VMWARE WORKSPACE ONE TRUST NETWORK

Sécurité pour l'espace de travail numérique évolutif

EN BREF

VMware Workspace ONE™ Trust Network™ met en œuvre une approche sécuritaire complète et moderne pour protéger les collaborateurs, les applications, les terminaux et les réseaux des entreprises. Grâce à ses capacités de protection, de détection et de suppression des menaces modernes, Workspace ONE Trust Network renforce les fonctionnalités de sécurité inhérentes à la plate-forme Workspace ONE intelligente en s'appuyant sur un écosystème enrichi de solutions de partenaires intégrées, afin d'assurer en continu la surveillance des risques et d'appliquer des mesures correctives rapides dans l'espace de travail numérique.

PRINCIPAUX AVANTAGES

Workspace ONE Trust Network simplifie la sécurité et la gestion en s'appuyant sur un cadre de confiance et de vérification. Grâce à Workspace ONE Trust Network, les départements informatiques peuvent :

- Supprimer les silos dans les solutions de sécurité à l'aide d'une structure d'actions qui fournit une vue agrégée et réduit la complexité à l'échelle de l'espace de travail numérique
- Combiner la sécurité et la gestion des accès, des terminaux et des applications grâce à des analyses intégrées et des fonctionnalités d'automatisation pour réduire les risques à l'échelle d'un écosystème informatique d'utilisateurs
- Profiter d'un écosystème de partenaires ouvert et sécurisé et continuer à utiliser les investissements existants afin de réduire les coûts

La sécurité, principal obstacle à une stratégie moderne d'espace de travail numérique

Un espace de travail numérique permet de multiplier la productivité des collaborateurs par 5[1] en leur offrant un accès simple et sécurisé aux applications et données sur le terminal de leur choix. En parallèle des entreprises qui poursuivent leur transition vers la transformation digitale, l'écosystème de collaborateurs, d'applications, de terminaux et de réseaux se développe et évolue au-delà du périmètre traditionnel, avec des tendances courantes telles que l'adoption de programmes BYOD et la consumérisation de l'informatique. Et à mesure que les barrières traditionnelles sautent, des cybermenaces avancées telles que les attaques Zero-Day, les attaques d'intercepteur, le hameçonnage, les robots et les rançongiciels commencent à émerger.

Dans les domaines de la mobilité et de l'espace de travail numérique, la sécurité est la priorité majeure en matière d'investissement[2]. Pourtant, du fait qu'ils reposent uniquement sur les fonctions de sécurité legacy et cloisonnées, les outils utilisés ne fournissent qu'une visibilité limitée au département informatique. Cette configuration se traduit par des solutions de fortune qui grèvent les coûts des entreprises, en raison de la complexité et des interventions manuelles requises pour protéger un espace de travail numérique. Aujourd'hui, la sécurité est donc le principal frein au développement d'une stratégie moderne dans ce domaine.

Sécurité complète et prédictive dans une entreprise non cloisonnée

Afin de répondre aux besoins de sécurité sans nuire à l'expérience utilisateur, de nouvelles exigences doivent être satisfaites :

1. Pour obtenir une vue agrégée, les entreprises doivent utiliser un cadre pour établir une relation de confiance entre les composants qui protègent leur écosystème.
2. Pour une réduction en continu des risques, les entreprises doivent pouvoir observer leur environnement pour prendre des décisions prédictives et automatisées liées à la protection de leur espace de travail numérique.

Workspace ONE Trust Network met en œuvre une approche sécuritaire complète et moderne pour protéger les collaborateurs, les applications, les terminaux et les réseaux des entreprises. Workspace ONE Trust Network fournit un ensemble de fonctionnalités qui reposent sur un cadre de confiance et de vérification, et qui permettent de protéger, d'identifier et de supprimer les menaces affectant un espace de travail numérique évolutif. L'établissement de la confiance au niveau de l'espace de travail numérique entraîne la création d'un système interconnecté de privilège minimum qui autonomise les collaborateurs tout en garantissant la sécurité. Afin de gérer les risques inhérents aux cybermenaces modernes, Workspace ONE Trust Network combine les analyses de la plate-forme Workspace ONE intelligente avec les solutions de partenaires de confiance pour fournir une sécurité prédictive et automatisée.

1 Source : https://www.vmware.com/radius/impact-digital-workforce/

2 CCS Insights Mobile Technology Buyer Survey (décembre 2017)

Protéger, détecter et corriger

La question n'est pas de savoir si une entreprise sera touchée par une cyberattaque, mais quand elle le sera. Face à ces menaces, les équipes en charge de la sécurité et des opérations informatiques peuvent gérer les risques de cybersécurité en simplifiant le mappage des fonctions de sécurité, en utilisant par exemple le cadre de cybersécurité (CSF) du NIST, sur les fonctionnalités de Workspace ONE Trust Network :

- La sécurité commence par la protection de l'espace de travail numérique ; il s'agit notamment d'empêcher tout logiciel malveillant de se propager à l'aide de technologies d'autoapprentissage, de bloquer l'exfiltration de données issues des applications d'entreprise basées dans le Cloud, et de micro-segmenter les réseaux pour combattre les menaces persistantes avancées.
- Les menaces qui s'introduisent dans l'espace de travail numérique peuvent être détectées grâce à une surveillance continue et évolutive, qui peut s'effectuer tant sur les postes de travail que sur les terminaux et applications mobiles des équipes de la sécurité et des opérations.
- Une fois que les menaces sont détectées, Workspace ONE Trust Network peut automatiser les actions correctives en s'appuyant sur un puissant moteur de décisions. Lorsqu'une attaque est identifiée sur la base d'anomalies comportementales, il est possible de mettre en application une règle automatisée permettant de bloquer l'accès aux données d'entreprise.

Unifier la gestion et la sécurité des accès, des terminaux et des applications grâce à des données chiffrées

Workspace ONE Trust Network associe les fonctionnalités de sécurité inhérentes à la plate-forme Workspace ONE intelligente, qui inclut la protection et la gestion des accès, des terminaux et des applications, à des capacités d'analyse, et ce afin de relier les silos que génèrent les solutions de sécurité. Le service Workspace ONE Intelligence exécute des fonctions d'analyse sur la plate-forme Workspace ONE ; il regroupe, met en corrélation et recommande également des données sur l'espace de travail pour fournir une visibilité intégrée et de puissantes capacités d'automatisation. Dans le monde moins cloisonné d'aujourd'hui, en intégrant les fonctionnalités de Workspace ONE Trust Network avec le service Intelligence, les entreprises peuvent assurer une surveillance des risques en continu et appliquer des mesures correctives rapides.

Afin de détecter les menaces et d'automatiser les actions correctives grâce à des règles d'accès, un moteur de décisions contribue à mettre en corrélation des informations portant notamment sur les terminaux d'entreprise hors réseau avec le comportement des utilisateurs. Une visibilité intégrée sur les menaces et sur l'état précis de conformité des terminaux permet facilement d'identifier et d'éliminer les problèmes de sécurité en temps réel, améliorant ainsi le niveau de sécurité dans l'espace de travail numérique. Grâce au moteur de décisions, le département informatique peut créer des règles pour automatiser et optimiser les tâches courantes, telles que la mise à niveau des terminaux Windows 10 vulnérables avec des correctifs majeurs, et la configuration de contrôles d'accès conditionnel aux applications et services au niveau d'un groupe ou de chaque utilisateur.

Profiter d'un vaste écosystème de solutions de partenaires de confiance

Une relation de confiance doit être établie entre les composants permettant de sécuriser un espace de travail numérique qui se développe et évolue. Workspace ONE Trust Network fournit un cadre de confiance en exploitant les API reposant sur la plate-forme Workspace ONE. Ces API permettent à un vaste écosystème de solutions de sécurité de communiquer avec Workspace ONE et de fournir la vue agrégée dont les administrateurs ont besoin pour simplifier la sécurité et la gestion. En reliant les silos inhérents aux solutions de sécurité, les clients peuvent s'appuyer sur leurs investissements existants pour améliorer considérablement la surveillance continue et l'analyse des risques, ce qui permet d'accélérer les temps de réponse. Résultat : une stratégie de sécurité prédictive, qui s'appuie sur des tendances et des modèles, pour évoluer avec le déploiement.

EN SAVOIR PLUS

Pour en savoir plus sur Workspace ONE Trust Network, rendez-vous sur : www.vmware.com/fr/products/workspace-one/security

Essayer gratuitement un laboratoire d'essai en ligne : https://www.vmware.com/go/workspace-hol

POUR EN SAVOIR PLUS OU POUR ACHETER DES PRODUITS VMWARE,

APPELEZ
le numéro international +1-650-427-5000,

VISITEZ
http://www.vmware.com/fr/products, ou recherchez un revendeur agréé sur Internet.

Principales fonctions

Les entreprises peuvent profiter de ces fonctionnalités de sécurité essentielles que fournit Workspace ONE Trust Network pour renforcer la protection, et identifier et supprimer les cybermenaces en constante évolution.

FONCTIONNALITÉ	DESCRIPTION
Plate-forme d'espace de travail numérique de base qui relie les solutions de sécurité	Simplifiez la sécurité et la gestion grâce à un cadre de confiance qui s'appuie sur des API pour permettre à un écosystème de sécurité ouvert de communiquer avec Workspace ONE.
Gestion des accès qui simplifie votre activité	Permettez à l'équipe informatique de provisionner les applications et de fournir un catalogue en libre-service, une authentification à plusieurs facteurs et une authentification unique (SSO) pour toutes les applications.
Règles contextuelles qui optimisent l'expérience utilisateur et la sécurité	Contrôlez l'authentification grâce à des règles d'accès conditionnel basées sur l'état de conformité du terminal, la force de l'authentification de l'utilisateur, la sensibilité des données, l'emplacement des utilisateurs et bien plus.
Règles de prévention des pertes de données (DLP) qui contribuent à éviter les fuites	Activez le chiffrement au niveau du terminal, le chiffrement des données et les règles relatives à la sécurité du matériel. Configurez des règles, y compris des listes noires d'applications, la sécurité du Wi-Fi et la mise en œuvre des services TLS. Vérifiez la présence de menaces, de logiciels malveillants, d'attaques en mémoire ou de logiciels débloqués, et résolvez automatiquement les problèmes identifiés à l'aide du verrouillage à distance, de l'effacement du contenu du terminal, du blocage des accès ou de contrôles de quarantaine des terminaux personnalisables.
Sécuriser les applications sans sacrifier l'expérience utilisateur	Utilisez des contrôles de sécurité intégrés dans les applications de productivité sécurisées de VMware : VMware Boxer™, Browser™ et Content Locker™. Détectez les menaces et automatisez les actions correctives pour l'ensemble des autres services Cloud et applications.
Chiffrement des données inactives et des données en cours de transfert	Authentifiez et chiffrez le trafic issu des applications sur les terminaux au sein du Data Center à l'aide de VMware Tunnel. Sécurisez les données au repos et les données en cours de transfert via le chiffrement AES 256 bits.
La micro-segmentation automatise la sécurité des réseaux	Réduisez la surface d'attaque dans le Data Center grâce aux fonctionnalités de micro-segmentation de VMware NSX® qui automatisent la sécurité sur l'ensemble du réseau.
Analyses intégrées et fonctions d'automatisation qui favorisent une sécurité prédictive	Identifiez et éliminez les problèmes de sécurité en temps réel grâce à une visibilité intégrée sur les données des menaces et sur l'état précis de conformité des terminaux fournie par Workspace ONE Intelligence.

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
Copyright © 2018 VMware, Inc. Tous droits réservés. Ce produit est protégé par les lois des États-Unis et internationales sur le copyright et la propriété intellectuelle. Les produits VMware sont couverts par un ou plusieurs brevets, répertoriés à l'adresse http://www.vmware.com/go/patents. VMware est une marque ou une marque déposée de VMware, Inc. et ses filiales aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et appellations commerciales mentionnées sont des marques déposées par leurs propriétaires respectifs. Référence : 130019wf-vmw-fy19q1 euc launch-trust network-ds-a4-106
3/18