant dépassé par les principes stricts d'un cadre « zero trust », qui contextualise l'accès selon les demandes. Citrix Workspace fournit une solution cloud sans VPN vous permettant d'accéder à toutes les applications Web Intranet, SaaS, mobiles et virtuelles, grâce à un accès managé, non managé et BYOD fonctionnant sur tous les réseaux. Ce brief solution explique pourquoi Citrix Workspace est un meilleur choix que le VPN pour répondre aux exigences de sécurité, de performance et de scalabilité des télétravailleurs.

La gestion d'un VPN est complexe

En fonction du rôle qu'ils occupent et des ressources auxquelles ils accèdent, les télétravailleurs ont généralement des méthodes d'accès très différentes. Un employé, un administrateur, un partenaire ou un fournisseur utiliseront un point de connexion différent au sein d'un même VPN. Plusieurs VPN sont souvent nécessaires, et l'accès aux applications SaaS s'effectue via un portail Single Sign-On distinct. Ce type de solution se révèle chronophage pour les administrateurs système et sa gestion nécessite souvent des ressources importantes. L'ajout de capacités d'urgence requiert une mise à niveau fastidieuse du matériel ou un processus interminable d'approvisionnement en licences.

Les VPN fournissent souvent une solution d'accès binaire : un accès complet ou pas d'accès du tout. Ils nécessitent la mise en place de stratégies complexes pour empêcher les terminaux non managés d'avoir un accès non restreint au réseau, aux ressources et aux données.

Lorsque vous remplacez les appliances VPN classiques par un service cloud entièrement managé et disponible partout dans le monde, les stratégies de sécurité réseau complexes deviennent superflues, car vos applications et vos données disposent d'un accès protégé.

Les VPN ne sont pas conçus pour un usage à volume élevé

Qu'importe où se trouvent les télétravailleurs, ils s'attendent à pouvoir accéder au réseau de leur entreprise de façon fluide. Et c'est aussi le cas des employeurs. L'utilisation d'un VPN laisse cependant tout le trafic utilisateur traverser le réseau d'entreprise, ce qui augmente les congestions et diminue les performances. De plus, puisqu'il est commun de

déployer un VPN sur un site central auquel des utilisateurs dispersés géographiquement se connectent pour accéder à des applications Web internes, la latence ajoutée dégrade l'expérience finale.

Les télétravailleurs peuvent être confrontés à des difficultés lorsqu'ils utilisent des applications à deux niveaux, comme celles utilisées pour la facturation et le CRM. Ces applications nécessitent qu'un client soit installé sur l'appareil de l'utilisateur final, utilisent des protocoles natifs ayant des exigences importantes en termes de bande passante, et surchargent rapidement les VPN et les canaux réseau.

L'augmentation de la congestion et de la latence réseau dégrade la réactivité des applications, ce qui résulte en une expérience hétérogène et parfois intolérable. Des conditions réseau sous-optimales du côté de l'utilisateur final ne vous permettent pas de contrôler les performances et l'expérience.

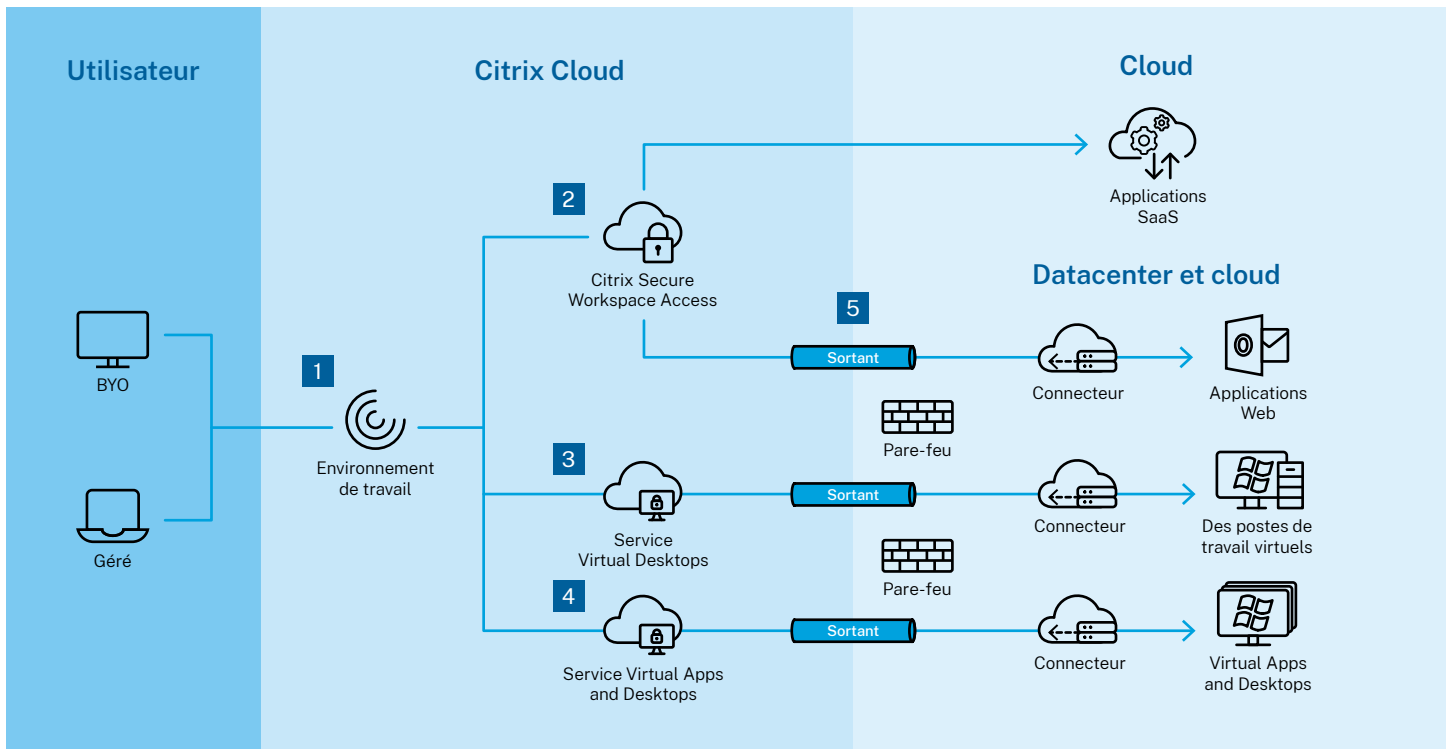
Citrix Workspace offre à vos utilisateurs un accès sans VPN aux applications Web

Le service Citrix Secure Workspace Access, composant de Citrix Workspace, fournit une expérience sans VPN aux applications accessibles depuis un navigateur. De cette façon, les applications modernes sont fournies nativement sur l'appareil de chaque utilisateur final et intègrent des contrôles de sécurité contextuels, sans nécessiter aucun mode d'accès au niveau du réseau.

Puisque Citrix Secure Workspace Access est disponible partout dans le monde, les utilisateurs sont redirigés vers le point de présence le plus proche. Les applications, SaaS et Web, sont ainsi accessibles en toute sécurité et peuvent fournir de meilleures performances.

Pour les applications traditionnelles à deux niveaux, la bande passante peut s'avérer une source de préoccupation et les performances se dégrader lorsqu'on y accède depuis des réseaux à forte latence comme le Wi-Fi domestique. La fourniture d'un accès via une plate-forme virtualisée améliore non seulement l'expérience de l'utilisateur final, mais assure également une sécurité granulaire au niveau de la couche applicative. La solution Citrix Virtual Apps and Desktops, composant de Citrix Workspace, garantit la meilleure sécurité et les meilleures performances pour ces applications en réduisant les exigences de bande passante et en ajustant de façon dynamique les performances et les contrôles de sécurité.

Citrix Virtual Apps and Desktops offre aux télétravailleurs une expérience meilleure que native. Les applications gourmandes en ressources réseau et informatiques sont virtualisées et optimisées dans le datacenter. Le client de l'application est également virtualisé et s'exécute à proximité de la source des données. Le télétravailleur bénéficie d'un protocole optimisé pour Internet, donc de bonnes performances même sur des réseaux congestionnés.



- 1 Choix du fournisseur d'identité (AD, AAD, Okta, Google, Radius, etc.)
- 2 Accès à des applications SaaS et Web sans VPN et avec une sécurité renforcée
- 3 Accès à des PC Windows 10 physiques sans VPN
- 4 Accès à des applications et des postes Windows et Linux sans VPN et avec une sécurité renforcée
- 5 Le canal de contrôle « sortant seulement » fournit un accès en fonction de la ressource

Les VPN compromettent la vie privée des collaborateurs

Les stratégies de sécurité nécessitent une surveillance réseau. Si un VPN est configuré pour désactiver le tunneling partagé, tout le trafic, y compris celui destiné aux applications personnelles et privées, traverse le réseau d'entreprise. Vous pourrez observer le trafic non lié au travail, ce qui pose un réel problème de confidentialité pour les télétravailleurs se servant de leur appareil durant leur temps libre. Les télétravailleurs s'inquiètent à juste titre de la possibilité de les espionner via leur connexion Internet, d'accéder à leurs ordinateurs et à leur réseau domestique, ou de collecter des données à partir des sites Web qu'ils visitent.

D'un autre côté, lorsque l'accès s'arrête à la couche applicative, les travailleurs sentent que leur vie privée est respectée. L'utilisateur final ne fait l'objet d'aucune surveillance et le trafic réseau personnel reste privé.

À cause des VPN, le BYOD peut mettre à rude épreuve les équipes et les infrastructures informatiques

Les initiatives BYOD se démocratisent, car bon nombre d'entreprises réalisent que laisser leurs employés utiliser leurs

propres appareils représente un véritable avantage. Cependant, lorsque des télétravailleurs se connectent à un réseau via un VPN, s'assurer que leurs appareils répondent aux exigences de sécurité, de conformité et de compatibilité peut nécessiter d'importantes ressources IT. C'est là où une initiative BYOD cesse de réduire les coûts de point de terminaison et d'accès et devient un poids pour l'infrastructure informatique.

De nombreux VPN ne fournissent pas de stratégie de sécurité contextuelle et granulaire adaptée à une approche BYOD et à des appareils non managés. Les travailleurs distants doivent utiliser un appareil fourni et managé par l'entreprise. De nombreuses entreprises font également appel à des entreprises tierces pour gérer certains services, comme la paie, les avantages sociaux et le support technique. Puisque les fournisseurs tiers autonomes disposent de leurs propres configurations d'appareil, il devient impossible de contrôler et sécuriser les points de terminaison.

En revanche, Citrix Workspace offre une expérience utilisateur riche sur n'importe quel appareil, via l'application Citrix Workspace ou un navigateur Web.

Les télétravailleurs peuvent avoir besoin d'accéder à un poste de travail physique depuis un appareil personnel ou BYOD. Citrix Remote PC Access permet aux utilisateurs finaux de

se connecter depuis n'importe quel lieu à leur PC Windows physique du bureau. Et pour les appareils mobiles, une capacité Micro-VPN par application réduit encore la nécessité d'une connectivité VPN complète par appareil. Il n'est plus nécessaire de configurer et de lancer un VPN client, ce qui renforce l'expérience et offre un accès fluide aux données d'entreprise.

Les VPN ouvrent un accès complet à votre réseau

Les VPN représentent un modèle de sécurité obsolète, avec un accès de type « tout ou rien ». Vous ne pouvez ni voir, ni contrôler qui accède à quoi. Il est donc difficile de gérer les menaces internes et le vol d'authentifiants.

Les VPN augmentent la probabilité d'attaques au niveau du réseau lorsque les utilisateurs n'ont besoin que d'un accès aux applications. Même les points de terminaison compromis peuvent devenir des participants au réseau, ce qui facilite la propagation des logiciels malveillants.

Citrix Workspace est une solution sans VPN sécurisée pour les télétravailleurs

Citrix offre un environnement de travail à distance unique et sans frustration qui répond aux défis auxquels votre entreprise est confrontée en matière de sécurité, de gestion et de scalabilité. Citrix Workspace regroupe toutes les ressources dans une interface utilisateur unique et personnalisée, accessible depuis n'importe quel appareil.

Qu'importe l'approche et l'appareil choisis, les télétravailleurs pourront accéder à vos applications, fichiers et données et profiter d'une expérience Single Sign-On sans VPN. La sécurité est renforcée grâce au service Citrix Secure Workspace Access, qui remplace les appliances VPN classiques par un service cloud entièrement managé et disponible partout dans le monde. En protégeant l'accès aux applications et aux données, les stratégies de sécurité complexes ne sont plus nécessaires.

Que vos travailleurs utilisent des applications virtuelles, Web ou SaaS, Citrix Workspace détermine les droits d'autorisation en fonction d'informations conditionnelles ou contextuelles basées sur l'utilisateur ou l'appareil. Les stratégies de sécurité contextuelles vous permettent non seulement d'identifier et d'authentifier un utilisateur, mais également de choisir quelles actions un utilisateur peut utiliser au sein d'une application en fonction de paramètres tels que l'état, l'emplacement géographique et l'adresse IP de l'utilisateur

et de l'appareil. Citrix Workspace permet également aux entreprises d'autoriser différents niveaux d'accès aux applications ou aux ressources. Seuls les utilisateurs et les appareils vérifiés pourront réaliser certaines actions, comme copier et coller vers le bloc-notes, imprimer et créer des copies locales des fichiers.

Avec le service Citrix Secure Workspace Access, vous pouvez ajouter une visibilité et des contrôles d'accès sécurisés aux applications SaaS et Web. Les stratégies de protection des applications empêchent l'utilisation de malwares pouvant enregistrer les frappes et réaliser des captures d'écran. L'utilisation de filigranes protège l'accès aux applications et aux informations sensibles. Plutôt que de refuser l'accès à un télétravailleur se connectant depuis un appareil non vérifié, vous pouvez restreindre les fonctions accessibles par les utilisateurs.

Afin de garantir une surveillance optimale, Citrix Workspace fournit aux administrateurs en charge de la sécurité une évaluation des risques liés aux utilisateurs et une notation des risques en continu. La stratégie de réduction des risques pour l'entreprise est mise en œuvre après la validation initiale de la connexion.

Les avantages de Citrix Secure Workspace Access :

- Simple à déployer et à configurer
- Facile à gérer et à entretenir
- Protège les réseaux sous-jacents
- Protège la vie privée de l'utilisateur final
- Utilise des accès contextuels et conditionnels
- Offre une expérience riche
- Rapidité de la scalabilité et du provisioning
- Offre de hautes performances aux télétravailleurs
- Permet aux utilisateurs finaux de choisir leur appareil (BYOD)
- Offre une assurance et une surveillance continues

Conclusion

Chaque entreprise a besoin de savoir que ses télétravailleurs peuvent se connecter avec la même sécurité que leurs collègues sur site, où qu'ils se trouvent et quel que soit l'appareil utilisé. Contrairement aux VPN traditionnels, Citrix Workspace vous offre la surveillance et le contrôle dont vous avez besoin.

Pour en savoir plus sur les fonctionnalités et les avantages de Citrix Workspace, contactez votre représentant commercial ou rendez-vous sur citrix.fr/workspace.



Ventes aux entreprises

Amérique du Nord | 800-424-8749

International | +1 408-790-8000

Sites

Siège social | 851 Cypress Creek Road Fort Lauderdale, FL 33309, États-Unis

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, États-Unis

©2020 Citrix Systems, Inc. Tous droits réservés. Citrix, le logo Citrix et les autres marques citées dans le présent document appartiennent à Citrix Systems, Inc. et/ou à l'une ou plusieurs de ses filiales, et peuvent être déposés au USPTO (U.S. Patent and Trademark Office) aux États-Unis et dans d'autres pays. Toutes les autres marques appartiennent à leur(s) propriétaire(s) respectif(s).
RES160 10/20