LIVRE BLANC

# À LIRE AVANT DE SE LANCER.

## Quatre points de conception à prendre en compte avant de s'engager dans un projet d'espace de travail numérique

vmware®

# Sommaire

# Introduction

Les applications mobiles représentent 60 % du temps total passé sur un environnement numérique. [1]

Le monde qui nous entoure est métamorphosé par la transformation digitale, et les technologies telles que le Cloud et la mobilité font rapidement évoluer les modes de travail et de vie des personnes. Les nouvelles manières de déployer des applications et services grand public gagnent en popularité et s'intègrent aux tendances du monde professionnel.

Les services applicatifs Cloud (SaaS, software as a service), l'un des segments les plus importants du marché international des services Cloud devrait croître de 21,7 % en 2016, d'après le sondage 2015 de Gartner sur l'adoption du Cloud. [2]

Plus que jamais, les utilisateurs travaillent essentiellement depuis des sources mobiles, aussi bien à partir de terminaux que de réseaux, et attendent une expérience homogène et sans accroc sur le terminal de leur choix. Leur entreprise opte également pour des solutions mobiles, cherchant à transformer les processus pour stimuler l'efficacité, améliorer les workflows pour les utilisateurs et favoriser un meilleur engagement collaborateur-client, tout en franchissant un nouveau cap dans la productivité. Pour atteindre ces nouveaux objectifs, nombre d'entre elles étudient les initiatives d'espace de travail numérique.

[1] « Enterprise Mobility Exchange: Engaging Customers with Mobility » (Implication des clients dans la mobilité)

[2] « Gartner Says Worldwide Public Cloud Services Market to Grow 17% in 2016 » (Selon Gartner, le marché international des services de Cloud public connaîtra une croissance de 17 % en 2016), 15 septembre 2016, http://www.gartner.com/newsroom/id/3443517

Aux États-Unis, 49 % des responsables informatiques se disent fortement d'accord avec le fait que les initiatives BYOD augmente la productivité des collaborateurs. [3]

## Gérer un personnel dynamique avec un espace de travail numérique

L'adoption d'une stratégie d'espace de travail numérique permet au département informatique d'exploiter les changements rapides induits dans l'entreprise par la consumérisation. C'est un changement global de la façon dont le département informatique fournit les services aux utilisateurs, et cela permet aux entreprises de fournir aux collaborateurs les applications et les informations dont ils ont besoin pour travailler, sur n'importe quel appareil.

VMware renforce les stratégies d'espace de travail numérique en offrant une expérience alliant convivialité et sécurité de classe d'entreprise. VMware Workspace ONE™ est une plate-forme unifiée dédiée au provisionnement, à la gestion, à l'application des règles associées aux applications et aux données aux terminaux et ce, sur tous les systèmes d'exploitation principaux (iOS, Android et Windows, entre autres). La solution est fondée sur une architecture software-defined qui simplifie la gestion des identités et de l'accès à tout type d'applications, on premise ou dans le Cloud.

L'espace de travail numérique présente un potentiel exceptionnel en matière de rationalisation des processus et de stimulation de l'agilité. Il vous faut cependant examiner plusieurs considérations de conception clés avant de passer à l'étape suivante.

## 1. Commencer par une approche humaine

Fondamentalement, le facteur humain est au cœur de chaque entreprise. Ainsi, tout projet d'espace de travail numérique devrait se baser sur une approche humaine. Il n'y a pas si longtemps, les responsables informatiques des entreprises caractérisaient les collaborateurs et leur service uniquement au travers des applications qu'ils employaient et peut-être par le type de PC qui leur était confié (portable ou bureau). Les collaborateurs des finances utilisaient des outils et applications de services financiers, tandis que les équipes de marketing utilisaient peut-être des applications de productivité personnelle.

De nos jours, à l'ère de l'espace de travail numérique, il est plus logique de penser aux collaborateurs en prenant non seulement compte de leur activité, mais également de leur mode et lieu de travail. Par exemple, en plus de posséder des applications spécifiques, les experts financiers d'aujourd'hui peuvent être amenés à travailler dans divers environnements à l'international, chacun impliquant des exigences lui étant spécifiques. Des entreprises emploient peut-être des financiers qui travaillent chez eux plutôt que de venir chaque jour sur site. Certains peuvent nécessiter un accès à des données sensibles ou strictement protégées. Prenez en compte les méthodes de travail des collaborateurs et élaborez des groupes en conséquence.

Des manières traditionnelles de réfléchir aux besoins d'infrastructure sont également axées sur les terminaux des collaborateurs. Les ingénieurs nécessitent des postes de travail dédiés très puissants, tandis que les collaborateurs du service des finances ont probablement besoin de grands écrans pour afficher des feuilles de calcul, par exemple.

Aujourd'hui, de nouvelles initiatives telles que le BYOD poussent les équipes informatiques à repenser leur façon de voir les terminaux. Au lieu de se limiter à l'adoption de quelques terminaux approuvés et ainsi réduire le choix des collaborateurs, les équipes informatiques envisagent de meilleures façons de maximiser le nombre d'alternatives qui leur sont proposées. Il faut donc pour cela développer une infrastructure capable de prendre en charge les terminaux les plus adaptés à chaque tâche spécifique. Jusqu'alors, la standardisation constituait le meilleur moyen de maîtriser les coûts.

[3] « The New BYOD: Best Practices for a Productive BYOD Program » (Les nouvelles meilleures pratiques BYOD pour un programme BYOD efficace), VMware.

Vous devez être en mesure de fournir le niveau de prise en charge nécessaire pour n'importe quel terminal, qu'il s'agisse de proposer un support technique pour le terminal personnel choisi par un collaborateur ou de répondre aux exigences et préférences particulières développées par un service ou une branche d'activité.

## 2. À qui ces terminaux appartiennent-ils ?

Les consommateurs des marchés matures utiliseront et seront propriétaires de trois à quatre terminaux d'ici à 2018.[4]

La transformation digitale vient également remanier les règles traditionnelles en matière de propriété de terminaux. Le fait que le terminal d'un collaborateur soit ou non acheté par l'entreprise ne doit faire aucune différence dans un espace de travail numérique, puisqu'il sera géré de la même manière. Cependant, lorsqu'un collaborateur est propriétaire de son terminal (et même si ce n'est pas le cas, la plupart du temps), il voudra savoir quelles modifications y sont apportées par l'équipe informatique, si sa vie privée est remise en cause ou si ses données risquent d'être perdues ou compromises.

Lorsqu'elle élabore un espace de travail numérique, l'équipe informatique doit décider s'il est réellement nécessaire d'être propriétaire du terminal d'un collaborateur. La sécurité est un facteur majeur de cette décision. Si l'entreprise juge nécessaire de pouvoir réinitialiser intégralement un terminal, il lui faut alors en être propriétaire pour éviter d'être déclarée responsable de la suppression des données personnelles d'un collaborateur.

D'après une enquête récente, 50 % des responsables informatiques, directeurs informatiques et directeurs des technologies attribuent un niveau de priorité moyen ou élevé à la gestion des utilisateurs et des terminaux mobiles.[5]

Toutefois, l'équipe informatique ne doit pas être systématiquement propriétaire du terminal d'un collaborateur. Si l'équipe informatique est en mesure d'effacer toutes les informations d'entreprise pouvant figurer sur un terminal et qu'elle dispose des fonctionnalités de gestion et des règles adaptées au maintien du contrôle de ces informations, il n'est souvent pas nécessaire d'être propriétaire d'un terminal. Les contrôles modernes de conteneurisation native disponibles sur tous les systèmes d'exploitation principaux (iOS, Android, Windows 10, etc.) sont conçus pour fournir une conteneurisation native protégeant les données et applications personnelles.

Même dans le contexte de popularité croissante des initiatives BYOD actuelles, la plupart des collaborateurs attendent toujours de leur employeur qu'il leur fournisse un terminal. Avec l'approche d'infrastructure adéquate, il peut suffire pour une entreprise de payer le terminal et de laisser le collaborateur choisir celui qu'il préfère, sans compromis sur la sécurité ou la conformité.

### Trouver le juste milieu entre le niveau de choix et la conformité durant l'intégration de nouveaux collaborateurs

Déterminer les modèles de propriété des terminaux représente une étape décisive de l'intégration des collaborateurs, étape dont l'équipe informatique est responsable. Jusqu'alors, les équipes informatiques configuraient un ordinateur portable d'entreprise, le provisionnaient puis le livraient au collaborateur. Avec un espace de travail numérique proposant un catalogue d'applications d'entreprise, les collaborateurs peuvent accéder aux applications et aux services dont ils ont besoin à partir de n'importe quel terminal, quel que soit son type de format ou son système d'exploitation. Il est possible que certaines applications nécessitent un degré de protection plus élevé et une conformité des terminaux plus stricte.

Le marché mondial du BYOD et de la mobilité d'entreprise devrait croître à un taux de 24,12 % (CAGR) entre 2017 et 2021. [6]

Dans le cadre du processus d'intégration, l'équipe informatique peut installer un profil sur un terminal afin d'assurer sa conformité. Il peut s'agir d'une démarche à faible impact, comme par exemple installer des certificats pour contrôler l'unicité et la propriété du terminal, ou encore veiller à ce que les exigences de base en matière de force de mot de passe soient modifiées régulièrement. Il est en revanche plus simple pour l'entreprise de garantir le respect de la conformité si elle est propriétaire du terminal.

[4] « Gartner Says Consumers in Mature Markets Will Use and Own Three to Four Devices by 2018 » (Selon Gartner, les consommateurs des marchés matures utiliseront et seront propriétaires de trois à quatre appareils numériques d'ici à 2018) Gartner, Inc., 8 décembre 2015.

[5] « IT Budgets: Drivers, trends, and concerns in 2016 » (Budgets informatiques : moteurs, tendances et enjeux en 2016) Tech Pro Research, août 2015.

[6] « Global BYOD and Enterprise Mobility Market 2017-2021 » (Marché mondial du BYOD et de la mobilité d'entreprise de 2017 à 2021), Infiniti Research, juillet 2017.

Le modèle de propriété que vous décidez d'adopter doit assurer un équilibre entre les choix offerts aux collaborateurs et la conformité. La flexibilité d'un espace de travail numérique réduit les compromis nécessaires par rapport aux approches classiques.

## 3. Tenir compte du mode de travail des collaborateurs

Une autre considération de conception cruciale au développement d'un espace de travail numérique est le mode de travail des collaborateurs. Un technicien de terrain équipé d'une tablette peut par exemple nécessiter de son employeur qu'il lui fournisse un terminal tout-terrain doté d'un appareil photo ou d'une capacité de lecteur de codes. Ils souhaitent peut-être également rester productifs le weekend ou hors de leurs heures de services à l'aide de leur smartphone personnel pour accéder à des applications d'entreprise ou contacter les ressources humaines.

Lorsque vous développez une stratégie d'espace de travail numérique, tenez compte des tâches que les utilisateurs peuvent souhaiter accomplir en différentes circonstances ainsi que de leurs éventuels besoins en termes de terminaux, expériences ou politiques différents.

Les objectifs d'un terminal varient également d'un modèle à l'autre. Les terminaux portables et toujours connectés peuvent effectuer des tâches irréalisables pour un PC de bureau standard. L'opportunité réelle que représente la mobilité accrue des collaborateurs est la capacité à tirer profit de ce type de format réduit afin d'augmenter leur productivité et leur agilité. Il s'agit d'une opportunité de changer les façons de travailler ou d'effectuer des tâches auparavant impossibles.

La session mobile moyenne, d'une durée de 72 secondes[7], est appelée « instant de mobilité ».

La conservation de cet avantage est essentielle lorsque vous développez un espace de travail numérique. En plus d'être rapide et intuitive, la gestion des accès doit mettre la mobilité à profit.

S'il est impossible pour un collaborateur mobile d'effectuer certaines actions sur son terminal en quelques secondes, comme par exemple transférer des informations au client, elles vont simplement s'ajouter à sa liste de tâches à accomplir de retour au bureau.

Pour un tiers des centres de support, plus de 30 % de leurs tickets concernent des réinitialisations de mot de passe, même si 69 % d'entre eux permettent aux clients de réinitialiser au moins quelques-uns de leurs mots de passe sans devoir contacter le support technique.[8] Le coût moyen d'une réinitialisation de mot de passe est de 18 $ par appel au support.[9]

S'adapter aux modes de travail des collaborateurs implique de simplifier autant de processus que possible. Adopter l'authentification unique (SSO) avec une authentification par certificat peut rationaliser les workflows et permettre aux collaborateurs de tirer parti des opportunités offertes par la mobilité, sans risques de sécurité. Les utilisateurs d'une architecture idéale devraient pouvoir accéder à une application d'entreprise sans saisir des mots de passe plusieurs fois ni configurer ou saisir des informations. Il faut automatiser ces processus à l'avance.

## 4. Utiliser des règles d'accès et de sécurité intelligentes

La sécurité et l'accès occupent une place importante parmi les considérations de conception d'un espace de travail numérique. Les collaborateurs sont déjà habitués aux terminaux mobiles et au téléchargement de leurs applications préférées, mais les équipes informatiques demeurent responsables des questions de sécurité, de conformité et de protection de la propriété intellectuelle, des collaborateurs et des clients de l'entreprise.

D'après le Ponemon Institute, les terminaux mobiles tels que les smartphones sont considérés comme les plus grands vecteurs de risques informatiques potentiels.[10]

Les menaces existantes se complexifient, les questions de sécurité se multiplient et l'approche traditionnelle de protection de la périphérie du réseau est désormais obsolète. À l'heure du Cloud et de la mobilité, il est préconisé de se méfier de tout.

---

[7] « Mobile User Experience: Limitations and Strengths » (Expérience utilisateur de mobile : Limitations et forces), Groupe Nielsen Norman, avril 2015.

[8] « Password-Reset Practices in Support » (Pratiques de réinitialisation de mot de passe des supports techniques), HDI Research, mai 2012.

[9] https://go.forrester.com/blogs/12-06-21-it_service_management_and_automation_now_thats_a_double_whammy_of_business_enabling_goodness/.

[10] « 2016 State of Endpoint Report » (Rapport 2016 sur l'état des terminaux) Ponemon Institute, avril 2016.

Il n'est toutefois pas nécessaire pour une approche « zéro confiance » d'adopter un modèle de sécurité universel restrictif. S'ils sont trop nombreux ou trop fréquents, les processus tels que des demandes d'authentification ou de jetons peuvent complexifier l'architecture, diminuant ainsi la facilité d'utilisation et l'adoption.

Tenez compte des éléments qu'il est réellement nécessaire de protéger et prenez le temps d'élaborer soigneusement les règles de sécurité et d'accès. Vous pouvez fixer des règles d'accès granulaires en fonction :

- de l'emplacement réseau ;
- de l'emplacement GPS ;
- des utilisateurs spécifiques ;
- du niveau d'authentification ;
- des préférences en matière de contrainte de temps des tâches d'authentification ;
- d'une réauthentification uniquement en cas de contexte différent.

Vous pouvez également appliquer des règles de sécurité hautement granulaires aux terminaux d'accès. Vous pouvez par exemple juger nécessaire d'utiliser des modules cryptographiques pour les données chiffrées, afin d'assurer une vérification de la conformité pour les applications plus stratégiques. Vous pouvez faire en sorte qu'une application requiert l'installation des dernières mises à jour de sécurité sur le système d'exploitation du terminal pour s'exécuter. Et si un terminal a été compromis ou modifié par débridage ou à l'aide d'un rootkit, vous pouvez bloquer l'accès aux applications d'entreprise. Une solution d'espace de travail numérique efficace vous apporte le contrôle ultra précis nécessaire pour assurer un état de conformité homogène.

### Vos applications sont-elles en sécurité ?

La sécurisation des applications d'entreprise est un élément de considération essentiel à la planification d'un espace de travail numérique. Avec un catalogue d'applications d'entreprise en libre service, vous pouvez décider à quelles applications les collaborateurs ont accès, et contrôler leur utilisation et leur emplacement.

Vous pouvez par exemple déterminer si des applications doivent être mises à disposition des collaborateurs par défaut ou si leur accès doit être soumis à une demande en libre service.

Certaines applications ne doivent en aucun cas être hébergées sur un terminal. En cas de vol d'un terminal contenant des dossiers clients, des informations confidentielles ou des données financières vitales, il n'est qu'une question de temps avant que le voleur des données ne soit capable d'en déchiffrer le contenu. La virtualisation des applications stratégiques et leur hébergement dans le Data Center peut en améliorer la sécurité, car aucune trace des données n'existe sur les terminaux. La virtualisation des applications ou des postes de travail des collaborateurs ou d'un espace de travail numérique ne doit pas être systématique, même si elle est nécessaire pour beaucoup d'entre eux.

## Conclusion

Le bon fonctionnement d'une stratégie d'espace de travail numérique dépend de sa faculté à permettre à l'équipe informatique de fournir un accès sans accroc basé sur les règles, depuis les terminaux choisis par les collaborateurs de leur entreprise. Associée à une planification minutieuse, la solution VMware Workspace ONE vous permet d'offrir une expérience alliant convivialité et sécurité de classe d'entreprise. Une fois que vous aurez tenu compte des besoins des membres de votre entreprise, de vos politiques en matière de propriété de terminaux et des besoins en sécurité de votre organisation, vous pourrez alors poursuivre la mise en œuvre de votre projet d'espace de travail numérique.

La solution Workspace ONE simplifie et accélère l'adoption de nouveaux services et workflows, tout en optimisant la sécurité avec des règles complètes d'accès contextuel.

Workspace ONE vous offre un moyen simple de gérer l'accès à tout type d'applications, on premise ou dans le Cloud. Vous pouvez également bénéficier d'une plate-forme unifiée pour le provisionnement, la gestion et la mise en conformité des terminaux sur iOS, Android et Windows. Grâce à sa structure de règles contextuelle, vous pouvez définir des règles granulaires et fournir des workflows mobiles révolutionnaires à l'aide d'une suite d'applications de productivité et de services mobiles.

En vous associant avec VMware, vous pouvez tirer parti de la transformation digitale, tout en accélérant les processus d'intégration, de sécurisation des données et de maîtrise des risques et coûts liés à l'informatique « fantôme ».

**EN SAVOIR PLUS**

## Faites vos premiers pas vers la simplification des applications et la gestion de l'accès

Rejoignez-nous en ligne :

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.fr