

# De l'infrastructure sur site au cloud

## Un voyage vers le service Workspace

Favorisez un travail flexible et sécurisé pour tout type de collaborateur avec les services Citrix Workspace.

# Sommaire

<b>Synthèse</b> .....	<b>3</b>
<b>Le passé : des déploiements sur site traditionnels</b> .....	<b>4</b>
<b>Le présent : un état fragmenté</b> .....	<b>6</b>
<b>Le futur : devenir favorable au cloud</b> .....	<b>8</b>
Étape 1 : utilisez l'expérience Citrix Workspace avec Virtual Apps and Desktops et Analytics .....	11
Étape 2 : fournissez un accès « zero-trust » et intégrez le SSO aux applications .....	12
Étape 3 : unifiez, sécurisez et digitalisez les contenus des utilisateurs et les workflows de documents .....	13
Étape 4 : rationalisez les workflows courants avec des microapplications .....	14
Étape 5 : consolidez la gestion et protégez l'accès aux appareils .....	15
<b>Conclusion</b> .....	<b>16</b>
<b>Index</b> .....	<b>17</b>

## Synthèse

La récente pandémie mondiale nous a obligés à envisager un nouveau mode de télétravail, et les prévisions post-COVID suggèrent des stratégies et des environnements plus flexibles en matière de lieu de travail. Une étude Gartner révèle que 48 % des collaborateurs continueront à télétravailler au moins à temps partiel lorsque les bureaux rouvriront.<sup>1</sup>

Les équipes IT continuent de prouver leur résilience en rendant le télétravail possible tandis que le déploiement sur site traditionnel des applications et postes de travail virtuels atteint ses limites physiques en termes de capacités. Une enquête LogicMonitor Cloud 2025 révèle que 87 % des entreprises accéléreront leur migration vers le cloud dans un futur proche.<sup>2</sup>

Citrix Workspace, avec des fonctionnalités et des capacités étendues intelligentes, aide votre équipe IT à proposer des expériences optimales à tous les collaborateurs, au bureau, au domicile ou en déplacement. Offrez-leur un accès sécurisé aux applications, fichiers et données, tout ce dont les collaborateurs ont besoin pour booster leur productivité, où et quand ils en ont besoin, le tout pris en charge depuis votre infrastructure existante.

Dans ce livre blanc, nous vous guiderons à travers le paysage passé, présent et futur du Workspace. Vous découvrirez les étapes successives et pratiques qui vous permettront de mettre à l'échelle votre déploiement Workspace pour qu'il soit toujours prêt à proposer, en toute fluidité, le travail du futur.

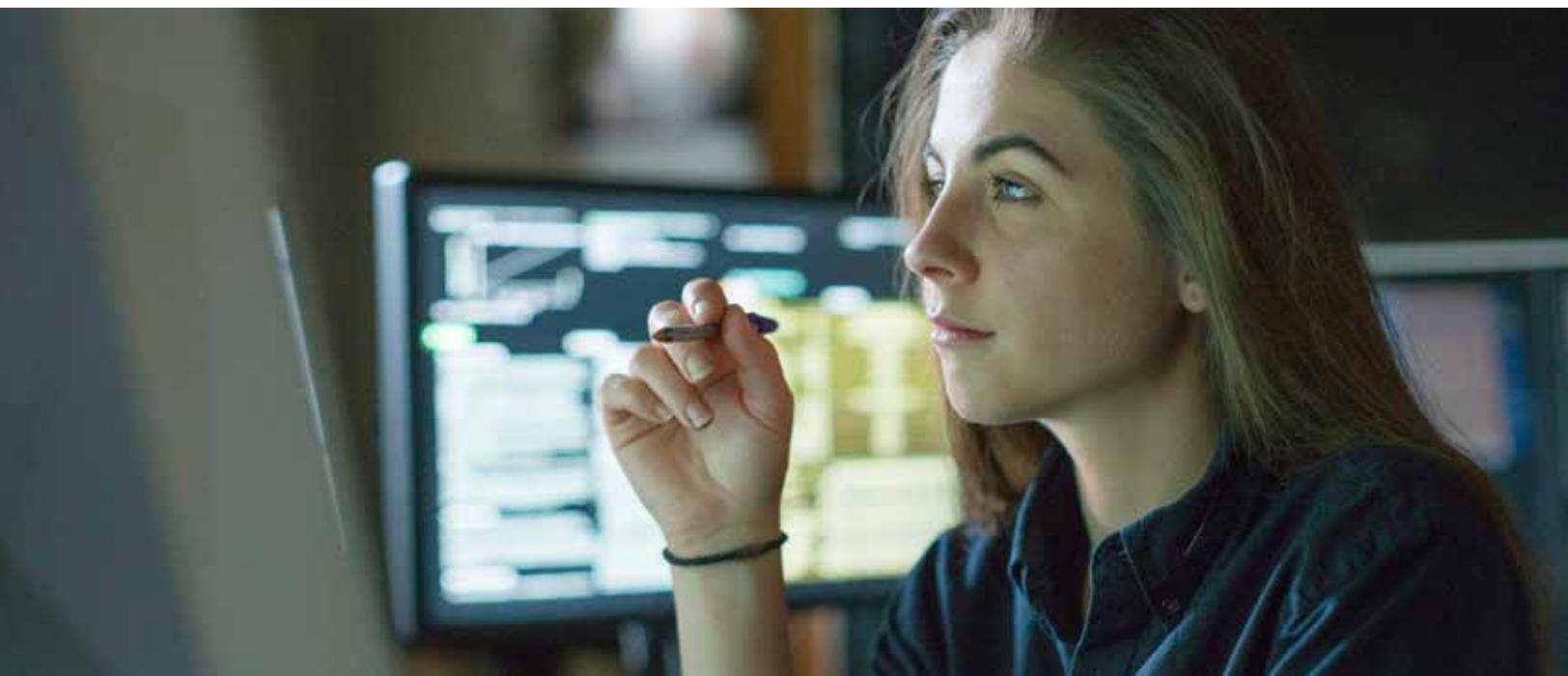
Lors de cette transition, vous pouvez compter à tout moment sur 3 valeurs métier essentielles :

- ✓ Time-to-value plus rapide : déployez des charges de travail jusqu'à 4 fois plus rapidement depuis n'importe quel cloud, datacenter sur site ou modèle hybride.<sup>3</sup> Simplifiez l'intégration d'utilisateurs en cas de fusions et d'acquisitions, de nouvelles embauches, pour les sous-traitants et une multitude de cas d'utilisation stratégiques.
- ✓ Déploiement flexible : adoptez des clouds publics à votre propre rythme, prenez en charge de nouvelles charges de travail et étendez votre continuité d'activité, ou bien accélérez votre passage au cloud selon vos besoins. Transférez des déploiements sur site vers des sites de ressources hybrides/cloud dans un délai adapté aux besoins métier.
- ✓ Simplifiez la gestion, la sécurité et la continuité d'activité : les services cloud intégrés simplifient la gestion des ressources sur site et hébergées dans le cloud. Réduisez vos coûts de cloud public jusqu'à 80 %, rationalisez la planification de la continuité d'activité et de la reprise après sinistre et sécurisez la propriété intellectuelle sensible.<sup>3</sup>

Sources : <sup>1</sup><https://www.gartner.com/smarterwithgartner/9-future-of-work-trends-post-covid-19/>

<sup>2</sup><https://www.logicmonitor.com/resource/cloud-2025>

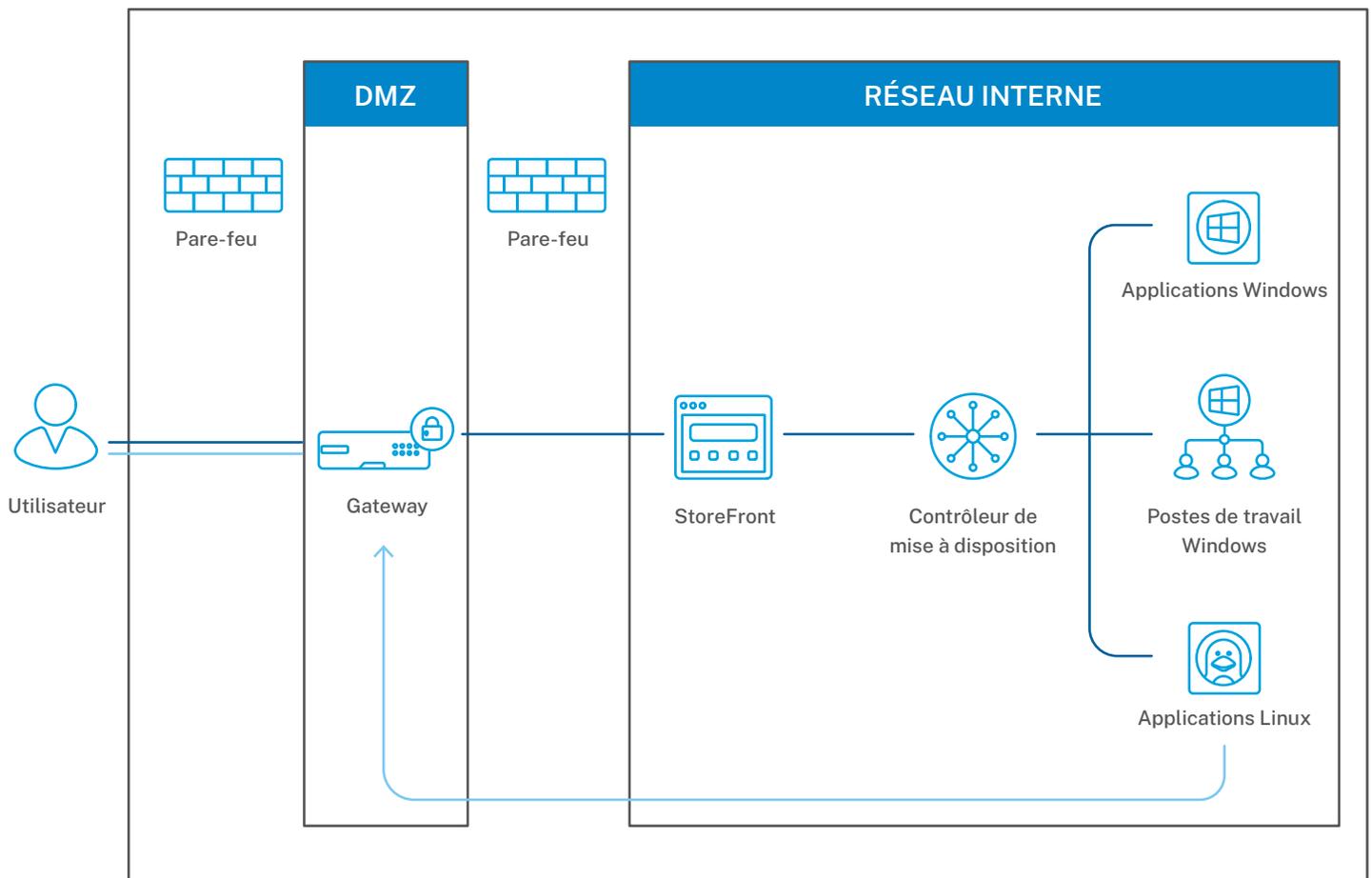
<sup>3</sup> Citrix, La valeur métier du service Citrix Virtual App and Desktop [Livre blanc](#)



## Le passé : des déploiements sur site traditionnels

Alors qu'une transition majeure est en cours dans la façon dont les entreprises favorisent l'accès à un nombre croissant d'applications et de contenus, il est utile de revenir dans le passé pour se rappeler ce qu'est un environnement PC traditionnel. À l'époque, les administrateurs IT géraient de façon centralisée la mise à disposition d'applications

et de postes de travail. Tandis que les applications et postes de travail virtuels devenaient peu à peu la norme, ils étaient déployés dans un datacenter sur site. L'IT devait alors batailler avec les principaux composants de mise à disposition et l'infrastructure associée hébergeant les applications et les postes de travail.



Sur site (géré par l'IT)

Les caractéristiques d'un Workspace sur site peuvent encore peser sur de nombreuses entreprises dans un monde de plus en plus basé dans le cloud. Voici à quoi ressemblait ce modèle :

- ✓ Les collaborateurs exécutaient toutes leurs tâches professionnelles depuis un unique appareil
- ✓ Tous les contenus étaient une combinaison de stockage local et réseau
- ✓ Les applications professionnelles étaient majoritairement basées sur Windows
- ✓ Il était demandé à tous les utilisateurs d'être présents physiquement

L'ampleur de la tâche était intimidante. Les mises à jour fréquentes, les mises à niveau d'appareils et les correctifs étaient synonymes de nuits et week-ends harassants pour les équipes qui devaient relever le défi du modèle sur site. Tandis que l'avantage était le contrôle de l'accès, les machines virtuelles, les applications, les postes de travail et la sécurité, ce modèle mettait à mal l'efficacité et les coûts.

L'expérience utilisateur était souvent dictée par l'unique appareil disponible pour chaque collaborateur. Avec l'émergence des appareils mobiles, il a été demandé aux collaborateurs de s'adapter à un Workspace spécifique aux mobiles. Alors que plusieurs appareils devenaient nécessaires pour chaque collaborateur, les Workspaces ont continué à se fragmenter, chaque appareil poursuivant son propre chemin pour des collaborateurs fatigués.

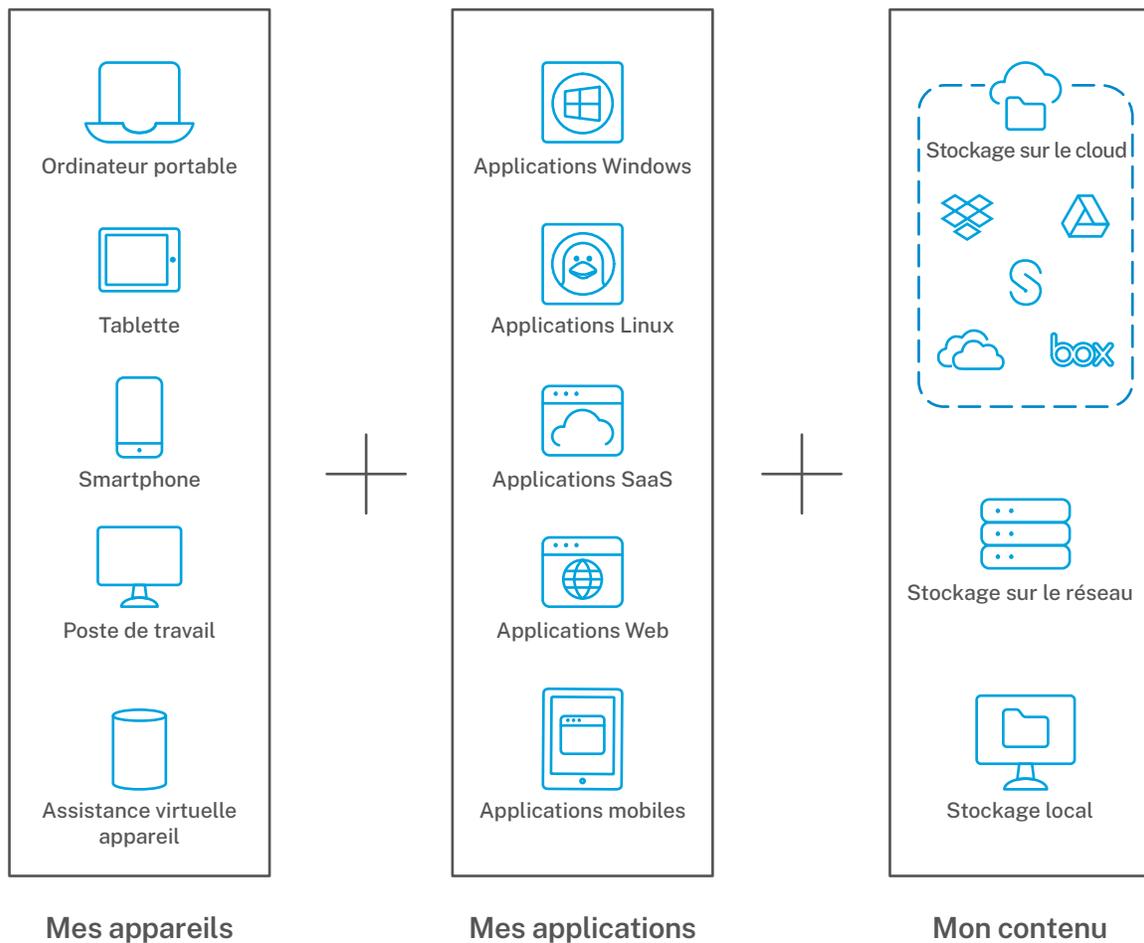
Le besoin d'unifier l'expérience collaborateur et de créer un modèle facile à gérer par les équipes IT a entraîné la création des services Citrix Workspace. En favorisant une architecture basée dans le cloud, les entreprises sont capables de connecter parfaitement des ressources et de fournir **une valeur plus immédiate, la flexibilité, l'agilité** ainsi qu'une **gestion et une sécurité simplifiées**.



## Le présent : un état fragmenté

Dans presque tous les secteurs, l'année 2020 a exigé des entreprises qu'elles adaptent le traditionnel modèle sur site pour se tourner vers un nouveau qui permette majoritairement le travail à distance, exerçant une pression sur la flexibilité et la sécurité de l'infrastructure. Les plans stratégiques à long terme visant à migrer les Workspaces hérités (legacy) dans le cloud sont soudain devenus des courses contre la montre pour garantir la continuité d'activité, la sécurité des données et la productivité des collaborateurs.

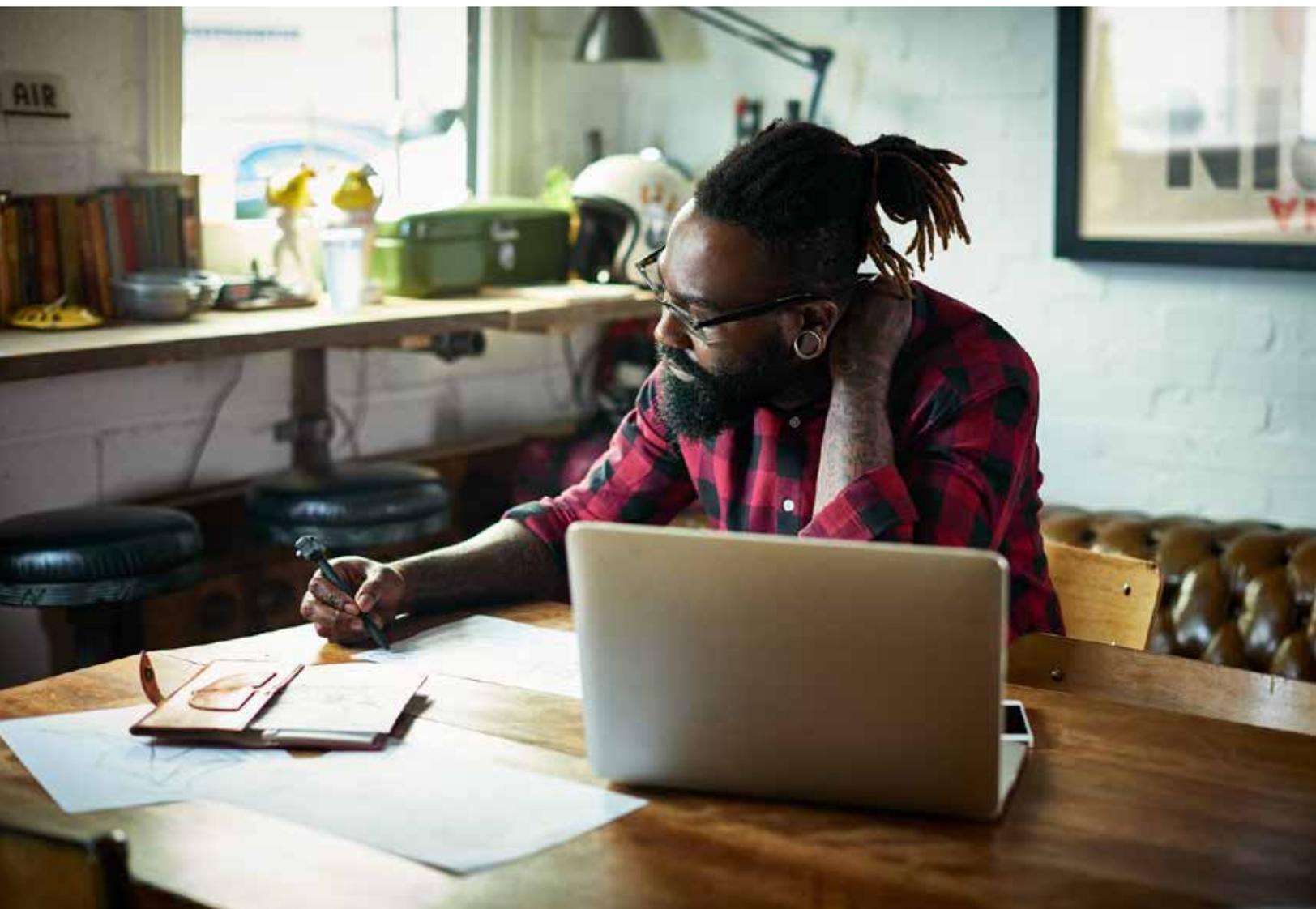
L'environnement Workspace d'aujourd'hui a évolué vers un ensemble inextricable d'appareils et d'applications pour chaque utilisateur, ce qui complique l'accès et la sécurité sur l'ensemble de l'entreprise.



Les VPN, autrefois points d'entrée des grands voyageurs d'une entreprise, ont également atteint leurs limites avec les télétravailleurs, qui deviennent rapidement flexibles et qui génèrent une augmentation exponentielle de nombre de points de terminaison. Les risques de sécurité entraînent l'ajout sans fin de produits unitaires, tels que le VPN SSL, le SSO (Single Sign-On) et la gestion des terminaux, pour rester en phase avec les nouveaux scénarios de sécurité.

Avec les télétravailleurs et les collaborateurs sous contrat qui doivent s'appuyer sur leurs propres appareils, le déferlement du BYOD ne fait qu'ajouter encore à la complexité. Un cadre de sécurité contextuel, avec authentification et vérification continues, est la route à suivre pour autoriser l'accès au nombre croissant d'applications web et SaaS dont les collaborateurs ont besoin pour travailler. Un modèle de sécurité « zero-trust » fournit un accès partiel à votre réseau, selon les besoins, tout en surveillant les comportements utilisateur aberrants.

Le défi des fournisseurs de technologie et des équipes IT consiste désormais à unifier et simplifier les environnements et les expériences. Les nouveaux collaborateurs ont l'habitude d'interactions digitales simples et puissantes et, du point de vue de la géralité, les équipes IT pourraient apprécier d'être moins dispersées. Tout cela est réuni dans les services Citrix Workspace.

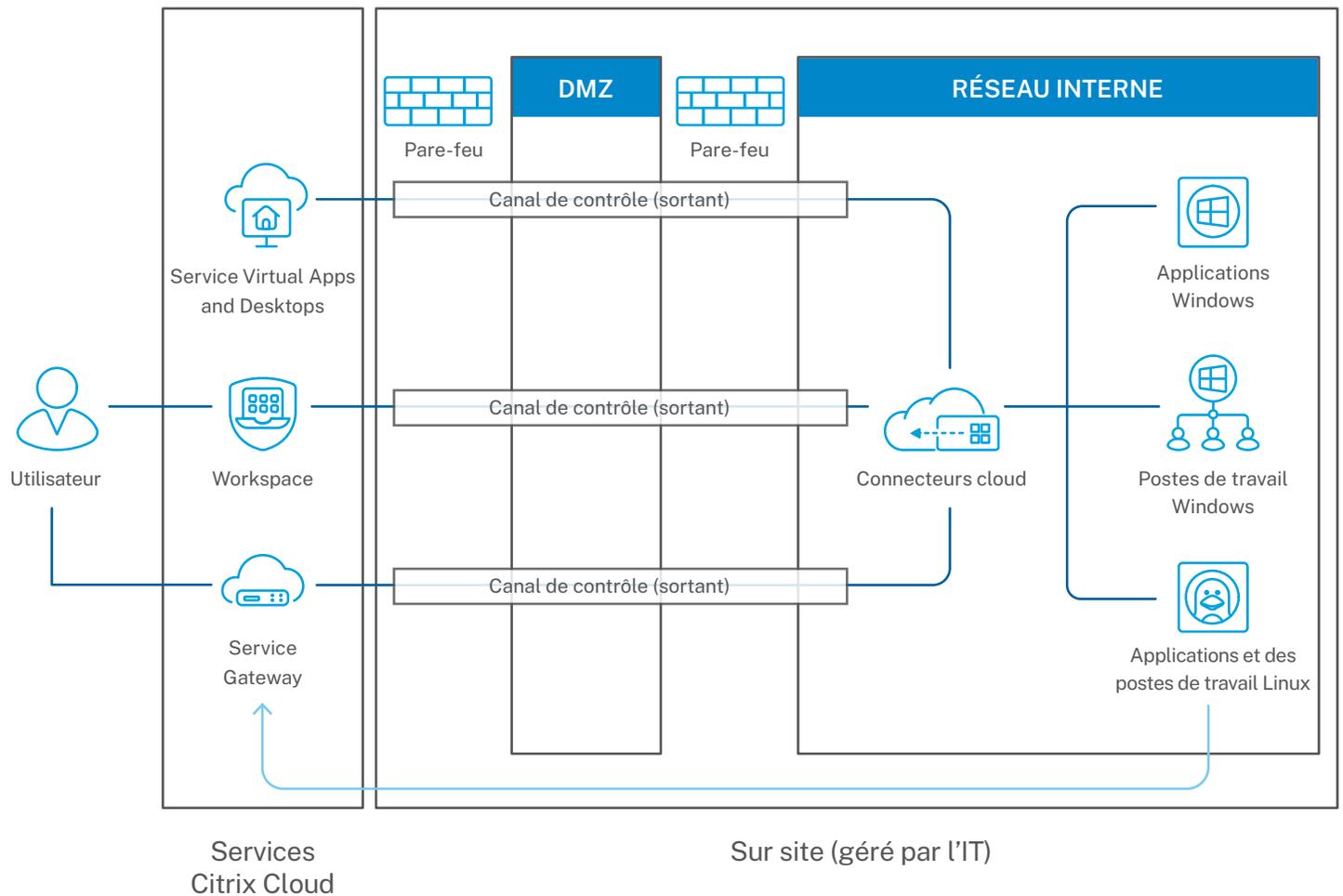


## Le futur : devenir favorable au cloud

Les Workspaces idéaux :

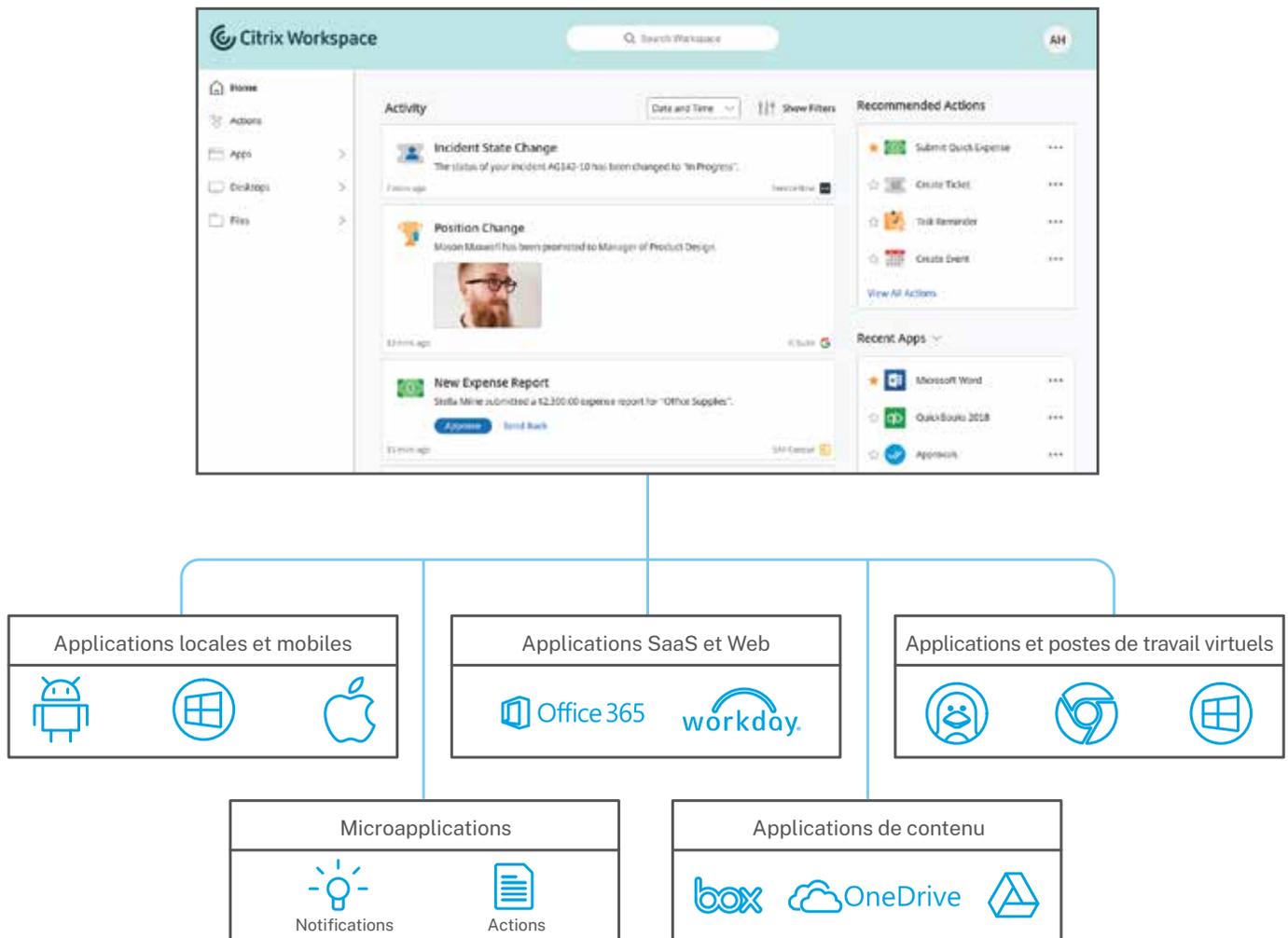
- ✓ Une technologie unifiée et simplifiée
- ✓ Une expérience utilisateur fiable, homogène et optimale sur tous les appareils
- ✓ Une sécurité renforcée sensible au contexte
- ✓ Une productivité optimisée pour tout type de collaborateur

Avec l'émergence des applications et des contenus basés dans le cloud, migrer depuis un modèle strictement sur site est une priorité dans la plupart des entreprises. Déplacer la couche de gestion de votre déploiement Citrix Virtual Apps and Desktops vers le service cloud de Citrix réduit la complexité de l'installation, de la configuration, de la gestion des mises à niveau et des intégrations.



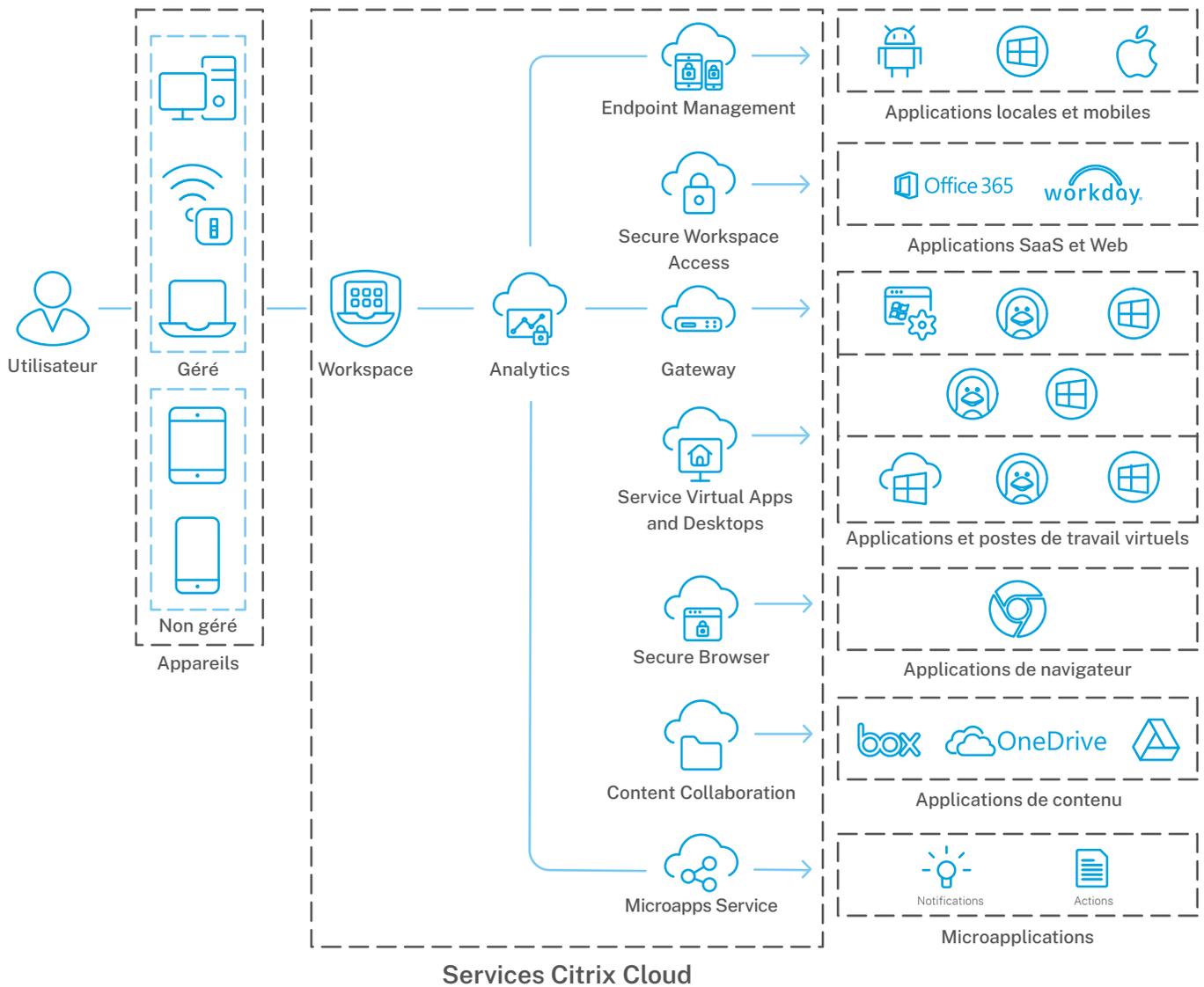
Avec les services Citrix Virtual App and Desktop, vous pouvez avoir des sites de ressources sur site ou hébergés dans le cloud, ce qui vous permet de gérer en toute sécurité vos applications, données et fichiers hérités (legacy), sans la complexité de la configuration d'une infrastructure. Aujourd'hui, vos équipes IT peuvent se concentrer sur les ressources qui apportent le plus de valeur à vos utilisateurs.

L'utilisateur, lui, bénéficie d'une expérience unifiée, simplifiée et homogène sur tous les appareils. Citrix Workspace met à disposition des applications et des fichiers locaux SaaS, web, mobiles, de navigateur et de contenu, le tout dans une interface utilisateur simplifiée, priorisée et personnalisée pour chaque collaborateur. De plus, cette expérience optimale, et optimisée en permanence, reste la même que les collaborateurs se trouvent à la maison, en déplacement ou au bureau.



Avec le travail du futur devant nous, un niveau reste encore à franchir : une plateforme Workspace unifiée qui simplifie les environnements et propose le chemin le plus rapide possible vers le ROI et la réalisation d'une valeur métier. Sécuriser et favoriser des collaborateurs de plus en plus mobiles et pérenniser votre entreprise est essentiel : entrez dans Citrix Workspace.

Optimiser l'expérience utilisateur, notamment en créant un environnement sécurisé et facile à gérer qui se met à l'échelle dynamiquement en fonction des besoins du travail du futur, commence en concrétisant les étapes suivantes pour tirer le meilleur parti de ce que Workspace peut faire pour vos équipes IT, vos collaborateurs et votre entreprise.



## Étape 1 : utilisez l'expérience Citrix Workspace avec Virtual Apps and Desktops et Analytics

Proposez une expérience utilisateur unifiée et intéressante en regroupant les applications sur site et hébergées dans le cloud ainsi que les postes de travail dans une identité consolidée avec Citrix Workspace.

### Les avantages pour l'IT :

- ✓ Service Cloud, qui fournit un accès distant aux postes de travail, applications et navigateurs virtuels
- ✓ Intégration de fournisseurs d'identité
- ✓ Agrégation de sites, qui intègre les déploiements CVAD existants
- ✓ Connectivité sécurisée et optimisée vers des ressources backend
- ✓ Surveillance du comportement des utilisateurs et des appareils et analyse des risques
- ✓ Surveillance proactive des performances et capacité à isoler les causes profondes et à les traiter avant la dégradation de l'expérience
- ✓ Mise à jour automatique durable et fluide et gestion centralisée
- ✓ Intégration efficace d'utilisateurs
- ✓ Flexibilité cloud hybride
- ✓ Mise à l'échelle automatique des ressources cloud pour maîtriser les coûts

- ✓ Réduction des frais de gestion
- ✓ Suppression de la nécessité d'utiliser un contrôleur de mise à disposition sur site, un serveur de licences et un serveur SQL

### Fonctionnalités supplémentaires :

- ✓ Fourniture d'une expérience de Digital Workspace unifiée pour les utilisateurs, avec la possibilité de choisir n'importe quel appareil et réseau pour accéder aux applications d'entreprise, postes de travail et données dans un environnement virtualisé
- ✓ Expérience homogène sur tous les appareils
- ✓ Détection et prévention des menaces internes avec l'analytique du comportement des utilisateurs
- ✓ Optimisation de l'expérience utilisateur avec l'analytique des performances

### Valeur métier :

- ✓ Réduction des frais généraux et maîtrise des coûts
- ✓ Augmentation du time-to-value des utilisateurs grâce à une intégration plus rapide
- ✓ Amélioration de l'expérience générale, qui participe à l'amélioration de l'expérience technologique des collaborateurs
- ✓ Passer au service Citrix Virtual App and Desktop accélère l'adoption de nouvelles fonctionnalités, ce qui augmente le chiffre d'affaires et la productivité et permet aux entreprises de répondre plus rapidement aux besoins stratégiques

### Stoppez les failles de sécurité avant qu'elles n'arrivent :

- ✓ 34 % impliquent des acteurs internes<sup>1</sup>
- ✓ 20 % sont causées par des erreurs d'utilisateurs<sup>1</sup>

Source : <sup>1</sup><https://enterprise.verizon.com/resources/executive-briefs/2019-dbir-executive-brief.pdf>

**« Ce n'est pas le moment de réduire nos efforts de développement des collaborateurs mais plutôt de renforcer nos engagements pour la création de collaborateurs résilients capables de s'adapter face à des changements constants. »**

## Étape 2 : fournissez un accès « zero-trust » et intégrez le SSO aux applications

Avec une identité consolidée de vos applications sur site, votre prochaine étape consiste à sécuriser vos applications web et SaaS.

### Les avantages pour l'IT :

- ✓ Accès cloud natif sans VPN aux applications SaaS et web et sécurité renforcée
- ✓ Mise en œuvre de contrôles de sécurité renforcés pour accéder aux données dans les applications SaaS et web
- ✓ Empêche les utilisateurs d'accéder à des sites web malveillants et non-approuvés
- ✓ Des navigateurs isolés intégrés apportent la flexibilité d'utiliser des appareils BYO pour accéder de façon sécurisée à des applications approuvées
- ✓ Protège les utilisateurs et les données d'entreprise contre le vol par des malwares de capture d'écran et d'enregistrement des saisies clavier

### Fonctionnalités supplémentaires :

- ✓ Isolation web et navigation sécurisée
- ✓ Single Sign-On (SSO) avec authentification deux facteurs pour les applications SaaS/web/virtuelles
- ✓ Amélioration des stratégies de sécurité autour des applications SaaS/web avec notamment la restriction de l'accès aux blocs-notes, de l'impression et des téléchargements et l'affichage de filigranes
- ✓ Stratégies d'accès sécurisé contextuelles et centralisées pour toutes les applications

### Valeur métier :

- ✓ Économies réalisées sur les tickets de support grâce au SSO : 5 401 260 \$<sup>1</sup>
- ✓ Augmentation de la productivité par application et par mois en raison d'un déploiement plus rapide des applications : valeur estimée entre 900 000 et 3 250 000 \$<sup>1</sup>

Source : <sup>1</sup> <https://www.citrix.com/content/dam/citrix/fr-fr/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf>



## Étape 3 : unifiez, sécurisez et digitalisez les contenus des utilisateurs et les workflows de documents

Stimulez la productivité en permettant aux collaborateurs d'accéder de façon sécurisée aux données depuis n'importe quelle source, sur n'importe quel appareil, tout en automatisant les workflows de documents pour solliciter des feedbacks et envoyer des approbations avec une signature électronique intégrée. Le tout en supprimant les menaces liées aux services de sauvegarde de fichiers et en protégeant les données avec des fonctionnalités robustes.

### Avantages :

- ✓ Fourniture d'une expérience de contenu de type grand public sur tous les appareils sans avoir besoin de migrer des données dans le cloud
- ✓ Unification de répertoires disparates
- ✓ Suppression des menaces posées par le partage de fichiers entre collaborateurs et fourniture d'un ensemble complet de fonctionnalités de protection des données

### Fonctionnalités supplémentaires :

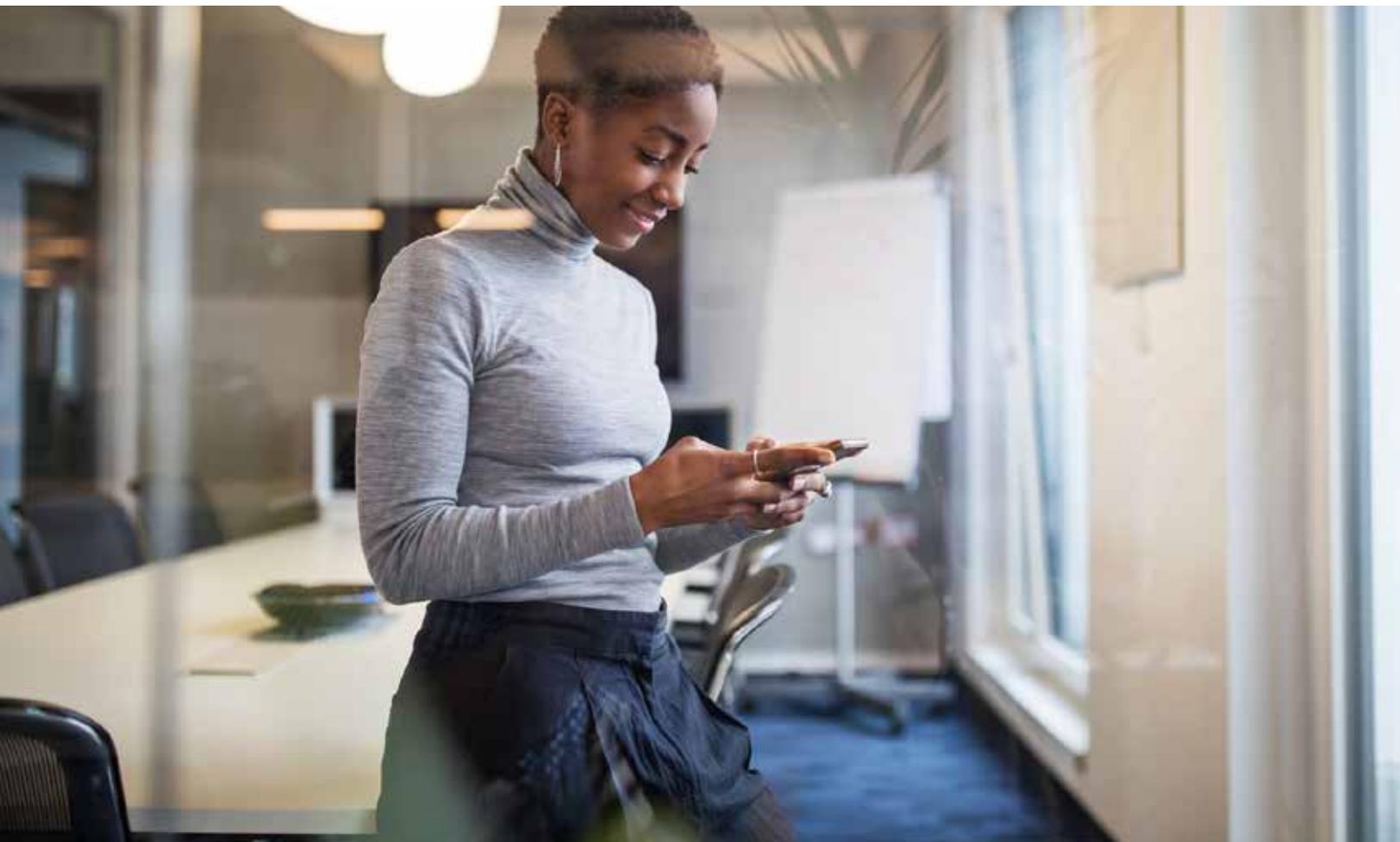
- ✓ Capacité à chercher sur les différents fichiers et applications
- ✓ Intégration d'applications mobiles
- ✓ SSO pour toutes les applications mobiles
- ✓ Intégration de fichiers et d'applications
- ✓ Workflows de contenus

### Valeur métier :

- ✓ Digitalisation des workflows avec une augmentation de l'efficacité de 20 % ou plus
- ✓ Coûts des incidents de sécurité par collaborateur : 7 938 \$<sup>1</sup>
- ✓ 27 % des enregistrements sont compromis chaque année avec un coût de 150 \$ par enregistrement<sup>2</sup>

Sources : <sup>1</sup><https://www.citrix.com/content/dam/citrix/fr-fr/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf>

<sup>2</sup><https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/>



## Étape 4 : rationalisez les workflows courants avec des microapplications

Créez des workflows orientés action pour les utilisateurs pris par le temps avec des microapplications à faible codage à partir d'applications héritées (legacy), sur site et SaaS. Les administrateurs configurent, construisent et modernisent des microapplications personnalisées directement depuis la console Citrix Cloud, favorisant et se concentrant sur des tâches selon un flux personnalisé et fluide et supprimant les pertes de temps résultant de la commutation de contexte.

### Des microapplications intelligentes

Les applications sont puissantes mais peuvent être encombrantes pour les tâches simples ou de routine. En utilisant des API publiquement disponibles dans des applications SaaS, web, héritées (legacy) et « développées en interne », les microapplications permettent aux utilisateurs de visualiser des informations et d'exécuter des actions sans nécessiter le lancement complet d'une application. Un flux de Workspace personnalisé et simplifié offre aux utilisateurs un site central pour réaliser ces actions, éliminant ainsi la commutation de contexte contre-productive.

### Avantages :

- ✓ Modernisation des applications par la fourniture d'actions et de notifications clés dans une interface utilisateur simple et personnalisée
- ✓ Donne à l'IT la capacité à fournir la meilleure expérience de Digital Workspace, avec des outils intégrés à faible codage ainsi que des intégrations faciles à utiliser pour les applications et l'intégration des fournisseurs d'identité. Provisioning, gestion et surveillance de toute l'infrastructure

- ✓ Workspace via une unique console de gestion
- ✓ Réduction de la formation sur les nouvelles applications et fonctionnalités grâce à l'utilisation de microapplications
- ✓ Conception de workflows pour toutes les applications, web, SaaS et sur site

### Fonctionnalités supplémentaires :

- ✓ Flux d'activité, y compris des actions et notifications sur des applications SaaS/sur site
- ✓ Intégration de MS Teams
- ✓ Outil de création de microapplications

### Valeur métier :

- ✓ Les collaborateurs peuvent économiser jusqu'à 4 heures/semaine<sup>1</sup>
- ✓ 18 % de gains de productivité pour des collaborateurs totalement engagés<sup>2</sup>
- ✓ Multiplication par 2,5 du chiffre d'affaires par collaborateur par rapport aux concurrents avec un engagement faible<sup>3</sup>
- ✓ Rentabilité par collaborateur de 21 % plus élevée que celle des entreprises de quartile inférieur<sup>4</sup>
- ✓ Les services d'aide coûtent 50 \$/ticket avec une moyenne de 6 appels par collaborateur et par an<sup>2</sup>

Sources : <sup>1</sup>McKinsey Insights

<sup>2</sup><https://www.citrix.com/content/dam/citrix/fr-fr/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf>

<sup>3</sup>Hay Group

<sup>4</sup>Gallup



## Étape 5 : consolidez la gestion et protégez l'accès aux appareils

Gérez, sécurisez et répertoriez une large gamme d'appareils depuis une unique console de gestion.

### Avantages :

- ✔ Utilisez un ensemble commun de stratégies d'appareils pour gérer les appareils pris en charge.
- ✔ Protégez les informations métier avec une sécurité stricte pour l'identité, les appareils BYO et d'entreprise, les applications, les données et les réseaux. Spécifiez des identités utilisateur disponibles pour authentifier les appareils. Configurez la façon dont vous séparez les données personnelles et d'entreprise sur les appareils.
- ✔ Mettez à disposition des utilisateurs n'importe quelle application, quel que soit l'appareil ou le système d'exploitation utilisé. Protégez vos informations au niveau applicatif et gardez une gestion des applications mobiles d'entreprise de niveau professionnel.
- ✔ Utilisez le provisioning et le contrôle des configurations pour paramétrer des appareils. Ces contrôles comprennent l'enregistrement d'appareils, l'application de stratégies et des privilèges d'accès.
- ✔ Utilisez des contrôles de sécurité et de conformité pour créer une base de sécurité personnalisée avec des déclencheurs actionnables. Par exemple, verrouillez, supprimez ou notifiez un appareil qui enfreint des normes de conformité définies.
- ✔ Utilisez les contrôles de mise à jour du système d'exploitation pour prévenir ou renforcer les mises à jour des systèmes d'exploitation. Cette fonctionnalité est essentielle pour la

prévention contre la perte de données par rapport à des vulnérabilités ciblées du système d'exploitation.

### Fonctionnalités supplémentaires :

- ✔ Prise en charge de nombreux scénarios d'utilisation avec un unique déploiement (profils d'enregistrement améliorés)
- ✔ Prise en charge complète de Android Enterprise
- ✔ Impulsion stratégique unique vers des appareils spécifiques pour la configuration utilisateur
- ✔ Prise en charge de stratégies supplémentaires pour macOS
- ✔ Groupement d'appareils pour les appareils Windows 10
- ✔ Gestion et mise à disposition d'applications Office 365
- ✔ Prise en charge complète pour l'enregistrement utilisateur iOS
- ✔ Amélioration du reporting pour la conformité des appareils

### Valeur métier :

- ✔ Visibilité améliorée pour la conformité des appareils ([Municipalité d'Oulu](#))
- ✔ Sécurité contextuelle renforcée : fourniture de stratégies MDM et MAM qui peuvent déclencher des actions automatisées
- ✔ Déploiements « low-touch », « no touch » qui permettent des expériences utilisateurs clés en main OTA (over-the-air)
- ✔ Diminution du recours à l'équipe de support d'aide
- ✔ Évitement des incidents de sécurité majeurs et des violations de données<sup>1</sup>

Source : <sup>1</sup><https://www.citrix.com/content/dam/citrix/fr-fr/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf>



## Conclusion

En l'espace d'un an, il est devenu évident que le changement est la seule chose sur laquelle nous pouvons compter. Alors que de plus en plus d'applications et de contenus sont déplacés dans le cloud, les équipes IT envisagent avec précaution des environnements hybrides ou entièrement cloud afin de réduire les frais de ressources associés aux déploiements, mises à jour et logiciels sous licence perpétuelle. Après le Covid, les collaborateurs attendent une plus grande flexibilité en termes d'outils et d'environnements de travail, ce qui nécessite un accès sécurisé et contextuel ainsi que des performances applicatives optimales. Citrix Workspace représente l'évolution logique : il relève ces défis avec une expérience Workspace unifiée, intelligente et flexible, sur n'importe quel appareil et pour tout type de collaborateur.

Unifiez et simplifiez votre environnement technologique avec une plateforme entièrement équipée qui propose le **chemin le plus rapide vers un accroissement de la valeur**, l'amélioration de **la flexibilité et de l'agilité** et la **simplification de la gestion et de la sécurité**.

[En savoir plus sur Citrix Workspace](#)

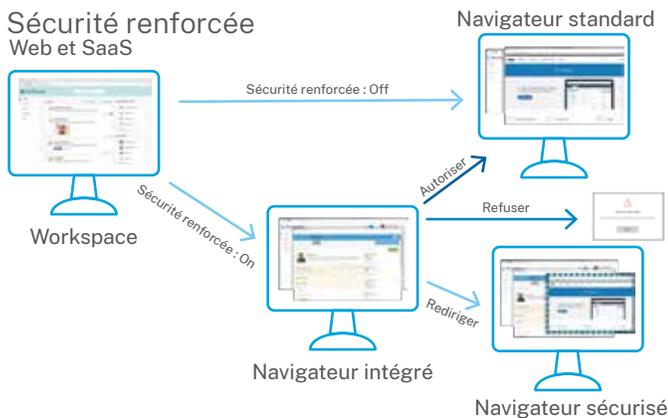
[Contactez un spécialiste Citrix](#)



## Index

### 1. Sécurité renforcée

- a. Donnez aux utilisateurs la possibilité d'accéder à des sites sur liste grise, y compris des emails personnels, grâce à une navigation avancée sécurisée et intégrée



### 2. Inclusion d'applications mobiles et d'applications locales

- a. Sur de nombreux appareils, nous avons des applications personnelles et des applications professionnelles.
- b. Ceci n'est pas limité aux téléphones sur iOS et Android ; Windows aussi propose cette fonctionnalité.
- c. Applications personnelles et applications professionnelles
- Comment pouvons-nous protéger les applications professionnelles ?
- d. Avec des conteneurs d'applications, nous pouvons séparer nos applications professionnelles des applications personnelles.
- e. Une fois que l'application est dans un conteneur, nous pouvons contrôler les interactions entre les applications.
- Le conteneur construit également un ensemble sécurisé de ressources qui ne sont accessibles que depuis les applications situées dans le conteneur.
  - Les applications professionnelles et les conteneurs associés sont configurés à l'aide de stratégies centralisées qui peuvent nécessiter un mot de passe pour utiliser l'application. Empêchez l'application de fonctionner depuis des appareils jailbreakés ou définissez si et comment l'application peut communiquer avec des ressources backend, via un micro-VPN.
- f. Le défi des utilisateurs mobiles réside dans le fait qu'ils ne se trouvent pas toujours dans les limites du datacenter.

- L'accès externe aux ressources internes est protégé par un pare-feu. D'une manière ou d'une autre, nous devons autoriser ces appareils à passer à travers le pare-feu du datacenter tout en protégeant le public.
- Traditionnellement, nous intégrerions un VPN complet dans notre datacenter. Cette approche présente cependant un certain nombre de problèmes.
- Problème 1 : Un VPN complet se place au niveau de l'appareil. Cela signifie que tous les composants et applications de l'appareil ont accès à nos ressources internes.
- Problème 2 : Un VPN complet donne aux utilisateurs la clé de toute la maison. Cela signifie que cette seule connexion autorise l'appareil et toutes les applications qu'il contient à accéder à toutes les ressources de notre réseau interne.

- h. Une approche alternative consiste à remplacer le VPN complet par un micro-VPN.

- Spécifique à l'application. Seules les applications qui sont autorisées à accéder au micro-VPN peuvent établir un tunnel.
- Celui-ci n'est établi que lorsque l'application fonctionne, ce qui évite de vider la batterie.
  - Spécifique à la ressource. Cela signifie qu'une application de terminal donnée ne peut accéder qu'à une ressource interne donnée.

### 3. Partage de contenu

- a. Ces défis concernent la façon dont nous gérons les contenus dans un environnement dans lequel les utilisateurs ont plusieurs appareils. Certains sont fiables, d'autres non, certains sont physiques, d'autres virtuels, certains sont persistants, d'autres non.
- Depuis chacun de ces appareils, les utilisateurs ont besoin d'accéder à leurs contenus, qui peuvent se trouver sur n'importe quel stockage réseau, stockage local ou fournisseur cloud.
- Comment les utilisateurs configurent-ils leurs terminaux pour accéder à ces contenus depuis tout type de terminaux ? L'expérience est-elle la même ou non ?
  - Pour finir, quelle sécurité est intégrée à tous ces répertoires de contenu et comment sont-ils appliqués sur différents terminaux ? Pouvons-nous autoriser l'accès à des tiers ? Que peuvent-ils faire (éditer ou visualiser) ? Pouvons-nous supprimer à distance des données sur un appareil ? Pouvons-nous sécuriser les données ?

### 3. Comment pouvons-nous faciliter les activités types pour les utilisateurs ?

#### 4. Analytique de la sécurité

- a. L'analytique peut être divisée en 3 domaines :
  - i. Télémétrie
  - ii. Analyse
  - iii. Actions
- b. En ce qui concerne la télémétrie, l'analytique collecte des informations sur les appareils, les sites, l'infrastructure, les applications et les contenus consultés/modifiés via les différents services intégrés.
  - i. Ces informations sont analysées par le micro-service de Machine Learning pour essayer d'identifier des modèles de comportement pour les utilisateurs, les applications et les données. Une fois que les comportements sont identifiés, le moteur d'analyse peut détecter des anomalies ou des modifications du comportement. Où se trouve l'utilisateur ? S'agit-il d'un appareil nouveau/ancien ? A-t-il déjà accédé à cette application auparavant ? Est-ce une heure inhabituelle pour l'utilisateur pour accéder à cette application ? Est-ce qu'il modifie un grand nombre de fichiers ? Télécharge des contenus ?
  - ii. Des changements dans le comportement ou les performances peuvent déclencher automatiquement une action, qui peut être aussi minime qu'une alerte à l'administrateur ou plus drastique comme le blocage de l'utilisateur ou la suppression de données sur l'appareil concerné.
    - Surveillance du comportement de l'utilisateur.
    - Détection d'activités anormales.
    - Automatisation du contrôle des stratégies.
    - Utilisation de plusieurs sources de données.

Des informations provenant de différentes sources de données sont envoyées au service Citrix Analytics. Elles sont évaluées en se basant sur les violations de stratégies, les anomalies d'IA, la modélisation du comportement de l'utilisateur dans le temps ou la normalisation par groupes de pairs. Le score de l'utilisateur est ensuite calculé en se basant sur le niveau global de risque que représente l'utilisateur pour l'entreprise.

L'analytique des performances est un outil puissant qui permet d'analyser les causes profondes qui génèrent une expérience utilisateur médiocre. Elle permet aux clients de quantifier les performances applicatives et l'expérience utilisateur. Elle permet également aux clients d'avoir un reporting et une agrégation multi-site.

Le score de l'expérience utilisateur est calculé à partir d'informations obtenues sur la latence, le délai de connexion, les défaillances et les reconnections de l'utilisateur. Il vous permet d'explorer plus profondément pour déterminer les causes profondes des problèmes rencontrés par vos utilisateurs.



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).