Microsoft 365

Des équipes en première ligne sécurisées

Empêcher la violation de données et protéger votre entreprise

Les espaces de travail de première ligne sont des environnements complexes et dynamiques où se ont lieu certaines des interactions clients les plus importantes d'une organisation. Pour les employés qui sont acteurs de ces échanges cruciaux, il est essentiel de disposer d'un accès sécurisé aux outils adaptés à leur travail, mais ces besoins technologiques en première ligne sont souvent insatisfaits.

Cette déconnexion entre les employés et les outils peut exposer les organisations à des menaces. Les équipes en première ligne s'appuient souvent sur un ensemble d'applications et d'appareils approuvés et non approuvés pour effectuer leur travail. Et ce fait est préoccupant, étant donné que 80 à 90 % des compromissions par rançongiciel proviennent d'appareils non gérés[1].

Ces attaques peuvent interrompre vos opérations en première ligne, perturber la productivité et réduire la confiance des clients dans votre organisation. De plus, les coûts associés aux violations ont augmenté de 15 % au cours des trois dernières années[2].

Jamais les équipes en première ligne n'ont davantage eu besoin d'un accès sécurisé aux outils de communication et de productivité spécialement conçus pour leurs besoins spécifiques. De même, la pression exercée sur les équipes informatiques pour assurer la gestion sécurisée des points de terminaison, tout en fournissant l'accès aux outils de l'entreprise ne fait qu'augmenter.

Table des matières

Certaines suites Microsoft 365 et Office 365 dans l'Espace économique européen et en Suisse n'incluent pas Microsoft Teams.

En savoir plus sur notre page de licences

01

Pourquoi protéger les équipes en première ligne est difficile

Un déficit technologique

Dans de nombreux espaces de première ligne, les employés ne disposent pas d'appareils fournis par l'entreprise ni d'un accès aux applications de courrier électronique, de messagerie et de productivité. De plus, les organisations ont souvent des difficultés à comprendre de quels outils et technologies ont besoin leurs employés de première ligne. Quel est le résultat? De nombreux employés de première ligne sont obligés de naviguer parmi un assortiment disparate d'applications et d'appareils incapables de prendre en charge la totalité de leur mission.

Ce déficit entraîne une prolifération des pratiques informatiques non conventionnelles, car les responsables et les employés en première ligne doivent recourir à leurs propres appareils et applications pour accomplir leur travail. En effet, 80 % des employés utilisent des applications non approuvées qui peuvent ne pas être conformes aux stratégies informatiques et de sécurité de l'organisation[3]. Cela expose les organisations à des risques, car les équipes informatiques ne sont pas en mesure de sécuriser ces appareils et applications non gérés.

3 500

Nombre moyen d'appareils connectés mais non gérés dans une entreprise[4].

71 %

Les utilisateurs sont plus susceptibles d'être infectés par des logiciels malveillants sur un appareil non géré[4].

Identités et points de terminaison non sécurisés

Les employés en première ligne doivent souvent jongler avec plusieurs applications et appareils tout au long de leur journée de travail. La gestion des équipes, la communication organisationnelle et les interactions avec les clients peuvent toutes avoir lieu sur différents appareils ou applications. Il n'est pas rare que des employés basculent entre des applications et des sites Web plus de 1 200 fois par jour[5].

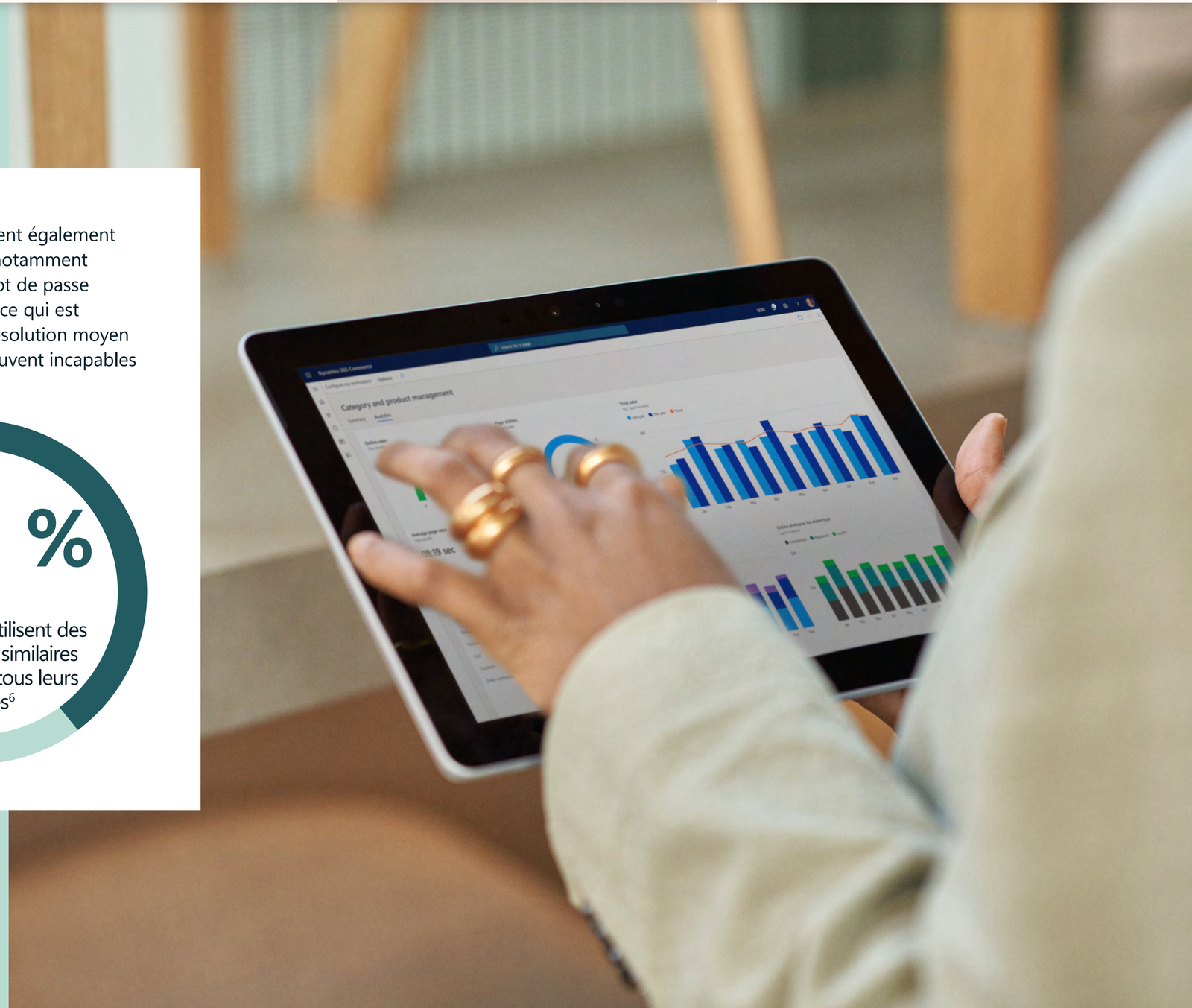
Ce défi est encore plus compliqué lorsque les employés partagent des appareils, surtout si l'organisation utilise encore un équipement ancien. Dans ces situations, les employés en première ligne doivent systématiquement se déconnecter de chaque appareil dès qu'ils ont fini de l'utiliser. Pendant les périodes de forte intensité d'interactions avec des clients, il peut être facile pour un employé d'oublier cette étape cruciale, laissant son appareil connecté et accessible à tous.

De plus, les employés peuvent être tentés de réutiliser les mêmes informations de connexion sur plusieurs identités dans l'idée de passer plus efficacement d'un client à l'autre. En conséquence, dès qu'un compte d'un employé est compromis, tous les comptes de cet employé sont en danger.

Au-delà du risque financier et de réputation, les organisations pâtissent également d'une perte de temps en raison de problèmes relatifs aux identités, notamment la gestion des mots de passe. Les demandes de réinitialisation de mot de passe représentent jusqu'à 50 % de tous les appels au service d'assistance, ce qui est source de retard pour les équipes informatiques[7]. Avec un délai de résolution moyen de 30 minutes par demande, les employés en première ligne sont souvent incapables d'accéder aux outils nécessaires à leur travail[7].

des employés réutilisent leurs mots de passe sur plusieurs comptes[6].

des employés utilisent des mots de passe similaires ou dérivés sur tous leurs comptes[6]



Sécurité des données

Pour les espaces de travail de première ligne dotés de règles étendues en matière de données et de confidentialité, la sécurité prend une autre dimension. Les employés de première ligne accèdent régulièrement aux données des clients et ces interactions doivent être consignées et sécurisées. En l'absence de protocoles de communication de données à l'échelle de l'entreprise, les employés de première ligne peuvent faire appel à des canaux non sécurisés comme des applications de courrier électronique, de partage de fichiers ou de messagerie personnelles ou grand public. Dans ces scénarios, les équipes informatiques peuvent être amenées à parcourir manuellement le patrimoine de données de l'organisation pour découvrir et sécuriser ces données.

Placer les équipes en première ligne au centre de l'attention

La bonne solution technologique doit être conçue avec une compréhension fine des défis spécifiques des espaces de travail en première ligne en matière de productivité et de sécurité. Cela implique de développer des outils sophistiqués capables d'aider les employés de première ligne à passer rapidement d'un appareil à un autre et d'une interaction client à la suivante. Plus ce processus est fluide, plus les employés peuvent se concentrer sur ce qui compte le plus : délivrer une expérience client exceptionnelle.

Dans le même temps, la solution ne doit pas compromettre la sécurité de l'organisation. La sécurité doit rester résiliente tout au long de chaque interaction et les équipes informatiques doivent conserver une visibilité totale sur chaque identité et chaque point de terminaison, dans l'ensemble de l'environnement en première ligne.

En bref, les employés de première ligne et les équipes informatiques ont besoin d'une technologie conçue pour leurs méthodes de travail.

02

Microsoft 365 for Frontline Workers

Conçu pour le travail en première ligne

Gérez les identités de première ligne et simplifiez l'accès aux applications

Solution technologique intégrée, Microsoft 365 for Frontline Workers offre un environnement numérique simplifié fondé sur le principe de la confiance zéro. Les systèmes à l'échelle de l'entreprise simplifient l'expérience des employés sur tous les appareils et un tableau de bord de sécurité donne aux équipes informatiques une visibilité complète de chaque identité et point de terminaison de votre organisation.

En déployant Microsoft 365 en tandem avec Microsoft Teams, les organisations peuvent simplifier encore davantage l'expérience de leurs employés. Les employés en première ligne peuvent accéder en toute sécurité aux canaux de communication, aux applications de gestion des équipes et des tâches et bien plus encore, le tout étant regroupé en un seul endroit.

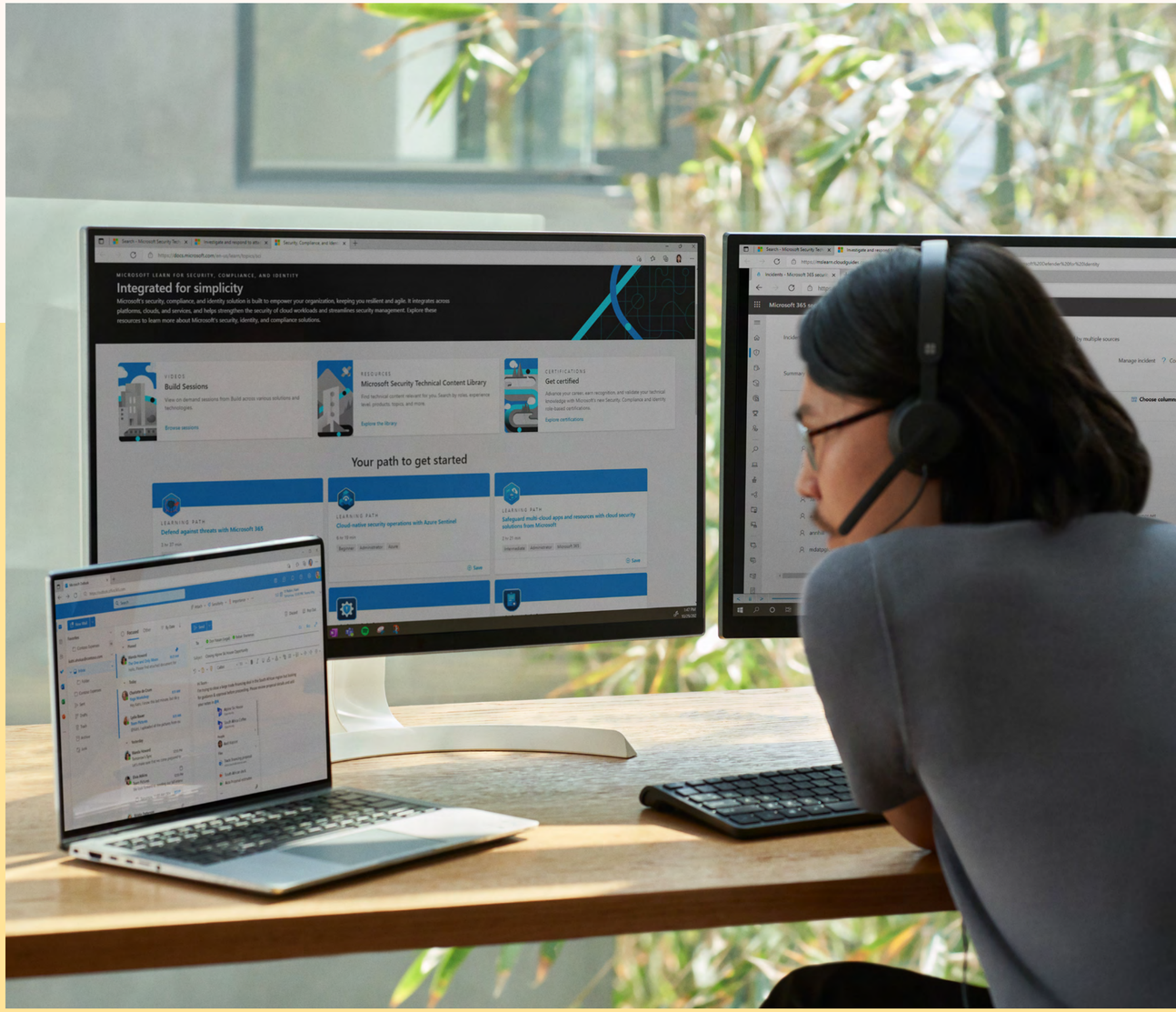
Automatiser les tâches informatiques triviales pour autonomiser les équipes en première ligne

Grâce à l'automatisation des tâches et de la sécurité, Microsoft 365 réduit les charges de travail informatiques, tout en renforçant le niveau de sécurité de votre organisation. La gestion automatisée des autorisations permet aux équipes informatiques d'établir des protocoles stratégiques pour certaines catégories d'identité données. Cela permet aux responsables et aux employés en première ligne d'assurer eux-mêmes les tâches informatiques de base comme la réinitialisation des mots de passe et les téléchargements d'applications.

Les équipes informatiques peuvent mettre en place un certain nombre de fonctionnalités d'accès conditionnel, notamment ce qui suit :

- Exiger des appareils gérés par l'organisation pour des applications spécifiques.
- Bloquer les ouvertures de session pour les utilisateurs qui essaient d'utiliser d'anciens protocoles d'authentification.
- Exiger des emplacements de confiance pour l'enregistrement des informations de sécurité.

Associées à la déconnexion automatique des appareils partagés, ces mesures soulagent le fardeau des employés en première ligne très sollicités, tout en permettant aux équipes informatiques de gagner du temps dans la gestion des problèmes courant concernant les identités. De plus, ces protocoles contribuent à réduire les pratiques informatiques non conventionnelles en restreignant automatiquement l'accès des employés aux applications non approuvées et aux sites non fiables.



Microsoft Entra est une solution infonuagique de gestion des identités et des accès, incluse dans Microsoft 365 pour l'entreprise.

Avantages sur trois ans* consécutif à un investissement dans Microsoft Entra[8] :

90 % ↓

de réduction du temps nécessaire pour accéder aux ressources.

75 % ↓

de diminution des demandes de réinitialisation de mot de passe adressées au service informatique.

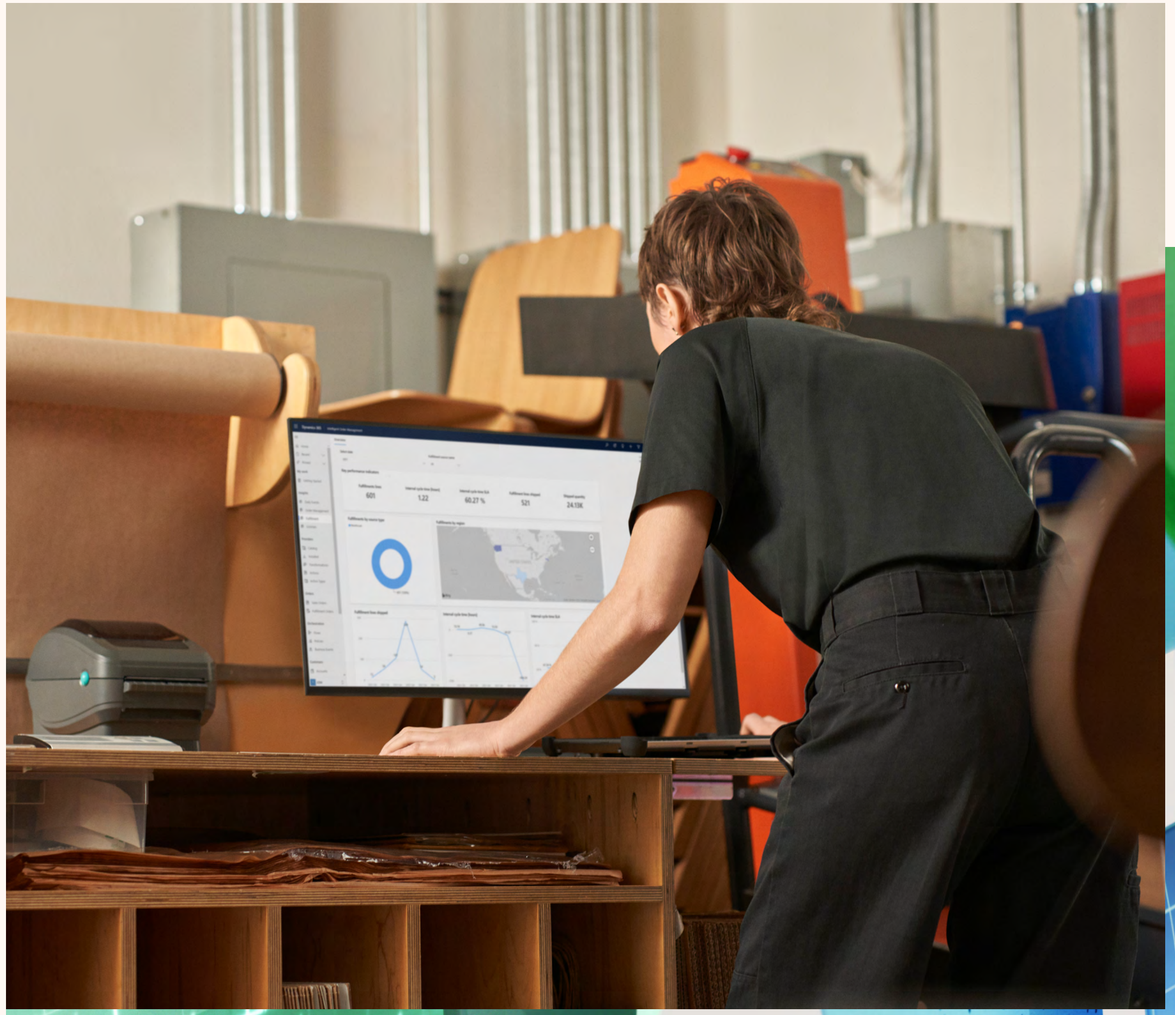
20 % ↓

de réduction de la probabilité d'une violation grâce au renforcement de la sécurité.

* Ces résultats sont basés sur une organisation composite unique, une entreprise de commerce interentreprises mondiale comptant 10 000 employés à temps plein.

Simplifier la conformité grâce à une visibilité accrue des données

Microsoft 365 for Frontline Workers donne à vos équipes informatiques une vision et un contrôle total sur l'ensemble du parc de données de votre organisation. Grâce à une carte et un tableau de bord détaillés des données de l'organisation, les équipes informatiques ont une vue directe sur tous les appareils; ceux-ci peuvent ainsi être gérés efficacement à partir d'un seul endroit.



Automatiser la gouvernance des données et appliquer un ensemble cohérent de stratégies

Avec Microsoft 365, les équipes informatiques ont la possibilité d'automatiser le classement et la gouvernance des données à grande échelle. Elles peuvent créer des systèmes de balises pour trier les données, puis détecter, classer et protéger les données confidentielles à l'aide d'un ensemble cohérent de stratégies appliquées à tous les points de terminaison. Microsoft 365 peut également identifier automatiquement les risques de non-conformité et les violations du code de conduite dans les comptes de courrier électronique, de messagerie et de réseaux sociaux de l'entreprise. Cela permet aux équipes informatiques d'arrêter les fuites de données avant même qu'elles ne se produisent. En cas de fuite ou de vol de données, Microsoft 365 peut détecter la violation et agir pour protéger votre organisation grâce à des protocoles de réponse automatique établis par vos équipes informatiques.

Donner aux employés en première ligne les moyens de collaborer et de partager des données en toute sécurité

Tandis que Microsoft 365 donne à vos employés en première ligne l'accès à une suite complète d'outils de productivité pour les aider à mieux faire leur travail, Teams propose une plateforme de communication qui leur permet de partager des données et de collaborer en toute sécurité, le tout au même endroit. Les données deviennent plus visibles et les employés sont moins susceptibles d'employer des méthodes non gérées pour partager des renseignements confidentiels. La gestion et la notation des données sont également améliorées grâce à Teams, avec la possibilité de fournir aux employés un accès en temps réel aux documents des procédures opérationnelles normalisées, ainsi que la possibilité de communiquer avec des superviseurs ou des experts.

Témoignage d'un utilisateur de Microsoft 365

Microsoft 365 a aidé le prestataire de soins à domicile Amedisys à protéger ses données confidentielles sur plus de 25 000 appareils (et à économiser 250 000 dollars).

“

Les gens nous font confiance pour prendre soin d'eux alors qu'ils sont les plus vulnérables. Il était important de trouver un fournisseur comme Microsoft qui attache autant que nous de valeur et de respect aux données des patients.

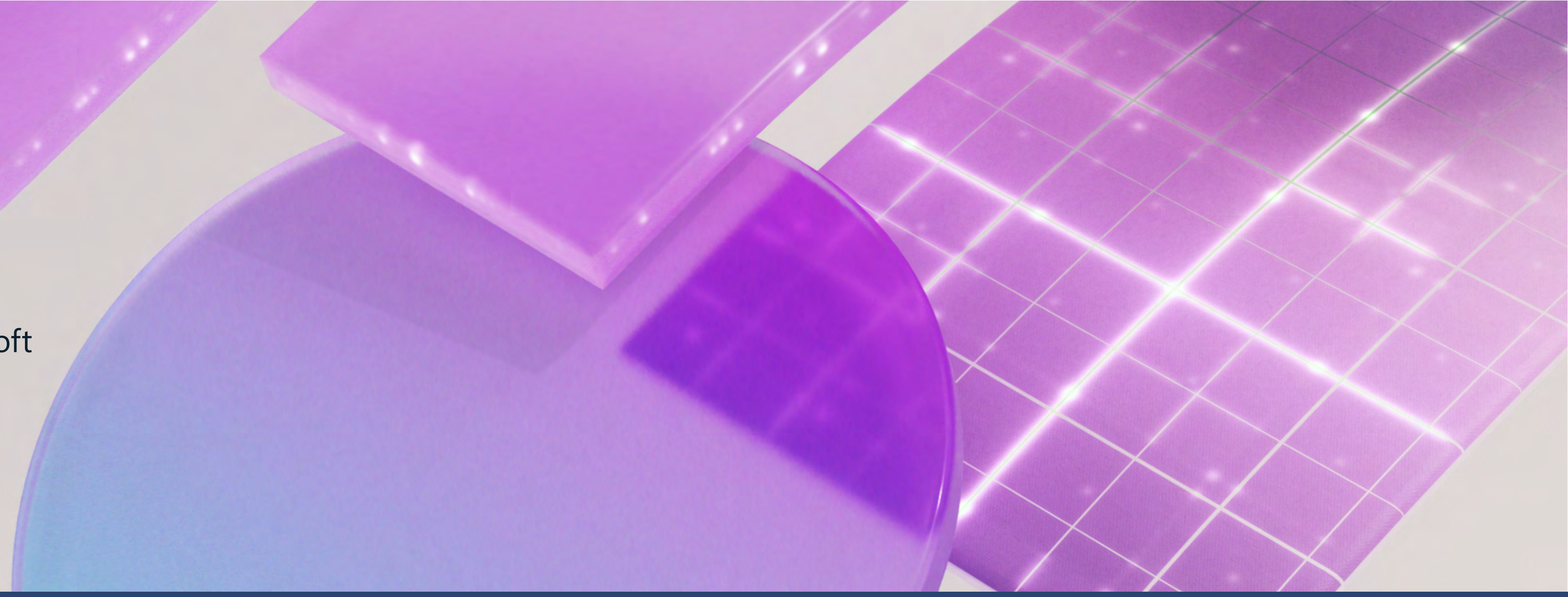
Keith Blanchard
Vice-président senior et directeur technologique, Amedisys

Microsoft 365

Microsoft 365 for Frontline Workers

Protégez votre entreprise avec la solution holistique de Microsoft personnalisée pour les espaces de travail de première ligne.

En savoir plus →



Sources :

[1]Microsoft Threat Intelligence. (2023 octobre). « Rapport 2023 sur la défense numérique de Microsoft ». https://www.microsoft.com/security/security-insider/microsoft-digital-defense-report-2023/.

[2]« Rapport 2023 sur les coûts d'une violation des données ». IBM, juillet 2023. https://www.ibm.com/reports/data-breach.

[3]« Découvrir et gérer les pratiques informatiques non conventionnelles : Microsoft Defender for Cloud Apps » Microsoft Learn, 24 mai 2023. https://learn.microsoft.com/defender-cloud-apps/tutorial-shadow-it

[4]« Anatomy of a Modern Attack Surface. » Microsoft Security Insider, 2 mai 2023. https://www.microsoft.com/security/business/security-insider/threat-briefs/anatomy-of-a-modern-attack-surface/.

[5]Murty, Rohan, Sandeep Dadlani et Rajath Das. « How Much Time and Energy Do We Waste Toggling between Applications? » Harvard Business Review, 29 août 2022. https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications.

[6]Jakkal, Vasu. « The Passwordless Future Is Here for Your Microsoft Account. » Blogue Microsoft dédié à la sécurité, 15 septembre 2021. https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/.

[7]« How Much Time Does Your Organisation Spend on Managing Passwords? » The Independent, 7 septembre 2022. https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html.

[8]The Total Economic Impact™ of Microsoft Entra, une étude commandée à Forrester Consulting, mars 2023. http://aka.ms/MicrosoftEntraTEI.

[9]The Total Economic Impact™ of Microsoft Teams, une étude commandée à Forrester Consulting, avril 2023. https://tools.totaleconomicimpact.com/go/microsoft/teams/index.html.