Microsoft

Déployer de nouvelles technologies comme un pro

4 conseils pour mettre en œuvre une solution matérielle performante et sécurisée

Gérez l'implémentation de nouveaux appareils comme un pro

Quand il s'agit de prendre d'importantes décisions dans le domaine informatique, qui concernent votre service et votre entreprise dans son ensemble, de nombreuses problématiques sont à prendre en compte. Lorsque vous êtes chargé(e) de mettre à jour le matériel informatique de votre société, penchez vous sur les appareils qui protégeront les données de votre entreprise de façon optimale sans générer d'inquiétude supplémentaire.

Ce livre blanc présente quatre conseils pour suivre un processus aussi indolore que possible pour votre équipe informatique et les utilisateurs finaux.

1. Procédez à une intégration en toute transparence
2. Garantissez une sécurité de pointe
3. Respectez les règles de conformité sans renforcer la complexité du réseau
4. Assurez un véritable contrôle sur le matériel

Le déploiement de nouvelles technologies dans votre entreprise pose de nombreuses questions :

- De quel type de nouveau matériel avons-nous besoin ?
- Comment le nouveau matériel s'intègrera-t-il avec celui que nous utilisons déjà ?
- Combien de temps durera la transition ?
- Le nouveau matériel est-il à la hauteur en termes de sécurité ?
- Les avantages des nouvelles technologies compensent-ils le temps et les ressources investis pour leur mise en œuvre ?

Surface peut vous aider à suivre chacun de ces conseils tout en protégeant les données de votre entreprise et en simplifiant la gestion.

CONSEIL 1 :

Choisissez des appareils qui **s'intègrent de manière transparente**

Les logiciels sont souvent disponibles d'un appareil à l'autre, mais le fait de savoir si vous allez perdre du temps ou réduire la productivité pendant la phase de transition matérielle ne devrait pas vous inquiéter. Assurez-vous d'avoir accès aux meilleurs outils et que vos appareils sont à jour.

Dans un monde où chaque minute compte, la mise en œuvre, l'intégration et le déploiement de nouveaux appareils doivent être transparents pour éviter tout risque inutile et gagner un temps précieux.

Surface est conçu pour tirer pleinement parti des fonctions de sécurité disponibles dans Windows 10. Par exemple, la sécurité basée sur la virtualisation crée une bulle de protection autour des solutions de sécurité afin de les préserver des logiciels malveillants. La plateforme unifiée Windows Update assure la distribution homogène des mises à jour des pilotes et des microprogrammes parallèlement aux mises à jour Windows, et ce afin de garantir la sécurité de votre système à tous les niveaux.

Procédez à une intégration en toute confiance grâce à des fonctions de sécurité avancées

Lorsque c'est à vous qu'il revient de moderniser les technologies utilisées au sein de votre entreprise, choisissez des appareils qui tirent profit de l'intégralité des solutions de sécurité disponibles. Faites en sorte que toutes les équipes soient opérationnelles sans exposer votre entreprise à des menaces supplémentaires.

Surface s'intègre parfaitement avec un ensemble complet de fonctions de sécurité Windows.

Antivirus Windows Defender

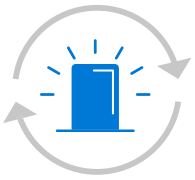
Cette solution anti-programmes malveillants intégrée assure la sécurité et la gestion des ordinateurs de bureau, portables et serveurs.

Protection Cloud

Les nouveaux logiciels malveillants sont détectés et neutralisés en quelques secondes. Inutile d'attendre plusieurs heures pour obtenir une mise à jour des définitions. Vous pouvez même personnaliser les informations partagées sur le Cloud et définir le niveau de blocage des nouveaux fichiers.

Analyse en continu

Les activités suspectes ou malveillantes sont identifiées grâce aux fonctions de protection en temps réel, d'analyse comportementale et de détection heuristique. Ces méthodes peuvent détecter certaines activités, notamment une modification inhabituelle apportée aux fichiers existants, le remplacement ou l'ajout de clés de Registre de type démarrage automatique et d'emplacements de démarrage, ainsi que d'autres ajustements de la structure ou du système de fichiers.



Mises à jour de protection dédiées

Reposant sur l'apprentissage automatique, l'analyse humaine et automatisée du Big Data et des recherches approfondies sur la résistance aux menaces, ces mises à jour garantissent que l'antivirus Windows Defender assure une protection constante.

AppLocker

Les logiciels malveillants ne peuvent pas atteindre les appareils de l'entreprise. Contrôlez les applications et fichiers que les utilisateurs sont autorisés à ouvrir, notamment les fichiers exécutables, scripts, fichiers Windows Installer, bibliothèques de liens dynamiques et applications prêtes à l'emploi (ainsi que leurs programmes d'installation). En éliminant les applications non approuvées, vous réduisez les tâches d'administration, ainsi que le nombre d'appels au support technique.

Bloquez les logiciels indésirables en ajoutant des applications à une liste d'exclusions ou en créant des règles qui autorisent exclusivement le téléchargement de logiciels sous licence sur les appareils.

Effectuez le suivi des applications qui ont accès aux informations de l'entreprise grâce à la gestion des stocks d'applications.

Personnalisez les stratégies en créant des règles spécifiques pour une personne ou un groupe.

Dossiers de travail

Vous accédez aux fichiers stockés dans ces dossiers depuis l'appareil de votre choix, même si vous travaillez en mode hors connexion. D'une part, cela renforce la sécurité car vous pouvez stocker des fichiers de manière centralisée sur un serveur de l'entreprise. D'autre part, cela vous permet d'appliquer des stratégies utilisateur-appareil spécifiques, comme des mots de passe de chiffrement et d'écran de verrouillage.

Des économies alliées à une intégration transparente Lorsque vous procédez à la mise à niveau des technologies de votre entreprise, il faut aussi parler de son coût. Bien entendu, les mises à niveau peuvent se révéler onéreuses, mais les attaques risquent de vous coûter encore plus cher à long terme. Choisissez un appareil de qualité optimale, comme Microsoft Surface Pro, un ordinateur très mobile, convivial et conçu pour Windows 10.

Selon les données recueillies par Gartner, la migration vers un appareil Windows 10 coûte

entre 155 et 242 dollars
par système, mais

entre 256 et 445 dollars
pour un appareil non-Windows 10.[1]

Surface garantit un déploiement simple et sécurisé à tous les membres de votre équipe.

CONSEIL 2 :

Choisissez des appareils qui **garantissent une sécurité de pointe**

Les logiciels malveillants évoluent à un rythme effréné. Il peut donc être difficile pour votre équipe informatique de rester à la page tout en garantissant la meilleure sécurité possible pour les appareils. Entre les stratégies BYOD et le développement des effectifs mobiles, votre équipe informatique doit gérer de plus en plus d'appareils, mais souvent avec le même nombre de ressources.

Selon une étude menée par Ponemon Institute, 67 % des personnes interrogées ne sont pas en mesure de détecter les employés qui utilisent des appareils mobiles non sécurisés.[2] Surface autorise la mobilité sans créer de risques de sécurité supplémentaires.

Grâce à une protection annexe au niveau du matériel, Surface propose des fonctions de sécurité sans égal. Elles permettent de contrôler la configuration matérielle et les processus du système d'exploitation à l'intérieur du microprogramme des appareils, ce qui est intelligemment pensé pour protéger les données, y compris dans les secteurs industriels les plus réglementés.

Surface protège l'utilisateur

Les informations d'identification de votre entreprise sont-elles en danger ?
Les identifiants d'accès aux sites Web, ordinateurs et réseaux constituent souvent la première barrière de sécurité défensive. Malheureusement, en l'absence d'outils de sécurité adéquats derrière le réseau et le matériel, ils représentent un point d'entrée vulnérable aux attaques.

90%

des accès aux applications Web et mobiles seraient réalisés à l'aide d'identifiants volés.[3]

3,3 milliards

d'identifiants auraient été volés en 2016.[3]

Windows Hello Entreprise

Remplacez les mots de passe par une authentification solide à deux facteurs sur les PC et les appareils mobiles. Reposant sur un nouveau type d'informations d'identification utilisateur lié à un appareil, cette méthode d'authentification fait appel à des données biométriques ou un code secret.

Dans la mesure où Surface stocke ces données biométriques sur l'appareil lui-même, elles ne circulent pas et ne sont envoyées à aucun serveur ou appareil externe, ce qui élimine les risques d'usurpation.

Sécurité avancée des appareils mobiles

Les capacités avancées de biométrie et de connexion par reconnaissance faciale ou par empreintes digitales constituent la première ligne de défense contre les menaces, parallèlement à l'authentification à deux facteurs.

Contrôle du matériel et vérification d'identité

Un mécanisme de vérification de l'identité de qualité professionnelle est intégré au matériel Surface. Il utilise une caméra spécialement configurée pour l'imagerie presque infrarouge afin d'authentifier et de déverrouiller les appareils Windows.

Cette caméra permet à Surface de réaliser les opérations suivantes :

- Reconnaissance faciale
- Vérification par authentification unique (SSO) pour déverrouiller Microsoft Passport
- Authentification de qualité professionnelle
- Imagerie constante dans différentes conditions d'éclairage

Les problèmes posés par les mots de passe

Les utilisateurs finaux répètent ou utilisent souvent les mêmes mots de passe. Selon l'institut Preempt, le chiffre inquiétant de 35 % des utilisateurs définissent des mots de passe faibles et les 65 % restants ont des mots de passe qui peuvent être percés.[4] D'après Microsoft, 63 % des intrusions impliquent des mots de passe faibles ou volés.[5] Il est extrêmement difficile d'effectuer le suivi et la gestion des mots de passe forts et de s'en souvenir, mais la sécurité d'une entreprise ne devrait pas être mise en péril à cause d'une erreur humaine.

Windows Hello résout les problèmes suivants :

- Il peut être difficile de mémoriser des mots de passe forts et les utilisateurs entrent généralement les mêmes mots de passe sur plusieurs sites.
- Des failles au niveau des serveurs peuvent exposer des mots de passe/informations d'identification réseau symétriques.
- Les mots de passe sont sujets aux attaques par relecture.
- Les utilisateurs peuvent accidentellement divulguer leurs mots de passe lors d'un hameçonnage.

Microsoft Passport + Windows Hello

Windows Hello Entreprise reconnaît les utilisateurs, puis identifie et authentifie de façon unique l'accès à Windows sur chaque appareil. Opération transparente pour l'utilisateur, Windows Hello transmet des informations d'identification stockées qui font office de facteur d'authentification secondaire pour Microsoft Passport.

CONSEIL 3 :

Choisissez des appareils qui **respectent les règles de conformité sans renforcer la complexité du réseau**

Bon nombre d'entreprises sont tenues de respecter des normes strictes, notamment dans les secteurs bancaire, de la santé (HIPAA) et de l'éducation. Auparavant, il fallait souvent avoir recours à des applications tierces pour atteindre le niveau élevé de conformité requis avec du matériel standard. Cela renforçait la complexité de la gestion pour votre équipe informatique.

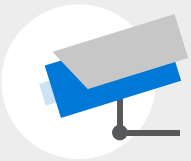
Selon un rapport de Verizon, 80 % des entreprises n'ont pas réussi leur évaluation provisoire en matière de conformité aux normes de sécurité PCI (Payment Card Industry).[6] Ces erreurs peuvent coûter cher à votre entreprise. On peut en effet vous infliger des amendes allant de 5 000 à 100 000 $ par mois pour non-respect de la conformité PCI.[7]

Surface offre des fonctions intégrées qui permettent à votre entreprise de respecter les normes imposées par l'administration.

Sérénité intégrée

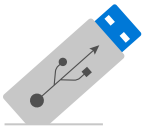
Grâce à des appareils qui proposent des fonctions permettant de respecter les normes administratives, les attentes envers votre service informatique sont réduites et vous profitez d'une plus grande tranquillité d'esprit. Surface est spécifiquement conçu pour atteindre ce niveau de sécurité.

- La technique de prédilection des pirates consiste à passer par le navigateur d'un appareil. Microsoft Edge est conçu pour contrer systématiquement l'hameçonnage, les logiciels malveillants et les attaques d'autre nature. Ainsi, vos collaborateurs peuvent continuer à se rendre sur le Web, votre entreprise reste protégée contre les menaces.
- Microsoft Intelligent Security Graph et l'expertise humaine sur laquelle il repose constituent une barrière de sécurité supplémentaire pour les données de votre entreprise, grâce à des IOC se composant de capteurs et d'éléments optiques exclusifs.



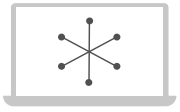
Conformité satisfaisante pour la NSA

La NSA a récemment ajouté Windows 10 et Surface à sa liste de solutions commerciales adaptées aux programmes confidentiels.[8] Utilisés dans une solution à plusieurs niveaux, le système d'exploitation Windows 10 et les appareils Surface peuvent répondre aux exigences les plus strictes en matière de sécurité dans des environnements classés secrets.



Surface Data Eraser

Cet outil se lance à partir d'une clé USB et vous permet d'effacer toutes les données stockées sur un appareil compatible avec Surface de manière sécurisée. Si vous ne parvenez plus à déverrouiller un appareil ou si vous devez procéder à sa réinitialisation pour une raison quelconque, vous pouvez effectuer cette opération en toute sécurité. Cela réduit le temps nécessaire pour réinitialiser un appareil, que ce soit après son utilisation par un ancien employé ou avant son envoi en réparation.



Administration et gestion de Microsoft BitLocker

Vous disposez de capacités de gestion d'entreprise et de fonctions centralisées de surveillance de la conformité et de génération de rapports. Par ailleurs, le déploiement et la récupération de clés sont simplifiés, et les coûts associés à la configuration et à la prise en charge des lecteurs chiffrés baissent.

CONSEIL 4 :

Choisissez des appareils qui **permettent d'assurer un véritable contrôle sur le matériel**

Dans l'environnement technologique actuel, chaque professionnel de l'informatique est en première ligne pour renforcer la cybersécurité de son entreprise.

Cela ne veut pas dire que les équipes IT se contentent de protéger votre entreprise contre l'hameçonnage ou les logiciels malveillants passant par un navigateur Internet. S'ils ne sont pas protégés et surveillés correctement, les périphériques intégrés (comme les caméras, ports USB et microphones) peuvent exposer des informations sensibles aux menaces.

Même vos collaborateurs férus de technologie peuvent être victimes d'une attaque. D'après une étude menée par les universités de l'Illinois et du Michigan en collaboration avec Elie Bursztein, 48 % des personnes qui trouvent une clé USB par hasard la connectent à leur ordinateur.[9] Un utilisateur ne peut pas s'imaginer que ce geste en apparence banal conduit parfois à une tentative d'intrusion. Votre entreprise est alors exposée à une forte menace de sécurité.

En ajoutant Surface à votre boîte à outils pour vous préserver efficacement des menaces (et les contrer, le cas échéant), les données de votre entreprise sont mieux protégées.

Le contrôle Cloud vous protège contre les menaces pesant sur les périphériques
Il vous permet aussi de surveiller activement leur sécurité. Vous pouvez soit désactiver l'utilisation de périphériques de manière proactive, soit réagir efficacement en cas d'intrusion. Windows Defender associe des capteurs intégrés dans le système d'exploitation à de puissants outils de sécurité Cloud. Cela représente une barrière de protection supplémentaire pour neutraliser les menaces liées aux périphériques sur les appareils eux-mêmes. Le Cloud d'analyse de la sécurité détecte les attaques qui ont réussi à déjouer tous les autres systèmes de défense en utilisant à la fois l'analyse comportementale et l'apprentissage automatique et en se fondant sur des informations récentes et historiques.

La protection du matériel de votre entreprise est une opération transparente sur les appareils Surface que vous pouvez gérer et surveiller pratiquement partout à distance.

Surface Enterprise Management Mode (SEMM)
Ce mode de gestion d'entreprise permet aux clients de gérer les paramètres du microprogramme de leurs appareils Surface. Ils peuvent notamment désactiver des périphériques, comme un port USB ou une caméra.

Implémentez une solution matérielle sécurisée en toute confiance

Prendre des décisions en matière de technologies représente un défi de taille. Si une entreprise ne dispose pas des outils adéquats, elle s'expose à des violations de sécurité qui peuvent lui coûter cher. C'est pourquoi il faut absolument choisir des appareils qui s'intègrent parfaitement, garantissent une sécurité de pointe, proposent des fonctions intégrées pour que votre entreprise respecte les normes administratives et puisse exercer un véritable contrôle sur le matériel. Optez pour une solution qui réunit tous ces critères.

Surface est conçu pour répondre à toutes ces attentes et bien d'autres encore. Procédez à sa mise en œuvre dès aujourd'hui.

Découvrez quels produits Surface conviennent à votre entreprise.

Sources :

1. « Faire des choix de déploiement critiques pour réussir avec Windows 10 », Gartner (2016)
2. « Le coût des appareils mobiles non sécurisés sur le lieu de travail », Ponemon (2014)
3. « Rapport sur le vol d'identifiants en 2017 », Shape Security (2017)
4. « 35 % des utilisateurs définissent des mots de passe faibles et les 65 % restants ont des mots de passe qui peuvent être percés », Preempt (2017)
5. « Conçu pour être la version la mieux sécurisée de Windows à ce jour », Microsoft
6. « Rapport sur la conformité à la norme PCI », Verizon (2015)
7. « Les conséquences de la non-conformité à la norme PCI », PCI DSS (2017)
8. « Solutions commerciales adaptées aux programmes confidentiels », NSA
9. « Les utilisateurs connectent vraiment les clés USB qu'ils trouvent », Université de l'Illinois, Université du Michigan et Elie Bursztein via Elie.com (2015)

Microsoft Surface