LIVRE BLANC - **MARS 2020**

Remarques importantes relatives à l'application des directives de télétravail en vue de la continuité d'activité

vmware®

Table des matières

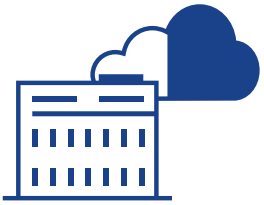
Les événements extraordinaires ont le potentiel de transformer la culture d'une entreprise plus rapidement que n'importe quel autre fait. Une catastrophe naturelle ou une pandémie, par exemple, pousse les entreprises à revoir ou à mettre en place rapidement de nouveaux processus et de nouvelles technologies de télétravail afin de limiter les pertes de productivité des collaborateurs lorsqu'une isolation imposée par soi-même, par la direction ou par les autorités s'avère nécessaire.

Il n'existe pas de remède miracle apte à transformer l'expérience des collaborateurs lorsqu'une perturbation survient. Les entreprises d'aujourd'hui peuvent toutefois adopter des mesures qui leur permettront d'améliorer les méthodes de travail à domicile de leurs collaborateurs tout en accélérant les objectifs de mise en priorité du télétravail à l'échelle de toute l'entreprise, grâce à une stratégie d'espace de travail numérique.

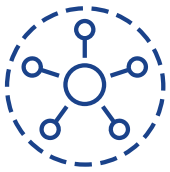
Cinq principes informatiques qui sous-tendent l'expérience des collaborateurs

Les mesures prises par les dirigeants pour améliorer l'expérience de leurs collaborateurs peuvent rapidement poser les jalons d'un avantage pour leur activité numérique ou leur mission par la suite. Pour cela, les équipes informatiques et de direction doivent s'entendre sur certains principes de base, qui ne sont pas nécessairement nouveaux :

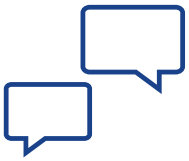
Applications dont les collaborateurs ont besoin



Localisation des applications et données clé



Accès actuel (et attendu) des collaborateurs aux ressources de l'entreprise



Modes de communication et de collaboration actuels (et attendus) des dirigeants et des collaborateurs

Aide à la disposition des collaborateurs si et quand des problèmes surviennent

Connaître les applications dont les collaborateurs ont besoin

C'est sur les applications que repose l'entreprise moderne, de l'expérience client aux opérations de la chaîne logistique. Même si nombre de spécialistes de l'information, notamment ceux qui travaillent généralement au bureau à heures régulières, peuvent être bien préparés au télétravail car ils utilisent surtout des applications de productivité répandues, ce n'est pas le cas de tout le monde.

En effet, les effectifs de collaborateurs non sédentaires dans les domaines du social ou de l'hôtellerie, ou encore les cliniciens et les techniciens, peuvent être amenés à se présenter sur place avant d'effectuer leurs tâches quotidiennes. Si les collaborateurs sont contraints à travailler à domicile au-delà d'une ou deux semaines, les applications stratégiques dont ils ont besoin hormis l'e-mail seront-elles accessibles en tout lieu sans faire courir de risque à l'entreprise ? Il est impératif pour les responsables de la partie activité et du département informatique de dresser la liste et de comprendre l'impact de l'utilisation de chaque application en dehors du réseau de l'entreprise.

Savoir localiser les principales applications et données

À partir de la liste des applications considérées stratégiques par chaque service ou groupe, le personnel informatique peut commencer à identifier l'emplacement de chaque application et de ses données (on premise dans un Data Center de l'entreprise ou dans un Cloud privé ou public), et en connaître toutes les dépendances. Par exemple, les applications client-serveur, .NET et Java traditionnelles sont souvent liées aux réseaux d'entreprise pour les données et sont extrêmement dépendantes des configurations de clients. À l'inverse, les applications internes sur navigateur bénéficient d'une portabilité de terminaux client, mais reposent encore sur les serveurs d'applications du réseau d'entreprise pour leur déploiement. Plus flexibles, les applications SaaS simplifient le déploiement car elles ne sont pas dépendantes du réseau d'entreprise, sauf si le département informatique a déjà établi des contrôles qui exigent que les terminaux résident sur le réseau de l'entreprise pour en autoriser l'accès.

Savoir quels terminaux vont se connecter (détenus par l'entreprise, personnels, ou les deux)

C'est seulement en connaissant les applications dont les collaborateurs ont besoin et en sachant localiser les données que les responsables informatiques et activité peuvent mettre en place une stratégie efficace qui définit les terminaux qui peuvent et doivent être autorisés à se connecter à l'entreprise, ainsi que leur mode de connexion. Des connexions VPN sont souvent pré-provisionnées sur les ordinateurs portables appartenant à l'entreprise, afin de permettre la mobilité et la portabilité des applications.

Pourtant, si ces terminaux quittent le réseau d'entreprise pendant des périodes prolongées, comment le département informatique pourra-t-il prendre en charge les mises à niveau, les correctifs et les règles de gestion qui réduisent le risque pour l'entreprise ? Et comment doit-il considérer les scénarios selon lesquels il est trop tard pour provisionner de nouveaux ordinateurs portables et où les collaborateurs sont obligés de se connecter au moyen de terminaux personnels, des smartphones et iPads aux stations de travail et aux PC, qui fonctionnent avec divers systèmes d'exploitation et logiciels non pris en charge ? Savoir quels terminaux peuvent être exposés à des attaques malveillantes sur Internet pour être ensuite réintroduits sur le réseau de l'entreprise est un casse-tête que les équipes informatiques peuvent se préparer à éviter.

Comprendre la collaboration et la communication organisationnelles

Dans les secteurs d'activité tels que l'informatique et de plus en plus les services financiers, où les dirigeants et les spécialistes d'une entreprise sont peut-être déjà habitués à échanger avec le personnel, les collègues, les clients et les partenaires sur des canaux en ligne, de la vidéoconférence à l'e-mail à la messagerie instantanée, les interruptions peuvent être maintenues à un minimum. En revanche, lorsqu'il devient nécessaire que l'entreprise et tous ses collaborateurs (par ex., services commerciaux, caissiers, maintenance, etc.) collaborent et communiquent davantage ou en permanence via des logiciels, des interruptions de service peuvent se produire le temps que la direction, les chefs de services et le personnel s'habituent à ces nouvelles méthodes de travail.

Pour un minimum d'interruption, le département informatique et la direction doivent rapidement se réunir lorsque le personnel est tout à coup plus distribué que de coutume, afin de documenter les nombreuses méthodes de communication quotidienne utilisées par différents sites, banques, hôpitaux, etc., avant de pouvoir être en mesure de mettre en place de nouveaux workflows et processus virtuels pour prendre en charge le télétravail.

Reconnaître que le support va être problématique

L'une des plus importantes inconnues du travail à domicile est le niveau de support dont les collaborateurs vont avoir besoin, avec quelles applications et sur quels terminaux, à quel endroit et à quel moment. Les responsables ou les équipes informatiques ou d'activité peuvent dresser une cartographie des processus actuels pour découvrir les plus importantes lacunes et travailler à les combler avant que les perturbations ne s'aggravent. Ils doivent notamment passer en revue les options de support à distance, les possibilités de libre-service, les effectifs, et plus encore.

Sur un marché du travail concurrentiel, les collaborateurs ont des choix et leur offrir une bonne expérience du télétravail est un facteur de différenciation. *Les conclusions d'une enquête récente* révèlent que 73 % des collaborateurs et des décisionnaires des RH s'accordent pour déclarer que la souplesse des outils (par ex., technologie, applications et terminaux) dont ils peuvent avoir besoin pour travailler influe sur leur décision de se porter candidats ou d'accepter un poste dans une entreprise.[1]

Rendre possible le télétravail de vos collaborateurs avec les solutions VMware

Dans les entreprises axées sur les applications d'aujourd'hui, il est déjà trop difficile de trouver des solutions pour chaque terminal, application, règle de conformité, identité et autorisation en temps normal, et encore moins en situation de crise. Les équipes informatiques n'ont jamais disposé du personnel, des budgets ou des incitations leur permettant de faire le tri parmi les diverses combinaisons de clients, de connexions, de problèmes de conformité, de types d'application et d'authentifications pour garantir un bon fonctionnement généralisé. La situation a été acceptable jusqu'à présent car la plupart des collaborateurs qui utilisaient le réseau d'entreprise--avec des identifiants de domaine sur un ordinateur de confiance et un courrier électronique fonctionnel sur site et hors site--étaient satisfaits. Lorsque tous les collaborateurs sont amenés à travailler à distance, cette supposition n'est plus nécessairement valide.

« C'est le moment de bien identifier les points forts et les points faibles de votre entreprise en matière de communication et de productivité.»[2]

— TECHCRUNCH

Le personnel se rend alors compte que les environnements informatiques d'entreprise sont complexes. Pourtant, avec des périodes d'interruption de plus en plus régulières, les collaborateurs de talent vont commencer à se renseigner plus souvent sur l'expérience au travail. C'est la raison pour laquelle les entreprises qui cherchent à offrir une expérience optimale à leurs collaborateurs, avec un risque moindre lorsque le personnel a obligation de travailler à domicile, choisissent l'espace de travail numérique de VMware.

La plate-forme de bout en bout, qui repose sur VMware Workspace ONE®, intègre le contrôle d'accès, la gestion applicative et la gestion des terminaux multi-plates-formes pour fournir un espace de travail unifié et cohérent sur l'ensemble des environnements informatiques.

Assurer l'accès à toutes les applications sur l'ensemble des terminaux et des réseaux

Les dirigeants d'activité et informatiques de l'entreprise peuvent compter sur la plate-forme Workspace ONE pour assurer l'accès à toutes les applications à partir de tous les terminaux et de tous les réseaux, en mettant en avant trois principes clés :

- Modernisation informatique
- Engagement des collaborateurs
- Sécurité zéro confiance

Gestion des terminaux

Grâce à Workspace ONE, le personnel informatique peut inscrire n'importe quel terminal (ordinateur portable, tablette, smartphone, poste de travail PC ou Mac) nécessitant un accès aux ressources de l'entreprise et le surveiller en permanence grâce à des points de vue intelligents et des fonctionnalités d'automatisation. La solution assure l'intégrité des terminaux par l'agrégation des données relatives au terminal, à l'application et à l'utilisateur, tout en identifiant les opportunités de réduire les coûts informatiques, d'améliorer la sécurité et d'optimiser l'expérience.

1 Vanson Bourne. « The Digital Employee Experience. » Mai 2019.

2 TechCrunch. « *How to work during a pandemic.* » Devin Coldeway, mars 2020.

Pour les sociétés qui fournissent des terminaux gérés par l'entreprise aux collaborateurs à domicile, cette solution fait gagner du temps d'administration : elle interprète rapidement l'état de chaque terminal et le gère depuis le Cloud, quel que soit le lieu à partir duquel il se connecte à Internet. Pour les collaborateurs qui télétravaillent à partir de terminaux personnels tels que les smartphones et les tablettes, Workspace ONE simplifie la gestion et permet au département informatique d'isoler les informations de l'entreprise de celles des applications personnelles, tout en appliquant des règles d'accès conditionnel minimales pour assurer la protection des ressources professionnelles.

Les entreprises qui utilisent l'espace de travail numérique de VMware peuvent gérer des règles et des processus cohérents sur iOS, Android, Windows 10, macOS, Chrome OS et d'autres encore, quel que soit le lieu à partir duquel les collaborateurs utilisent leurs terminaux. Il offre une approche Cloud en temps réel pour compléter ou remplacer la gestion du coût et du cycle de vie des produits legacy.

Cette plate-forme VMware complète propose de nombreuses options rationalisées pour les utilisateurs sur terminaux mobiles, macOS et Windows 10, afin de permettre aux équipes informatiques d'intégrer simplement les nouveaux terminaux et les nouveaux utilisateurs. Elle prend en charge la configuration, les règles, les correctifs et les mises à jour over-the-air par l'intermédiaire de règles automatisées. Les équipes informatiques peuvent facilement autoriser, provisionner et déployer des applications sur l'ensemble des terminaux, ainsi qu'éviter les pertes de données. Elles peuvent distribuer des applications efficacement over-the-air ou par déploiement peer-to-peer, même dans le cas de volumineuses applications Win32. Par ailleurs, avec Workspace ONE® Assist, le département informatique et le personnel de support technique peuvent identifier et résoudre en temps réel les problèmes survenant sur les terminaux Android, iOS, macOS et Windows par l'intermédiaire de fonctionnalités de gestion ou de prise en main à distance.

Le recrutement ne doit pas nécessairement s'arrêter au cours des périodes de télétravail obligatoire. En effet, l'espace de travail numérique de VMware offre une fonctionnalité unique permettant au personnel informatique de faire livrer directement des ordinateurs portables provisionnés pour le Cloud aux nouveaux collaborateurs travaillant à distance, afin d'assurer la conformité.

Services d'implication des collaborateurs

Workspace ONE améliore l'expérience de collaborateur pour les prospects, les nouvelles recrues et les talents de longue date contraints de télétravailler. La solution Workspace ONE® Intelligent Hub à destination unique offre aux utilisateurs des workflows d'intégration unifiés et automatisés, un catalogue d'applications mis à jour et un accès aux services de hub. L'application Intelligent Hub fournit également des applications natives à installer.

Les services Hub suivants offrent une expérience inter-plates-formes intrinsèquement sécurisée et cohérente, qui permet aux utilisateurs et à la société de communiquer et de collaborer.

- **VMware Workspace ONE® Notifications** : fournit des notifications push et intégrées aux applications administrées par le département informatique avec des données ou des connexions personnalisées à des systèmes d'entreprise tiers avec VMware Workspace ONE® Mobile Flows.™
- **VMware Workspace ONE® Catalog** : permet aux collaborateurs de visualiser, de lancer et d'installation des applications de tous types (par ex. Web, SaaS, virtuelles et Cloud) avec authentification unique (SSO), quel que soit le terminal utilisé.
- **VMware Workspace ONE® People** : permet aux collaborateurs de rechercher rapidement des collègues dans un annuaire du personnel ; contient un organigramme avec nom, e-mail, téléphone et fonction de recherche.
- **VMware Workspace ONE® Home** : permet aux collaborateurs d'accéder aux ressources de l'entreprise par l'intégration d'un intranet ou d'un portail de société.
- **VMware Workspace ONE® Assist** : offre aux collaborateurs un accès aux questions fréquentes (FAQ) et aux articles de la base de connaissances pour leur permettre de résoudre les problèmes de façon autonome, afin de continuer à être productifs. Un assistant numérique virtuel, ou chatbot, intégré à l'application Intelligent Hub fournit des réponses rapides et aide les équipes informatiques à accélérer la résolution lorsque des collaborateurs en télétravail ont des questions.

Déploiement de postes de travail et d'applications virtuels

La prise en charge des interdépendances entre les applications Windows toujours présentes sur de nombreux systèmes d'entreprise est un élément vital pour toutes les solutions d'espace de travail numérique mettant la priorité sur le travail à distance. Workspace ONE avec VMware Horizon® Service permet de résoudre les conflits lorsque les applications nécessitent des configurations, des navigateurs et des plug-ins spécifiques, en particulier lorsqu'il existe des problèmes connus avec l'interaction des applications.

Workspace ONE avec Horizon Service prend également en charge les besoins réseau stratégiques des secteurs d'activité étroitement soumis aux réglementations, tels que la santé et le secteur public. Une infrastructure de postes de travail virtuels (VDI) utilisant des postes de travail virtuels en tant que proxys permet d'isoler totalement les terminaux clients et leurs applications en leur évitant d'entrer en contact avec le réseau d'entreprise.

Si une entreprise fournit des ordinateurs portables à ses collaborateurs, l'infrastructure VDI autorise les accès distants à partir de n'importe quel terminal personnel doté d'un navigateur. Elle couvre les Data Centers on premise et les environnements de Cloud et fournit à ces intégrations des avantages clés en mains.

- **On premise** : les équipes informatiques qui utilisent la plate-forme d'espace de travail numérique de VMware avec une infrastructure virtuelle et une capacité existantes peuvent simplement ajouter les ressources VDI par l'intermédiaire d'une orchestration du Cloud et une infrastructure hyperconvergée VMware, telle que VMware Cloud Foundation™, qui repose sur Dell EMC VxRail.
- **Hybride et multicloud** : les équipes informatiques qui utilisent la plate-forme d'espace de travail numérique de VMware peuvent rapidement mettre en service de nouveaux postes de travail via VMware Horizon® Cloud on Azure ou VMware Horizon® 7 sur VMware Cloud™ on AWS, en bénéficiant même d'un essai gratuit leur permettant d'en évaluer rapidement les capacités.
- **Accès à distance à des PC physiques** : les équipes informatiques qui utilisent la plate-forme d'espace de travail numérique de VMware peuvent configurer un accès distant à des PC Windows 10 physiques qui doivent demeurer dans les bureaux ou le périmètre de l'entreprise, afin de permettre la poursuite du travail à distance en tout lieu.

Services d'accès

Les menaces de sécurité sont une préoccupation constante pour les responsables informatiques et d'activité. Elles ne peuvent qu'augmenter les incertitudes liées au fait de demander aux collaborateurs de travailler à domicile. Même avec une technologie de VPN fiable, il est toujours problématique pour le personnel informatique de régler les questions d'accès et d'authentification.

Workspace ONE simplifie la mise en place d'un contrôle d'accès « zéro confiance ». Les services d'accès VMware dans le Cloud fournissent une authentification SSO avec intégration ou prise en charge de l'authentification multifacteur (MFA) existante. La plate-forme s'intègre également en toute transparence avec les technologies d'identité Cloud existantes, telles qu'Okta.

Les équipes informatiques d'entreprise peuvent être assurées que leurs applications et leurs données sont protégées par une appliance unique qui relie les ressources on premise en appliquant des règles d'accès conditionnel à tous les cas, de Microsoft SharePoint et ses partages de fichiers aux sites intranet et aux API internes, aux postes de travail et applications virtuels (par ex. Horizon et Citrix).

Sécurité des terminaux

L'ensemble des directives de télétravail des collaborateurs sont moins intimidantes pour les équipes informatiques qui gèrent les terminaux avec l'espace de travail numérique de VMware car la plate-forme établit un suivi permanent de l'état des terminaux, des détails utilisateur et du contexte d'authentification, afin de déterminer les risques encourus par les utilisateurs et les terminaux. Il autorise ou refuse également les accès de manière automatique, et requiert une authentification MFA ou une correction pour accorder l'accès.

De plus, le personnel informatique peut appliquer un état souhaité à l'ensemble des terminaux détenus par l'entreprise, ou déclarer un état minimum de conformité pour chaque application ou connexion à des ressources sensibles. Dans le cadre des fonctionnalités d'accès conditionnel, Workspace ONE établit et gère des règles sur l'ensemble des scénarios d'identité, de terminaux et d'applications. L'analyse avancée des risques détecte les anomalies qui pourraient indiquer une intention malveillante.

Cette plate-forme est également idéale pour contrer les menaces. Elle peut, par exemple, intervenir en cas de tromperie des télétravailleurs par une opération d'hameçonnage identifiée par VMware Carbon Black EDR. La réponse automatisée aux menaces de la plate-forme met en quarantaine les utilisateurs ou les terminaux qui présentent un risque élevé. Pour renforcer la protection des applications et des données, la plate-forme VMware sécurise le transport des données en fournissant à chaque application un VPN qui limite l'exposition des ressources internes en réduisant les accès à certaines d'entre elles.

Mettre en place une stratégie délibérée de priorité au télétravail

Comme rien n'arrête Mère Nature et que la plupart des perturbations sont inattendues, les entreprises doivent commencer dès maintenant à se préparer au prochain scénario du pire cas en mettant délibérément en place une stratégie de priorité au télétravail et un environnement d'espace de travail numérique qui soutient en toute transparence les collaborateurs, l'entreprise et le département informatique.

Quel que soit le lieu ou le moment où elles sont mises en œuvre, les directives de télétravail représentent un choc pour les cultures d'entreprise. Les entreprises qui sont déjà en train d'accorder davantage de responsabilités à leurs collaborateurs et évoluent vers un modèle de résultats reposant sur les objectifs rencontreront sans doute moins d'obstacles que les équipes forcées à s'adapter.

Pour les entreprises qui ne sont pas encore pleinement préparées, il est temps de profiter de l'évolution des états d'esprit et des allocations budgétaires pour répondre aux attentes du travail à domicile aujourd'hui et demain. Les équipes doivent repenser intégralement la sécurité pour garantir aux collaborateurs dispersés un accès à la demande facilité à toutes les applications et données dont ils ont besoin pour améliorer la collaboration et la productivité, où et quand ils sont contraints de travailler.

Pour en savoir plus sur la manière dont VMware applique les directives de télétravail qui affectent la continuité d'activité, visitez *notre site sur la continuité d'activité*.

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 Quartier Boieldieu, 92042 Paris La Défense Cedex, France Tél. +33 1 47 62 79 00 www.vmware.com/fr

Référence : FY20-5807-BC-GUIDE-WP-WEB-A4-20200316_FR 3/20