

Chiffrement des données dans Microsoft 365

Microsoft 365 applique plusieurs couches de chiffrement pour protéger les données de votre organisation, tant au repos que lors de leur transit.

1. Chiffrement des données au repos

- Les données stockées dans Microsoft 365, comme les fichiers dans SharePoint, OneDrive, les emails dans Exchange Online, sont chiffrées automatiquement au repos.

- Le chiffrement utilise des technologies robustes telles que BitLocker dans les centres de données Microsoft, ainsi que le Distributed Key Manager (DKM) et Customer Key pour Microsoft 365, garantissant que les données sont protégées même lorsqu'elles sont stockées sur disque.

Ce chiffrement est transparent pour l'utilisateur et ne dégrade pas les performances.

Par exemple, dans Windows 365, les disques des Cloud PC sont chiffrés avec AES 256 bits, conforme FIPS 140-2, sans coût supplémentaire.

BitLocker n'est pas utilisé pour Windows 365 Cloud PC, mais reste un standard pour d'autres environnements Microsoft.

- Les objets chiffrés incluent les disques, les snapshots, et les images dans Windows 365.

2. Chiffrement des données en transit

- Microsoft 365 utilise le protocole Transport Layer Security (TLS) pour sécuriser les données en transit entre les utilisateurs et les serveurs Microsoft, ainsi qu'entre les serveurs eux-mêmes.
- Pour les emails, les fichiers partagés, les conversations Teams, TLS garantit l'authentification forte, la confidentialité et l'intégrité des messages, empêchant l'interception ou la falsification.
- Dans Teams, les messages instantanés sont chiffrés avec TLS et MTLS, tandis que le trafic média utilise Secure RTP (SRTP) avec des algorithmes conformes aux normes FIPS.
- Windows 365 utilise TLS 1.2 pour les connexions vers l'infrastructure Azure Virtual Desktop, avec prise en charge de TLS 1.3 pour le transport reverse connect.

3. Résumé des technologies de chiffrement utilisées

Type de contenu	Technologies de chiffrement
Données au repos (fichiers, emails, disques)	BitLocker, Distributed Key Manager (DKM), Customer Key, AES 256 bits (Windows 365)
Données en transit (emails, fichiers, conversations Teams)	TLS 1.2/1.3, MTLS, Secure RTP (SRTP) pour média Teams

Le chiffrement est une composante essentielle de la stratégie globale de protection des informations dans Microsoft 365, garantissant que seules les parties autorisées peuvent accéder aux données, que ce soit au repos ou en transit.

Pour plus de détails techniques, vous pouvez consulter les références sur le chiffrement dans Microsoft 365 et Windows 365, notamment sur les protocoles TLS, les algorithmes utilisés, et les options de gestion des clés.

Sources : [\[Data encry...indows 365\]](#) [\[Encryption...rosoft 365\]](#)

En savoir plus: [Data encryption in Windows 365](#) [Encryption in Microsoft 365](#)