COMPRENDRE LA GESTION UNIFIÉE DES TERMINAUX

Surmonter les problèmes de sécurité des terminaux et construire un environnement plus fort.

Quest | KACE™ | ITPro Today™

Table des matières

Introduction

Auparavant, la gestion et la sécurisation des terminaux étaient des tâches relativement simples. Chaque fois qu'une organisation ajoutait un utilisateur, le service informatique déployait un nouvel ordinateur de bureau ou portable, le connectait au réseau et le chargeait d'un logiciel antivirus pour lutter contre les logiciels malveillants. Il collait un code-barres sur chaque ordinateur portable en espérant qu'il ne se perde pas.

Puis, tout a changé. Les smartphones, les tablettes et toute une variété d'appareils mobiles spécifiques ont fait leur apparition, et la gestion des terminaux s'est considérablement complexifiée. La complexité s'est encore accrue lorsque les organisations ont commencé à adopter leurs propres stratégies BYOD (apportez vos appareils personnels), qui permettent aux salariés d'accéder aux données de l'entreprise avec des smartphones, tablettes et ordinateurs portables personnels. Le BYOD est une pratique courante aujourd'hui, avec 44 % des entreprises qui l'ont adopté et 19 % qui envisagent de le faire, selon une étude Informa Engage commandée par Quest Software.

Cela a créé de sérieux problèmes de gestion et de sécurité, mais les solutions de gestion des appareils mobiles (MDM, Mobile Device Management) ont soulagé les organisations. Et juste au moment où il semblait que le défi avait été relevé, l'Internet of Things (IoT) est venu poser de nouveaux problèmes.

L'IoT relie les appareils entre eux et avec les humains pour collecter et analyser les données. Des capteurs et des traqueurs capturent les données dans divers environnements et les transmettent via Internet, des réseaux cellulaires ou des réseaux sans fil dédiés. Lorsque les données atteignent leur destination, elles sont analysées et, si nécessaire, déclenchent une action. Il peut s'agir d'envoyer une alerte à un véhicule connecté pour l'informer d'un accident à venir. Si les données proviennent d'un appareil de monitoring sur un patient, l'action pourrait être d'envoyer une ambulance à un patient sur le point d'avoir un accident vasculaire cérébral ou une attaque Si l'alerte indique qu'une machine est sur le point de tomber en panne, un technicien peut être envoyé sur place pour la réparer.

Les appareils connectés seront bientôt quatre fois plus nombreux que les êtres humains, car ils dépasseront la barre des 30 milliards en 2020. Les équipes informatiques et de cybersécurité devront gérer non seulement les terminaux traditionnels tels que les postes de travail, les ordinateurs portables et les smartphones, mais aussi une quantité vertigineuse de terminaux connectés à l'IoT, notamment des capteurs et traqueurs installés sur les équipements de fabrication, les oléoducs, les véhicules, les palettes d'expédition, et même les personnes équipées de stimulateurs cardiaques, pompes à insuline et autres dispositifs de monitoring. Certains environnements connectés comprendront des dispositifs de toutes formes, disséminés sur de vastes zones géographiques.

GESTION UNIFIÉE DES TERMINAUX

À mesure que les terminaux prolifèrent, se diversifient et se dispersent, les organisations ont besoin de solutions automatisées et centralisées de gestion unifiée des terminaux (UEM). Les solutions UEM permettent de traiter tous les appareils d'un environnement de la même manière, quels que soient la taille, le système d'exploitation et l'emplacement. Elles apportent une certaine uniformité à la gestion des terminaux, permettant aux administrateurs de spécifier les règles et fonctionnalités pour déployer, inventorier, configurer et sécuriser tous les dispositifs connectés.

Les solutions UEM permettent aux organisations de rationaliser la prolifération rapide et la diversité croissante des terminaux, car elles permettent de :

- Gérer tous les appareils de manière cohérente à partir d'une console centrale
- Sécuriser tous les terminaux, quels que soient leur emplacement et leur système d'exploitation
- Suivre et inventorier les logiciels afin de garantir le respect des contrats de licence
- Assurer la conformité aux réglementations et normes industrielles applicables afin d'éviter les amendes et de réduire au minimum les risques d'infraction en cas de non-conformité

Les terminaux sont les dispositifs sur lesquels les utilisateurs effectuent la majeure partie de leur travail avec des applications de productivité, de communication et de collaboration. Il n'est pas surprenant que ce soit là que se produisent la plupart des vulnérabilités de sécurité, les pirates informatiques trouvant constamment de nouveaux moyens de s'introduire dans les réseaux. Cela fait peser une pression importante sur les équipes informatiques et de cybersécurité chargées de protéger les appareils, les utilisateurs et le réseau.

Plus le nombre d'appareils augmente, plus le défi devient difficile à relever, surtout si vous essayez de gérer et de sécuriser manuellement les terminaux. Les administrateurs ont besoin de visibilité et de fonctionnalités de suivi dans les environnements de terminaux, c'est pourquoi une gestion unifiée des terminaux est nécessaire et se développe en tant que technologie.

DANS CE LIVRE ÉLECTRONIQUE

Les pages suivantes analysent en profondeur les facteurs qui favorisent le développement de la gestion des terminaux, en particulier la nécessité de suivre, sécuriser et gérer tous les types de dispositifs connectés à partir d'une solution UEM automatisée et centralisée.

CHAPITRE 1

La sécurité des terminaux devient de plus en plus complexe

La sécurité des terminaux est un enjeu majeur pour les organisations d'aujourd'hui. C'est l'une des principales raisons pour lesquelles les entreprises déploient une gestion unifiée des terminaux (UEM). Les appareils se connectant au réseau ont proliféré ces dernières années sous l'effet des plateformes mobiles et des stratégies BYOD, mais cela ne sera bientôt plus qu'un lointain souvenir en comparaison de ce qui est à venir. Avec la mise en œuvre de l'IoT, le nombre d'appareils connectés va augmenter de façon exponentielle dans un avenir proche.

Deux groupes d'utilisateurs d'ordinateurs surveilleront de près cette croissance fulgurante : les services informatiques et les pirates informatiques Pour les cybercriminels, un plus grand nombre d'appareils signifie plus de possibilités de s'introduire dans les réseaux, de provoquer des perturbations et de voler des données importantes. Les cybercriminels ont des motivations différentes pour détourner les données des organisations. La principale étant le profit ; les pirates informatiques savent que les dossiers médicaux personnels, les numéros de carte de crédit et de compte bancaire peuvent leur rapporter beaucoup d'argent au marché noir. Les autres sont le cyberespionnage, la rancune et le cyberactivisme.

Les services informatiques et les équipes de cybersécurité reconnaissent qu'avec un si grand nombre d'appareils qui s'infiltrent dans les réseaux d'entreprise, leur travail se complique. Il devient plus difficile et plus chronophage de suivre et de protéger tous les appareils du réseau. Dans une étude réalisée en 2018 par Performa Engage pour Quest Software, 62 % des personnes interrogées ont déclaré que le nombre de dispositifs IoT ou BYOD dans leur organisation avait augmenté au cours des deux dernières années, et 69 % s'attendent à ce que cette tendance se poursuive.

Les cybermenaces sont de plus en plus sophistiquées et dangereuses. S'en défendre exige une vigilance constante. Alors que la main-d'œuvre devient de plus en plus mobile et disséminée, et que l'IoT se développe, les organisations ont besoin d'une visibilité totale de leur environnement pour protéger leurs données et leurs utilisateurs. Elles ont besoin d'une gestion automatisée, simplifiée et centralisée de l'UEM. Sans cela, elles courent de grands risques :

- Les vulnérabilités des réseaux et des applications passent inaperçues, laissant le champ libre aux pirates informatiques pour s'introduire dans le réseau.
- Certains terminaux ne sont pas pris en compte parce que l'environnement n'a pas été correctement inventorié ou contrôlé. Si vous ne pouvez pas voir tous vos terminaux, vous ne pouvez pas les gérer ou les sécuriser.
- L'accès aux actifs stratégiques n'est pas réglementé, car les administrateurs n'ont pas une visibilité totale et ne peuvent donc pas mettre en place les contrôles nécessaires.

En raison de l'effort herculéen requis pour sécuriser les terminaux, il peut être tentant de maintenir le statu quo et de les gérer manuellement ou d'utiliser des solutions disparates qui ne communiquent pas entre elles. Une telle démarche est chronophage, coûteuse et dangereuse. Sans automatisation, il est presque impossible de mettre en œuvre des stratégies et pratiques uniformes. Le risque d'erreur humaine est plus élevé, ce qui peut ajouter des vulnérabilités que les cybercriminels peuvent exploiter. Et c'est une chose que toutes les organisations doivent éviter, sachant que selon le Ponemon Institute, la cyberviolation moyenne coûte 3,86 millions de dollars en perte de productivité et vente, atténuation et réputation.

62 % des personnes interrogées ont constaté une **augmentation de l'utilisation des appareils IoT ou BYOD** au cours des 2 dernières années.

69 % **s'attendent à ce que les tendances se poursuivent** avec **des augmentations** au cours des 2 prochaines années.

Préoccupations liées à la gestion des terminaux

À mesure que les terminaux se multiplient et se diversifient, leur gestion devient plus complexe et plus longue. Il arrive un moment où les organisations ne sont plus en mesure de gérer et de sécuriser correctement tous leurs terminaux sans une certaine automatisation et surveillance. C'est ce qui ressort de l'étude Informa/Quest, qui a révélé que bien que 81 % des organisations comptent plusieurs sites, seulement 19 % possèdent une stratégie UEM pour tous leurs utilisateurs. Avec de plus en plus d'applications mobiles ayant accès à des données d'entreprise sensibles, c'est une question qui ne peut être laissée de côté.

L'absence de plan de gestion cohérent et unifié des terminaux place les organisations dans une situation précaire. Les cybermenaces s'intensifient. Si le volume global des menaces est peut-être en baisse, le nombre de menaces critiques présentant un potentiel de dommages plus élevé est en augmentation. De nouvelles souches plus malignes de logiciels malveillants, notamment des variantes de rançongiciels qui peuvent traverser les continents en quelques heures, continuent d'apparaître. Cela signifie que les menaces deviennent de plus en plus dangereuses à mesure que le nombre de terminaux augmente. Tout dispositif qui n'est pas correctement sécurisé est en réalité une incitation manifeste à s'introduire dans le réseau.

Actuellement, la principale préoccupation des organisations concernant les terminaux est de prévenir les logiciels malveillants et autres exploits. C'est le cas des deux tiers des réponses (67 %) recueillies par Informa/Quest. Venaient ensuite :

- Gestion centralisée efficace (45 %)
- Fonctionnalités de correction et de mise à jour des logiciels faciles à gérer (39 %)
- Correction et endiguement des activités malveillantes et vulnérabilités potentielles (38 %)
- Détection des activités malveillantes après l'exécution (34 %)

Parmi les autres préoccupations figurent le temps nécessaire au déploiement des stratégies de gestion, le risque de perte de données, le manque de gestion, les médiocres fonctionnalités d'inventaire et la complexité associée au fonctionnement d'un trop grand nombre de consoles pour assurer la sécurité. Il est trop difficile de résoudre l'un ou l'autre de ces problèmes sans l'automatisation et la visibilité qu'une solution UEM peut apporter.

ITPro Today

Quest

Les enjeux de la gestion des terminaux

Les organisations sont confrontées à de multiples difficultés pour sécuriser les terminaux. Même si les vulnérabilités informatiques diminuent globalement, les menaces et les exploits critiques sont en augmentation. Les équipes de cybersécurité doivent travailler plus dur et plus longtemps pour sécuriser leurs environnements.

ENJEU : PROLIFÉRATION DES DISPOSITIFS

Le nombre d'appareils ne cesse d'augmenter. La plupart des entreprises doivent non seulement suivre et sécuriser les appareils appartenant à l'entreprise, mais aussi ceux qui relèvent des programmes BYOD. Cela complique encore la sécurisation du réseau, car les administrateurs doivent séparer les données personnelles des données de l'entreprise et mettre en place des contrôles d'accès appropriés aux ressources de l'entreprise.

Le nombre d'entreprises qui ont subi une violation liée aux solutions BYOD est relativement faible : 12 %, selon l'étude Informa/Quest. Mais parmi elles, 62 % ont dû procéder à un audit. Si un audit réalisé par un organisme de régulation révèle qu'une entreprise n'a pas mis en place de contrôles de sécurité adéquats, celle-ci peut devoir payer une amende.

SOLUTION : SUIVI DES TERMINAUX

La solution Quest KACE Cloud Mobile Device Manager (MDM) aborde le problème de la prolifération des appareils en suivant les appareils mobiles et en les gérant à distance, ce qui permet aux organisations de gérer efficacement les programmes BYOD ainsi que les appareils mobiles appartenant à l'entreprise à partir d'un tableau de bord central. La solution KACE Cloud MDM identifie, inventorie, sécurise et contrôle à distance tous les appareils qui accèdent au réseau. Si un appareil mobile vient à manquer, les administrateurs peuvent le verrouiller et en effacer le contenu afin d'assurer la sécurité des données de l'entreprise.

60 % des personnes interrogées sont plus susceptibles de **corriger et/ou de mettre à jour** leurs terminaux à l'aide d'une **plateforme centralisée**.

1/3 des personnes interrogées **font état de difficultés ou de complications** concernant les correctifs et les mises à jour.

ENJEU : IDENTIFIER LES MENACES ET Y REMÉDIER

Le paysage des menaces est vaste et change constamment. Entre 80 000 et 360 000 nouvelles variantes de logiciels malveillants sont découvertes chaque jour. Cela signifie que les réseaux sont continuellement attaqués, et que les organisations ont besoin d'un moyen rapide et efficace pour identifier les menaces et y remédier.

SOLUTION : RECRÉATION AUTOMATISÉE DES IMAGES DES TERMINAUX

L'appliance de déploiement de systèmes KACE (SDA) recrée les images des terminaux au moyen d'un processus automatisé. Cela permet aux administrateurs de recréer rapidement les images des terminaux, tant sous Windows que sous MacOS, dès qu'ils soupçonnent qu'un logiciel malveillant a infecté un système, empêchant ainsi la propagation d'une infectionqui pourrait entraîner des temps d'arrêt.

ENJEU : GÉRER LES MISES À JOUR

La prolifération des dispositifs complique les mises à jour des terminaux, qui sont nécessaires pour remédier aux vulnérabilités pouvant conduire à une infection par un logiciel malveillant. Aussi critique que soit l'application des correctifs, force est de constater que trop souvent les organisations ne formalisent pas la gestion des correctifs, ce qui peut avoir de graves conséquences. En 2017, les attaques des rançongiciels WannaCry et Petya ont franchi les frontières et les continents en exploitant des vulnérabilités logicielles non corrigées. WannaCry a même interrompu les opérations dans certains hôpitaux britanniques, ce qui a coûté environ 92 millions de livres (120 millions de dollars) au NHS (National Health Service).

La plupart des personnes interrogées (60 %) dans le cadre de l'étude Informa/Quest ont déclaré être plus enclines à corriger et/ou mettre à jour leurs terminaux si elles disposent d'une plateforme centralisée. Environ un tiers (34 %) des personnes interrogées ont fait état de problèmes liés à la correction des terminaux, tels que le manque de visibilité des appareils appartenant aux salariés et les difficultés à prendre en charge différents types d'appareils et de systèmes d'exploitation.

SOLUTION : AUTOMATISATION DE LA GESTION DES CORRECTIFS DES TERMINAUX

L'appliance de gestion des systèmes (SMA) Quest KACE centralise et automatise la gestion et le déploiement des correctifs. Ainsi, les administrateurs peuvent envoyer des correctifs sur les bons appareils au bon moment, et confirmer que les stratégies et règles de conformité sont appliquées sur les appareils appartenant à l'entreprise et sur les appareils BYOD. Cela renforce la cohérence du processus et minimise le risque d'erreur, ce qui crée des environnements informatiques plus sûrs.

ENJEU : CONTRÔLER L'ACCÈS DES UTILISATEURS

Donner accès à un trop grand nombre d'utilisateurs à des systèmes contenant des données d'entreprise sensibles peut entraîner des violations de sécurité. Les utilisateurs ne devraient avoir accès qu'aux systèmes dont ils ont besoin pour faire leur travail, mais souvent les administrateurs ne peuvent même pas savoir qui accède à quoi, car ils n'ont pas de visibilité sur tous les terminaux.

SOLUTION : RESTREINDRE LES PRIVILÈGES DES UTILISATEURS

La solution Quest KACE Privilege Manager apporte une solution à ce problème en attribuant aux utilisateurs des niveaux de droits d'administration différents sur leurs machines Windows. Par défaut, les utilisateurs se voient attribuer des droits de moindres privilèges pour accéder aux systèmes dont ils ont besoin, et seuls certains utilisateurs reçoivent des droits d'administrateur. Ainsi, les utilisateurs non autorisés ne peuvent pas accéder aux données sensibles et les infecter au moyen de logiciels malveillants.

ENJEU : SÉCURISER LES PORTS USB

Les terminaux regroupent aussi les imprimantes, appareils photo, disques externes et autres appareils munis de ports USB à divers emplacements. Laissés sans surveillance, les ports USB de ces appareils peuvent être exploités pour introduire des logiciels malveillants dans le réseau.

SOLUTION : RESTREINDRE L'ACCÈS USB

Les administrateurs peuvent restreindre l'accès aux ports USB à l'aide de la solution Quest KACE Desktop Authority, qui sécurise les terminaux équipés de ports USB tels que les lecteurs de DVD, les imprimantes, les appareils photo et autres périphériques externes. En utilisant une approche de moindres privilèges, les administrateurs ont un contrôle granulaire sur qui a accès à quels ports USB et où afin de bloquer les logiciels malveillants et prévenir le vol de données.

La solution : une gestion unifiée des terminaux (UEM)

Il est clair que la prolifération des dispositifs et la complexité croissante des environnements informatiques ont introduit de nouveaux défis de sécurité pour les organisations. Ces défis ne feront que s'aggraver à mesure que la diversité et le nombre de dispositifs continueront d'augmenter avec la mise en œuvre de l'IoT. Les entreprises ont besoin d'une sécurité efficace des terminaux, sans quoi elles mettent leurs données et leurs utilisateurs en danger, car les pirates ne se lassent pas de tenter de s'introduire dans les réseaux pour voler des données.

La solution Quest UEM comprend cinq composants principaux : l'appliance de gestion des systèmes (SMA) Quest KACE, l'appliance de déploiement de systèmes KACE (SDA), la solution Quest KACE Cloud Mobile Device Manager (MDM), la solution KACE PM (Privilege Manager) et la solution KACE DA (Desktop Authority). La solution UEM Quest apporte une cohérence dans la gestion et la protection des environnements informatiques. Les solutions KACE sont faciles à déployer et ne demandent aucune expertise en matière d'implémentation ou d'intégration. Une interface intuitive permet aux utilisateurs de résoudre les problèmes par eux-mêmes tout en offrant un tableau de bord centralisé qui donne aux administrateurs une visibilité sur l'ensemble de l'environnement.

Depuis la console centrale, les administrateurs peuvent surveiller l'environnement, définir des règles de sécurité et mettre en œuvre un programme automatisé de gestion des correctifs qui garantit que les vulnérabilités des terminaux sont toujours traitées en temps utile. Comme nous l'avons déjà indiqué, les correctifs sont essentiels, car les vulnérabilités non corrigées sont faciles à exploiter. KACE simplifie le processus d'application des correctifs, en permettant une approche du type « on le configure et on l'oublie ».

La visibilité sur l'environnement est absolument essentielle pour le protéger, et c'est quelque chose qui fait défaut à trop d'organisations. Il est facile de comprendre pourquoi cela pose problème : si vous ne savez pas qu'un appareil est là, vous ne pouvez pas le gérer ou le protéger.

La solution UEM Quest sécurise et contrôle uniformément les ordinateurs de bureau, ordinateurs portables, smartphones et tablettes. Ceci permet entre autres de gagner du temps et de simplifier la gestion de l'ensemble de l'environnement informatique, notamment des sites distants et des appareils IoT. Le gain de temps et la simplicité sont des attributs appréciés par les équipes chargées de l'informatique et de la cybersécurité. Dans l'étude Informa/Quest, l'avantage le plus souvent cité par les personnes interrogées (58 %) était l'amélioration de la sécurité des appareils et des données en la rendant moins chronophage. Elles recherchaient également une expérience utilisateur cohérente pour tous les types d'appareils (49 %) et la simplification de la gestion des appareils BYOD, mobiles et IoT (48 %).

La solution UEM Quest répond à toutes ces exigences et apporte la tranquillité d'esprit en garantissant que les terminaux sont correctement protégés et fermés aux cybercriminels. Avec la simplicité et l'uniformité de la gestion qu'offre la solution UEM Quest, l'environnement est plus sûr et mieux géré.

58 %

assurent une meilleure **sécurité des appareils et des données** en rendant l'opération moins chronophage.

49 %

créent une **expérience utilisateur cohérente** pour tous les types d'appareils.

48 %

Simplification de la gestion des appareils **BYOD, mobiles et IoT**.

45 %

Accès et prise en charge à distance des **appareils des utilisateurs**.

CHAPITRE 2

S’attaquer au casse-tête de la conformité des terminaux

Au-delà de la sécurité, la conformité est le plus grand défi que les organisations doivent relever dans le cadre de leurs stratégies de gestion unifiée des terminaux (UEM). Tous les terminaux doivent être conformes aux réglementations gouvernementales, aux normes industrielles et aux contrats de licence logicielle. Selon une étude réalisée par Informa Engage pour Quest Software, plus de la moitié des entreprises (54 %) ont mis en place des obligations de conformité, et 19 % élaborent des plans pour les mettre en œuvre.

La mise en œuvre d'une stratégie de conformité des terminaux est impérative, puisque chaque organisation ou presque est soumise à un certain type de réglementation ou d'exigence de norme industrielle. Les entreprises doivent aussi respecter des critères d'utilisation des logiciels et des stratégies internes qui empêchent les utilisateurs d'introduire des vulnérabilités dans le réseau. Si vous exercez une activité commerciale, vous ne pouvez pas vous soustraire à cette conformité.

Mais la mise en conformité est compliquée. Sur le plan de la réglementation, les organisations doivent faire face à un patchwork complexe de lois et obligations qui changent à mesure que de nouvelles lois entrent en vigueur. En 2018, l'Union européenne a instauré le Règlement général sur la protection des données de l'Union européenne (RGPD). Peu de temps après, la loi CCPA (California's Consumer Privacy Act) qui protège les données personnelles des résidents de l'État est entrée en vigueur. D'autres États sont susceptibles de suivre l'exemple de la Californie en adoptant des lois de type RGPD.

Ces changements exigent des organisations qu'elles réévaluent et actualisent fréquemment leurs stratégies de conformité. Il est difficile de tout suivre, mais le non-respect des règles a des conséquences, notamment des amendes réglementaires, des actions en justice, des violations de sécurité et la perte de confiance des partenaires et des clients. Le non-respect des critères d'utilisation des logiciels peut aussi entraîner des amendes, des poursuites judiciaires et même la perte de licences.

Heureusement, une aide est disponible sous la forme de solutions UEM automatisées et centralisées qui offrent une visibilité totale sur tous les terminaux, et facilitent et rendent plus efficace la mise en œuvre des règles de conformité.

Réglementations gouvernementales

Les réglementations gouvernementales s'appliquent à des industries et à des fonctions commerciales spécifiques. La loi HIPAA (Health Insurance Portability and Accountability Act) exige que les hôpitaux, cliniques, cabinets médicaux et compagnies d'assurance protègent les dossiers médicaux. La loi SOX (Sarbanes Oxley) régit les pratiques comptables. La loi GLBA (Gramm-Leach-Bliley) porte sur les informations privées des investisseurs financiers. Le RGPD protège les informations personnelles des résidents de l'UE en imposant des limites strictes à toute entité qui touche aux données.

Normes industrielles

Les normes industrielles les plus courantes auxquelles les entreprises doivent se conformer sont les normes PCI DSS (Payment Card Industry Data Security Standard) et ISO (International Organization for Standardization). Toute entité qui traite des paiements par carte de crédit doit respecter les règlements PCI DSS conçus pour protéger les informations des titulaires de cartes de paiement contre la fraude et le vol. La conformité ISO concerne les normes d'interopérabilité et de pratiques commerciales. Elle constitue une marque de confiance pour les organisations qui cherchent à établir des partenariats ou à effectuer des transactions avec d'autres.

Quest

Conformité logicielle

Le plus grand défi que doivent relever les organisations en matière de conformité des logiciels tourne autour des audits de vérification de la conformité des licences Microsoft. Tout client détenant une licence Microsoft pourrait être sélectionné à tout moment pour un audit visant à s'assurer qu'il respecte les conditions de sa licence.

Stratégies internes

Dans certains cas, la conformité est auto-infligée. Les organisations émettent des stratégies d'utilisateur final pour sauvegarder leurs actifs numériques par des processus d'authentification à partir de divers types de dispositifs. Cela permet de contrôler et de sécuriser les terminaux, en particulier lorsque des stratégies BYOD (apportez vos appareils personnels) qui compliquent la prévention des utilisations non autorisées sont en place.

Conséquences de la non-conformité

La conformité est une question de protection. Que ce soit dans le cadre des réglementations, des normes industrielles ou des licences logicielles. La non-conformité a des conséquences, notamment des violations de sécurité, des coûts liés aux corrections, des frais juridiques et réglementaires. Une entreprise qui enfreint la norme PCI, par exemple, peut perdre le privilège de traiter les cartes de crédit.

Sur le plan réglementaire, les amendes sont une conséquence tangible de la non-conformité. La menace d'un audit réglementaire est toujours présente dans des circonstances normales, et devient une quasi-certitude après une violation. En cas de négligence, une organisation risque d'être condamnée à une amende. Le RGPD est particulièrement strict avec des amendes punitives.

Toute personne victime de la violation, y compris les clients et les partenaires, peut également intenter une action en justice. Les recours collectifs sont une conséquence courante des violations. Les organisations peuvent aussi perdre la confiance de leurs clients, partenaires et fournisseurs, ce qui a des répercussions sur les résultats.

Concernant la conformité logicielle, des amendes peuvent également être infligées si une entreprise abuse de son contrat de licence. Microsoft et d'autres fournisseurs n'hésitent pas à faire payer des amendes. De nombreux cas documentés ont été recensés où Microsoft a infligé des amendes à des clients pour non-respect de la licence.

Une surutilisation des licences peut également entraîner des poursuites judiciaires de la part des fournisseurs, ce qui peut avoir des conséquences sur les résultats d'une organisation. Il y a un revers à la médaille : une sous-utilisation entraîne des dépenses excessives inutiles et détourne le budget d'autres projets informatiques.

Les enjeux de la conformité

Il ne fait aucun doute que la conformité est un casse-tête majeur pour les organisations. Les exigences changent constamment, ce qui rend le contrôle et la maintenance permanents absolument nécessaires. À mesure que les données et les appareils se multiplient, la mise en conformité des logiciels devient de plus en plus longue et ajoute le risque de non-conformité aux obligations réglementaires et industrielles. Dans l'étude Informa/Quest, 45 % des personnes interrogées ont déclaré qu'il était difficile de respecter les obligations de conformité, et 41 % s'inquiètent de faire l'objet d'un audit et de se voir infliger une amende en cas de violation.

ENJEU : SUIVRE TOUS LES APPAREILS

Plus le nombre d'appareils augmente, plus il devient difficile de les suivre, surtout lorsque des stratégies BYOD sont en place. Les utilisateurs téléchargent parfois leurs propres logiciels, ce qui rend encore plus difficile le suivi de l'utilisation des logiciels et du nombre de licences dont dispose une entreprise. Avec la mise en place de l'Internet of Things (IoT), le suivi des dispositifs devient encore plus délicat.

SOLUTION : VISIBILITÉ EN TEMPS RÉEL

L'appliance de gestion des systèmes (SMA) Quest KACE fournit une vue complète de l'utilisation des logiciels et de la mise en œuvre en temps réel dans l'entreprise, ce qui permet de simplifier la gestion des actifs et d'entretenir plus efficacement les appareils des utilisateurs finaux. L'appliance KACE SMA dresse l'inventaire de tous les appareils, identifiant les logiciels sur- ou sous-utilisés, afin que vous puissiez prendre les mesures nécessaires pour assurer la conformité.

ENJEU : PROLIFÉRATION DES DISPOSITIFS MOBILES

Smartphones, tablettes et ordinateurs portables sont devenus les outils de travail de tout un chacun. La main-d'œuvre est de plus en plus mobile et éloignée, ce qui exige de recourir à des appareils mobiles pour effectuer les tâches quotidiennes et se connecter aux ressources du réseau. Les stratégies BYOD permettent aux utilisateurs d'accéder aux systèmes de l'entreprise avec leurs propres appareils. Si elles ne sont pas correctement suivies et sécurisées, cela peut poser de sérieux risques, exposant les organisations à des violations de sécurité et à des vols potentiels de données.

SOLUTION : SURVEILLANCE EN TEMPS RÉEL

La solution Quest KACE Cloud Mobile Device Manager (MDM) offre une visibilité en temps réel de tous les types d'appareils mobiles depuis une console centrale. Elle peut être intégrée à l'appliance Kace SMA afin de simplifier la gestion. Avec la solution KACE MDM, les administrateurs peuvent gérer les applications téléchargées et assurer la conformité aux licences logicielles. Les inventaires des appareils mobiles à la demande fournissent des données sur les attributs des appareils, les stratégies configurées, les profils installés, les certificats et les paramètres réseau pour les connexions Wi-Fi et VPN.

ENJEU : PRÉVENIR LES INFRACTIONS À LA RÉGLEMENTATION

La conformité aux normes en vigueur est compliquée. Les entreprises doivent connaître les lois, comprendre leurs exigences et s'assurer qu'elles sont respectées. Chaque loi a des oblations et des objectifs différents, mais la plupart exigent de limiter l'accès des utilisateurs afin d'éviter tout risque de non-conformité et de sécurité. Les privilèges d'administrateur local ne devraient pas être accordés à des utilisateurs dont le travail ne l'exige pas, mais il est difficile de savoir quels utilisateurs devraient avoir quels privilèges.

SOLUTION : GÉRER LES PRIVILÈGES DES UTILISATEURS

La solution Quest KACE Privilege Manager permet de s'assurer que seuls les utilisateurs qui ont besoin de droits d'administrateur en disposent. Il est ainsi plus facile de se conformer aux réglementations et normes industrielles telles que HIPPA, SOX, GLBA et PCI. La solution Quest KACE Privilege Manager permet aux organisations d'élever le processus, et non l'utilisateur, ce qui leur permet d'être prêtes pour les audits tout en étant sûres de leur conformité.

Une meilleure conformité avec la gestion unifiée des terminaux

Les obligations de conformité sont une réalité pour les entreprises. La plus courante est liée à la loi HIPAA, qui a été citée par 39 % des participants à l'étude Informa/Quest. Venaient ensuite le RGPD européen (37 %), et les normes ISO (36 %) et PCI DSS (25 %). En plus de ces exigences, les organisations doivent également se conformer aux contrats de licence logicielle ainsi qu'aux stratégies internes visant à promouvoir des pratiques informatiques sûres.

Sans une visibilité totale, l'automatisation et la surveillance en temps réel de tous les terminaux d'une organisation, la conformité est pratiquement impossible. Les organisations ont besoin d'une approche unifiée. La solution de gestion unifiée des terminaux (UEM) Quest assure le suivi de tous les terminaux, notamment les ordinateurs de bureau, appareils mobiles, routeurs, imprimantes et appareils IoT, depuis un tableau de bord centralisé. La solution UEM Quest comprend l'appliance de gestion des systèmes (SMA) Quest KACE, l'appliance de déploiement de systèmes KACE (SDA), la solution Quest KACE Cloud Mobile Device Manager (MDM), la solution KACE PM (Privilege Manager) et la solution KACE DA (Desktop Authority). L'appliance Kace SMA inventorie les terminaux chaque fois que cela est nécessaire pour s'assurer que toutes les obligations de conformité sont respectées, qu'elles soient liées aux réglementations, aux normes industrielles ou aux licences logicielles.

L'appliance Kace SMA automatise les tâches de gestion des terminaux de manière cohérente, ce qui permet aux entreprises d'économiser du temps et de l'argent en remplaçant les processus de conformité manuels et en garantissant une utilisation correcte des licences logicielles. Avec sa fonctionnalité de gestion des licences logicielles, elle optimise la gestion des licences logicielles, en évitant la surutilisation et en éliminant la sous-utilisation des licences, qui est coûteuse. Avec ses fonctionnalités de création de rapports complètes, l'appliance Kace SMA fournit la preuve de la conformité, essentielle en cas d'audit.

La solution UEM Quest répond à un enjeu important pour toute organisation informatique. Préparez, rassemblez, maintenez et examinez les licences logicielles afin d'être toujours prêt pour le prochain audit. D'un point de vue réglementaire, elle permet de s'assurer que toutes les lois sont respectées, ce qui réduit les risques de sécurité et protège les entreprises contre les amendes réglementaires.

CHAPITRE 3

L’enjeu de la prolifération des appareils

L'une des principales raisons pour lesquelles les organisations ont besoin d'une solution de gestion unifiée des terminaux tient au fait qu'ils ne cessent de se multiplier. Les terminaux se diversifient également avec la mise en œuvre de systèmes de l'Internet of Things (IoT). Alors que les organisations commençaient à reprendre leur souffle après la croissance exponentielle des appareils mobiles, elles doivent maintenant faire face aux difficultés qu'un boom des appareils connectés est sur le point de créer.

Les terminaux se multiplient pour de bonnes raisons. Les appareils mobiles, ainsi que les appareils connectés qui sont désormais en ligne, contribuent de manière substantielle à la productivité, à l'efficacité et à l'innovation. Les systèmes mobiles relient les utilisateurs entre eux pour communiquer et collaborer sans contraintes géographiques. Les utilisateurs peuvent effectuer des tâches critiques où qu'ils aillent sans devoir respecter les horaires de travail habituels.

Pendant ce temps, l'IoT relie les humains aux machines pour faciliter la collecte et l'analyse des données. La manière dont ces données sont utilisées peut modifier la position concurrentielle d'une entreprise en stimulant l'agilité, l'innovation et, in fine, la rentabilité.

Mais les avantages de la prolifération des dispositifs ont un coût : les administrateurs informatiques doivent relever d'énormes défis pour suivre, gérer et sécuriser les terminaux. Avec le développement de l'IoT, il devient impossible de gérer manuellement les terminaux. Les organisations ont besoin d'une solution UEM pour gérer et sécuriser les terminaux. Il est également essentiel de veiller à ce que le coût de la prolifération des dispositifs ne soit pas supérieur aux avantages qu'elle procure.

Une croissance soutenue

Le nombre de dispositifs connectés devrait dépasser les 30 milliards d'ici 2020. Les applications IoT seront responsables de la majeure partie de ces dispositifs, qui seront quatre fois plus nombreux que les humains.

Une étude menée par Informa Engage pour Quest Software montre que 69 % des organisations ont vu le nombre de leurs appareils augmenter au cours des 18 mois la précédant. Près de la moitié des entreprises (44 %) ont déclaré avoir une stratégie BYOD (apportez vos appareils personnels), ce qui contribue à expliquer l'augmentation du nombre d'appareils. Par ailleurs, 19 % des personnes interrogées prévoient de mettre en œuvre le BYOD dans un avenir proche.

Alors que les entreprises adoptent des stratégies BYOD, augmentant le nombre d'appareils et de systèmes d'exploitation qu'elles doivent gérer, la plupart d'entre elles ont constaté que leur gestion est loin d'être facile. Plus des trois quarts des personnes interrogées (77 %) dans le cadre de l'enquête ont estimé que la gestion de tous ces dispositifs et systèmes d'exploitation était problématique.

À mesure que l'IoT se développe, le problème risque de devenir encore plus difficile à résoudre sans une gestion automatisée des terminaux. Déjà 37 % des organisations disent gérer l'IoT et les appareils connectés, mais 29 % comptent divers appareils connectés non gérés. Comme nous l'avons vu en détail dans le chapitre sur la sécurité, les dispositifs non gérés font courir des risques sérieux aux organisations.

Avantages et enjeux des stratégies BYOD

Les organisations adoptent des stratégies BYOD parce que permettre aux salariés d'utiliser leurs propres appareils au travail présente des avantages. Cela permet de réduire les coûts d'investissement des entreprises, d'augmenter la productivité et de soutenir le moral des salariés en leur permettant d'utiliser leurs appareils préférés. En outre, cela permet aux entreprises de se tenir au fait des nouvelles technologies mobiles par une mise à jour fréquente des appareils.

Des organisations issues de divers secteurs, de la santé à l'éducation en passant par le gouvernement fédéral, récoltent les fruits d'une stratégie BYOD. Les professionnels de la santé utilisent des appareils mobiles pour vérifier les dossiers des patients et recevoir des informations des dispositifs de monitoring, comme les stimulateurs cardiaques et les pompes à insuline. En milieu scolaire, les élèves utilisent smartphones et tablettes pour effectuer des recherches en ligne, faire leurs devoirs et passer des tests d'évaluation en vue de l'obtention d'un diplôme. Les enseignants utilisent les tablettes et smartphones pour faire cours et vérifier le travail de leurs élèves. Les administrateurs utilisent également des tableaux pour évaluer les performances des enseignants et des élèves.

En raison de la nature sensible des données auxquelles accèdent les appareils dans ces conditions, la sécurité est essentielle. Il en va de même dans d'autres secteurs, notamment la finance et les services publics qui traitent et stockent des données très sensibles.

La sécurité et la gestion sont les plus grands défis que posent les stratégies BYOD. Les organisations doivent contrôler l'accès aux données privées et aux sites Web, et empêcher le téléchargement d'applications non autorisées qui pourraient contenir des virus. Pour empêcher une utilisation non autorisée du réseau, les administrateurs doivent suivre, maintenir et mettre à jour les dispositifs BYOD. Si ces questions ne sont pas abordées, elles font courir des risques à l'organisation. Les dispositifs BYOD peuvent créer de nouvelles vulnérabilités qui permettent aux pirates de pénétrer dans les réseaux pour propager une infection et voler des données.

Le facteur IoT

Alors que les organisations s'efforcent de gérer et de sécuriser les dispositifs BYOD, elles doivent commencer à réfléchir aux nouveaux défis posés par la mise en œuvre de l'IoT. Le monde compte déjà plus de 17 milliards d'appareils connectés, dont 7 milliards pour l'IoT, et devrait en compter 25 milliards d'ici 2022.

Les appareils IoT seront déployés dans un nombre presque infini de contextes, notamment les villes intelligentes, les voitures connectées, les sites de construction, les droits pétroliers, les hôpitaux et les cliniques, les bâtiments et les usines automatisés.

Parmi les déploiements IoT existants figurent les capteurs installés sur les systèmes HVAC (chauffage, ventilation et climatisation) et les systèmes mécaniques qui surveillent les performances et envoient des alertes lorsque quelque chose d'inhabituel se produit, comme une augmentation des vibrations ou un changement de température. Dans les établissements scolaires, des tableaux blancs interactifs connectés sont utilisés pour l'apprentissage. Dans les universités, des applications mobiles permettent de suivre les étudiants afin d'assurer leur sécurité, et les étudiants peuvent suivre les bus connectés pour arriver à l'heure en cours. Dans le domaine de la santé, les fonctionnalités de surveillance des pompes à insuline et des stimulateurs cardiaques peuvent prévenir les urgences en alertant le personnel médical si un patient a besoin de soins. Les capteurs de température installés dans les réfrigérateurs des hôpitaux permettent de prévenir l'altération des réserves de sang et les traqueurs sur les fauteuils roulants évitent qu'ils ne se perdent.

Dans certains cas, les appareils connectés sont dotés de nouvelles normes de connectivité et de nouveaux systèmes d'exploitation, ce qui rend la sécurité et la gestion plus complexes. À l'instar des dispositifs informatiques traditionnels, ils devront être surveillés, inventoriés et gérés pour s'assurer qu'ils ne créent pas plus de problèmes qu'ils n'en résolvent.

Les organisations ont besoin d'une solution pour gérer les terminaux traditionnels ainsi que les nombreux nouveaux terminaux qui sont mis en ligne. Cela leur permettra d'assurer la pérennité de leur activité et d'éviter les difficultés que les appareils mobiles peuvent poser aux entreprises qui n'y étaient pas préparées, à savoir un déploiement sans stratégie de gestion ou de sécurité claire.

Relever le défi de la prolifération

Alors que la gestion des dispositifs devient plus complexe, la visibilité des environnements de terminaux est absolument essentielle. Les solutions UEM doivent couvrir tous ces domaines :

- Ordinateurs traditionnels et autres terminaux de réseau
- Appareils BYOD/mobiles
- Une grande diversité de dispositifs connectés

ENJEU : GÉRER TOUS LES TERMINAUX AVEC DES SOLUTIONS MULTIPOINTS

Face à la prolifération des appareils, de nombreuses organisations ont tenté de les gérer soit manuellement, soit à l'aide de solutions multipoints disparates qui gèrent certains appareils, mais pas d'autres. Le résultat final est une solution pour les terminaux traditionnels, une pour les appareils mobiles, et éventuellement des solutions distinctes pour le centre d'assistance, la création d'images et les correctifs.

SOLUTION : GESTION AUTOMATISÉE ET CENTRALISÉE DES APPAREILS

L'appliance de gestion des systèmes (SMA) Quest KACE s'attaque au problème en automatisant les analyses pour découvrir et identifier les dispositifs connectés de tous types. Elle capture un inventaire détaillé du matériel et des logiciels pour les systèmes Windows, Mac, Linux et Unix. L'appliance Kace SMA utilise également les API Google pour inventorier les systèmes d'exploitation et le matériel pour les Chromebooks. Les administrateurs informatiques peuvent saisir des données sur toute une série de dispositifs, notamment l'équipement réseau, les imprimantes et la téléphonie IP.

ENJEU : GÉRER ET SÉCURISER LES TERMINAUX

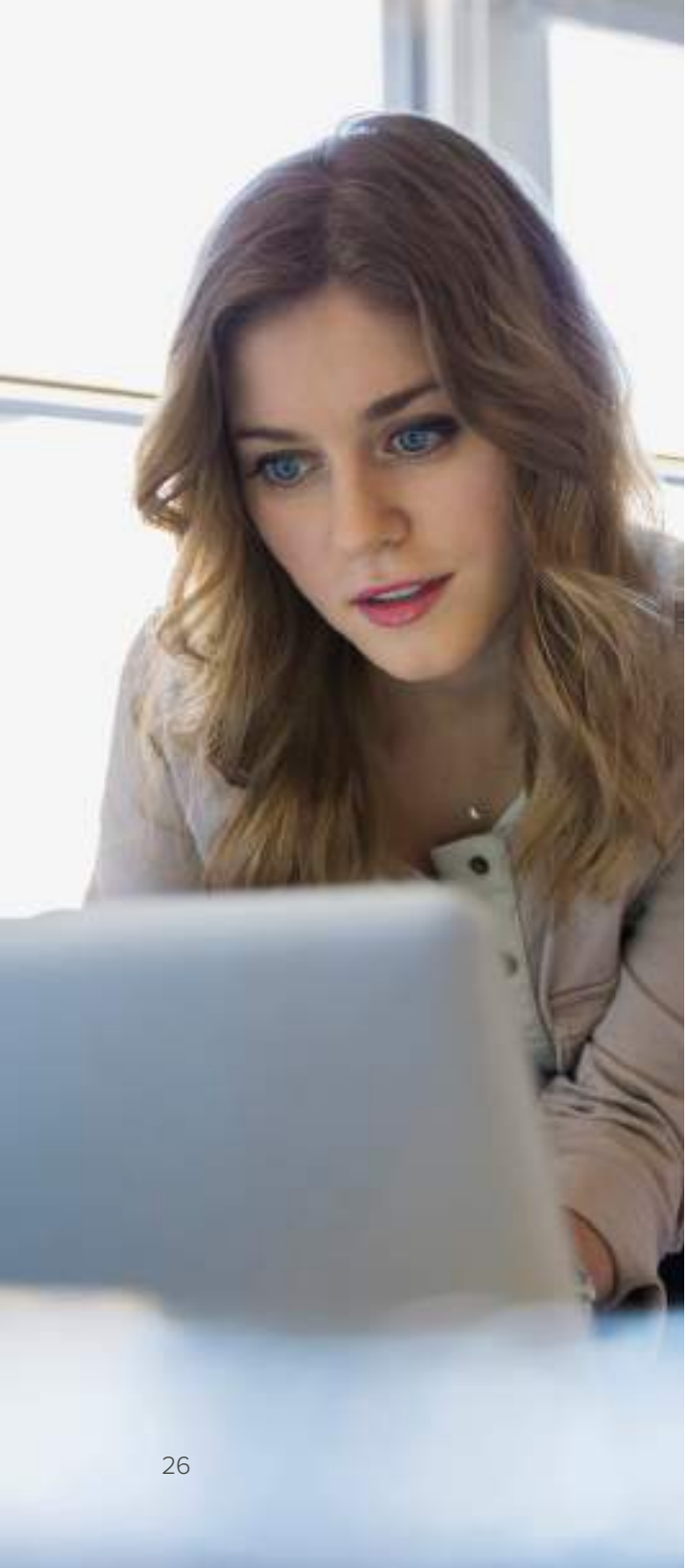
Sans visibilité, automatisation et création d'images rationalisée pour les nouveaux terminaux, il est impossible de gérer et de sécuriser les nouveaux environnements de terminaux hybrides. Si vous ne savez pas combien de dispositifs sont déployés, ni où ils se trouvent, vous ne pouvez pas les gérer ni les protéger. L'inventaire, l'audit et le suivi automatisé des appareils font partie intégrante d'un environnement sûr et bien géré.

SOLUTION : AUTOMATISATION DU DÉPLOIEMENT DES IMAGES ET DE LA GESTION DES ACTIFS

Quest offre une solution unifiée avec des applications interconnectées qui mettent de l'ordre dans la prolifération et la gestion des dispositifs. Le fournisseur associe l'appliance KACE SMA aux solutions suivantes :

La solution Quest KACE Cloud Mobile Device Manager (MDM) suit et gère à distance les appareils mobiles depuis un tableau de bord central, ce qui permet aux organisations de gérer plus facilement la prolifération des appareils. La solution KACE Cloud MDM identifie, sécurise et contrôle tous les appareils qui accèdent au réseau. Si un appareil est volé ou perdu, la solution permet aux administrateurs informatiques de le verrouiller et d'en effacer les données.

L'appliance de déploiement de systèmes KACE (SDA) automatise le déploiement des fichiers de configuration, des états utilisateurs et des applications sous forme d'images vers un dispositif unique ou simultanément vers plusieurs appareils depuis une console centrale. Elle automatise les déploiements dans des environnements hybrides, ce qui permet de pérenniser l'activité en y ajoutant différents types d'appareils connectés.



UEM : visibilité et contrôle parfaits

La solution UEM Quest comprend cinq composants principaux : l'appliance de gestion des systèmes (SMA) Quest KACE, l'appliance de déploiement de systèmes KACE (SDA), la solution Quest KACE Cloud Mobile Device Manager (MDM), la solution KACE PM (Privilege Manager) et la solution KACE DA (Desktop Authority). Les solutions KACE fonctionnent ensemble comme une seule solution UEM avec un riche ensemble de fonctionnalités qui donnent aux organisations une visibilité et un contrôle parfaits sur leurs terminaux. L'approche UEM de Quest hiérarchise les charges de travail en automatisant les processus de gestion des terminaux depuis une console centrale, ce qui permet d'accroître l'efficacité et de consacrer moins de temps à la gestion des terminaux. Elle permet aussi aux organisations de sécuriser tous les terminaux pour empêcher les menaces de les exploiter et de propager l'infection.

L'UEM améliore l'expérience utilisateur en minimisant les processus manuels tout en répondant à un besoin vital des organisations de toutes formes et de toutes tailles, compte tenu notamment du fait que le nombre d'appareils va continuer d'augmenter dans un avenir prévisible. Les utilisateurs et les appareils étant de plus en plus disséminés, la visibilité, l'inventaire, le suivi et les fonctionnalités de sécurité d'une solution UEM complète sont plus que jamais essentiels. À ce titre, la solution UEM Quest aide à préparer les entreprises à leur croissance et à leur réussite futures, et à faire en sorte que la prolifération des dispositifs aide les entreprises à atteindre leurs objectifs.

Ce qu'il faut retenir

Voici les principaux éléments à retenir de ce que vous venez de lire :

SÉCURITÉ

- La sécurité est un enjeu majeur pour les environnements de terminaux d'aujourd'hui, car les menaces se multiplient et deviennent plus dommageables.
- La sécurité est un problème à multiples facettes qui nécessite une approche à plusieurs niveaux basée sur une variété d'outils et de pratiques.
- Une sécurité efficace des terminaux demande une solution centralisée et automatisée qui offre de multiples fonctions, notamment la gestion des correctifs, le contrôle des accès et des privilèges des utilisateurs et une restriction des connexions USB.

CONFORMITÉ

- Les obligations de conformité sont une réalité pour les entreprises et affectent la façon dont les terminaux doivent être gérés et sécurisés.
- Les entreprises doivent mettre en œuvre des politiques de conformité pour satisfaire aux obligations réglementaires et aux normes industrielles, ainsi qu'aux conditions des contrats de licence avec les fournisseurs de logiciels.
- La conformité, qu'elle soit liée aux réglementations, aux normes ou aux licences logicielles exige une visibilité, un suivi et des pratiques d'inventaire efficaces.

PROLIFÉRATION DES APPAREILS

- Bien qu'elle soit bénéfique, la prolifération des appareils crée des défis importants en matière de gestion et de sécurisation des terminaux.
- La croissance rapide du nombre d'appareils va se poursuivre dans un avenir prévisible car l'IoT crée divers écosystèmes de terminaux connectés.
- La gestion de la prolifération des appareils exige une automatisation des fonctionnalités d'analyse, d'identification, d'inventaire, de gestion et de sécurisation des appareils.

Conclusion

Comme la prolifération des appareils va se poursuivre sans relâche dans un avenir prévisible, les organisations doivent se préparer à un avenir connecté dans lequel elles pourront prospérer et réussir face à la concurrence. À mesure que le nombre d'appareils augmente et, avec les utilisateurs, se généralise, les solutions UEM peuvent aider les organisations à renforcer la sécurité, améliorer l'expérience utilisateur et rendre la gestion des appareils plus efficace et plus rapide. Les solutions UEM automatisées permettent aux entreprises de contrôler et sécuriser les appareils existants tout en ajoutant de nouveaux terminaux de manière efficace, systématique et sécurisée. En tant que telles, les solutions UEM pérennisent l'activité de l'entreprise en l'aidant à progresser sur la voie d'un avenir connecté.

À PROPOS DE QUEST

Quest fournit des solutions logicielles adaptées au monde de l'informatique d'entreprise en rapide évolution. Nous simplifions les défis associés à l'explosion des données, à l'expansion dans le Cloud, aux datacenters hybrides, aux menaces de sécurité et aux exigences de conformité. Nous fournissons des solutions à 130 000 entreprises dans 100 pays, dont 95 % des entreprises du classement Fortune 500 et 90 % des entreprises du classement Global 1000. Depuis 1987, nous développons une gamme de solutions qui couvre désormais la gestion des bases de données, la protection des données, la gestion des accès et des identités, la gestion des plateformes Microsoft et la gestion unifiée des terminaux. Avec Quest, les entreprises consacrent moins de temps à la gestion informatique et plus de temps à l'innovation. Pour en savoir plus, consultez le site www.quest.com.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :

www.quest.com/fr-fr/company/contact-us.aspx

Ebook-UnderstandingUEM-US-KS-FR-WL-58230