Dropsuite

Fiche de vente

Votre environnement Microsoft 365 est-il réellement sécurisé ?

Protégez plus que votre contenu. Protégez vos accès avec Dropsuite Entra Backup.

Vous faites confiance à votre MSP pour protéger votre business, et c'est justifié. Mais la plupart des gens ignorent qu'un des plus grands risques dans l'environnement cloud actuel n'est pas la perte de fichiers, mais bien la perte d'accès.

Microsoft Entra ID (anciennement Azure AD) contrôle les personnes qui peuvent se connecter, les contenus auxquels elles peuvent accéder et les applications ou appareils fiables. Si ces paramètres d'accès sont modifiés, supprimés ou compromis, même accidentellement, vos activités peuvent être interrompues.

Pourquoi est-ce important

L'erreur est humaine

Les erreurs humaines représentent 60 % des violations de données.[1] Un simple clic erroné de la part d'un membre de votre équipe peut bloquer des utilisateurs, supprimer des réglages clés ou exposer votre environnement à des risques.

Les cyberattaques ciblent principalement les systèmes d'identité

Les identifiants volés (22 %) et les vulnérabilités exploitées (20 %) sont les principales voies d'entrée, selon un rapport récent.[1] Et Entra ID en est souvent la première cible. Une fois à l'intérieur, les pirates peuvent désactiver des politiques, contourner la MFA (authentification multi-facteurs) et prendre le contrôle des applications sans être repérés.

Microsoft ne propose pas de sauvegarde complète

Microsoft ne garantit pas la récupération totale des politiques ou permissions Entra ID supprimées. Sans sauvegarde, la restauration de l'accès peut prendre des heures, voire être impossible.

Ce niveau d'interruption est coûteux : 46 % des petites entreprises ont subi une cyberattaque, et près d'une sur cinq a dû fermer ou faire faillite.[2] Pour les PME, même quelques heures d'indisponibilité peuvent être dévastatrices, car une seule heure peut coûter jusqu'à 100 000 USD en perte de productivité, revenus et frais de récupération.[3]

Ce qui peut mal tourner sans Entra Backup

> *« Des suppressions accidentelles et des erreurs de configuration se produiront dans votre environnement. Pour réduire l'impact de ces événements non souhaités, vous devez préparer leur survenue. »*[4]
>
> **- Microsoft**

Lorsque les systèmes d'identité ne sont pas protégés, les disruptions surviennent rapidement et violemment :

- Une politique d'accès conditionnel supprimée bloque votre personnel à distance.
- Un changement accidentel dans les règles de conformité des appareils empêche la connexion des laptops.
- Un pirate désactive la gestion MFA, et personne ne s'en aperçoit jusqu'à ce qu'il soit trop tard.
- Vous n'avez aucun registre de qui a effectué les changements, compliquant ainsi les enquêtes.

Sans sauvegarde, la résolution de ces incidents peut prendre des heures, perturber les opérations et nuire à votre relation avec les clients.

Protégez le système qui protège tout le reste

Votre MSP sauvegarde déjà vos emails et fichiers. Mais Entra Backup ajoute une couche essentielle pour protéger les règles d'accès et politiques de sécurité qui maintiennent votre activité en marche. Avec Entra Backup, votre MSP peut vous aider à :

- **Récupérez rapidement** après une erreur ou une attaque
- **Évitez les interruptions** dues à la perte d'accès ou à des erreurs de configuration
- **Protégez vos collaborateurs, appareils et applications** contre l'utilisation non autorisée
- **Maintenez la conformité** en conservant un enregistrement complet des modifications d'identité et d'accès

Agissez rapidement avant qu'il ne soit trop tard.

Parlez à votre MSP de Dropsuite Entra Backup, car protéger vos données, c'est aussi protéger l'accès.

1. Verizon, *Data Breach Investigations Report*, 2025.
2. Mastercard, *cybersécurité pour PME*, 2025.
3. ITIC, *rapport sur les interruptions serveurs et applications*, 2022.
4. Microsoft, *meilleures pratiques en matière de récupération*, 2024.