pc21.fr

Windows 11
Guide de Sécurité :
Une sécurité renforcée par essence

Windows

Introduction

Les technologies émergentes et les tendances commerciales en constante évolution offrent de nouvelles opportunités et de nouveaux défis pour les entreprises de toutes tailles. Les technologies et les modes de travail se transforment, tout comme le paysage des menaces, avec un nombre croissant d'attaques de plus en plus sophistiquées contre les organisations et les employés.

Pour prospérer, les organisations ont besoin d'une sécurité qui leur permette de travailler n'importe où. Le "Microsoft's 2022 Work Trend Index" montre que "Les problèmes et les risques liés à la cybersécurité" sont les principales préoccupations des responsables d'entreprises, qui s'inquiètent de problèmes tels que les logiciels malveillants, le vol d'informations d'identification, l'absence de mises à jour de sécurité sur les appareils, et les attaques physiques sur les appareils perdus ou volés.

Par le passé, le réseau des entreprises et la sécurité logicielle constituaient les premières lignes de défense. Avec une main-d'œuvre de plus en plus distribuée et mobile, l'attention s'est déplacée vers la sécurité matérielle des points terminaux. Les personnes sont désormais la principale cible des cybercriminels, 74 % des violations étant dues à des erreurs humaines, à des abus de privilèges, au vol d'informations d'identification ou à l'ingénierie sociale. La plupart des attaques sont motivées par des considérations financières, et le vol d'informations d'identification, le phishing et l'exploitation de vulnérabilités sont les principaux vecteurs d'attaque. Le vol d'informations d'identification est le vecteur d'attaque le plus répandu, représentant 50 % des violations.[1]

Chez Microsoft, nous travaillons dur pour aider les organisations à évoluer et à rester agiles tout en se protégeant contre les menaces modernes. Nous nous engageons à aider les entreprises et leurs employés à se sécuriser et à le rester. Nous synthétisons 43 billions de signaux pour comprendre les menaces numériques et s'en protéger. Nous avons plus de 8 500 professionnels de la sécurité dans 77 pays et plus de 15 000 partenaires dans notre écosystème de sécurité qui s'efforcent d'accroître la résilience de nos clients.[2]

Les entreprises du monde entier évoluent vers les stratégies "secure-by-design" et "secure-by-default" (sécurité par défaut). Avec ces modèles, les entreprises choisissent des produits de fabricants qui considèrent la sécurité comme une exigence commerciale, et non comme une simple caractéristique technique. Avec une stratégie de sécurité par défaut, les entreprises peuvent réduire de manière proactive les risques et l'exposition aux menaces dans l'ensemble de leur organisation, car les produits sont livrés avec des fonctions de sécurité déjà intégrées et activées.

Pour aider les entreprises à se transformer et à prospérer dans une nouvelle ère, nous avons conçu Windows 11 de manière à ce qu'il soit sécurisé dès sa conception et par défaut. Les appareils Windows 11 sont livrés avec davantage de fonctions de sécurité activées dès leur sortie de l'emballage. En revanche, les appareils Windows 10 sont livrés avec de nombreuses protections désactivées, à moins qu'elles ne soient activées par le service informatique ou les employés. La sécurité par défaut fournie par Windows 11 renforce la protection sans qu'il soit nécessaire de configurer les paramètres. En outre, il a été démontré que les appareils Windows 11 augmentent la résistance aux logiciels malveillants sans avoir d'impact sur les performances.[3]

Windows 11 est le système d'exploitation Windows le plus sûr jamais conçu en partenariat étroit avec les fabricants d'équipements informatiques (OEM) et les fabricants de circuits imprimés. Découvrez pourquoi des entreprises de toutes tailles, y compris 90 % des sociétés du classement "Fortune 500", tirent parti de la puissante protection par défaut de Windows 11..[4]

Priorités et avantages en matière de sécurité

Sécurité par essence et sécurité par défaut

Windows 11 est conçu avec des couches de sécurité activées par défaut, afin que vous puissiez vous concentrer sur votre travail, et non sur vos paramètres de sécurité. Des fonctionnalités prêtes à l'emploi, telles que la protection des informations d'identification, la protection contre les logiciels malveillants et la protection des applications ont entraîné une baisse de 58 % des incidents de sécurité, y compris une réduction de 3,1 % des attaques par micrologiciel.[5]

Les fonctionnalités de base telles que la protection des applications, des informations d'identification, et contre les logiciels malveillants ont entraîné une baisse de 58 % des incidents de sécurité, et une réduction de 3,1 % des attaques par microprogrammes.

Dans Windows 11, le matériel et les logiciels travaillent ensemble pour réduire la portée des attaques, protéger l'intégrité du système, et protéger les données précieuses. Les fonctionnalités nouvelles et améliorées sont conçues pour la sécurité par défaut. Par exemple, les apps Win32 isolées (aperçu public)[6], la protection par "jeton" (aperçu public)[6] et Microsoft Intune Endpoint Privilege Management[7] sont quelques-unes des dernières fonctionnalités qui aident à protéger votre organisation et vos employés contre les attaques. Windows Hello et Windows Hello for Business fonctionnent avec des fonctionnalités matérielles telles que TPM 2.0 et des scanners biométriques pour protéger les informations d'identification et faciliter l'ouverture de session sécurisée. Les fonctions de sécurité existantes, comme le cryptage BitLocker, ont également été améliorées pour optimiser la sécurité et les performances.

Protéger les employés contre l'évolution des menaces

Avec des attaques ciblant les employés et leurs appareils, les organisations ont besoin d'une sécurité contre des cyber-menaces de plus en plus forte et sophistiquées. Windows 11 offre une protection proactive contre le vol d'informations d'identification. Windows Hello et TPM 2.0 fonctionnent ensemble pour protéger les identités.

Les entreprises ont signalé 2,8 fois moins de cas d'usurpation d'identité grâce à la protection matérielle de Windows 11.[5]

L'ouverture de session biométrique sécurisée élimine pratiquement le risque de perte ou de vol des mots de passe. Une protection renforcée contre le phishing renforce la sécurité. En fait, les entreprises ont signalé 2,8 fois moins de cas d'usurpation d'identité grâce à la protection matérielle de Windows 11.[5]

Obtenir des garanties pour les applications essentielles

Contribuez à la sécurité des données de l'entreprise et à la productivité des employés grâce à de solides mesures de protection et de contrôle des applications. Windows 11 dispose de plusieurs couches de sécurité des applications qui protègent les données critiques et l'intégrité du code. La protection des applications, les contrôles de confidentialité et les principes de moindre privilège permettent aux développeurs d'intégrer la sécurité dès la conception. Cette sécurité intégrée protège contre les violations et les logiciels malveillants, contribue à préserver la confidentialité des données et donne aux administrateurs informatiques les contrôles dont ils ont besoin. Ainsi, les organisations et les autorités de régulation peuvent être sûres que les données critiques sont protégées.

Protection de bout en bout avec une gestion moderne

Augmentez la protection et l'efficacité avec Windows 11 et la sécurité "chip-to-cloud". Microsoft propose des services cloud complets pour la gestion des identités, du stockage et de l'accès. En outre, Microsoft fournit également les outils nécessaires pour attester que les appareils Windows 11 qui se connectent à votre réseau ou qui accèdent à vos données et à vos ressources sont dignes de confiance. Vous pouvez également assurer la conformité et l'accès conditionnel grâce à des solutions modernes de gestion des appareils telles que Microsoft Intune[9] et Microsoft Entra ID (anciennement Azure Active Directory).

La sécurité par défaut permet non seulement de travailler en toute sécurité de n'importe où, mais elle simplifie également l'informatique. Une solution de sécurité rationalisée, de la puce au cloud, basée sur Windows 11 a amélioré la productivité des équipes informatiques et de sécurité de 25 %.[8]

Sécurité par essence et par défaut

Dans Windows 11, le matériel et les logiciels travaillent ensemble pour protéger les données sensibles depuis le cœur de votre PC jusqu'au cloud. Une protection complète permet à votre entreprise de rester sécurisée, quel que soit l'endroit où les employés travaillent. Ce diagramme simple illustre les couches de protection de Windows 11, tandis que chaque chapitre propose une analyse approfondie des fonctionnalités, couche par couche.

Merci.

1. “2023 Data Breach Investigations Report,” Verizon, 2023.
2. “Microsoft Digital Defense Report 2022,” Microsoft, 2022.
3. Par rapport aux appareils Winows 10. “Improve your day-to-day experience with Windows 11 Pro laptops,” Principled Technologies, février 2023.
4. Basé sur des données d'appareils mensuellement Actifs. “Earnings Release FY23 Q3,” Microsoft, Avril 2023.
5. Les résultats de Windows 11 sont comparés à ceux de Windows 10. “Windows 11 Survey Report,” Techaisle, février 2022.
6. Nécessite l'activation des développeurs.
7. Nécessite Microsoft Entra ID (formerly AAD) et Microsoft Intune ou d'une autre solution moderne de gestion des appareils, vendu séparément.
8. Étude commandée par Forrester Consulting. “The Total Economic Impact™ of Windows 11 Pro Devices”, Décembre 2022. Remarque : les résultats quantifiés des bénéfices sur trois ans sont combinés en une seule organisation composite qui génère un chiffre d'affaires annuel de 1 milliard de dollars de chiffre d'affaires annuel, emploie 2 000 personnes, renouvelle son matériel tous les quatre ans et fait migrer l'ensemble de son personnel vers des appareils Windows 11.
9. Vendu séparément

Part No. Septembre 2023