Anatomie des données à risque dans Microsoft 365

Comprendre les risques cachés derrière le partage quotidien de fichiers et comment reprendre le contrôle.

Livre électronique

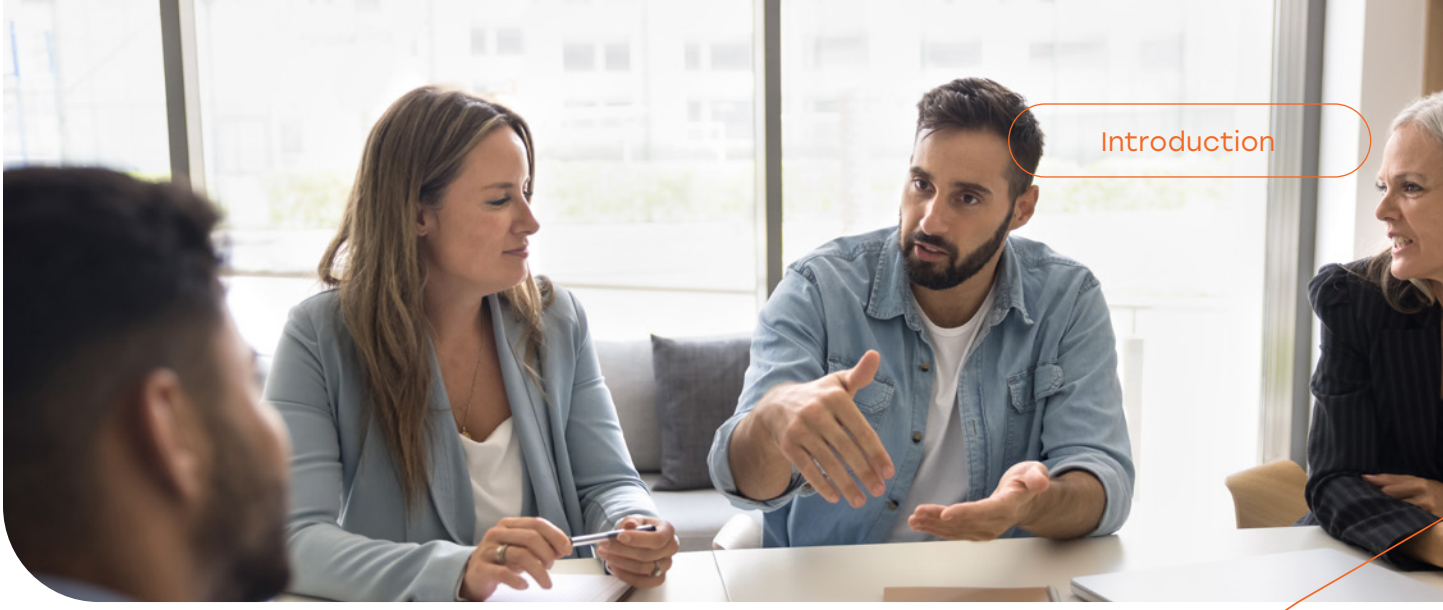
WeActis
par Mondata

Résumé

Vous pensiez que les données partagées par vos employés étaient en sécurité ? Détrompez-vous !

Les partages à l'ensemble de l'organisation, les liens périmés et les fichiers sensibles sans permission restreinte sont autant de données à risque en circulation chaque jour dans votre organisation

Dans ce guide pédagogique, nous décortiquons ce qu'est un fichier « à risque », nous vous expliquons pourquoi c'est important pour VOUS et pas juste une affaire de TI, et comment les nouvelles méthodes de collaboration intégrant l'IA amplifient les risques.



Si vous utilisez des environnements de travail collaboratifs, vous détenez plus de risque que vous ne le pensez.

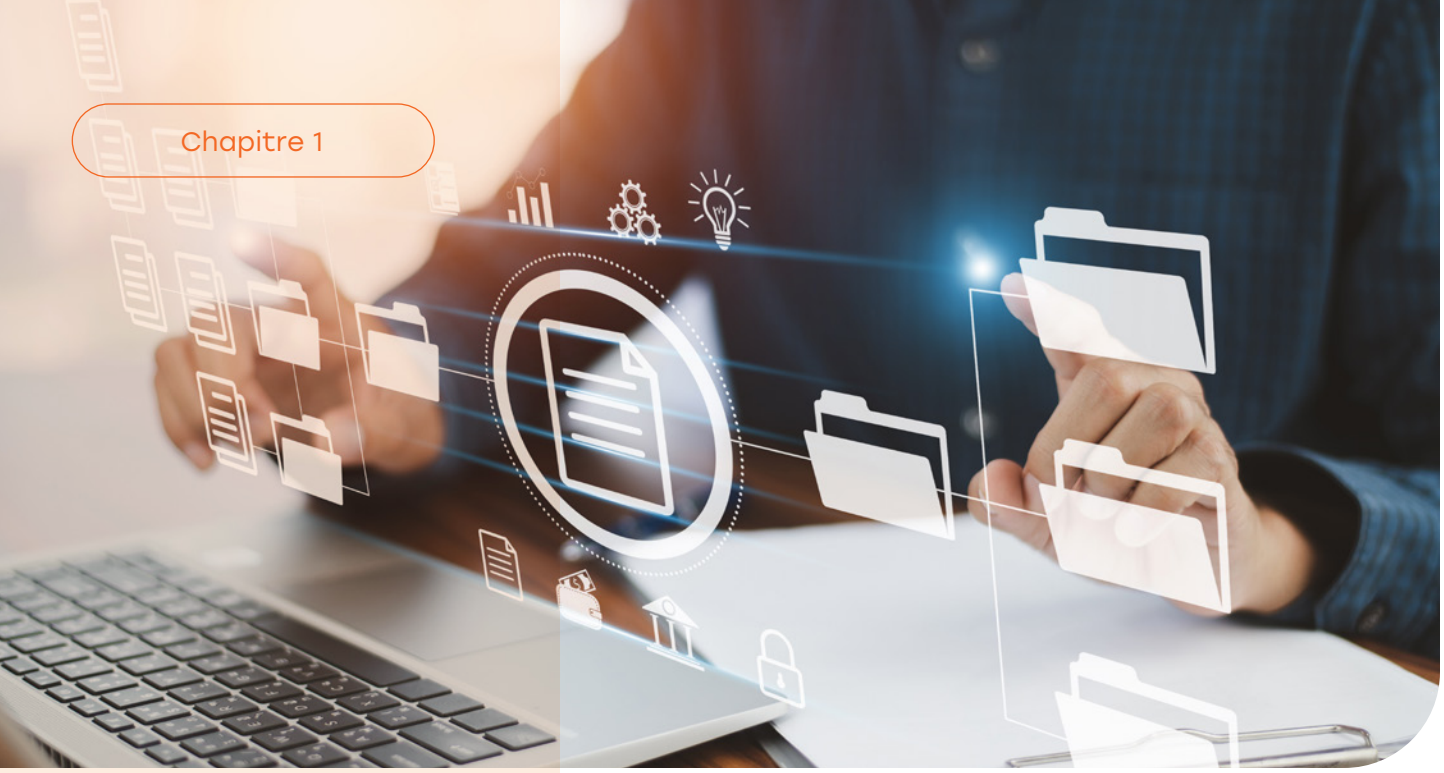
Collaborer n'a jamais été aussi facile et aussi risqué qu'aujourd'hui. Tous les jours, des fichiers sont téléchargés, partagés et oubliés. Les employés pensent qu'ils font ce qu'il faut. Les gestionnaires pensent que le service informatique a tout sous contrôle.

Mais c'est faux : la sécurité des données avec Microsoft 365 est une responsabilité partagée et les partages de fichiers non gérés génèrent un risque invisible que personne ne contrôle. C'est ainsi que les données sensibles peuvent fuiter, être corrompues ou mal utilisées, en particulier aujourd'hui, à l'ère de l'IA générative.

Afin de s'attaquer à l'origine du problème, nous devons reconnaître cette réalité : la sécurité des données n'est plus seulement du ressort des TI. Si nous voulons que les employés prennent leurs responsabilités, nous devons leur faciliter la tâche.

C'est la raison pour laquelle nous avons créé WeActis. Mais avant de vous montrer comment nous fonctionnons, dressons le portrait d'une menace que vous n'avez probablement jamais remarquée, mais qui prend toujours plus d'ampleur dans votre quotidien : les données à risque.

Chapitre 1



Qu’est-ce qu’une « donnée à risque » à l’ère de la collaboration Cloud ?

Les « données à risque », ce sont des fichiers et des dossiers qui :

- sont surexposés à une audience inintentionnellement trop large (à l’interne ou à l’externe)
- contiennent des informations sensibles sans classification ou protection appropriées
- ont été partagés avec des paramétrages de permissions risquées (par exemple des liens avec droits de modification sans date d’expiration)
- perdurent non gérés et non sécurisés sur de longues périodes de temps, alors qu’ils sont toujours accessibles

Il ne s’agit pas de logiciel malveillant ou de pirates informatiques.

Il s’agit de données qui fuitent sans qu’on s’en rende compte, se corrompent et dépérissent à l’intérieur de votre propre écosystème.

Les quatre éléments clé du risque

(Caractéristiques de donnée à risque)

Chaque document ou dossier partagé avec Microsoft 365 comporte sa propre combinaison de risques potentiels. Chez WeActis, on les décortique ainsi:

1

Analyse de l'accès : qui peut consulter le fichier ?

Plus l'accès est large, plus le risque de fuite de données est grand.

Nous évaluons le public ciblé par le fichier :

- public (toute personne avec le lien d'accès).
- Une organisation entière
- Des collaborateurs externes
- Des usagers spécifiques ou des groupes.

Nous évaluons aussi le type d'élément partagé :

- des fichiers (le risque est restreint à un seul document)
- des dossiers (le risque touche tous les fichiers contenus, même les plus sensibles).

EXEMPLE CONCRET

Un responsable des opérations partage un dossier avec toute son organisation pour donner l'accès à un gabarit de document particulier.

Le dossier, cependant, contient aussi d'anciens contrats de fournisseur archivés et les rapports d'audits internes qui n'auraient jamais dû être partagés avec un aussi large public.

Personne ne l'a remarqué car le partage partait d'une bonne intention. Cependant, désormais, tous les membres de l'entreprise ont accès à des dizaines de fichiers sensibles, y compris les nouveaux stagiaires, les partenaires extérieurs ajoutés sur Teams, voire même, peut-être, les outils d'IA intégrés à Microsoft 365.

Résultat : Une bonne intention au départ entraîne un risque de conformité et de confidentialité, des données qui peuvent passer inaperçu pendant des mois.

COMMENT WEACTIS VOUS AIDE

WeActis notifie le responsable des opérations que le dossier qu'il vient de partager contient des données à risque et le guide jusqu'à la révocation du partage.

2

Sensibilité : à quel point l'information est-elle confidentielle ?

Vous ne pouvez pas protéger ce que vous n'avez pas clairement étiqueté.

WeActis évalue :

- les étiquettes de confidentialité de Microsoft
- les risques encourus par votre organisation selon les étiquettes attribuées (public, interne, confidentiel, très confidentiel)

Si un fichier n'a pas d'étiquette, WeActis lui attribue une importance modérée. Cela revient à :

- surestimer le risque pour un document destiné à un large public
- sous-estimer le risque pour un document sensible qui n'aurait pas d'étiquette

BONNE PRATIQUE

Il vaut mieux n'étiqueter que les fichiers sensibles, quitte à laisser les autres sans identification, plutôt que de n'en étiqueter aucun.

EXEMPLE CONCRET

Un contrat légal, contenant les informations du client, partagé sans étiquette de sensibilité **ne déclenchera jamais un avertissement.**

COMMENT WEACTIS VOUS AIDE

WeActis **identifie** le document comme contenant des données modérément sensibles et **avertit** l'utilisateur lorsque le nombre de partages atteint le palier défini par l'entreprise pour cette catégorie.

3

Type d'autorisations : que peut faire le destinataire du document ?

L'accès est une chose, le contrôle en est une autre.

WeActis analyse si le destinataire peut :

- éditer (c'est à dire modifier le document sans laisser de trace)
- éditer en mode révision (les changements sont enregistrés)
- lire
- lire sans possibilité de téléchargement

Chaque autorisation comporte un risque différent :

- en termes d'intégrité des données : les documents modifiables peuvent être réécrits.
- en termes de diffusion : les fichiers téléchargeables peuvent être repartagés sans contrôle.
- d'empoisonnement pour l'IA : changer volontairement le contenu des fichiers de telle manière que l'IA croit que c'est le document original et partage l'information fausse ou modifiée aux utilisateurs.

EXEMPLE CONCRET

Un stagiaire obtient la « permission d'édition » sur un tableur de prévisions. **Une formule est modifiée.** Les résultats pour l'entreprise sont erronés, mais personne ne s'en aperçoit avant plusieurs mois.

COMMENT WEACTIS VOUS AIDE

WeActis **signale** à la personne qui a partagé le document qui sont les personnes qui ont obtenu l'autorisation d'éditer le fichier.

4

Durée des autorisations : depuis combien de temps le document est-il à risque ?

Plus la durée des autorisations est longue, plus le risque est grand.

WeActis examine :

- depuis combien de temps les autorisations sont mises en place
- Quels sont les paliers mis en place par l'organisation :
  - Court-terme (moins de 30 jours)
  - Long terme (plus de 30 jours)

Un partage oublié via un lien accessible à « quiconque ayant le lien » est plus susceptible d'être mal utilisé qu'un fichier partagé la veille.

EXEMPLE CONCRET

Un chef d'équipe partage des prévisions financières avec un responsable régional durant la période du budget. Le fichier inclut des informations sensibles sur les revenus estimés des projections d'affaires.

La collaboration prend fin, mais le lien partagé reste actif avec une autorisation d'édition.

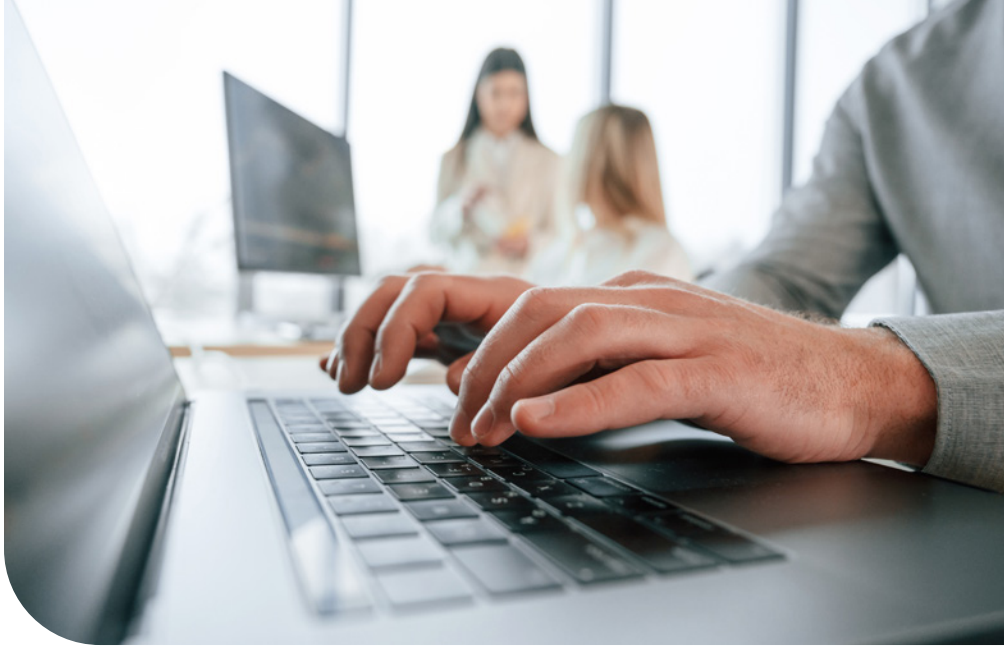
Les mois passent. Le directeur régional change de poste. Le fichier reste accessible à une personne qui n'en a plus besoin et dont le remplaçant ne saura peut-être même pas que ce fichier existe.

Résultat :
Un fichier à haut risque est accessible plus longtemps que nécessaire, sans supervision. Le problème n'est pas seulement qu'il est disponible mais surtout que personne ne contrôle si le partage est encore justifié.

COMMENT WEACTIS VOUS AIDE

WeActis indique au propriétaire du SharePoint où est rangé le fichier des prévisions budgétaires afin qu'il puisse en réviser ou en supprimer l'accès.

Chapitre 2



Comment WeActis vous aide à détecter et à protéger les données sensibles

WeActis utilise une approche proactive, centrée sur l'utilisateur pour gérer les risques.

Étape 1 : Analyse

- Nous scannons Microsoft 365 (OneDrive, Teams, SharePoint).
- Nous analysons des millions de points dans les niveaux d'autorisations liés aux fichiers.
- Nous générons un inventaire en temps réel de fichiers identifiés comme « à risque ».

Étape 2 : Attribution

- Nous identifions l'auteur du partage à risque.
- Nous identifions aussi le propriétaire de la ressource (par exemple, OneDrive ou Sharepoint).

Étape 3 : Notification

Nous envoyons des notifications contextualisées directement aux utilisateurs concernés.

Nous les guidons pour qu'ils corrigent eux-mêmes le risque, sans avoir besoin de faire un ticket informatique.

Étape 4 : Résolution (au choix)

Les utilisateurs peuvent :

- révoquer le partage risqué
- modifier les autorisations
- partager dans un espace de travail réservé à l'équipe plutôt que d'utiliser des liens privés

Tolérance du risque variable

Chaque organisation a différents besoins et accepte différents niveaux de risque.

C'est la raison pour laquelle aWeActis vous laisse :

- personnaliser la pondération du risque acceptable
- ajuster la pondération de sensibilité pour chaque étiquette
- définir votre propre palier de durée acceptable pour un partage

Pourquoi est-ce que cela concerne tout le monde ?

Les employés →

Vous n'êtes pas simplement des collaborateurs. Vous êtes les gardiens des données de votre organisation. WeActis vous permet de les protéger efficacement rapidement, directement via Teams sans pour autant nuire à la réalisation de vos tâches quotidiennes.

Les chefs d'entreprise →

Le risque s'accroît tous les jours, invisible et silencieux.

Chaque jour qui passe sans une vue globale est une nouvelle possibilité de faille de sécurité. WeActis transforme les risques passifs en mesures proactives en incitant les employés à prendre des actions sécuritaires, sans augmenter la charge de travail du service informatique ou nuire à la productivité de l'organisation.

Les Comités de direction →

Vous ne pouvez pas vous permettre de risquer la réputation ou la sécurité de votre entreprise à cause d'une erreur de partage.

WeActis offre enfin une visibilité sur l'ensemble des risques liés à la collaboration, suit toutes les actions entreprises, mesure et démontre l'amélioration continue afin de renforcer la posture de sécurité de l'organisation.

En conclusion : le partage des données est le nouveau pare-feu.

Si vous ne contrôlez pas comment cela se déroule , vos précieuses données sont à risque et l'IA ne fait que renforcer ce danger.

Grâce à WeActis, tous vos employés deviennent votre meilleure ligne de défense.

À propos de WeActis

WeActis révolutionne la cybersécurité en transformant les employés en contributeurs actifs, et en faisant de la sécurité une responsabilité collective, et non pas un fardeau informatique.

Intégrée à Microsoft Teams, l'application **WeActis** encourage les employés à prendre des actions sécuritaires simples permettant de diminuer les risques de leur organisation en moins de cinq minutes par semaine.

En favorisant une meilleure hygiène des données dans Microsoft 365, en renforçant la gouvernance et en simplifiant la gestion des risques, **WeActis** permet aux organisations de bâtir une culture de cyberrésilience. Cela se traduit par une meilleure conformité, une réduction de l'exposition des données et des améliorations en sécurité, à la fois mesurables et durables.

info@weactis.com
1 833 666-3282
WeActis.com

WeActis
par Mondata