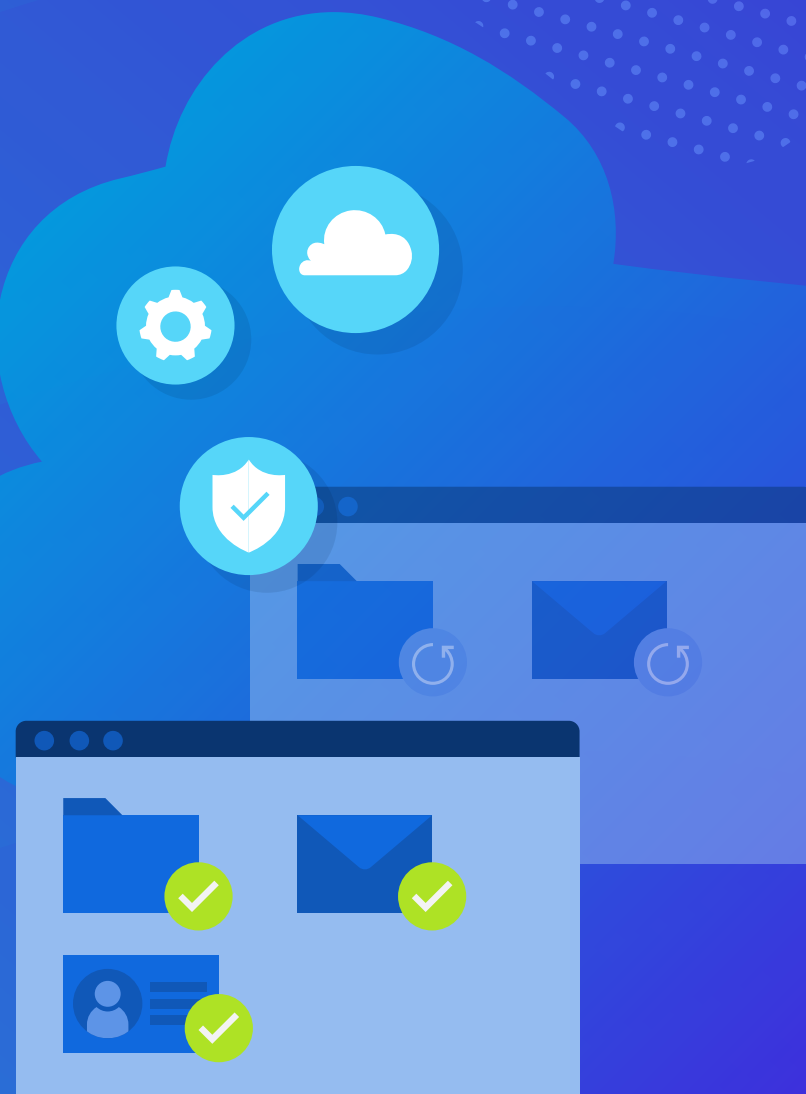


3 principales raisons de sauvegarder vos données SaaS

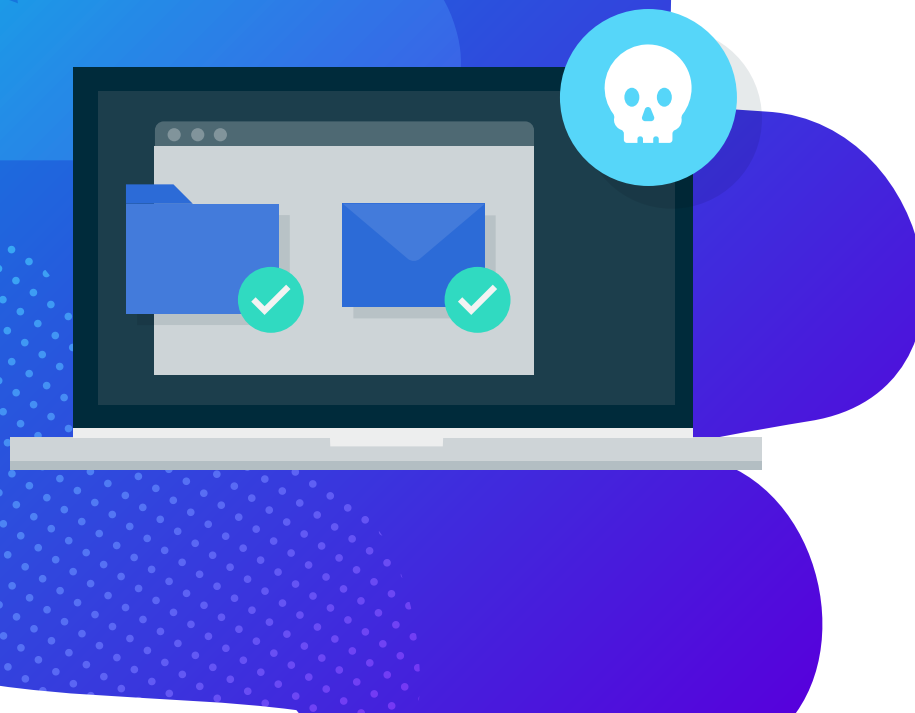
Microsoft 365 et Google Workspace sont adoptés par les entreprises dans des proportions gigantesques. Et c'est cette popularité qui en fait une cible de choix pour la cybercriminalité.

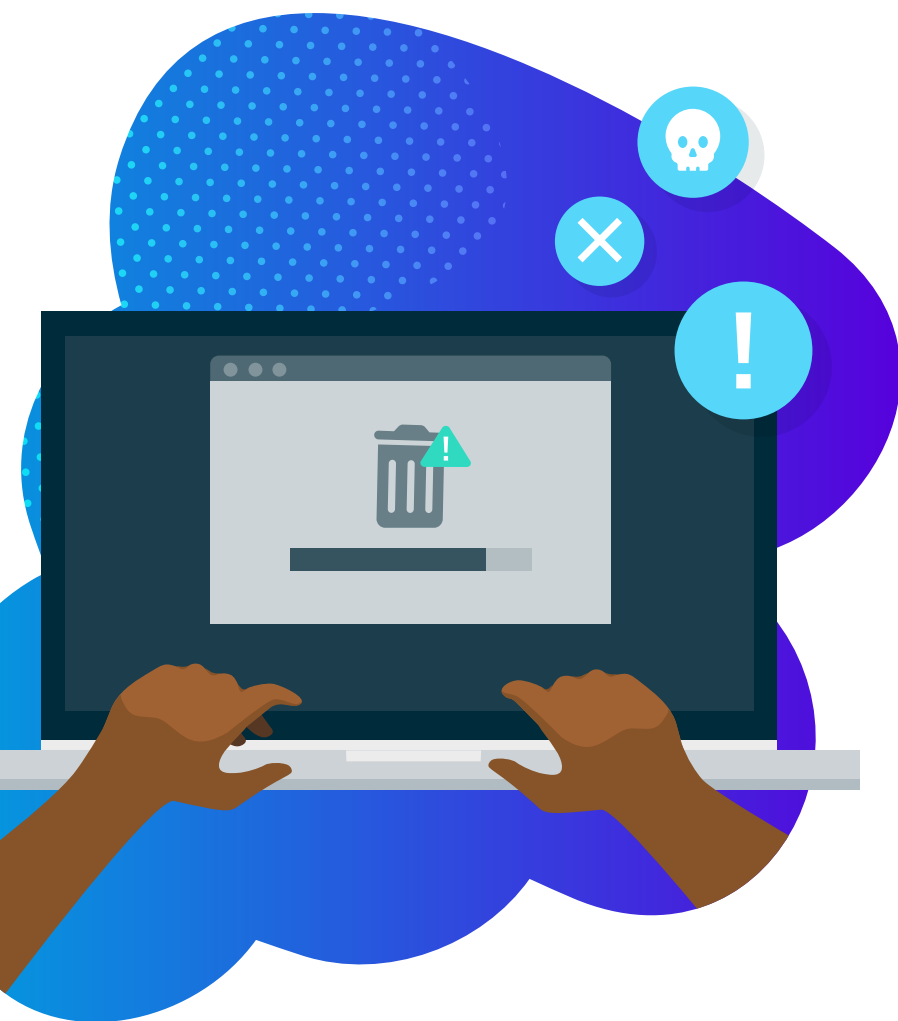


Introduction

Au cours des dernières années, l'augmentation rapide des applications cloud telles que Microsoft 365 et Google Workspace a été une des innovations les plus favorables aux entreprises. Ces applications SaaS (Software-as-a-Service) ont radicalement changé notre façon de faire des affaires en permettant aux entreprises de réaliser des économies d'échelle et de réduire les coûts d'infrastructure informatique. Bien que ces applications offrent de nombreux avantages, elles ne peuvent néanmoins pas protéger totalement les données de votre entreprise contre les menaces extérieures, comme les cybercriminels.

Pourquoi devriez-vous sauvegarder vos données pour vous défendre contre ces cyberprédateurs ? Voici les trois raisons à considérer.





1. Les applications SaaS ne sauvegardent pas vos données

De nombreuses entreprises pensent que le passage à des applications basées sur le cloud signifie que la sauvegarde n'est plus nécessaire. C'est une hypothèse qui peut s'avérer dangereuse. Bien que Microsoft et Google s'assurent *qu'ils* ne perdront pas vos données, ils n'offrent aucune garantie quant à la restauration des données si *vous* les perdez. En d'autres termes, vos données cloud sont aussi vulnérables à la suppression accidentelle ou malveillante, aux ransomwares et à d'autres types de perte de données que les applications sur site.

Comment votre entreprise ferait-elle face si vous perdiez définitivement vos données ou si, dans un cas plus favorable, vous deviez attendre 6 heures ou plus pour récupérer un fichier ? Si vous faites confiance à des applications pour vous fournir le niveau et les mesures de protection dont vous avez besoin, vous faites courir à votre entreprise le risque de perdre des données et un temps précieux.

Saviez-vous ?
La cause #1 de la perte de données est l'erreur humaine.

Source : [Aberdeen Group](#)

2. Les cyber attaques ne ralentissent pas

En janvier 2020, ce sont 480000 comptes Microsoft qui ont été la cible d'attaques de pulvérisation. Il s'agit d'une attaque réalisée en utilisant un mot de passe commun (comme « Winter2020! ») contre des listes contenant des milliers de comptes, dans l'espoir que certains d'entre eux auront utilisé ce mot de passe commun. Si ce chiffre vous paraît important, gardez à l'esprit le fait que [Microsoft](#) arrête quotidiennement 300 millions de tentatives de connexions frauduleuses. 300 millions par jour, pas par année ou par mois !

Quelles seraient les conséquences si le courrier électronique de votre entreprise n'était pas accessible pendant 30 minutes ? Ou pendant une journée entière ? Ou encore une semaine ? La productivité diminue avec chaque tic-tac de l'horloge. C'est pourquoi la mise en place d'un logiciel de sécurité supplémentaire, d'un solide processus de continuité des activités et de reprise après sinistre (BCDR) fera toute la différence.

Ce sont au moins 3,4 milliards de faux e-mails qui sont envoyés chaque jour dans le monde entier.

Source : [Vailmail](#)





3. La violation des données nuit considérablement aux petites entreprises

En matière de cybercriminalité, les petites et moyennes entreprises (PME) sont doublement susceptibles d'être des victimes. En effet, en plus du coût potentiel d'être la cible de pirates et autres cybercriminels, ils risquent également de perdre la confiance des consommateurs.

Les témoignages présentés dans le rapport [Small Business Reputation and the Cyber Risk](#) le démontre clairement. Puisque 89 % des PME indiquent que les conséquences potentielles d'une cyber-violation peuvent être « énormes et durables ». En particulier :

- **31 % des PME** font état d'une publicité négative pour leur marque
- **30 % des PME** indiquent qu'elles ont perdu des clients
- **29 % des PME** font état d'une diminution de leur capacité à remporter de nouveaux contrats

Et si cela ne suffit pas pour vous convaincre que vous devez investir dans la sauvegarde dans le cloud, vous devez alors tenir compte des amendes potentielles attachées au règlement général sur la protection des données (RGPD). Les risques et amendes associés au non-respect du RGPD l'emportent largement sur les coûts initiaux de mise en œuvre d'une solution de sauvegarde SaaS.

Présentation de la protection SaaS Datto SaaS

Une sauvegarde simple, automatisée et sécurisée

Si vous exploitez des applications SaaS, assurez-vous de traiter ces données comme vous le faites pour vos données sur site : en les sauvegardant avec une solution fiable. Il s'agit d'une pratique standard qui doit être mise en œuvre pour assurer la sécurité des données de votre entreprise où qu'elles soient stockées.

Renoncer à une sauvegarde peut permettre de réaliser des économies à court terme, mais le coût d'une violation de données peut aller d'un inconvé- nient mineur à une atteinte à la réputation à long terme, à la perte de données client, aux amendes et, en fin de compte, à la fermeture de l'entreprise.

Grâce à la protection SaaS de Datto et à notre expertise, vous pouvez éviter les temps d'arrêt et sécuriser davantage vos données d'entreprise. **Contactez-nous dès aujourd'hui pour en savoir plus sur la manière dont la sauvegarde dans le cloud peut éviter un désastre au niveau des données.**

