3 MANIÈRES DE RÉDUIRE LES PERTES DE DONNÉES

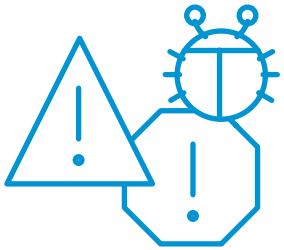
Protégez vos informations avec la stratégie de sécurité appropriée

vmware®

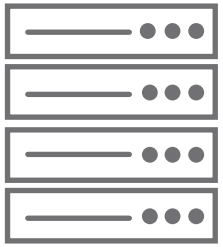
La sécurité est plus importante que jamais

La rapide évolution du paysage numérique actuel favorise la croissance des risques de sécurité. Les personnes, les appareils et les objets sont plus connectés que jamais, d'où une augmentation du nombre de terminaux à protéger par le département informatique. Dans le même temps, les environnements évoluent rapidement pour devenir plus dynamiques, ce qui complique la détection et le traitement des menaces.

Pour préserver la sécurité des informations, le département informatique doit sécuriser l'ensemble des interactions entre les utilisateurs, les applications et les données, une tâche d'autant plus difficile que ceux-ci ne cessent de se déplacer et de se multiplier. Il est cependant hors de question de baisser les bras, et l'enjeu est trop important pour continuer à se reposer sur les solutions de sécurité traditionnelles, désormais dépassées.



3,62 M $
Coût moyen d'une violation de données en 2017, contre 3,2 M $ en 2015[1]



+20 %
Augmentation de la cybercriminalité entre 2010 et 2016 ; parmi toutes les causes de panne de Data Center, c'est celle qui connaît la croissance la plus rapide[2]

740 357 $
Coût moyen d'une panne de Data Center en 2016[3]

1. Ponemon Institute, Étude des coûts liés aux atteintes à la sécurité en 2017 : aperçu mondial, juin 2017
2, 3. Ponemon Institute, « Cost of Data Center Outages », janvier 2016

Prévention des pertes de données au travail : les problématiques d'entreprise

La gestion d'utilisateurs, de terminaux et de modèles de propriété disparates à l'échelle de toutes les plates-formes s'avère de plus en plus complexe.

Les équipes informatiques sont confrontées à de nombreux défis, notamment :

- Octroyer des autorisations d'accès distinctes aux différents types d'utilisateurs
- Gérer les différents modèles de propriété, tels que : terminaux personnels (BYO) ; terminaux appartenant à l'entreprise ; ou terminaux appartenant à l'entreprise et personnalisés par les utilisateurs (COPE)
- Préserver la visibilité sur un nombre croissant de types de terminaux, notamment mobiles, tout-terrain, IdO et ordinateurs portables
- Assurer l'accès à un nombre sans précédent de plates-formes, dont iOS, Android, Windows, macOS et Chrome OS
- Rester en phase avec le paysage en perpétuelle mutation des cybermenaces : exploits, logiciels malveillants, botnets et autres

Le fardeau de la conformité s'alourdit

Le département informatique a également la responsabilité de gérer les risques et la conformité, ce qui représente une charge particulièrement importante dans les secteurs d'activité fortement réglementés tels que les services financiers et la santé. Mais en réalité, tous les secteurs d'activité sont concernés. À mesure que les départements informatiques développent leur infrastructure et adoptent le Cloud public, les enjeux de conformité ne font que gagner en importance.

Prévention des pertes de données au travail : problématiques liées aux utilisateurs

Pour les utilisateurs aussi, l'ère numérique peut être synonyme de complexité croissante. Aussi indispensables soient-elles, les mesures de sécurité peuvent nuire à l'expérience des utilisateurs lorsqu'elles bloquent inutilement l'accès à certaines données ou introduisent des contraintes qui ralentissent leur travail au point de susciter leur exaspération. Soucieux de maintenir leur productivité, les collaborateurs chercheront alors un autre moyen de mener à bien leurs tâches. Ils risquent ainsi de basculer dans « l'informatique parallèle », c'est-à-dire de télécharger des applications ou de recourir à des solutions de contournement non conformes aux règles mises en place par le département informatique.

Autant les collaborateurs tiennent à accéder à toutes les ressources dont ils ont besoin, autant ils sont préoccupés par le risque d'exposer leurs informations personnelles à leur employeur. Si le respect de la vie privée et la disponibilité d'un accès sans restrictions constituent une priorité pour les collaborateurs, il demeure que même des tâches aussi banales que le partage de fichiers ou la réception de courriers électroniques peuvent compromettre la sécurité des données.

Les utilisateurs ne vont pas renoncer pas à leurs terminaux et applications personnels, mais le département informatique ne peut pas prendre le risque de perdre des informations au quotidien. Comment les départements informatiques peuvent-ils sécuriser les données, les utilisateurs et les applications sans dégrader la facilité d'utilisation et la productivité ? Tout commence par une approche stratégique de l'espace de travail numérique.

L'amélioration de la protection des données, une question d'approche avant tout

Avec une stratégie d'espace de travail numérique, vous avez l'assurance que votre entreprise est protégée. Plus qu'une simple technologie, une stratégie d'espace de travail numérique donne au département informatique le moyen de passer d'une approche axée sur la standardisation et la gestion des actifs à un modèle privilégiant les utilisateurs, qui renforce la sécurité et optimise l'expérience utilisateur quels que soient le terminal, le réseau, le site et le système d'exploitation.

VMware propose une plate-forme d'espace de travail numérique unifiée offrant de nombreuses possibilités au département informatique :

1. Développer une stratégie de gestion d'accès englobant les applications Cloud et les applications mobiles natives
2. Moderniser la gestion du cycle de vie des applications de façon à intégrer le chiffrement et l'effacement des applications et des données associées
3. Virtualiser les applications et les postes de travail de telle sorte qu'ils ne laissent jamais aucune trace

Nous allons explorer ces différentes possibilités dans les pages qui suivent.

1. Développer une stratégie de gestion d'accès englobant les applications Cloud et les applications mobiles natives

Une conception intrinsèque de la sécurité permet d'intégrer la protection dans chaque composant du fabric numérique, depuis le Data Center jusqu'au Cloud. Cette approche prévient toute faille de sécurité en couvrant l'ensemble des utilisateurs, des appareils et des cas d'usage à l'échelle de l'infrastructure applicative et du parc de terminaux. Elle requiert également une solution de gestion d'accès complète protégeant les applications et les données d'entreprise présentes sur n'importe quel réseau.

VMware rend cette approche possible en proposant des solutions qui englobent les utilisateurs, les terminaux, les applications, les données et les réseaux.

La solution de gestion d'accès de VMware réunit les composants suivants :

- Accès avec authentification unique à toutes les ressources, notamment les applications et infrastructures natives, Web, distantes, virtuelles et Windows
- Authentification multifacteur sur tous les terminaux
- Catalogue d'applications permettant d'accéder instantanément à l'ensemble des applications et services informatiques
- Fonctions de libre-service pour les utilisateurs
- Restriction de l'accès Administrateur en fonction du rôle
- Approche axée sur la confidentialité qui garantit aux utilisateurs que leurs applications et données personnelles restent invisibles pour le département informatique
- Tunnellisation VPN par application, qui permet une sécurisation extrêmement efficace des terminaux mobiles distants

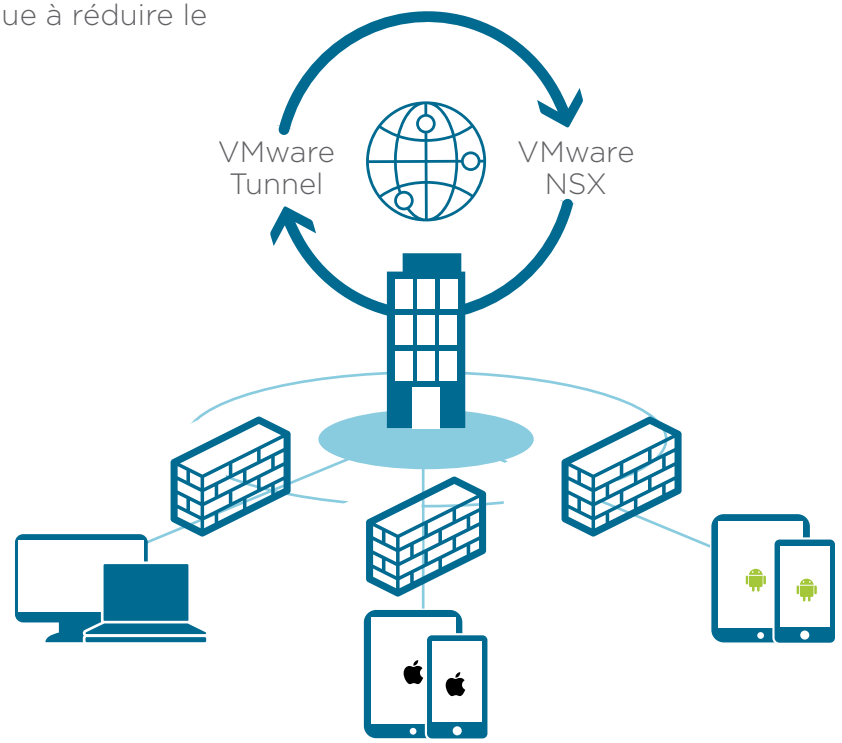
Changer la donne : du VPN de terminal à la tunnellisation par application

Méthode traditionnelle pour accéder aux données stockées sur le réseau d'entreprise, le VPN de terminal comporte des failles de sécurité. Si l'une des applications installées sur le terminal contient un logiciel malveillant, celui-ci pourra s'introduire sur le réseau de l'entreprise.

VMware a donc opté pour une approche plus puissante appelée VPN par application, ou VMware Tunnel, qui permet à chaque application d'accéder par VPN aux ressources de l'entreprise résidant sur un réseau interne sécurisé. En associant VMware Tunnel avec VMware NSX®, le département informatique peut renforcer encore la sécurité à l'échelle du réseau d'entreprise en recourant à la micro-segmentation, qui contribue à réduire le risque de propagation des logiciels malveillants au sein du Data Center.

Le VPN par application offre les avantages suivants :

- **Connexion silencieuse.** Lors du lancement d'une application autorisée, VMware Tunnel établit une connexion silencieuse, qui offre un accès transparent et sécurisé sans demander à l'utilisateur de se connecter au VPN d'entreprise.
- **Accès restreint.** Cette approche met en place une sécurité de niveau application en autorisant uniquement certaines applications internes ou publiques à accéder aux ressources de l'entreprise.
- **Trafic sécurisé.** Il est également possible d'associer VMware Tunnel à NSX pour bénéficier de la micro-segmentation, qui permet de sécuriser le trafic est-ouest au sein du Data Center contenant les applications et données d'entreprise.



2. Moderniser la gestion du cycle de vie des applications de façon à intégrer le chiffrement et l'effacement des applications et des données associées

Face à la prolifération des utilisateurs et des terminaux, le département informatique doit avoir la possibilité de protéger les données de l'entreprise par chiffrement, au moyen de codes d'accès et de règles de prévention des pertes de données, ou encore par verrouillage et effacement du contenu des terminaux compromis.

Les contrôles suivant des règles prédéfinies fournis par VMware offrent de nombreuses possibilités au département informatique :

- Préserver la sécurité des informations personnelles des utilisateurs
- Maintenir la sécurité sans détériorer l'expérience utilisateur
- Fournir un dispositif de sécurité complet de bout en bout
- Définir des règles d'accès fondées sur les données, le terminal, les applications, l'utilisateur et l'emplacement
- Limiter le partage de contenu entre les applications professionnelles au moyen de puissantes règles de prévention de perte de données incluant notamment le contrôle du copier-coller, le chiffrement et le géoblocage

Mais les contrôles suivant des règles prédéfinies ne constituent qu'un aspect de l'automatisation de l'informatique.

La visibilité, la planification et l'automatisation intelligentes comme leviers d'amélioration de la sécurité

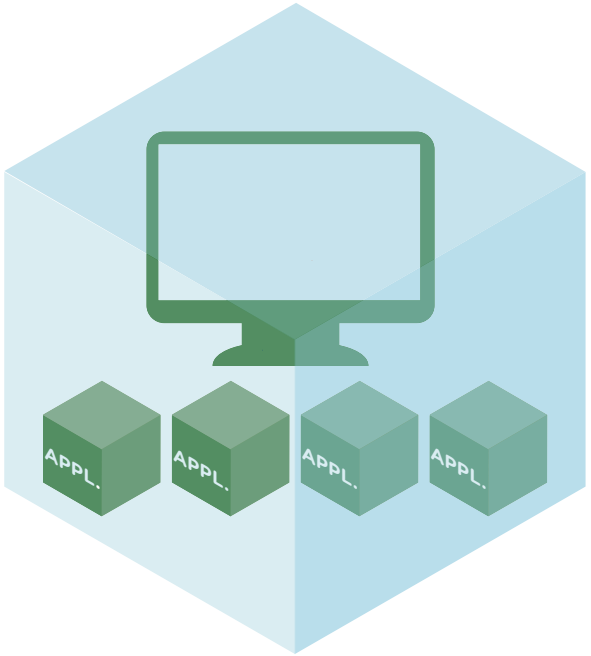
L'interprétation de la masse de données relatives aux terminaux, aux applications et aux utilisateurs d'une entreprise nécessite le recours à des technologies intelligentes. Visibilité améliorée, capacités de planification intelligente des déploiements et fonctions d'automatisation avec actions correctives : voilà trois façons de mettre à profit les informations fournies par une plate-forme d'espace de travail numérique. Celles-ci permettent également d'améliorer la sécurité, la conformité et l'expérience utilisateur au sein de l'environnement d'espace de travail numérique.

Le gain de visibilité permet au département informatique d'explorer et d'interroger l'environnement afin d'analyser les données, d'identifier les tendances et de détecter les anomalies. La planification des déploiements d'applications et de règles permet au département informatique de distribuer les correctifs et les règles de sécurité de manière plus intelligente. L'automatisation des processus informatiques aide à améliorer la sécurité et à garantir la conformité.

VMware simplifie la gestion de la sécurité en rassemblant tous ces éléments ci-après sur une console unique :

- Gestion adaptative donnant aux utilisateurs la possibilité d'adopter des programmes BYO
- Règles d'accès conditionnel en fonction du risque permettant de protéger les droits d'accès
- Actions correctives automatisées avec détection des menaces aux niveaux application, utilisateur, terminal ou réseau
- Plate-forme de conformité conçue pour standardiser l'automatisation et rationaliser la mise en conformité
- Cadre de conformité prenant en charge l'exécution de services de sécurité supplémentaires, on premise ou dans le Cloud

3. Virtualiser les applications et les postes de travail de telle sorte qu'ils ne laissent jamais aucune trace



La solution d'espace de travail numérique de VMware donne au département informatique la possibilité de déployer en toute sécurité des applications publiées et des postes de travail virtuels (VDI). Une fois l'environnement virtualisé, les utilisateurs bénéficient en tout lieu d'un accès sécurisé à leurs applications et postes de travail Windows. Pour renforcer la sécurité, un accès cloisonné grâce aux applications virtuelles garantit que les terminaux non approuvés n'atteignent jamais le réseau d'entreprise, tandis que les utilisateurs distants peuvent accéder aux applications d'entreprise dont ils ont besoin.

Cette approche de l'espace de travail numérique va au-delà de l'effacement des applications sur les ordinateurs portables ou fixes potentiellement non sécurisés, perdus ou volés : elle offre le moyen d'englober la gestion des identités et la gestion intégrée des terminaux pour un contrôle renforcé.

Les fonctionnalités sous-jacentes sont les suivantes :

- Gestion des mots de passe
- Effacement/actualisation des postes de travail virtuels à chaque connexion
- Règles conditionnelles
- Contrôle des accès utilisateur
- Sauvegarde centralisée
- Application centralisée des correctifs

Vous pouvez également associer les applications publiées et les postes de travail virtuels avec VMware NSX, de façon à renforcer la sécurité en isolant les réseaux par micro-segmentation pour l'ensemble du trafic est-ouest du Data Center.

N’attendez plus pour minimiser votre risque

Compte tenu de la volatilité du paysage actuel des cybermenaces, il n’est pas trop tôt pour faire le point sur les risques de violations de sécurité et de pertes de données. Et si la sécurisation des données se présente comme un défi, elle est néanmoins parfaitement réalisable. En adoptant une solution d’espace de travail numérique leader du marché, vous pouvez transformer votre sécurité informatique en une approche visible, rationalisée et très efficace.

VMware propose la solution d’espace de travail numérique dont vous avez besoin pour réduire les risques de violations concernant l’ensemble de vos données, applications et utilisateurs – sans aucun compromis sur la facilité d’utilisation ou d’accès. Avec une plate-forme logicielle omniprésente couvrant à la fois l’infrastructure et les terminaux, vous pouvez répondre aux besoins de votre activité et de vos utilisateurs. Pourquoi ne pas commencer maintenant ?

COMMENCER DÈS AUJOURD’HUI !

En savoir plus sur les espaces de travail numériques >
Testez un espace de travail numérique dans le cadre d’un laboratoire d’essai en ligne >

Rejoignez-nous en ligne :

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