CINQ FONCTIONNALITÉS DE WINDOWS 11 POUR UN TRAVAIL SANS FAILLE

Windows 11 | Computacenter

La réalité des entreprises aujourd'hui repose sur un équilibre entre l'amélioration de l'expérience collaborateur, l'optimisation de la productivité et une sécurité des données optimale.

Sous l'effet du travail hybride, les schémas organisationnels traditionnels se sont transformés.

Mais cette mutation s'accompagne d'une hausse des menaces pour la sécurité. Les données manipulées par les entreprises sont toujours plus convoitées et menacées, notamment pour leur valeur financière. En 2022, 52% des entreprises ont subi une cyberattaque, entraînant une perte de revenu de 6,7% en moyenne[1].

Les organisations cherchent donc à garantir la sécurité de leur parc et de leurs données, sans entraver l'efficacité de leurs équipes. Le télétravail a ajouté une nouvelle couche de complexité.

Une étude menée par Microsoft révèle que trois décideurs sur quatre estiment que le passage au travail hybride rend leur organisation plus vulnérable face aux attaques. Les collaborateurs travaillent plus souvent en dehors du bureau, ce qui rend la protection des équipes et de leurs équipements IT plus difficile[2]. La vulnérabilité humaine est la première cause de violation de données[3], et on estime que 47 % des individus tombent dans le piège de l'hameçonnage lorsqu'ils travaillent à domicile[4].

PRÊT À VOUS LANCER ?

1. Rapport d'enquête Windows 1, Techaisle, Décembre 2022
2. Signaux de sécurité pour les décideurs en matière de sécurité (microsoft.com)
3. 88 % des failles de sécurité sont dues à des erreurs humaines (eccouncil.org)
4. Impact de COVID-19 sur la cybersécurité (deloitte.com)

Historiquement, la sécurité sur le lieu de travail se résumait à un simple enjeu de sécurité physique. L'attention des décideurs informatiques était restreinte au périmètre des locaux de l'entreprise. La sécurité a été conçue pour empêcher les menaces d'entrer et pour protéger les actifs au sein de ce périmètre. Il y avait un équilibre à trouver et un compromis à faire entre des politiques de sécurité strictes et l'impact qu'elles auraient sur l'expérience de l'utilisateur.

Aujourd'hui, avec le passage au cloud, les équipes chargées de la sécurité doivent adopter une nouvelle approche afin de se concentrer sur la protection des données. Or, celles-ci ne peuvent plus être cantonnées et circonscrites entre les quatre murs d'un bâtiment physique. Les données sont partagées, échangées, elles circulent entre les métiers, entre les utilisateurs… où qu'ils se trouvent.

Vos collaborateurs exigent de la flexibilité sans sacrifier la simplicité d'utilisation ou la collaboration avec leurs collègues. Ils souhaitent se sentir productifs, quels que soient le lieu et le moment où ils travaillent, avec des équipements opérationnels, dès leur sortie de l'emballage.

Si les mesures de sécurité sont trop restrictives, ils cherchent des solutions de contournement, ce qui rend l'organisation vulnérable aux attaques, en l'exposant au « shadow IT ». Microsoft a conçu Windows 11 de façon à aider les entreprises à relever les nouveaux défis posés par le travail hybride. Ses fonctionnalités avancées et intégrées, permettent aux organisations de poser des fondations plus solides et plus résilientes face à l'évolution des menaces.

Cette sécurité native, intégrée à Windows 11 s'incarne dans 5 fonctionnalités clés.

1 UNE AUTHENTIFICATION USER-FRIENDLY

Les mots de passe faibles sont le point d'entrée favori des cybercriminels pour accéder aux données de l'entreprise. Windows 11 utilise l'authentification par code PIN et la biométrie (pour les appareils qui la prennent en charge), telle que les empreintes digitales et la reconnaissance faciale. De cette façon, les utilisateurs n'ont pas à mémoriser plusieurs mots de passe.

Ils sont également moins susceptibles de les noter ou de les oublier, ce qui minimise les temps d'arrêt et réduit la nécessité de recourir à des plugins de gestion de mots de passe, qui peuvent présenter leurs propres risques de sécurité.

2 UNE SÉCURITÉ INTÉGRÉE DANS L'ADN DES MACHINES

Une étude menée par Microsoft a révélé que 80 % des décideurs estiment que les logiciels à eux seuls ne suffisent pas à protéger contre les menaces émergentes[5]. Avec Windows 11, la sécurité s'articule autour de l'appareil, de l'identité de l'utilisateur et des services cloud. Le nouveau système d'exploitation repose sur les principes de sécurité Zero Trust, avec une sécurité physique intégrée à une puce, un démarrage sécurisé intégré, une protection basée sur la virtualisation (VBS) et une intégrité du code protégée par l'hyperviseur (HCVI). Les données sensibles sont automatiquement chiffrées et l'accès est protégé dans une partie sécurisée de la mémoire du système.

Cela signifie que les personnes malveillantes ne peuvent pas aller loin, même si elles pénètrent dans le système. Il s'agit d'une vision plus holistique de la sécurité, de l'appareil aux données stockées dans le cloud, et inversement.

3 UNE SÉCURITÉ PROACTIVE

Les méthodes de cyberattaque évoluent plus vite que les protocoles de sécurité. Plus d'un tiers (35 %) des cyberattaques en 2020 ont utilisé des logiciels malveillants ou des méthodes inédites[6]. Les entreprises doivent donc adopter une approche plus proactive, plutôt que réactive, en matière de sécurité.

Chez Microsoft, plus de 10 000 experts en sécurité analysent chaque jour plus de 65 billions de signaux d'attaque[7].

Avec Windows 11, l'intelligence artificielle et l'apprentissage automatique soulagent l'utilisateur du fardeau de la sécurité, grâce à un antivirus nouvelle génération et à une défense contre les logiciels malveillants.

Des dispositifs qui restent en permanence à l'affût des applications suspectes et des tentatives de piratage à distance. Le logiciel est en permanence mis à jour, sans frais supplémentaires, et comprend des paramètres personnalisables pour les organisations individuelles.

5. Google avertit les utilisateurs de LastPass qu'ils ont été exposés à une fuite de données concernant leur dernier mot de passe (forbes.com)
6. Impact de la COVID-19 sur la cybersécurité (deloitte.com)
7. microsoft.com

4 TRAVAILLER PLUS EFFICACEMENT DANS LE CLOUD

Grâce à la synchronisation des données entre le cloud et l'ordinateur, les équipes peuvent travailler plus rapidement et plus efficacement. Microsoft investit chaque année environ 1 milliard de dollars dans la recherche sur la sécurité et sa licence E5 permet aux organisations de rationaliser les stratégies de sécurité et de se défaire d'un large éventail d'applications de sécurité devenues superflues (avec toutes les économies financières qui en découlent)[8]. Les équipements fonctionnant sous Windows 11 démarrent plus rapidement et offrent une meilleure expérience utilisateur, tandis que la pile de sécurité Microsoft 365 E5 protège le réseau dans le cloud.

5 UNE SÉCURITÉ SUR MESURE POUR UNE PRODUCTIVITÉ MAXIMALE

Les caractéristiques combinées de Windows 11 ont permis de réduire de 58 % l'incidence des logiciels malveillants, en particulier grâce à l'isolation des applications, aux contrôles de confidentialité et à la possibilité de définir des paramètres sur mesure en fonction des besoins[9]. Travailler avec un partenaire expérimenté comme Computacenter vous permet d'évaluer votre degré de préparation à la migration vers Windows 11. Vous pourrez ainsi planifier le bon moment pour migrer, mais aussi bénéficier d'un accompagnement de bout-en-bout, avec des équipements livrés préconfigurés pour fournir une protection dès leur mise en service.

8. RWMv11 (microsoft.com)
9. Windows 11 offre une protection de la puce TPM au Cloud afin de répondre aux nouveaux défis de sécurité du travail hybride. (Microsoft Security Blog)

POUR EN SAVOIR PLUS ?

Computacenter aide les organisations à évaluer leur degré de préparation à Windows 11. Pour en savoir plus sur la façon dont Computacenter peut vous aider à évaluer et à adopter Windows 11 pour votre organisation, veuillez contacter votre Gestionnaire de Compte Computacenter ou envoyez un e-mail à **communication@computacenter.com**.

À propos de Computacenter

Computacenter est un fournisseur indépendant de technologies et de services de premier plan, qui bénéficie de la confiance des grandes organisations publiques et privées. Nous accompagnons nos clients dans les phases d'approvisionnement, de transformation et de gestion de leur infrastructure technologique pour leur assurer une transformation numérique permettant à leurs employés et à leur entreprise de se développer. Computacenter est une société cotée à la bourse de Londres (indice FTSE 250) et compte environ plus de 20 000 collaborateurs à travers le monde.

www.computacenter.com

Computacenter