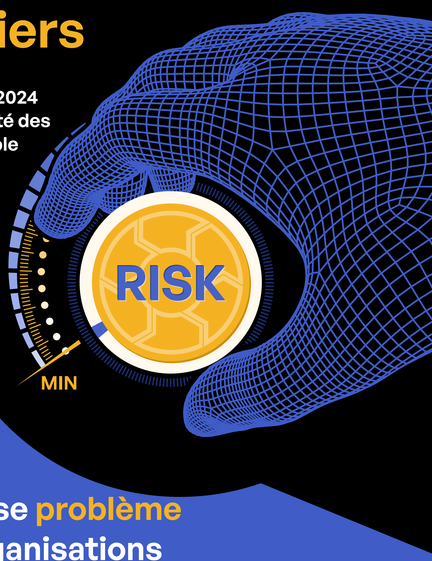
Analyse de la gestion des risques tiers

Conclusions du rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible



PRÉAMBULE

Le risque tiers lié au contenu sensible pose problème à de nombreuses organisations

66%

des organisations échangent du contenu sensible avec plus de 1000 interlocuteurs

77%

La région APAC est la plus exposée aux risques tiers, 77 % des entreprises échangeant des contenus sensibles avec plus de 1 000 entités

51%

Les professions libérales échangent des contenus sensibles avec plus de tiers que tout autre secteur d'activité (51 % avec plus de 2 500 personnes)

47%

L'enseignement supérieur est le deuxième secteur le plus exposé aux risques, avec 47 % qui partagent et envoient des contenus sensibles à 2500 personnes

La région EMEA est la plus confrontée à ce problème, avec **45%** des répondants se déclarant incapables de contrôler et de suivre **plus de 50%** des contenus sensibles une fois qu'ils ont quitté leur périmètre

69% des établissements d'enseignement supérieur sont incapables de suivre et de contrôler **plus de 50%** des contenus sensibles une fois qu'ils ont quitté leur périmètre

Les collectivités locales sont le deuxième secteur le plus exposé aux risques tiers, avec **54%** admettant perdre le suivi et le contrôle des données sensibles lorsqu'elles quittent leur organisation

39%

des organisations déclarent ne pas être en mesure de suivre et de contrôler l'accès de plus de 50 % des contenus sensibles

Kiteworks simplifie la gestion des risques tiers

Le réseau de contenu privé (PCN) de Kiteworks consolide et sécurise tous les canaux de communication tiers : messagerie électronique, SFTP, partage de fichiers, transfert de fichiers MFT et formulaires web

Surveillance en temps réel pour analyser le contenu sensible entrant et sortant de l'entreprise

Intègre des contrôles d'accès granulaires et évolutifs basés sur des attributs, avec un chiffrement en transit et au repos

S'intègre à l'infrastructure de sécurité existante comme DLP, ATP, SIEM ou encore CDR

Utilise un hébergement à locataire unique avec possibilité de déploiement FedRAMP pour une conformité réglementaire et un contrôle total de l'environnement du serveur

Pour connaître toutes les conclusions du rapport 2024 sur la confidentialité et la conformité des communications sensibles, vous pouvez le télécharger ici