

3 signes indiquant qu'il est temps de passer à un environnement de travail digital

Comment le fait de voir plus loin que les postes de travail peut améliorer la productivité, donner de l'autonomie aux équipes informatiques et améliorer la sécurité de vos données

Il n'y a pas si longtemps, un poste de travail virtuel ou d'entreprise suffisait pour intégrer rapidement les nouveaux collaborateurs. Plus le temps passe, moins cela est vrai. Trois tendances émergentes indiquent que si vous voulez répondre aux exigences de productivité croissantes de votre entreprise, il est temps de passer à l'environnement de travail digital sécurisé.

- 1. Des collaborateurs de plus en plus mobiles**
- 2. La modernisation des applications**
- 3. La disparition du périmètre de sécurité**

Découvrez comment le fait de voir plus loin que les postes de travail peut vous aider à améliorer la productivité des utilisateurs, donner de l'agilité à vos équipes informatiques et accroître la protection de vos données d'entreprise.



Saviez-vous que



Plus de 1/3

des employés changeraient de travail pour avoir une plus grande flexibilité¹ ?



Seuls 57 %

travaillent au même endroit que leurs collègues 100 % du temps¹.

1. Des collaborateurs de plus en plus mobiles

Les collaborateurs veulent choisir quand et comment ils travaillent. En réalité, un rapport d'étude Gallup suggère que 37 % des collaborateurs changeraient de travail s'ils pouvaient travailler où ils veulent au moins une partie du temps. L'étude révèle également que seuls 57 % des collaborateurs travaillent au même endroit que leurs collègues 100 % du temps¹. Les entreprises reconnaissent aujourd'hui le potentiel du travail à distance pour l'augmentation de la productivité, de l'agilité et de l'expérience des collaborateurs, que ce soit à la maison, chez le client, à l'hôtel ou dans un café. Il ne tient qu'aux équipes informatiques d'évoluer en ce sens. Alors qu'il est possible de livrer des applications virtuelles à des collaborateurs mobiles, d'autres facteurs, notamment les applications modernes, ajoutent à la difficulté de la virtualisation.

2. La modernisation des applications

Les applications sont de plus en plus conçues pour fonctionner sur toutes les plateformes. Microsoft Office est un bon exemple d'applications modernes car ses applications peuvent être exécutées sur différentes plateformes parmi lesquelles Windows 10, iOS, Android et Macintosh. De plus, Microsoft Office peut être livré sous la forme d'applications natives ou même de service SaaS. Mais les applications modernes introduisent de nouveaux défis. Comment sécurisez-vous et administrez-vous des applications modernes ? Par exemple, un outil traditionnel de gestion des postes clients tel que SCCM vous permet de livrer et d'administrer

d'anciennes applications de bureau Windows sur un ordinateur portable Windows 7, mais ne vous permet pas d'administrer des applications modernes Windows 10 sur un smartphone BYOD ni de séparer les données personnelles d'un collaborateur des données de l'entreprise. Par conséquent, les outils traditionnels de gestion des postes clients doivent être complétés par des outils de gestion de la mobilité d'entreprise. L'association de la gestion des postes clients et de la gestion de la mobilité d'entreprise est connue sous le nom de gestion unifiée des terminaux (UEM).

3. La disparition du périmètre de sécurité

Avec des collaborateurs de plus en plus mobiles, il devient de plus en plus difficile de conserver les données d'entreprise dans des datacenters. Vos utilisateurs doivent avoir accès à leurs fichiers, que ces fichiers se trouvent sur des serveurs protégés par votre pare-feu, sur un serveur hébergé par un fournisseur de confiance ou sur leur poste de travail au bureau. Certains de vos utilisateurs ont peut-être dû se résoudre à utiliser des clients de messagerie mobile native par opposition aux messageries virtuelles, stockant les pièces jointes des emails sur leur smartphone personnel dans un format non chiffré. En parallèle, ces collaborateurs utilisent peut-être également un VPN dont un hacker peut facilement se servir pour accéder à vos ressources par-delà votre pare-feu, au moyen d'une application mobile compromise que votre collaborateur a téléchargée.

Allez au-delà de la virtualisation et adoptez un environnement de travail digital avec Citrix

Un environnement de travail digital intégré et complet permettra aux utilisateurs d'accéder partout et de façon sécurisée à leurs applications, postes et données. L'environnement de travail Citrix associe une technologie de virtualisation Citrix à d'autres fonctionnalités, notamment la gestion unifiée des terminaux (UEM), la synchronisation et le partage des fichiers d'entreprise (EFSS), la passerelle d'accès sécurisé au réseau et l'analytique pour une supervision intelligente de la sécurité et de la performance applicative.

Gestion unifiée des terminaux (UEM)

L'UEM de Citrix permet aux organisations informatiques d'administrer plus facilement leurs environnements de travail mobiles en pleine croissance. Cette solution fournit une gestion centralisée sur plusieurs plateformes et appareils, notamment les postes de travail, les ordinateurs portables, les smartphones, les tablettes, les appareils IoT et autres clients légers tels que Google Chromebook. De plus, Citrix vous permet d'administrer non seulement des applications mobiles, mais aussi des applications modernes. Seule la gestion unifiée des terminaux de Citrix donne accès à des fonctionnalités qui ajoutent de la valeur à Microsoft EMS/Intune, y compris micro-VPN pour O365. Vous pourrez conserver des données chiffrées sur des appareils mobiles, réduisant ainsi le problème de la disparition du périmètre de sécurité digital.

Fonctionnalités principales de l'UEM de Citrix :

- Gestion des appareils mobiles (MDM) sur des plateformes populaires (notamment Windows 10, iOS, Android, MacOS et IoT)
- Gestion flexible des applications mobiles (MAM) avec prise en charge des plateformes MAM (telles que les applications gérées par iOS, Samsung KNOX, la communauté AppConfig, la Protection des informations Windows) ; Citrix MAM avec la technologie MDX qui fournit un second niveau de chiffrement des applications sans enregistrement des appareils ; prise en charge de Intune MAM pour protéger O365
- Applications sécurisées de productivité de niveau professionnel, y compris Secure Mail et Secure Web

•Gestion du contenu mobile (MCM), y compris la technologie de partage et de synchronisation des fichiers de Citrix, intégrée à Secure Mail, qui permet à vos collaborateurs d'accéder de n'importe où à leurs fichiers de travail en cliquant sur un lien dans leurs emails et qui évite aux utilisateurs de devoir envoyer des pièces jointes

•Gestion des identités (IDM) avec prise en charge de l'authentification à 2 facteurs et de l'authentification Single Sign-On (SSO) pour toutes les applications (mobiles, virtuelles, SaaS, web) via un App store personnalisable

•Sécurité de la passerelle d'accès au réseau avec une micro-application VPN unique qui réduit le risque d'accès non autorisé à votre réseau

Synchronisation et partage de fichiers d'entreprise (EFSS)

Tandis que la virtualisation d'applications et de postes de travail permet aux utilisateurs d'accéder à leurs fichiers depuis des applications virtuelles, comme indiqué précédemment, un nombre croissant d'utilisateurs adoptent des applications modernes et ont donc besoin d'une solution sécurisée et complète pour accéder à leurs fichiers, quel que soit le type d'application et l'endroit où elle est stockée. L'EFSS de Citrix vient compléter la virtualisation des applications et des postes de travail dans le cadre d'un environnement de travail digital complet.

L'EFSS de Citrix propose :

- Un accès aux données depuis tout endroit et tout appareil via des outils et des applications de synchronisation des données
- Un accès sécurisé aux données au sein du réseau, y compris sur SharePoint et les lecteurs réseau
- Une expérience utilisateur fluide et conviviale, intégrant notamment le plug-in Microsoft Outlook®, Windows Explorer et Mac Finder ; une grande capacité de stockage (jusqu'à 100 Go) ; un éditeur de contenu mobile intégré
- Le contrôle sur l'endroit où résident les données, via StorageZones et StorageZone Connectors pour SharePoint et les lecteurs réseau, offrant aux équipes informatiques la flexibilité et le contrôle nécessaires pour stocker les données aux endroits qui répondent au mieux aux prérequis en matière de conformité réglementaire, de stratégie informatique et d'infrastructure

- Une gestion et une sécurité centralisées, y compris de solides fonctionnalités de création de rapports et de notification, ainsi qu'une intégration DLP

- Des stratégies de sécurité des appareils natifs afin d'étendre la sécurité aux terminaux

- Une synchronisation à la demande pour les postes virtuels

Citrix Unified Gateway

De plus en plus de types d'appareils et d'applications étant utilisés, l'accès distant peut aisément devenir très complexe pour les équipes informatiques, avec une multitude de nouveaux produits ponctuels pour différents appareils, modèles de propriété, réseaux et applications. Les équipes informatiques doivent consolider et simplifier l'infrastructure d'accès distant, tout en proposant aux utilisateurs un moyen simple d'accéder à leurs applications, quel que soit l'appareil qu'ils utilisent.

Citrix Unified Gateway fournit un accès distant depuis n'importe quel type d'appareil vers des environnements virtualisés, un accès distant SSL basé sur VPN vers des applications d'entreprise, des applications web et des services SaaS, et l'intégration de l'accès sécurisé aux appareils mobiles dans la gestion unifiée des terminaux de Citrix.

Citrix Unified Gateway propose également :

- Une URL pour accéder à toute application en utilisant tout type d'appareil fournissant un accès sécurisé unifié
- Des fonctionnalités micro-VPN avec l'UEM de Citrix pour un accès sécurisé aux appareils mobiles
- Une expérience applicative haute performance stable sur n'importe quel réseau
- Single Sign-On sur les applications virtuelles, mobiles, web et SaaS
- Une authentification multifacteur, un contrôle de bout en bout pour l'ensemble du trafic applicatif et un contrôle d'accès contextuel

Citrix Analytics

En utilisant une large gamme d'algorithmes de machine learning, Citrix Analytics fournit une sécurité contextuelle : il met en corrélation et analyse des données multiproduits pour détecter et isoler des activités utilisateur à risque, que celles-ci proviennent d'un collaborateur interne ou d'un pirate externe malveillant.

Ces activités utilisateur à risque sont combinées pour créer un profil de risque global pour l'utilisateur. Une fois que les activités utilisateur à risque sont identifiées, Citrix Analytics applique différents contrôles granulaires pour réduire ou supprimer totalement la menace, notamment en autorisant l'authentification multifacteur, en enregistrant des sessions utilisateur, en paramétrant des seuils d'accès aux données plus stricts, en bloquant les applications suspectes voire en mettant en quarantaine certains utilisateurs.

Citrix Analytics fournit :

- Une analytique de la sécurité basée sur le comportement de l'utilisateur en associant l'analytique de la sécurité des accès, l'analytique de la sécurité des applications et l'analytique de la sécurité des données
- Une analytique de la performance et des opérations pour suivre l'usage, contrôler la performance et mettre en avant les problèmes et leur origine
- Il opère en temps réel en circuit fermé en modifiant les politiques produit pour réduire les menaces
- Il fonctionne sur site, dans un cloud public ou dans des environnements hybrides

Par où commencer

De nombreux clients Citrix entreprennent de passer à un environnement de travail digital via une mise en œuvre progressive axée sur des catégories d'utilisateurs et des scénarios d'utilisation pour leurs collaborateurs mobiles. Il vous faudra également identifier les workflows et les scénarios d'utilisation clés. Envisagez ces différentes questions du point de vue des utilisateurs, de leurs besoins, préférences et modes de travail, avec différents types d'appareils, d'applications et de réseaux. Votre évaluation devra aussi inclure les exigences de l'entreprise en matière de sécurité et de conformité. Il se peut que beaucoup de ces scénarios d'utilisation soient liés à des projets en cours tels que la migration vers Windows 10 ou l'adoption de O365.

Créez ensuite une solution conceptuelle établissant l'expérience utilisateur et les workflows proposés. Concentrez-vous d'abord sur les objectifs à portée de main qui permettent d'obtenir des résultats rapides comme l'adoption de l'UEM de Citrix pour administrer aussi bien des appareils Windows 10 et des applications modernes que d'autres appareils et applications. Vous pouvez également ajouter l'EFSS de Citrix pour prendre en charge le partage de fichiers importants et réduire la perte de données.

Votre preuve de concept doit inclure des représentants de chaque division opérationnelle, afin d'assurer le respect de l'ensemble des prérequis. Mettez en œuvre votre solution sur site, dans le cloud ou de manière hybride selon une approche progressive basée sur les catégories d'utilisateurs et les cas d'utilisation que vous avez identifiés.

Conclusion

L'augmentation des modes de travail mobiles et des applications modernes et la disparition du périmètre digital posent des défis qui ne peuvent pas être relevés par la virtualisation ou une approche technologique fragmentaire impliquant plusieurs fournisseurs. Seule une solution complète et unifiée d'environnements de travail mobiles peut permettre aux utilisateurs d'être pleinement productifs sur tout appareil, avec toute application, en offrant l'expérience de qualité qu'ils exigent et la sécurité requise par les équipes informatiques.

Un environnement de travail complet qui prend en charge intégralement la mobilité permet de rationaliser et de simplifier les tâches des équipes informatiques. Travailler avec un fournisseur unique pour un environnement de travail digital mobile complet permet de gagner du temps, réduit les besoins en formation du personnel, simplifie le support technique, diminue les coûts globaux et offre aux utilisateurs une expérience fluide et conviviale. Pour améliorer son implication et sa productivité, le collaborateur a besoin d'un environnement de travail digital basé sur le contexte, fiable et suffisamment intelligent pour proposer un accès, une vision et une performance adaptés au travail à accomplir.

Avec Citrix Workspace, les entreprises peuvent surmonter les problèmes de sécurité et de gestion, proposer un riche éventail d'applications de productivité mobile de niveau professionnel, permettre le partage de fichiers sécurisé sur n'importe quel appareil et offrir une expérience fluide au travers d'une solution globale unique. En mettant progressivement en œuvre Citrix Workspace sur la base de vos scénarios d'utilisation les plus importants, vous pourrez effectuer la transition vers la mise à disposition d'un environnement de travail digital tout en apportant une valeur ajoutée optimale à votre entreprise.

Étapes suivantes

[En savoir plus sur Citrix Workspace](#)

[Évoluez vers Citrix Workspace pour faire des économies](#)

Sources

¹ Gallup : State of the American Workplace, 2017



Ventes aux entreprises

Amérique du Nord | +1 800 424 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

© 2018 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).