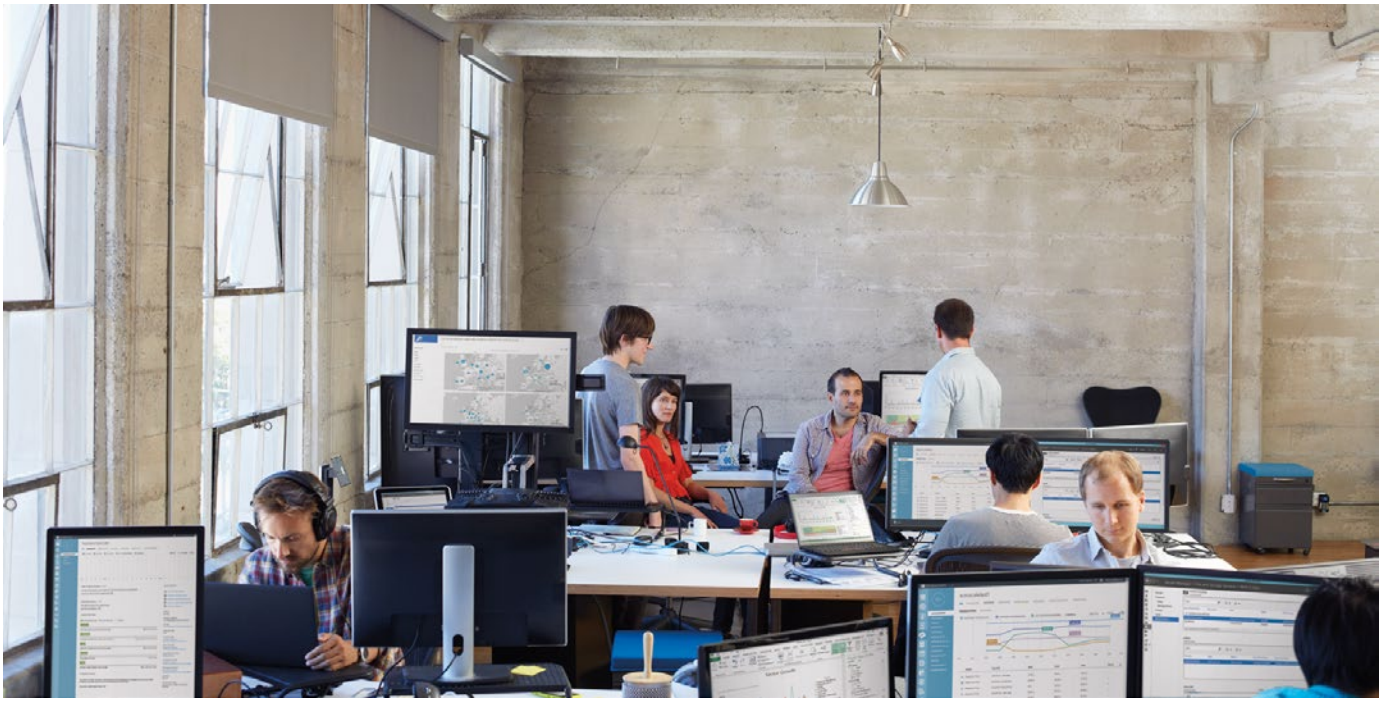
Microsoft

Identifiez les maillons faibles de votre système de sécurité



Améliorez votre protection en détectant et en contrôlant rapidement les problèmes de sécurité.

Les maillons faibles de votre chaîne de sécurité, quelle que soit leur taille, exposent votre entreprise à des violations coûteuses. La perte d'informations est désormais la conséquence la plus dommageable de la cybercriminalité, suivie de près par l'interruption de l'activité et la baisse de productivité.[1] Le rythme effréné des entreprises actuelles, auquel s'ajoute la demande croissante de données et d'innovation, exige une sécurité qui évolue au moins aussi vite que les menaces.

Une sécurité solide s'appuie sur la force du système dans son ensemble. Un seul maillon faible peut avoir un impact significatif sur votre activité. Explorez les sources de fuites les plus courantes, l'impact qu'elles peuvent avoir sur votre activité, et la manière de mieux protéger l'ensemble de votre réseau.

Quand votre sécurité est compromise de l'intérieur

Même avec l'aide des meilleurs systèmes de sécurité, le caractère imprévisible des utilisateurs finaux au sein de votre réseau a souvent pour effet d'affaiblir les dispositifs. Découvrez les activités des utilisateurs finaux pouvant générer des failles dans votre chaîne de sécurité, ainsi que des conseils de prévention.

42 %

Bien que 42 % des violations de données proviennent d'erreurs techniques, l'erreur humaine reste la première cause, à hauteur de 58 % à l'échelle internationale.[2]

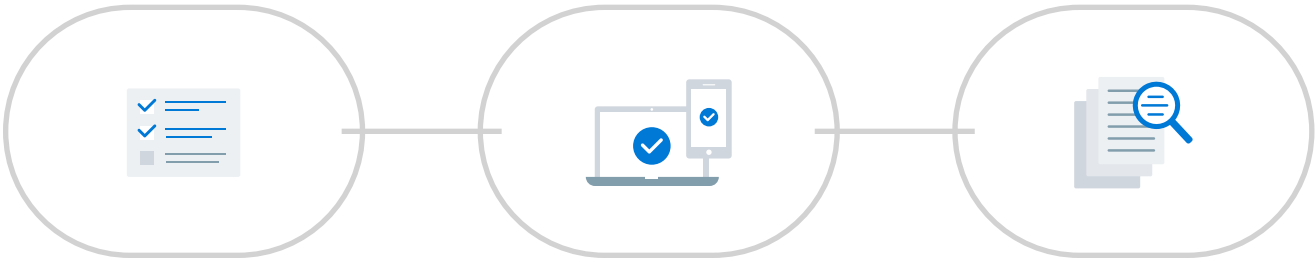
Violations possibles par les ressources locales et à distances

Les menaces potentielles augmentent en même temps que le nombre d'appareils et de lieux d'utilisation. Les activités ne sont plus confinées à un seul emplacement, mais s'étalent sur différents pays et fuseaux horaires. Parallèlement, nos systèmes mettent en relation des employés à temps plein, des fournisseurs et des prestataires extérieurs par le biais de divers appareils. Tout nouvel appareil et utilisateur final connecté à votre réseau représente un nouveau point d'entrée pour une attaque potentielle.

67 %

des professionnels de la sécurité informatique sont incapables de détecter les employés qui utilisent des appareils mobiles non sécurisés, ce qui expose les données sensibles.[3]

Renforcez votre chaîne :



01

Lorsque vos employés rencontrent des difficultés pour accéder aux informations, les utilisateurs finaux essaient de contourner les stratégies de sécurité ou informatiques afin de mener à bien leur travail de manière rapide et efficace. Pour les aider à rester en conformité, offrez-leur un accès facile aux outils et aux données d'entreprise autorisés sur tous les appareils, aussi bien au bureau et qu'à distance.

02

Tirez parti de l'authentification multifacteur et de la gestion des applications mobiles pour empêcher l'accès non autorisé aux informations de l'entreprise.

03

Donnez à votre équipe informatique les outils nécessaires pour surveiller, ainsi qu'identifier et résoudre les problèmes à distance, ou effacer les données des appareils en cas de menace.

Violations intentionnelles internes

Malheureusement, il arrive que des employés fassent une utilisation abusive intentionnelle des données d'entreprise. Même une fuite infime peut entraîner des pertes significatives.

60 %
des employés qui partent avec des données sécurisées le font dans l'idée d'en tirer parti ultérieurement.[3]

71 %
des cas d'utilisation abusive en interne qui ciblent des informations personnelles et médicales.[3]

Renforcez votre chaîne :

01
Utilisez des outils capables de surveiller les activités suspectes sur votre réseau et de fermer un compte d'utilisateur.

02
Personnalisez l'accès pour des rôles et des responsabilités spécifiques au sein de votre organisation.

03
Simplifiez les processus d'octroi et de suppression d'accès par l'équipe informatique.

Microsoft 365 E5

Découvrez la solution Microsoft 365 Entreprise adaptée à votre entreprise

- La solution Gestion de la sécurité avancée Office 365 fournit des informations sur les activités suspectes, qui vous permettent de mener des investigations en lien avec des situations potentiellement problématiques et, le cas échéant, de prendre des mesures pour résoudre des problèmes de sécurité.

- Avec Cloud App Security, découvrez toutes les applications cloud de votre réseau, bénéficiez d'une meilleure visibilité du Shadow IT et évaluez les risques, le tout sans mobiliser d'agents.

- Windows Hello Entreprise remplace les mots de passe par l'authentification à deux facteurs renforcée sur les ordinateurs et appareils mobiles. Cette authentification s'appuie sur un nouveau type d'informations d'identification associées à un appareil et utilise une caractéristique biométrique ou un code confidentiel.

- Azure Active Directory est une solution cloud complète de gestion de l'accès et des identités dotée d'un jeu de fonctionnalités robuste pour gérer les utilisateurs et les groupes. Elle permet de sécuriser l'accès aux applications locales et cloud, notamment à des services web Microsoft tels qu'Office 365 ainsi qu'à de nombreuses applications SaaS tierces.

Quand votre infrastructure est menacée par des sources malveillantes externes

Les attaques malveillantes provenant de l'extérieur sont l'une des principales causes de violations de sécurité. Des méthodes telles que le social engineering existent depuis toujours, ou tout au moins depuis l'avènement des e-mails et d'Internet. L'amélioration des connaissances pousse les attaquants à redoubler de créativité, et même les utilisateurs finaux les plus avertis ne sont pas à l'abri.[5]

3,3
milliards d'informations d'identification ont été volées en 2016.[6]

23 %
des attaques d'hameçonnage de social engineering réussissent parce que les destinataires ouvrent les messages.[6]

Voici 5 types courants d'attaques de social engineering :[7]

Hameçonnage

Redirige les utilisateurs vers des URL suspectes en apparence légitimes, pour voler des informations d'identification ou autres informations personnelles.

Faux-semblant

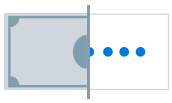
Crée un scénario fictif pour gagner la confiance de l'utilisateur dans le but de lui extorquer des informations personnelles.

Appâtage

Des disques ou clés USB infectés sont abandonnés dans des lieux publics, dans l'espoir qu'ils seront insérés dans un ordinateur. Cette tactique se rencontre également sur le web sous la forme de liens de téléchargement.

Talonnage

Les attaquants obtiennent l'accès à des zones réglementées en suivant un employé autorisé.



Quid pro quo

Promet un avantage en échange des informations de la victime.

Récupération de vos données contre de l'argent

Le phénomène des Ransomware (séquestration de données assortie d'une demande de rançon) n'augmente pas seulement en fréquence, mais également en nombre de victimes qui paient pour récupérer leurs données. Il est possible d'éviter les Ransomware en revenant aux fondamentaux : sensibilisation, formation, hygiène, sauvegardes fréquentes, plan d'action et, naturellement, logiciels.

6 000 %

Le nombre de Ransomware a augmenté de 6 000 % entre 2015 et 2016.[8]

40 %

Les ransomware infectaient près de 40 % de la totalité des messages indésirables en 2016.[8]

70 %

des victimes ont payé pour récupérer leurs données. Parmi elles, 50 % ont déboursé plus de 10 000 USD, et 20 % plus de 40 000 USD.[8]

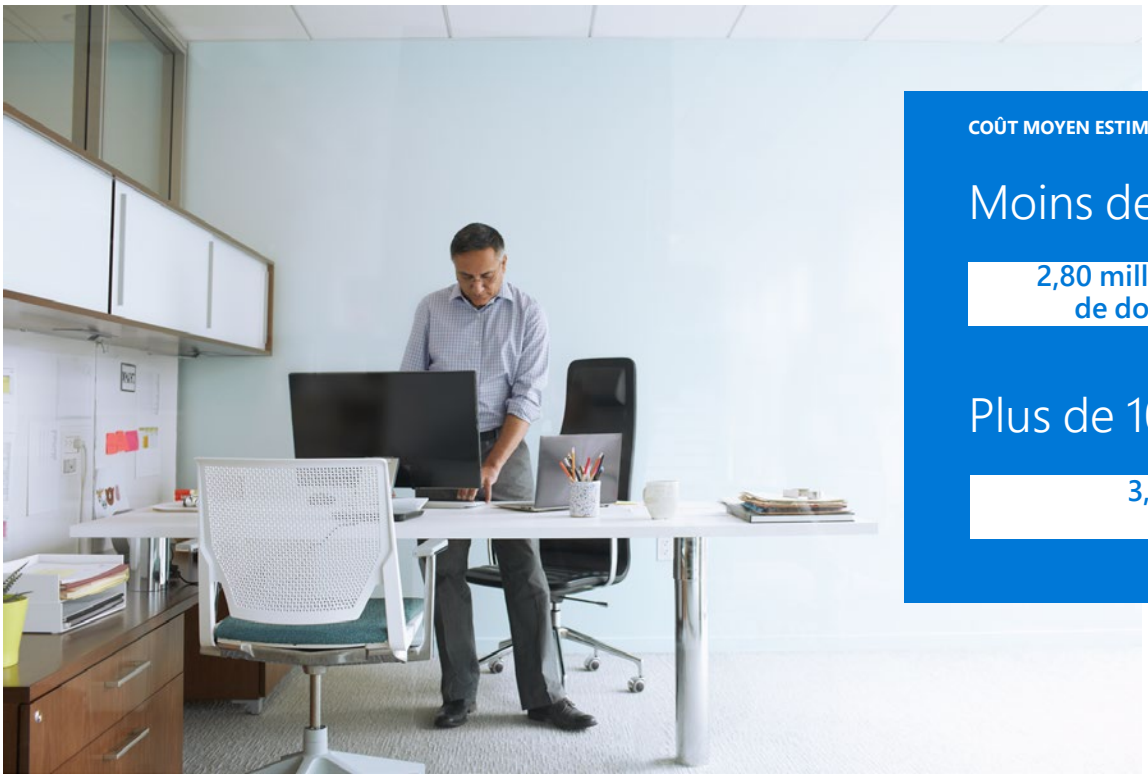
Microsoft 365 E5

Découvrez la solution Microsoft 365 Entreprise adaptée à votre entreprise

- Lorsque votre ordinateur est protégé par Windows Defender Antivirus, vous bénéficiez d'une protection complète pour votre système, vos fichiers et vos activités en ligne contre les virus, logiciels malveillants, logiciels espions et autres menaces.
- Advanced Threat Protection d'Office 365 protège le courrier de votre entreprise en temps réel contre des attaques inconnues et sophistiquées en sécurisant votre environnement Office 365 contre les menaces avancées, les fichiers potentiellement dangereux et les liens malveillants consultés au sein de ces fichiers.
- BitLocker Drive Encryption fonctionne parfaitement avec Windows 10. Il gère les menaces liées au vol ou à l'exposition de données stockées sur des ordinateurs perdus, volés ou désaffectés de manière inappropriée.

Détectez et gérez rapidement les failles de sécurité

Le coût d'une violation de données dépend beaucoup du temps consacré à identifier et à contrôler celle-ci. Votre capacité à récupérer rapidement peut représenter une économie de plusieurs millions de dollars.



COÛT MOYEN ESTIMÉ D'UNE VIOLATION[9]

Moins de 100 jours

2,80 millions de dollars

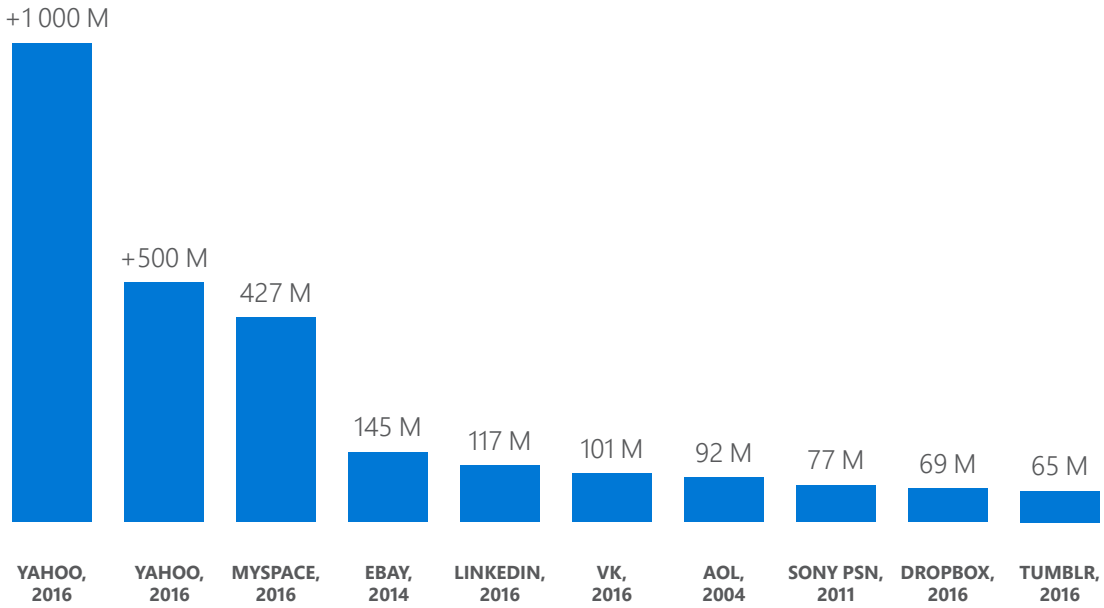
Plus de 100 jours

3,83 millions de dollars

Les violations de données sont coûteuses, surtout si aucun travail de détection n'est réalisé en amont. Découvrez l'impact qu'ont eu des violations coûteuses sur de grandes entreprises.

Si l'on considère la sécurité comme une chaîne, il est important de s'assurer que tous les maillons sont robustes. La mise en place hâtive de solutions inadéquates peut compromettre votre sécurité et il sera trop tard lorsque vous vous en rendrez compte.

Les plus grandes violations de données entre 2004 et 2016[10]



À l'échelle internationale, les organisations sont parvenues à diminuer le nombre de jours nécessaires pour identifier une violation de données, passant d'environ 201 jours en moyenne en 2016 à 99 en 2017. Le nombre de jours moyen pour contrôler une violation de données est passé de 70 à 66 jours.[9] Plus une violation de données est identifiée et contrôlée rapidement, plus les coûts sont faibles. Il est donc important de s'assurer que votre activité dispose d'outils appropriés pour identifier et contrôler rapidement les violations.

Microsoft 365 E5

Découvrez la solution Microsoft 365 Entreprise adaptée à votre entreprise

- Windows Defender Advanced Threat Protection vous aide à détecter des attaques avancées et autres violations de données sur vos réseaux, ainsi qu'à enquêter sur celles-ci et à y réagir.
- Advanced Threat Analytics diminue le risque de dommages coûteux, et vous présente toutes les informations dont vous avez besoin dans une vue concise et en temps réel du déroulement de l'attaque. De plus, toutes les informations permettant d'apprendre, d'analyser et d'identifier les comportements normaux et suspects des utilisateurs et des appareils sont intégrées.
- Office 365 Threat Intelligence offre une large visibilité du paysage des menaces, élimine le bruit, et fournit de précieuses informations concernant l'impact de ces menaces sur votre organisation. Fondamentalement, cette visibilité et ces informations permettent aux organisations de mettre à jour de manière proactive leurs stratégies et services de sécurité pour atténuer l'impact des incidents.

Adoptez une approche holistique pour traiter les maillons faibles et renforcer l'ensemble de votre chaîne de sécurité.

Microsoft 365 fournit un kit de ressources de défense de bout en bout entièrement intégré et aborde chaque composant des mesures de votre chaîne de sécurité. Choisissez une méthode de travail fiable, productive et sécurisée qui réunit le meilleur en matière de matériel, de logiciel et de sécurité réseau.

Découvrez de quelle manière Microsoft 365 Entreprise peut protéger votre entreprise à l'aide de solutions intelligentes qui favorisent la créativité et la collaboration pour tous et en toute sécurité.

Sources :

1. « Cost of Cyber Crime Study & the Risk of Business Innovation », 2016, Ponemon Institute
2. « International Trends in Cybersecurity », 2016, Comptia
3. « The Cost of Insecure Mobile Devices in the Workplace », 2014, Ponemon Institute
4. « 2017 Data Breach Investigations Report », 2017, Verizon
5. « 2017 Credential Spill Report », Shape Security
6. « Anatomy of a Social Engineering Attack: Exploiting Human Behavior », 2016, PricewaterhouseCoopers
7. « 5 Social Engineering Attacks to Watch Out For », 2015, The State of Security
8. « Ransomware: How Consumers and Businesses Value Their Data », 2016, IBM
9. « 2017 Cost of Data Breach Study », Ponemon Institute
10. « Latest Yahoo Attack is the Largest Data Breach to Date », 2016, Statista

Microsoft