RAPPORT DE TENDANCES

DIRE STOP AUX PERTES DE DONNÉES

Découvrez les dernières tendances en matière de protection des données pour les espaces de travail numériques

vmware®

EN BREF

Une stratégie courante en matière de sécurité consistait à limiter le nombre d'applications et le volume de données que les collaborateurs pouvaient utiliser, jusqu'à ce que des utilisateurs plus hardis commencent à contourner le département informatique pour satisfaire leurs besoins. Ce développement d'une **informatique parallèle** a augmenté l'exposition aux risques des entreprises.

En 2018, l'enjeu prioritaire pour les responsables informatiques est la mise en œuvre d'un espace de travail numérique flexible qui :

- Héberge les applications et les terminaux permettant d'accélérer l'innovation
- Permet aux utilisateurs de travailler quand, où et comme ils le veulent

Bienvenue dans l'espace de travail numérique

Les entreprises modernes se composent de différents types d'utilisateurs ayant des types de besoins différents en matière d'accès aux applications, données, documents et autres ressources numériques.

Les applications et terminaux (PC, ordinateurs portables, tablettes et smartphones) que les collaborateurs utilisent au bureau, chez eux ou en déplacement, constituent ce que l'on appelle l'*espace de travail numérique*. Cet espace promeut une technologie flexible et centrée sur les collaborateurs, permettant de renforcer la productivité et de libérer le potentiel des collaborateurs, des équipes et des entreprises.

Selon M. Sumit Dhawan, VP senior et directeur général de l'informatique pour l'utilisateur à VMware, les entreprises qui déploient des fonctionnalités d'espace de travail numérique pour leurs collaborateurs ont deux objectifs majeurs.

« Le premier objectif », confie Dhawan, est la garantie pour les entreprises de pouvoir mettre en œuvre et « d'assurer la conformité et la sécurité d'une large variété de terminaux, notamment ceux qu'elles ne possèdent et n'exploitent pas. » Ces terminaux sont des postes de travail, des smartphones, des tablettes ou d'autres appareils, qu'ils soient personnels ou professionnels.

Pour Dhawan, le second objectif consiste à « donner aux collaborateurs, qui sont des acteurs majeurs du projet de transformation digitale, les moyens de réussir l'adoption et l'exploitation des nouvelles technologies. » Le but, insiste-t-il, est de créer un espace de travail numérique qui reflète l'expérience dont bénéficient déjà les collaborateurs dans leurs vies personnelles.

L'espace de travail numérique nécessite d'être soutenu par des stratégies de sécurité évoluées

Imaginez la scène. Un employé de votre entreprise a accédé à au réseau via un VPN, et un logiciel malveillant s'est introduit dans le réseau en franchissant le pare-feu du périmètre.

Il n'a probablement pas du tout conscience qu'il est à l'origine de la violation de la sécurité. Il a peut-être eu accès au réseau via le VPN sur un poste appartenant à l'entreprise dont les correctifs de sécurité étaient obsolètes. Ou il s'est peut-être connecté à sa messagerie Web et a téléchargé sans le savoir un document à risques, puis enregistré ce document sur le serveur d'entreprise.

Mais peu importe ce qui s'est produit, le réseau a été victime d'une intrusion, et votre objectif maintenant est d'éviter que cette situation tourne au désastre. Tous les yeux sont tournés vers vous dans l'attente que vous identifiez la source du problème, que vous le résolviez, et que vous vous assuriez que cela ne se reproduise plus.

Ce scénario est fréquent et personne ne veut le vivre. Dans le monde d'aujourd'hui, les consommateurs, les terminaux et les objets sont devenus plus connectés que jamais, et les équipes informatiques doivent sécuriser les interactions accrues entre utilisateurs, applications et données.

Pendant longtemps, une stratégie populaire en matière de sécurité consistait à limiter le nombre d'applications et le volume de données que les collaborateurs pouvaient utiliser, jusqu'à ce que des utilisateurs plus hardis commencent à contourner le département informatique pour satisfaire leurs besoins. Ce développement d'une informatique parallèle a augmenté l'exposition aux risques des entreprises.

Par voie de conséquence, la mise en place d'un espace de travail numérique de pointe et fiable suffisamment flexible pour héberger les applications et les périphériques permettant d'accélérer l'innovation, et suffisamment accessible pour laisser les utilisateurs travailler dans des conditions optimales afin de booster leur efficacité, est une des priorités des responsables informatiques.

LES ESPACES DE TRAVAIL NUMÉRIQUES DOTÉS DE FONCTIONS DE SÉCURITÉ DE NIVEAU ENTREPRISE FONT GAGNER DU TEMPS AU DÉPARTEMENT INFORMATIQUE ET AUX UTILISATEURS EN OFFRANT LES AVANTAGES SUIVANTS :

Déploiement rapide : intégration des collaborateurs sur leurs terminaux *en une heure*.

Contrôle contextuel : mise en place de règles d'accès pour toutes les applications *sur un espace centralisé*.

Accès mobile : exécution de workflows transactionnels *en moins de 72 secondes*.

Gestion à distance : configuration d'un ordinateur portable professionnel depuis n'importe où et *en quelques minutes*.

Aujourd'hui plus que jamais, le moyen le plus efficace de renforcer la sécurité consiste à proposer aux collaborateurs un large choix d'applications et de périphériques. Dans cette optique, les administrateurs réseau doivent (1) élaborer des stratégies de prévention des pertes de données, et (2) exploiter une plate-forme qui fournit les fonctions d'intelligence, d'automatisation, et le moteur de règles nécessaires pour appliquer les règles définies aux applications mobiles, bureautiques et sectorielles on premise ou dans le Cloud.

1. Offrir à la fois portabilité ET protection

Pour offrir certains services apparemment simples qu'attendent les collaborateurs de la plupart des entreprises, comme par exemple un accès sans faille à leurs applications à distance, le département informatique est susceptible d'avoir encore à résoudre de nombreuses problématiques.

Les VPN, qui ont fait leur apparition dans les années 1990, permettent aux collaborateurs qui travaillent à domicile ou dans un hôtel par exemple, d'accéder au LAN de leur entreprise. Concrètement, les collaborateurs peuvent ainsi accéder à distance à l'intégralité de leur réseau depuis un terminal contrôlé et travailler dans des conditions similaires à celles dont ils bénéficient lorsqu'ils sont directement connectés au réseau interne.

Les solutions VPN utilisant une procédure d'authentification multifacteur peuvent être coûteuses et compliquées à déployer. En outre, les mots de passe peuvent être piratés à la suite d'attaques brutales, et les jetons physiques dont nombreuses de ces solutions imposent l'utilisation sont complexes, difficilement mémorisables, ou peuvent être perdus. Résultat : les organisations repensent leur approche et adoptent une plate-forme d'espace de travail numérique offrant simplicité d'utilisation et sécurité de classe d'entreprise. Elles virtualisent des applications ou des postes de travail complets et assurent automatiquement leur provisionnement sur le Cloud ou sur une infrastructure on premise. Les collaborateurs peuvent accéder à tout moment à ces applications ou postes de travail virtuels hautement disponibles sur n'importe quel terminal ou réseau, via un catalogue commun.

Toutefois, les réseaux sont accessibles par différents types de terminaux s'exécutant sur différentes plates-formes. Et les modèles de propriété en vigueur sont divers : terminaux d'entreprise, terminaux appartenant à l'entreprise et personnalisés par les utilisateurs (COPE) et terminaux personnels utilisés dans le cadre d'une stratégie BYOD, par exemple. Les collaborateurs qui accèdent au réseau via un VPN sur leurs terminaux personnels exposent leur entreprise au risque d'introduction de logiciels malveillants sans s'en rendre compte. En effet, ces terminaux ne sont pas gérés, ou ne sont pas sécurisés, et rien dans la procédure de connexion au VPN ne permet d'évaluer l'état d'un périphérique. Lorsqu'un logiciel malveillant, quel qu'il soit, pénètre un terminal d'accès, il peut facilement se propager sur le réseau dans son ensemble par l'intermédiaire du VPN. La surface d'attaque est donc considérable.

Même les terminaux de l'entreprise peuvent poser problème. Les utilisateurs distants doivent en effet être connectés au domaine de l'entreprise pour découvrir et télécharger les correctifs permettant d'actualiser les protocoles de sécurité. Ces utilisateurs peuvent passer très peu de temps sur le domaine, et peuvent même ignorer qu'un correctif est nécessaire.

De nombreuses entreprises mettent en œuvre la virtualisation des postes de travail et des applications pour améliorer la sécurité informatique des clients et offrir une plus grande mobilité d'entreprise. La virtualisation permet d'héberger de manière centralisée et de conteneuriser les applications ; ainsi les données d'application ne sont jamais en contact avec le terminal qui utilise l'application concernée. La virtualisation protège les données inactives, empêche les accès non autorisés aux applications, et fournit un moyen plus efficace de corriger, gérer et mettre à niveau les images.

GESTION UNIFIÉE DES TERMINAUX (UEM)

Cette approche consiste à sécuriser et à contrôler les postes de travail, les ordinateurs portables, les smartphones et les tablettes connectés sur un Cloud de manière cohérente à partir d'une plate-forme et d'un moteur de règles uniques.

Cependant, avec la virtualisation des postes de travail et des applications, de nouveaux risques de sécurité peuvent survenir derrière le pare-feu du Data Center, là où des centaines, voire des milliers, de postes de travail résident.

Ces postes de travail sont très proches d'autres utilisateurs et d'autres charges de travail stratégiques, ce qui les rend beaucoup plus vulnérables face aux logiciels malveillants et à d'autres attaques. Ces attaques peuvent progresser du poste de travail au serveur en exposant une large surface d'attaque au sein du Data Center.

Ce scénario de menace « est-ouest » est courant et affecte de nombreux clients aujourd'hui, en particulier ceux ayant des obligations de sécurité et de conformité strictes.

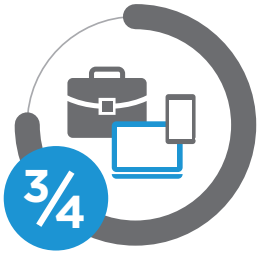
La virtualisation du réseau permet aux applications de s'exécuter de la même manière que si elles se trouvaient sur un réseau physique. Elle présente les périphériques et services réseau logiques (ports, commutateurs, routeurs, pare-feu, répartiteurs de charge, VPN et autres) aux charges de travail connectées. Les réseaux virtuels offrent les mêmes fonctions et garanties que les réseaux physiques, avec les avantages opérationnels et l'indépendance vis-à-vis du matériel assurés par la virtualisation. La virtualisation de réseau, qui fait partie des meilleures pratiques, assure la micro-segmentation d'applications et de postes de travail virtuels spécifiques et de leurs connexions aux autres hôtes au sein du Data Center.

Aujourd'hui, alors que les besoins portent non plus sur la connectivité, mais sur l'innovation inter plate-forme, les entreprises pensent de façon plus globale et se tournent vers des solutions de gestion unifiée des terminaux (UEM).

Avec une solution UEM, le département informatique a les moyens de savoir si un terminal est fiable et, si tel est le cas, accroître les privilèges du terminal en question. En cas de perte du terminal, ou si l'utilisateur quitte l'entreprise, les privilèges correspondants peuvent être supprimés. Les solutions UEM intègrent également un mécanisme de chiffrement permettant de sécuriser les applications de productivité telles que VMware Boxer™, capable de chiffrer et de conteneuriser les e-mails, ainsi que d'isoler les pièces jointes. Ainsi, les applications fiables peuvent être séparées logiquement des applications non sécurisées.

2. Éliminer les obstacles auxquels sont confrontés les utilisateurs

En matière d'horaires, de lieux et de méthodes de travail, il n'existe rien de constant si ce n'est le changement. Voyez plutôt ces statistiques :



Les travailleurs mobiles, qu'ils soient télétravailleurs, commerciaux itinérants ou travailleurs sur le terrain, constitueront **près des trois quarts** de la main-d'œuvre totale des États-Unis en 2020 (prévisions d'IDC[1])

Aujourd'hui, les collaborateurs travaillant dans des bureaux passent uniquement **40 à 50 % de leur temps devant un poste de travail** (statistiques de GlobalWorkplace Analytics[2])

71 % des collaborateurs travaillent au minimum deux heures par semaine sur leurs terminaux mobiles (chiffres de Fierce Mobile IT[3])

L'ESPACE DE TRAVAIL NUMÉRIQUE : UN VECTEUR DE L'INNOVATION NUMÉRIQUE

Une plate-forme d'espace de travail numérique fournit l'infrastructure nécessaire pour :

- Sécuriser la gestion des accès
- Unifier la gestion des points d'accès
- Simplifier les déploiements Windows

Aujourd'hui, les collaborateurs veulent profiter de la portabilité des applications sur tous les types de terminaux, n'importe où, et quel que soit le modèle de propriété en vigueur. La fourniture d'applications standard nécessite cependant l'utilisation de navigateurs, versions, et autres éléments spécifiques qui compliquent le déploiement et la gestion des applications.

Les méthodes traditionnelles d'accès et de gestion des applications et des données, souvent non conformes aux critères recherchés, ont conduit les entreprises à explorer d'autres approches qui répondent davantage aux besoins de l'espace de travail numérique.

Par exemple, l'utilisation d'un catalogue d'applications d'entreprise peut faciliter le déploiement optimal de tous types d'applications sur tous types de terminaux. Et le déploiement des applications ne représente que la moitié du problème. Les utilisateurs doivent pouvoir accéder instantanément et facilement aux applications à partir de n'importe quel terminal ou site. L'accès fluide aux applications et données est assuré via une authentification unique mobile directe. Les solutions VMware incluent également une fonctionnalité d'authentification multifacteur sur les terminaux mobiles. Son approche axée sur la confidentialité garantit aux utilisateurs que leurs applications et données personnelles restent invisibles pour le département informatique.

Un catalogue d'applications d'entreprise peut fournir les applications adéquates sur n'importe quel terminal, notamment :

- Applications Web internes via un navigateur sécurisé et un tunnel VPN transparent
- Applications SaaS avec authentification unique basée sur SAML et infrastructure de provisionnement
- Applications mobiles publiques natives distribuées par courtage de boutiques d'applications publiques
- Applications Windows modernes disponibles via Windows Business Store
- Applications Windows héritées, fournies sous forme de packages MSI ou par déploiement en temps réel avec App Volumes
- Applications de systèmes d'enregistrement stratégiques et sécurisées par un proxy HTML5 grâce à l'hébergement dans le Data Center ou le Cloud du fournisseur avec VMware Horizon® Cloud Service™
- Fourniture de postes de travail complets, gérés et virtualisés dans le Cloud ou dans des Data Centers on premise

Conclusion

Avec la prolifération des applications, services et données s'exécutant sur une multitude de plates-formes et utilisés sur un grand nombre de terminaux, notre approche de la sécurité doit changer en profondeur.

En s'appuyant sur un espace de travail numérique, les entreprises peuvent virtualiser les applications ou des postes de travail complets et assurer automatiquement leur provisionnement sur le Cloud ou sur une infrastructure on premise. Les utilisateurs peuvent y accéder à partir de n'importe quel terminal.

COMMENCEZ DÈS AUJOURD'HUI

Découvrez les moyens de simplifier les déploiements Windows.

EN SAVOIR PLUS >

Rejoignez-nous en ligne :

Sources :

1. IDC, U.S. Mobile Worker Population to Surpass 105 Million by 2020 (le nombre de travailleurs mobiles aux États-Unis devrait dépasser 105 millions d'ici 2020), 23 juin 2015
2. GlobalWorkplace Analytics.com, Latest Telecommuting Statistics (dernières statistiques en matière de télétravail), 2005 – 2015
3. Fierce Mobile IT, 2017

vmware

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.com/fr