Windows 11 Pro

Guide de sécurité complet pour les lieux de travail hybride

La cybersécurité est une priorité pour 88 % des PME interrogées qui se disent mal préparées pour faire face aux cybermenaces.[1]

Voici quelques-unes des façons dont une infrastructure informatique sécurisée et évolutive aide à protéger votre entreprise contre les cybermenaces :

Adoptez une approche Confiance Zéro

Le modèle de sécurité Confiance Zéro réduit les risques en vérifiant explicitement les points de données tels que l'identité de l'utilisateur, l'emplacement et l'intégrité de l'appareil pour chaque demande d'accès, sans aucune exception. Une fois vérifiés, les utilisateurs et les appareils ont un accès limité aux seules ressources nécessaires.

Les principes Confiance Zéro vont par trois :

1

Tout d'abord, effectuez une vérification explicite. Cela signifie de toujours authentifier et autoriser en fonction de tous les points de données disponibles, y compris l'identité de l'utilisateur, l'emplacement, l'intégrité de l'appareil, le service ou la charge de travail, la classification des données et les anomalies.

2

Deuxièmement, utilisez l'accès avec le moins de privilèges, ce qui limite l'accès des utilisateurs dans le temps et son champ d'action, tandis que les politiques adaptatives basées sur les risques et la protection des données évitent tout problème en ce qui concerne les données et la productivité.

3

Troisièmement, faites face aux violations. Faites face aux violations en limitant autant que possible l'accès aux segments et les dégâts potentiels. Le chiffrement de bout en bout est constamment vérifié et les analyses permettent d'obtenir de la visibilité et d'améliorer la détection des menaces et leurs défenses.

Pour mettre en œuvre une approche Confiance Zéro, les organisations doivent comprendre leurs propres données et savoir où ces données sont hébergées.

Les entreprises doivent connaître le niveau de sensibilité des données et les risques potentiels d'exposition pour déterminer les applications obligatoires de la Confiance Zéro. Pour le stockage et les applications basés sur le cloud, comme les services de messagerie et le stockage de données dans le cloud, la mise en place d'un environnement Confiance Zéro est logique et cruciale pour atténuer les risques. Sans cette approche, les mots de passe, les appareils et les données sensibles de l'entreprise sont inévitablement exposés aux attaques.

Mettez en œuvre des méthodes d'authentification avancées

Une faille de sécurité devient beaucoup plus probable si les méthodes d'authentification des utilisateurs sont compromises. L'accès non autorisé à l'appareil d'un employé permet souvent à un acteur malveillant potentiel d'accéder à l'ensemble du réseau d'une organisation. La mise en œuvre est un moyen sécurisé de s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être. Celle-ci est essentielle dans l'environnement de travail hybride actuel. L'authentification multifacteur peut grandement contribuer à créer un environnement plus sécurisé. Les mots de passe ne suffisent plus à atténuer les menaces de plus en plus sophistiquées, car ils sont souvent facilement compromis. Des techniques telles que l'authentification à deux facteurs, combinées aux capacités biométriques déjà disponibles sur de nombreux appareils modernes, tels que Windows Hello Entreprise, sont beaucoup plus efficaces pour protéger les organisations et leurs réseaux contre les cyberattaques, en particulier lorsqu'elles sont renforcées par une stratégie de sécurité Confiance Zéro.

Renforcez la sécurité matérielle

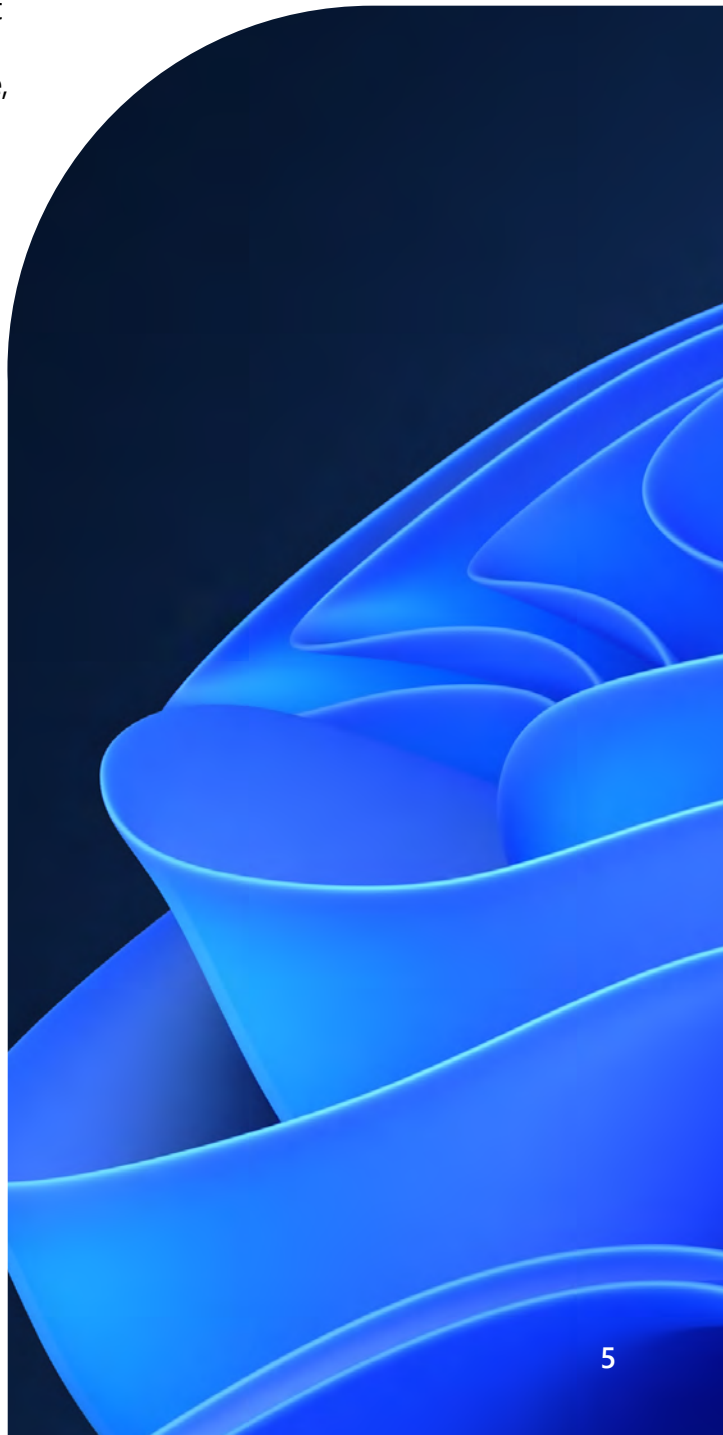
Le système d'exploitation seul ne peut pas être utilisé pour se protéger de la vaste gamme d'outils et de techniques que les cybercriminels peuvent utiliser pour compromettre un ordinateur. Les intrus, une fois à l'intérieur, peuvent déployer des logiciels malveillants difficiles à supprimer dans le micrologiciel de l'appareil, ou encore ils peuvent voler des données sensibles et des informations d'identification importantes. Il peut être difficile de détecter ces intrus une fois qu'ils ont obtenu l'accès. Il est nécessaire d'aligner étroitement la sécurité matérielle et les applications de sécurité logicielles. Les menaces modernes nécessitent un matériel informatique sécurisé au niveau de la puce et du processeur, protégeant les informations commerciales sensibles là où elles sont stockées. Il existe des catégories entières de failles qui peuvent être éliminées simplement en disposant de capacités de sécurité intégrées au niveau du matériel.

Par exemple, de telles capacités peuvent être trouvées dans tous les PC Windows 11 à noyau sécurisé. De plus, des améliorations significatives des performances peuvent être obtenues par rapport au déploiement de capacités de sécurité similaires avec un logiciel seul. Cela augmente le niveau de sécurité globale d'un système sans sacrifier les performances du système.

Utilisez des contrôles d'accès pour une protection basée sur l'identité

Au sein du cloud, les administrateurs peuvent contrôler et gérer les identités et les accès depuis un seul emplacement. Par exemple, avec Microsoft Azure Active Directory (Azure AD), ils peuvent gérer de manière centralisée les identités du personnel ainsi que configurer et déployer des politiques d'accès aux applications, aux sites et aux groupes. Les administrateurs peuvent intégrer des exigences de conformité et toute nouvelle règle peut être incorporée au fur et à mesure qu'elle se présente.

Les contrôles basés sur le cloud augmentent la sécurité et renforcent la conformité. Les recherches de Microsoft ont révélé que l'authentification multifacteur peut, à elle seule, bloquer plus de 99,9 % des attaques par compromission de compte.[2] L'accès conditionnel permet aux administrateurs de créer des règles basées sur l'activité ou l'emplacement, ce qui réduit davantage la possibilité pour les auteurs d'attaques d'exploiter les vulnérabilités. Par exemple, les tentatives de connexion provenant de l'extérieur du pays ou arrivant à des heures inhabituelles peuvent être rejetées. De plus, les administrateurs peuvent activer l'authentification unique, permettant aux utilisateurs d'accéder en toute sécurité aux applications partout tout en facilitant la gestion des mots de passe pour le service informatique.



Microsoft a récemment introduit la disponibilité générale de la prise en charge de la sécurité multicloud. Désormais, les entreprises peuvent intégrer des ressources multicloud à Azure Security Center, telles que Google Cloud Platform (GCP) et Amazon Web Services (AWS), ainsi que protéger des serveurs avec Azure Defender pour les serveurs basés sur Azure Arc.

Protégez les appareils à distance

Le cloud Microsoft facilite la gestion des appareils et des applications. Par exemple, avec Microsoft Intune, le déploiement des appareils peut être géré en toute sécurité et ce, à distance, tandis que les applications peuvent facilement être mises à l'échelle pour répondre à la demande.

Microsoft Windows Autopilot utilise des paramètres de sécurité et d'autres contrôles pour aider à protéger les appareils avant qu'un employé ne se connecte à des ressources.

Applications sécurisées

Obtenez une meilleure protection contre les sources non fiables en ouvrant les fichiers et les sites web dans un conteneur isolé grâce à Windows Defender Application Guard. La conception axée sur le cloud permet une extensibilité simple avec Microsoft 365, Microsoft Defender pour le cloud et Microsoft Defender pour les points de terminaison.[3]

Simplifiez la gestion de la sécurité sur divers sites et étendez la sécurité au cloud. Aidez à protéger les appareils, les données, les applications et les identités, où que vous soyez. Effectuez des déploiements en toute sérénité : 99,6 % des applications sont compatibles avec Windows 11.[4]

Automatisez la maintenance de la sécurité

Les technologies basées sur le cloud permettent aux administrateurs informatiques d'appliquer automatiquement des mises à jour, des correctifs et des sauvegardes sur les systèmes et les appareils. Cela réduit les erreurs de configuration et limite les temps d'arrêt tout en protégeant les systèmes contre les nouvelles menaces. Les tâches de routine peuvent être automatisées, ce qui permet aux administrateurs de se concentrer sur des tâches importantes qui nécessitent vraiment leur expertise.

Assurez la sécurité de votre entreprise avec des appareils Windows 11 Professionnel

La transformation de la sécurité de votre organisation doit être une priorité et équiper votre personnel de dispositifs sécurisés est la clé de la réussite. Les nouveaux appareils Windows 11 Professionnel, associés à Microsoft 365, sont conçus pour un travail hybride sécurisé.

- Protégez vos employés contre les logiciels malveillants, les virus, les tentatives d'hameçonnage, et les liens malveillants, et contribuez à la sécurité des données importantes de l'entreprise.

- Bénéficiez de couches de sécurité puissantes sur les appareils, les applications et le cloud, mais aussi concernant les données et les identités.

- Facilitez l'informatique avec des outils de gestion des terminaux unifiés basés sur le cloud, notamment Microsoft Endpoint Manager, Azure Active Directory et Windows Autopilot. Définissez et appliquez des politiques à distance, gérez les applications ainsi que les identités, et déployez facilement des appareils prêts pour l'entreprise.

- Surmontez les obstacles de la collaboration à distance avec une solution unique qui inclut la vidéoconférence, les applications de productivité, le partage de fichiers et bien plus encore. Assurez-vous que vos employés disposent d'un accès sécurisé aux applications et informations professionnelles importantes grâce à une solution de collaboration unifiée.

- Pour les utilisateurs manipulant des données sensibles, les PC à noyau sécurisé sont les appareils Windows les mieux protégés. Ils sont notamment dotés de toutes les fonctionnalités de sécurité avancées de Windows 11.

Réduisez considérablement les risques de cyberattaque en remplaçant vos PC vieillissants par de nouveaux appareils modernes optimisés pour la sécurité et le travail hybride. Windows 11 Professionnel et Microsoft M365 réunissent le matériel et les logiciels pour une protection puissante et prête à l'emploi de vos appareils, données, applications, identités et services.

Windows 11 Pro

[1] *https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Vendu séparément.*

[4] *Données du programme Soutien aux applications de Microsoft, octobre 2018 à février 2022. Depuis 2018, le Soutien aux applications a accompagné des milliers de clients et évalué plus de 1,1 million d'applications, avec un taux de compatibilité final de 99,6 %. Pour en savoir plus, rendez-vous sur le site web du Soutien aux applications et consultez l'article de blog Windows IT Pro sur le Soutien aux applications*