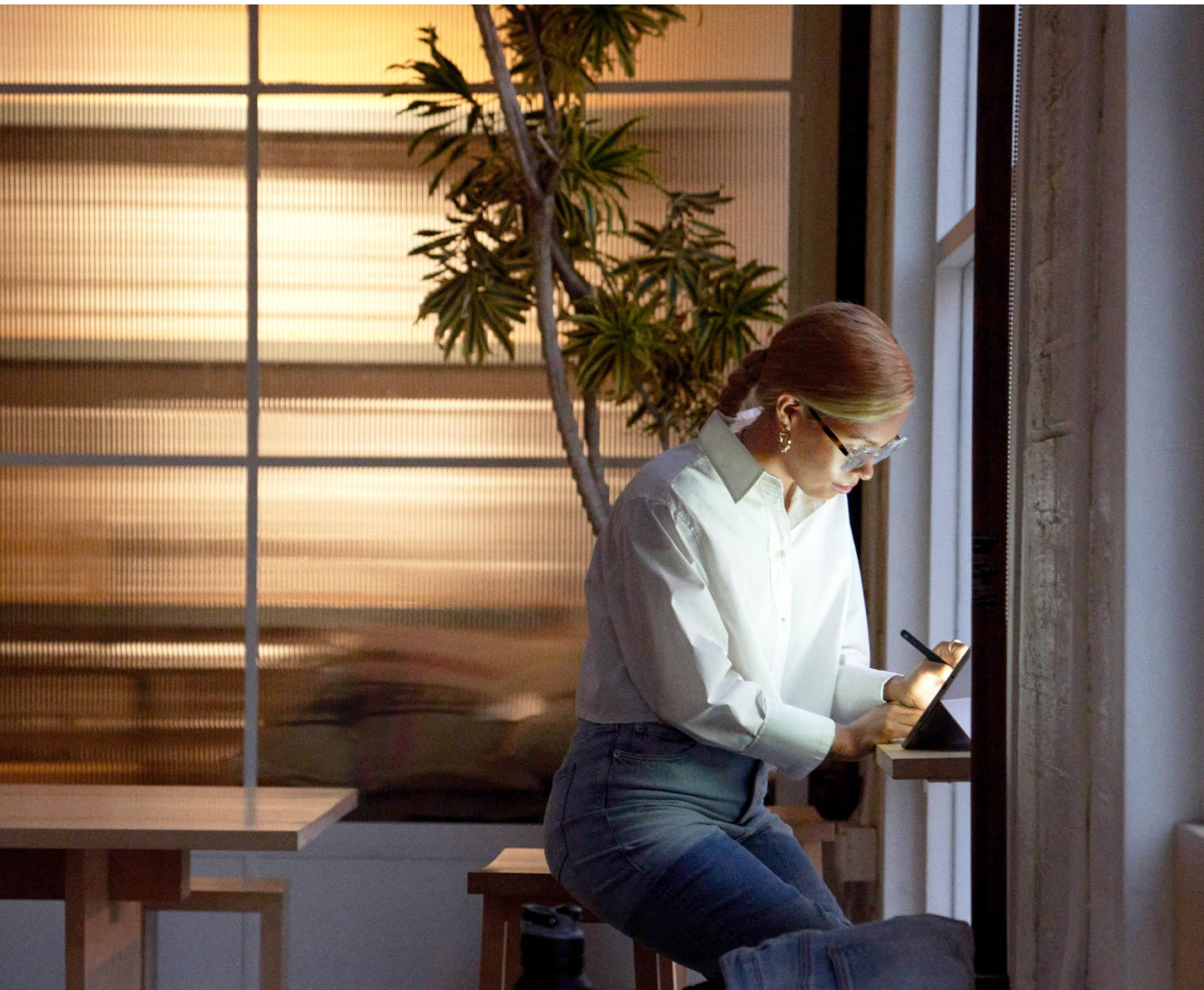
Microsoft Surface

Faire le bon choix : comment le choix des appareils peut faire ou briser votre plan de cyber-résilience



Que signifie être cyber-résilient ?

Presque toutes les organisations d'aujourd'hui, des cafés de quartier aux entreprises mondiales, dépendent des données, de l'analyse, de l'automatisation et des technologies numériques. Cette dépendance, associée à une main-d'œuvre distante, a fait augmenter le risque et le coût des cyberattaques sur une échelle d'impact qui va du local au global.

À mesure que ces scénarios se multiplient, en fréquence et en sophistication, les bons responsables de la sécurité doivent maintenant pousser leurs efforts au-delà de la prévention. La cyber-résilience est la capacité d'une organisation à réagir rapidement devant un événement néfaste et à s'en remettre efficacement, tout en minimisant l'impact fiscal des failles de sécurité. La résilience peut faire la différence entre un rétablissement qui fait perdre du terrain ou qui fait avancer l'entreprise.

5x plus de cyberattaques contre les appareils gérés à distance entre mai 2021 et mai 2022.[1]

4,24 M de dollars est le coût moyen mondial d'une violation de données en 2022.[1]

[1]Microsoft, Rapport 2022 sur la défense numérique de Microsoft, 2022.

(suite) Que signifie être cyber-résilient ?

Comment est-ce possible ? Il existe des principes clés que toute entreprise, qu'elle soit grande, moyenne, petite ou très petite, peut adopter pour gagner en résilience en cas de crise. Il faut adopter une vision pragmatique de la cybersécurité qui suppose que les violations sont inévitables. En d'autres termes, cela signifie « supposer la violation ».

Supposer la violation constitue un vrai changement de paradigme par rapport à la posture de sécurité traditionnelle. Auparavant, les professionnels de l'informatique croyaient pouvoir construire un réseau sécurisé avec un périmètre fortifié, confinant toutes les opérations de l'entreprise dans le réseau tout en limitant étroitement les appareils des utilisateurs finaux.

Toutefois, l'approche traditionnelle néglige de prendre en compte les exigences des environnements de travail modernes, l'évolution des business models, les nouvelles technologies et l'évolution des menaces de sécurité. Pour cultiver la résilience, les organisations doivent adopter le principe Zero Trust, établir un partenariat collaboratif entre les acteurs de l'entreprise, les responsables informatiques et les professionnels de la sécurité, et utiliser les technologies avancées conçues pour améliorer la protection.

D'ici 2026

50 % des cadres dirigeants intégreront des exigences de performances liées aux risques dans leurs contrats de travail.[1]

D'ici 2025

60 % des organisations utiliseront le risque de cybersécurité comme déterminant principal dans la conduite de transactions et les engagements commerciaux avec des tiers.[1]

[1]Communiqué de presse de Gartner : « Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23 », 21 juin 2022. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

Deux étapes pour commencer à développer la cyber-résilience

01 Mettre en œuvre des mesures élémentaires

La majorité des cyberattaques peuvent être stoppées par la mise en œuvre de pratiques simples, notamment la suppression des applications, des appareils et des infrastructures obsolètes. Il est également conseillé d'automatiser les processus fortement manuels, de permettre l'authentification multifacteur (AMF), d'adopter les principes Zero Trust et d'utiliser des logiciels anti-programmes malveillants modernes.

L'application régulière des mises à jour des microprogrammes et des logiciels élimine les vulnérabilités en continu. Les attaques de microprogramme représentent l'un des risques les plus importants pour les entreprises : elles peuvent donner aux acteurs malveillants un accès illimité et indétectable à votre réseau via les appareils, des ordinateurs portables aux imprimantes, aux routeurs et autres.

Une première mesure clé dans l'élaboration de la cyber-résilience consiste à auditer les points de terminaison des utilisateurs afin d'identifier ceux qui contiennent des microprogrammes accessibles.

---

98 % des attaques peuvent être stoppées par la mise en œuvre de mesures d'hygiène de base.[1]

45 % des professionnels de la sécurité identifient les outils de messagerie et de collaboration comme l'aspect de leur organisation le plus vulnérable aux attaques.[2]

[1]Microsoft, Rapport 2022 sur la défense numérique de Microsoft, 2022.
[2]Microsoft, Cyber-résilience, 2022.

Principaux composants de la cyber-résilience

Protéger et défendre

Toute bonne stratégie de résilience commence par la protection des systèmes, des applications et des données. N'accordez l'accès qu'aux utilisateurs autorisés qui ont besoin de données sur les clients, les collaborateurs et l'activité. Analysez également les applications et les appareils aux points de terminaison à la recherche des vulnérabilités qui peuvent exister n'importe où, de la puce au cloud.

Détecter et inspecter

À mesure que les cyberattaques deviennent plus fréquentes et sophistiquées, il devient de plus en plus important d'exécuter des diagnostics sur les appareils et les logiciels, en surveillant continuellement les anomalies. L'automatisation peut s'avérer utile dans ce domaine, en déclenchant la réponse du système à certaines menaces et en donnant la priorité à celles qui doivent être transférées à un membre de l'équipe.

Rétablir

Les attaques sont inévitables. Accepter cette réalité ouvre la voie à des dispositions visant à réduire au minimum les perturbations et à rétablir efficacement les appareils conçus pour la cyber-résilience.

02 Investir dans des technologies qui résistent aux perturbations

Les décisionnaires de la sécurité (SDM) investissent fortement dans la sécurité logicielle. Les pare-feu et le chiffrement des données, la détection des intrusions et la prévention des attaques sont en haut de leur liste. Toutefois, négliger de comprendre la vulnérabilité du matériel peut saper les meilleures initiatives.

Une infrastructure de sécurité typique se compose de plusieurs couches qui agissent de concert pour protéger les actifs, les données et les opérations d'une entreprise.

Une compromission au niveau du matériel, au travers d'un appareil physique tel qu'un ordinateur portable, une tablette, un smartphone ou un dispositif IoT, peut se propager et compromettre d'autres couches pour atteindre les données et les réseaux qu'elles sont censées protéger.

Il est essentiel pour votre plan de cyber-résilience de collaborer avec les décideurs technologiques pour choisir les bons appareils. De nombreux facteurs entrent en ligne de compte, tels que les performances taillées pour l'utilisation, l'évolutivité, la compatibilité, la fiabilité et la sécurité des appareils eux-mêmes.

Les composants clés d'une infrastructure cyber-résiliente

- Créer un plan de protection du microprogramme et restez au fait des mises à jour des microprogrammes, des systèmes UEFI et du système d'exploitation qui peuvent assurer une protection supplémentaire contre les menaces émergentes.
- Accélérer l'automatisation des tâches manuelles telles que les mises à jour à distance et l'activation des appareils, ce qui laisse davantage de temps aux équipes IT pour les activités fortement manuelles.
- Activer une planification pour que les mises à jour de sécurité, de l'UEFI et du microprogramme soient toujours à jour.
- Activer l'AMF pour tous les utilisateurs finaux et mettre en œuvre une stratégie d'accès conditionnel.
- Mettre en œuvre l'analyse biométrique, telle que Windows Hello Entreprise, pour réduire la dépendance à l'égard des codes, des cartes d'accès et des mots de passe.
- Adopter des appareils considérés comme Secured-core ou configurer vos appareils pour répondre à des exigences similaires.
- Réduire le niveau de vulnérabilité des appareils aux points de terminaison en désactivant les fonctionnalités inutilisées, telles que les caméras vidéo ou le Bluetooth.

Choisir des appareils cyber-résilients

- Recherchez les bonnes pratiques et appliquez les normes de sécurité concernant les appareils dans votre secteur d'activité.
- Évaluez votre parc actuel d'appareils et identifiez les manquements ou les risques en termes de fonctionnalité, d'âge, de version ou de sécurité.
- Comparez les différentes options des appareils en fonction de leurs fonctionnalités, avantages, inconvénients, ainsi que des commentaires et des évaluations.
- Consultez des experts ou des fournisseurs capable de donner des conseils ou des recommandations quant au choix des appareils.
- Testez et évaluez les performances et la sécurité de vos appareils sélectionnés avant de les déployer au sein de votre organisation.
- Surveillez et gérez régulièrement vos appareils afin de vous assurer qu'ils fonctionnent correctement et en toute sécurité.

Tenir les appareils à jour

Bien que votre équipe informatique puisse toujours effectuer des tests et bâtir une enceinte de sécurité, la bonne tenue à jour des appareils au niveau du microprogramme constitue une bonne réduction du risque, et permet aux équipes informatiques de se concentrer sur la résilience et la croissance plutôt que sur la défense et la réparation.

Au-delà du microprogramme, les attaques contre les appareils gérés à distance sont en hausse. Ces appareils sont notamment les ordinateurs portables, les caméras et les technologies de salle de conférence intelligente qui peuvent être exposées via des ports ouverts et peuvent être exploitées par les pirates. Une étude récente a révélé que 46 % des types d'attaque IoT/OT provenaient des appareils gérés à distance.[1]

[1]Microsoft Security Insider, Exposés et sans correctifs, les dispositifs présentent un risque unique, 2022.

Choisir un partenaire pour élaborer une stratégie de cyber-résilience

Dans un monde de défis informatiques complexes, le choix du bon partenaire informatique peut aider les entreprises à se protéger et à bien préparer leur rétablissement. Un bon partenaire IT recommande les solutions matérielles, logicielles et de sécurité les plus adaptées pour l'entreprise. Il réduit le besoin de jongler avec plusieurs fournisseurs ou solutions. Un partenaire IT valable dispose des connaissances et de l'expérience suffisantes pour participer à la conception et à la mise en œuvre d'un plan de cyber-résilience complet capable d'évoluer avec l'entreprise. Enfin, un bon partenaire IT doit avoir à cœur l'intérêt de ses clients et s'efforcer de les aider à atteindre leurs objectifs commerciaux.

Avec ses partenaires, Microsoft a conçu les appareils Surface pour réduire au minimum le risque des menaces contre les microprogrammes, le système d'exploitation et les applications cloud. Le principe Zero Trust étant intégré à la base, les décideurs de la sécurité et de l'informatique peuvent investir leurs ressources dans des stratégies et des technologies susceptibles de prévenir les attaques du futur, plutôt que de se défendre constamment contre les attaques qui les visent aujourd'hui.

Trouvez un partenaire Microsoft : Revendeurs Microsoft agréés – Surface pour les entreprises

Comment Microsoft Surface participe à la cyber-résilience

Les appareils Microsoft Surface sont conçus pour faciliter l'hygiène de sécurité de base, chaque couche étant gérée par Microsoft, du microprogramme jusqu'au cloud, en passant par le système d'exploitation. Les appareils Surface, Windows 11 et Microsoft 365[1] contribuent à atteindre la résilience organisationnelle grâce à une approche Zero Trust de la sécurité et de la gestion des risques, qui ne sacrifie en rien l'innovation et la productivité.

En concevant les appareils Surface, nous avons envisagé toutes les façons dont les appareils et les utilisateurs pouvaient être compromis par les attaques. La sécurité est plus effective lorsqu'elle est intégrée dès la conception pour protéger les zones les plus vulnérables, et c'est exactement ce que nous avons fait. En conséquence, les appareils Surface sont protégés de la puce jusqu'au cloud. Nous avons conçu les appareils Surface pour assurer votre tranquillité d'esprit, sachant qu'une solution intégrée gérée par Microsoft protège votre entreprise. Penchons-nous davantage sur la façon dont Microsoft Surface participe à la cyber-résilience.

Les entreprises qui possèdent des appareils Surface peuvent rencontrer jusqu'à 34 % en moins d'incidents de sécurité, ce qui réduit le temps consacré à la réponse aux incidents.[2]

*Exclusif à Microsoft Surface.
**Les unités remplaçables par le client (CRU) sont des composants disponibles à l'achat via votre revendeur de périphériques Surface agréé. Les composants peuvent être remplacés sur site par un technicien qualifié suivant le Guide de maintenance de Microsoft. L'ouverture et/ou la réparation de votre appareil peuvent présenter des risques d'électrocution, d'incendie et de blessures, ainsi que d'autres dangers. Faites preuve de prudence si vous procédez à des réparations par vous-même. Les dommages causés aux appareils lors de la réparation ne seront pas couverts par les plans de protection ou de garantie du matériel de Microsoft. Les composants seront disponibles peu après le lancement initial ; le calendrier de disponibilité varie selon le composant et le marché.
[1]Licence logicielle requise pour certaines fonctions. Vendu séparément.
[2]Un livre blanc Business Value, commandé par Microsoft, septembre 2022 | Doc. Étude IDC US49453722 menée à partir d'enquêtes et d'entretiens entre décembre 2021 et février 2022. Tous les répondants étaient des décisionnaires IT de grandes entreprises (de 250 à plus de 5000 salariés) représentant des organisations des États-Unis, d'Australie, d'Inde, d'Espagne, de France, du Royaume-Uni, de Nouvelle-Zélande et d'Allemagne. Les résultats en matière de coûts et d'économies sont basés sur des estimations moyennes de coûts et de temps fournies directement par les répondants ; les coûts et économies réels peuvent varier en fonction de votre combinaison d'appareils et de votre déploiement spécifiques. Pour obtenir l'étude détaillé, cliquez ici.

Appliquer la cyber-résilience du matériel au Cloud, en passant par la collaboration

« Microsoft fournit tous les services et moyens de défense dont nous avons besoin pour nous-mêmes et pour nos clients sur la même plateforme. »

– NIP Group

Microsoft Surface peut aider à combler les manques de sécurité en donnant des moyens de s'impliquer aux équipes de sécurité, aux chefs d'entreprise et aux collaborateurs. Conçus pour être sécurisés, les appareils Surface combinés avec Windows 11 et Microsoft 365* proposent une solution intégrée, avec des couches de protection incorporées et une gestion des appareils à distance qui couvrent le matériel, le microprogramme et même le cloud.

Windows 11 intègre étroitement les fonctionnalités de sécurité matérielle et logicielle dès son installation, assurant une protection et une résilience proactives contre les menaces en constante évolution.

*Licence logicielle requise pour certaines fonctions. Vendu séparément.

« Le PC sécurisé est une tentative d'établir « le meilleur environnement au monde. » Je pense que nous avons réussi à créer cet environnement en combinant les dernières technologies, notamment Microsoft 365, avec nos propres technologies. »

– NTT Communications Corporation

Conçus pour la sécurité

Notre approche de la sécurité commence par le matériel. Surface protège les données grâce au chiffrement au démarrage de l'appareil. Un **Module de plateforme sécurisée 2.0** (TPM 2.0) tient lieu de coffre-fort pour le stockage des mots de passe, des codes PIN et des certificats. Il protège le matériel des altérations et limite l'accès aux seules personnes autorisées. À chaque étape du cycle de démarrage, le code du microprogramme est inspecté pour garantir son authenticité et éviter que le système n'exécute du code malveillant.

Au démarrage, une connexion sécurisée sans mot de passe avec **Windows Hello Entreprise** offre le niveau de sécurité biométrique le plus élevé grâce aux capteurs de sa caméra infrarouge qui améliorent la reconnaissance faciale. La connexion biométrique est la plus difficile à répliquer, elle assure que seuls les utilisateurs autorisés puissent accéder à l'appareil.

Nous concevons de nombreux appareils Surface avec des disques SSD amovibles[1] pour fournir une couche supplémentaire de protection aux données sensibles stockées sur l'appareil.

Microsoft est reconnu comme leader dans le rapport® Magic Quadrant™ 2022 de Gartner pour les outils de gestion unifiée des terminaux.[2]

Les entreprises qui utilisent Surface ont constaté une réduction de 40 % du temps consacré par l'équipe IT à la maintenance continue.[3]

Conçus pour la confiance

Le Portail de gestion de Surface est intégré à **Microsoft Intune***, ce qui compose une solution dédiée et centralisée de gestion des points de terminaison cloud. Le Portail de gestion de Surface est conçu pour relever les défis liés à la gestion et à la configuration des utilisateurs, des applications et des appareils à grande échelle, tandis que Microsoft Intune* assure la gestion des applications mobiles (MAM) et la gestion des appareils mobiles (MDM).

---

*Licence logicielle requise pour certaines fonctions. Vendu séparément.
[1]Les unités remplaçables par le client (CRU) sont des composants disponibles à l'achat via votre revendeur de périphériques Surface agréé. Les composants peuvent être remplacés sur site par un technicien qualifié suivant le Guide de maintenance de Microsoft. L'ouverture et/ou la réparation de votre appareil peuvent présenter des risques d'électrocution, d'incendie et de blessures, ainsi que d'autres dangers. Faites preuve de prudence si vous procédez à des réparations par vous-même. Les dommages causés aux appareils lors de la réparation ne seront pas couverts par les plans de protection ou de garantie du matériel de Microsoft. Les composants seront disponibles peu après le lancement initial ; le calendrier de disponibilité varie selon le composant et le marché.
[2]Gartner, Magic Quadrant for Unified Endpoint Management Tools, Tom Cipolla, Dan Wilson et al., 1 août 2022. GARTNER est une marque déposée et une marque de service de Gartner Inc. et/ou de ses filiales aux États-Unis et à l'international, et MAGIC QUADRANT est une marque déposée de Gartner, Inc. et/ou de ses filiales. Toutes deux sont utilisées ici avec l'autorisation de la société. Tous droits réservés. Gartner ne soutient aucun fournisseur, produit ou service représenté dans ses publications de recherche, et ne conseille pas aux utilisateurs de technologies de choisir les fournisseurs classés parmi les meilleurs, ni ne fournit d'autres recommandations. Les publications de recherche de Gartner représentent les opinions de l'organisme de recherche Gartner et ne sauraient être interprétées comme un exposé des faits. Gartner décline toute garantie, explicite ou implicite, concernant cette étude, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.
[3]livre blanc Business Value, commandé par Microsoft, septembre 2022 | Doc. Étude IDC US49453722 menée à partir d'enquêtes et d'entretiens entre décembre 2021 et février 2022. Tous les répondants étaient des décisionnaires IT de grandes entreprises (de 250 à plus de 5000 salariés) représentant des organisations des États-Unis, d'Australie, d'Inde, d'Espagne, de France, du Royaume-Uni, de Nouvelle-Zélande et d'Allemagne. Les résultats en matière de coûts et d'économies sont basés sur des estimations moyennes de coûts et de temps fournies directement par les répondants ; les coûts et économies réels peuvent varier en fonction de votre combinaison d'appareils et de votre déploiement spécifiques. Pour voir l'étude détaillée, cliquez ici.

Windows Update gère le déploiement et la mise à jour des microprogrammes, des logiciels et des pilotes. La protection end-to-end garantit que seul le contenu approuvé est installé.

La capacité de gérer la sécurité des appareils à distance peut engendrer un gain de temps considérable pour votre équipe IT, en réduisant la possibilité des attaques contre les microprogrammes ou de ransomware, et en corrigeant les problèmes avant qu'ils ne deviennent trop graves.

Conçu pour fonctionner avec Microsoft Intune,* **Windows Autopilot** fait encore gagner du temps en rationalisant les déploiements sécurisés à distance et en préconfigurant les nouveaux appareils avec les paramètres et stratégies de sécurité préconisés.

« La sophistication de l'authentification biométrique à l'aide de la reconnaissance faciale de Windows Hello, comme nous l'avons vu avec Surface, est absolument incomparable sur le marché. »

– Mashreq

Un microprogramme verrouillé

Les appareils Surface bloquent les menaces de manière proactive en supprimant un important point d'accès au microprogramme via l'interface UEFI (Unified Extensible Firmware Interface). L'UEFI conçu par Microsoft est accessible par Windows Update, ce qui réduit le risque d'accès externe au microprogramme.

L'UEFI Microsoft joint à **l'interface DFCI (Device Firmware Configuration Interface)** permet un contrôle plus granulaire du microprogramme via Microsoft Intune.*

L'interface DFCI réduit la surface d'attaque en désactivant les composants matériels inutiles et supprime la dépendance au mot de passe UEFI local (BIOS). L'interface DFCI offre la possibilité de verrouiller les options de démarrage pour empêcher les utilisateurs de démarrer dans un autre système d'exploitation, et les mises à jour de sécurité exécutées en arrière-plan offrent une protection continue et toujours à jour contre les dernières menaces.

---

34 % d'incidents de sécurité en moins avec les appareils Surface.[2]

30 % de temps nécessaire en moins au personnel IT pour traiter les incidents de sécurité lors de l'utilisation d'appareils Surface.[2]

---

*Licence logicielle requise pour certaines fonctions. Vendu séparément.
[1]Surface Go et Surface Go 2 utilisent une interface UEFI tierce et ne prennent pas en charge la norme DFCI. Pour plus d'informations sur la protection Microsoft pour Surface Go et Surface Go 2, rendez-vous sur https://www.microsoft.com/en-us/surface/business/surface-go-2.
[2]Un livre blanc Business Value, commandé par Microsoft, septembre 2022 | Doc. Étude IDC US49453722 menée à partir d'enquêtes et d'entretiens entre décembre 2021 et février 2022. Tous les répondants étaient des décisionnaires IT de grandes entreprises (de 250 à plus de 5000 salariés) représentant des organisations des États-Unis, d'Australie, d'Inde, d'Espagne, de France, du Royaume-Uni, de Nouvelle-Zélande et d'Allemagne. Les résultats en matière de coûts et d'économies sont basés sur des estimations moyennes de coûts et de temps fournies directement par les répondants ; les coûts et économies réels peuvent varier en fonction de votre combinaison d'appareils et de votre déploiement spécifiques. Pour voir l'étude détaillée, cliquez ici.

La puissante sécurité de Windows 11 activée par défaut

Les appareils Surface avec Windows 11 incluent un nouvel ensemble de fonctionnalités de sécurité matérielle activées dès l'installation. **La sécurité basée sur la virtualisation (VBS)** et **l'intégrité du code surveillée par l'hyperviseur (HVCI)**, également connue sous le nom **d'intégrité de la mémoire,** sont conçues pour créer une base encore plus solide et plus résistante aux attaques. Le VBS et le HVCI fonctionnent en tandem pour fournir une meilleure protection contre les logiciels malveillants courants et sophistiqués, en effectuant les opérations de sécurité délicates dans un environnement isolé. En vérifiant les exécutions de code avant leur démarrage, le VBS et le HVCI empêchent les logiciels malveillants de se frayer un chemin jusqu'à la mémoire système. Si un logiciel malveillant parvient à accéder aux ressources système, le HVCI peut limiter et contenir ses effets.

Les appareils Surface sortent de l'usine équipés de Windows 11, avec les **fonctionnalités de sécurité activées**. Cela permet aux responsables de la sécurité et aux chefs d'entreprise de normaliser les comportements axés sur la sécurité dans leur organisation, ce qui répond au besoin de responsabilisation de vos équipes.

Avant même que vous ne vous connectiez à l'aide d'un éventail d'options biométriques pour éviter les mots de passe et les codes PIN, **Secure Boot permet** de vérifier que le microprogramme est aussi authentique qu'à sa sortie de l'usine. Ensemble, Secure Boot et Trusted Boot empêchent les logiciels malveillants et les composants corrompus de se charger au démarrage.

Après le démarrage, **le chiffrement BitLocker** permet de rendre les données inaccessibles, même sur les appareils perdus, volés ou mis hors service de manière inappropriée.

Une cybersécurité robuste implique d'évoluer de la simple maintenance de la protection à l'élaboration de la résilience face aux menaces actuelles et évolutives. La cyber-résilience est un effort organisationnel qui exige la responsabilisation de tous.
Les organisations ont besoin d'une approche intégrée (où la sécurité est intégrée à chaque couche, de la puce au cloud) afin de garantir la protection des données et des personnes partout où elles travaillent.

Vous voulez en savoir plus sur les solutions intégrées et cyber-résilientes conçues par Microsoft et intégrées à Surface, Windows 11 et Microsoft 365 ? Contactez votre représentant dès aujourd'hui.

Microsoft Surface

Liste de contrôle de la cyber-résilience

Questions à prendre en compte lors de l'évaluation de l'impact de vos appareils sur la cyber-résilience

Ces questions et ces sujets vous aideront à comprendre où se situe votre parc d'appareils au fil de votre progression dans la planification de la sécurité :

- ☐ Quelle priorité la direction accorde-t-elle à la sécurité en ce qui concerne les vulnérabilités des appareils de nos utilisateurs finaux ?
- ☐ Quel budget la direction a-t-elle l'intention d'investir dans la mise à niveau des appareils pour assurer la sécurité ?
- ☐ Quel serait le coût d'une violation de notre sécurité ?
- ☐ Comprenez-vous parfaitement le fonctionnement des points de terminaison et de l'endroit où ils créent des vulnérabilités ? Aussi bien en quantité qu'en qualité.
- ☐ Votre entreprise permet-elle aux employés de déplacer ou d'apporter leurs propres appareils pour se connecter au travail ?
- ☐ Combien de solutions utilisez-vous dans votre écosystème de sécurité actuel ?
- ☐ Utilisez-vous plusieurs types d'appareils et systèmes d'exploitation ? Pouvez-vous les regrouper ?

Parler de sécurité aux dirigeants

Utilisez ces amorces de conversation pour lancer la discussion sur le thème de la sécurité et influer sur les choix favorables à la cyber-résilience :

- Quel est le niveau de priorité que nous accordons à la sécurité de nos adresses IP, de nos données et de nos collaborateurs ?
- Si l'on met en balance la sécurité et l'expérience des collaborateurs, laquelle est la plus importante et dans quelle mesure ?
- Avons-nous des engagements envers nos fournisseurs ou est-ce l'occasion d'opérer des simplifications ?
- L'adoption d'un modèle de sécurité Zero Trust améliorera notre cyber-résilience. Notre état d'esprit concernant la sécurité est-il propice à ce changement ?

La cyber-résilience est un travail d'équipe

Pour que les entreprises soient résilientes, les décideurs technologiques doivent amener les décideurs commerciaux de tous les domaines organisationnels à la table de discussion concernant la résilience.

Rôle	Pertinence du choix de l'appareil	Élément à évaluer
Directeur financier	Retour sur investissement des appareils	Évaluation de l'argument commercial et du coût total de possession Microsoft
Responsable du développement durable	Alignement sur les objectifs ESG	Estimateur Microsoft des émissions de Surface
Responsable de la sécurité	Intégration dans l'écosystème de sécurité, protection des données et de la propriété intellectuelle	Sécurité de Microsoft Surface et des points de terminaison
Directeur des ressources humaines	Prise en charge de la productivité, de la polyvalence, des appareils et de l'expérience des collaborateurs	Compréhension du rôle des PC modernes dans l'optimisation de l'environnement de travail hybride

Ressources supplémentaires

Microsoft Security Insider

Microsoft Secure

En savoir plus sur le Zero Trust

5 étapes vers la cyber-résilience

Résilience de l'entreprise : Cadre d'adoption du Cloud | Microsoft Learn

Atelier pour le directeur de la sécurité de l'information (DSI) : documentation de la sécurité | Microsoft Learn

Vous avez une petite entreprise ? Découvrez comment Surface et sa sécurité peuvent libérer votre potentiel.