Optrium
Gouvernance & Cybersécurité des Systèmes d'Information

Op365
Powered by Torsion

NOVEMBRE 2022

Aujourd'hui, il est devenu presque incontournable d'encourager les collaborateurs de nos entreprises à être propriétaires d'équipe Teams dans Microsoft 365 ainsi que dans SharePoint et OneDrive.

Cependant, ce développement exponentiel de l'utilisation de Microsoft 365 soulève une problématique de sécurité : comment rendre les propriétaires d'équipe entièrement responsables de leurs données s'ils ne sont pas en mesure de savoir « qui a accès à quoi » sur l'ensemble des partages Microsoft 365 ?

Comme beaucoup le savent, dans Microsoft 365, en tant que propriétaire d'un partage, vous n'avez qu'une capacité limitée pour élever ou rétrograder des utilisateurs, ainsi que pour ajouter ou supprimer des personnes. Le sujet de la maîtrise de « qui a accès à quoi » n'est pas nouveau, il arrive depuis plusieurs années alors que Microsoft 365 est de plus en plus axé sur l'utilisateur.

UN GLISSEMENT DE LA RESPONSABILITÉ

Progressivement, la responsabilité est passée de l'informatique centralisée aux utilisateurs de Microsoft 365 eux-mêmes. C'est source de difficultés importantes pour les entreprises lorsqu'il s'agit de démontrer leur sécurité et leur conformité sur leurs partages Teams, OneDrive et SharePoint.

La sécurité et la conformité relevaient autrefois uniquement de la responsabilité du service informatique, mais elles sont maintenant beaucoup plus nuancées et complexes.

Dans la majorité des cas, cette transition est passée inaperçue pour la plupart des utilisateurs de Microsoft 365. Selon les cas, les entreprises ont soit ignoré le problème soit mis en place des mesures de protection strictes qui ont complètement supprimé le partage externe de leurs équipes.

LES ENTREPRISES DANS L'IMPASSE

Le partage excessif et le sous-partage des données ont aujourd'hui atteint des proportions épidémiques. Dans le premier cas les entreprises sont en situation de risque majeur pour la sécurité, dans le second, elles ont créé un énorme frein à la collaboration et à la créativité.

Le moment est venu pour les entreprises qui utilisent Microsoft 365 de repenser la sécurité de leur Microsoft 365 et la façon dont elles gouvernent « qui a accès à quoi ».

OP365 POUR UNE GOUVERNANCE OPTIMISÉE EN MODE SaaS

Dans le domaine de la sécurité de l'information / cybersécurité, « qui a accès à quoi » entre dans la catégorie de la gouvernance de l'accès aux données.

Pour ceux qui ne sont pas familiers avec ce terme, la gouvernance de l'accès aux données est le processus par lequel une entreprise régit son accès aux données.

Il s'agit de démontrer la sécurité et la conformité en utilisant des classifications actives pour auditer et identifier qui a accès à quelles informations.

GESTION DE LA CONFORMITÉ DES PARTAGES, NOUS AVONS LA SOLUTION.

OP365 S'IMPOSE COMME UN OUTIL PRIVILÉGIÉ EN MODE SaaS
POUR TOUTES LES ENTREPRISES QUI UTILISENT MICROSOFT 365.
OP365 EST DISPONIBLE SUR Azure

Notre solution de gouvernance est centrée sur l'accès des propriétaires (SharePoint, Teams, OneDrive) à la visibilité et au contrôle de « qui a accès à quoi ».

Nous permettons ainsi aux propriétaires d'équipes d'assumer la responsabilité de la gouvernance de l'accès à leurs données et d'obtenir une meilleure sécurité.

Nous les aidons non seulement en leur fournissant une visibilité, mais aussi en **DÉTECTANT** les problèmes d'accès aux données, en **AUTOMATISANT** toutes les actions correctives à un simple choix de **RÉSOUDRE LE PROBLÈME** ou **ACCEPTER LE PROBLÈME**.

UNE SOLUTION AUX MULTIPLES AVANTAGES

La qualité de l'entreprise et son amélioration continue sont nos priorités.

Très simple d'utilisation avec l'affichage d'informations sur les problèmes en suspens et le statut de partage, les utilisateurs ont accès à la configuration de sécurité des données en clic.

Autre avantage, la solution OP365 génère ses résultats sous forme de rapports qui facilitent la démonstration de la conformité en vue d'un audit. Elle est également certifiée ISO 27001, ce qui constitue un gage de confiance incontestable.

Mais encore, l'implémentation d'OP365 de chaque client dispose de sa propre base d'audit Azure isolée et entièrement chiffrée et d'une connexion autorisée en toute sécurité à son tenant Microsoft 365.

C'est une sécurité automatisée garantie pour la suite Microsoft 365 en place dans l'entreprise, quel que soit le type de licence utilisée.

Pour plus d'informations sur OP365 Powered by Torsion ou pour tester gratuitement (30 jours)
PRENEZ RENDEZ-VOUS

OP365 Powered by Torsion

- **Interfacé avec Azure AD** (comptes, groupes, attributs).
- **Visibilité et contrôle** sur « qui a accès à quoi » dans Microsoft 365.
- Permet aux propriétaires d'équipes Microsoft d'être **véritablement responsables de leurs données**.
- **Conformité** par la visibilité.
- **Administration des accès simplifiée** en textes simples pour les utilisateurs non techniques.
- Il s'agit d'une **solution fiable de gouvernance** de l'accès aux données pour la sécurité et la conformité, vous permettant de communiquer librement et avec un risque réduit.
- **Les atouts d'OP365 :**
  - accès aux données contrôlé,
  - collaboration libre entre les utilisateurs,
  - conformité simplifiée,
  - fonctionnement autonome du système.