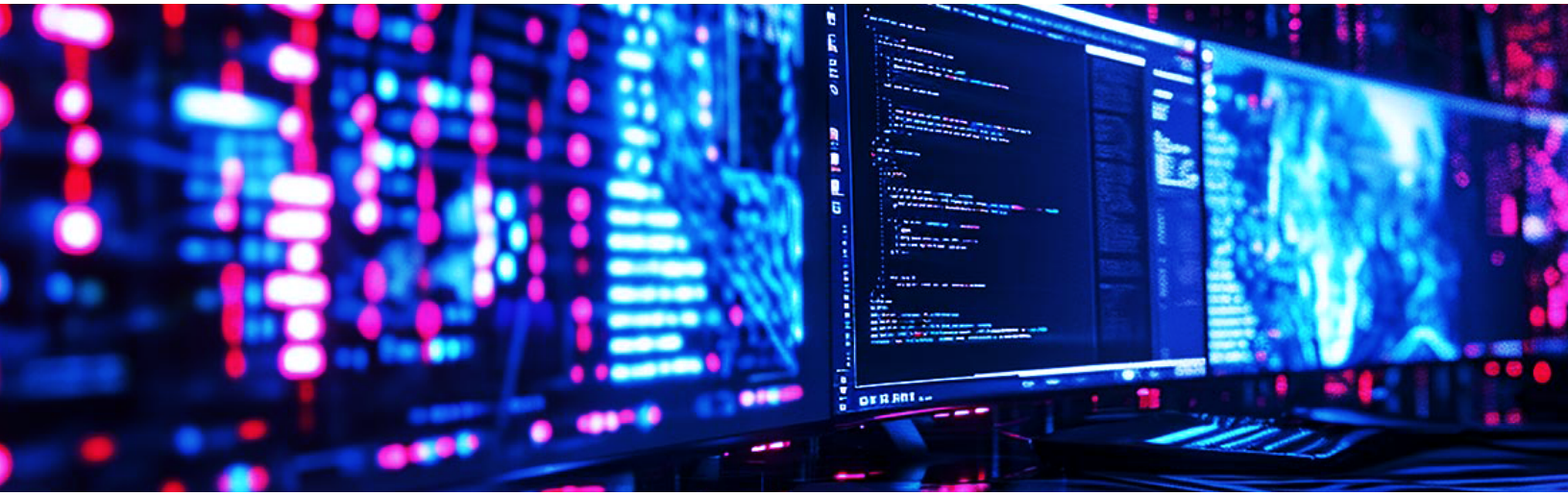
Kiteworks

Rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible

Protection des communications de contenu sensible

RÉSUMÉ



Le rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible révèle les principales vulnérabilités et problèmes rencontrés par les entreprises dans le traitement et la maîtrise de leurs informations confidentielles. Avec 572 réponses collectées auprès de responsables IT, sécurité, gestion des risques et conformité, cette enquête exclusive souligne l'importance de bien protéger les données sensibles : informations personnelles identifiables (PI), informations médicales protégées (PHI) et propriété intellectuelle (PI). Les résultats montrent l'impact considérable des violations de données pour les entreprises, comme les arrêts d'activité, la perte de chiffre d'affaires ou encore l'impact négatif sur l'image de marque.

Méthodologie de l'étude

Le rapport repose sur une enquête menée par Centiment entre février et mars 2024, avec 33 questions sur la sécurité des données, la confidentialité et la conformité règlementaire. Les répondants sont originaires de huit pays d'Amérique du Nord, d'Europe, du Moyen-Orient, d'Afrique (EMEA) et de la région Asie-Pacifique. Ils sont issus de secteurs divers tels que la sécurité et la défense, l'industrie, la santé, la finance, le secteur public et l'éducation. La diversité des personnes interrogées garantit une vision globale des difficultés et des priorités en matière de protection des contenus sensibles.

Conclusions du rapport d'enquête

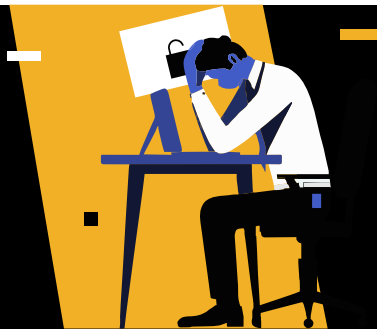
1. Les risques associés aux informations sensibles

Les pirates informatiques s'attaquent de plus en plus aux contenus sensibles. D'après le rapport, près d'un tiers des personnes interrogées ont subi au moins sept attaques externes l'année dernière. Voici quelques faits marquants :

32%
des personnes interrogées ont subi 7 violations de données minimum

68%
l'enseignement supérieur, la sécurité et la défense, le pétrole et le gaz sont les secteurs les plus touchés en nombre de violations de données subies (plus de 68 % ont vécu plusieurs attaques)

28%
des laboratoires pharmaceutiques ont signalé plus de 4 violations de données.



2. Risques informatiques de l'IA sur les communications de contenu sensible

Les technologies d'IA, en particulier l'IA générative (GenAI) et les grands modèles de langage (LLM), posent de gros problèmes de sécurité. Près de la moitié des responsables sécurité s'inquiètent que des tiers accèdent à des données sensibles via des outils d'IA, et redoutent des violations de données et des erreurs de décision de la part des systèmes d'IA. Autres résultats intéressants :

48%
des personnes interrogées trouvent qu'il est difficile d'appliquer les principes du zéro trust sur site et dans le cloud

45%
des organisations n'ont pas encore atteint un niveau de sécurité zéro trust pour le contenu

Seuls
35%
des répondants du Royaume-Uni

et

39%
des répondants du Moyen-Orient et de la région Asie-Pacifique

ont instauré des politiques zéro trust.

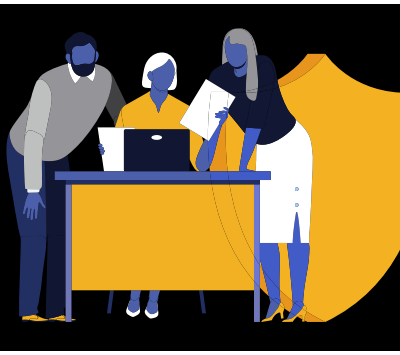
3. Problèmes de non-conformité pour les communications de contenu sensible

Pas simple de suivre les évolutions des réglementations en matière de protection des données, en particulier du RGPD et du CCPA qui demandent des adaptations constantes. Le rapport révèle que 93 % des organisations ont dû revoir leurs stratégies de cybersécurité pour répondre aux changements de réglementation.[1] En quelques chiffres :

93%
des organisations ont dû revoir leur stratégie de cybersécurité pour répondre aux changements de réglementation [1]

Seuls
11%
des répondants ont déclaré que leur système de management des risques ne nécessitait aucune amélioration

43%
des organisations ont admis ne pas être capable de suivre, contrôler et tracer tous les échanges de contenu externe.



4. Importance du facteur humain dans les violations de données

L'erreur humaine est une source de risque importante, responsable de 68 % des violations. Pour atténuer ce risque, les organisations ont plusieurs leviers : former régulièrement leur personnel, mettre en place une authentification multifactorielle (MFA), des contrôles d'accès stricts, un chiffrement des données et un plan de réponse aux incidents efficace. Parmi les résultats les plus marquants :

Les utilisateurs finaux sont responsables de 68% des erreurs entraînant des violations de données

La santé et la finance sont des secteurs particulièrement touchés par les violations de données liées aux utilisateurs

5. Confidentialité et conformité des communications de contenu sensible

Le rapport souligne le coût élevé des violations de données, avec des frais de justice dépassant souvent les 2 millions de dollars annuels, voire les 7 millions dans certains cas. Même si c'est efficace, peu d'entreprises arrivent aujourd'hui à classer leurs données. En quelques chiffres :

60%

des répondants ont indiqué avoir dépensé plus de 2 millions de dollars en frais juridiques liés aux violations de données l'année dernière

49%

des organisations affirment qu'au moins 75 % de leurs données non structurées sont étiquetées ou classifiées

41%

des organisations déclarent que le RGPD et les lois sur la protection des données des États américains sont leurs deux priorités en termes de conformité règlementaire

6. Conformité et Risk management pour les communications de contenu sensible

Les rapports de conformité restent un vrai problème pour les organisations qui ne sont pas en mesure de suivre et de tracer tous les échanges de contenu externe. Le rapport suggère d'investir dans des outils de sécurité avancés pour alléger la charge des rapports de conformité et gagner en sécurité. Voici quelques éléments de réflexion :

53%

des répondants privilégient les normes ISO

42%

se concentrent sur la norme NIST 800-171

62%

des organisations consacrent plus de 1500 heures par an à préparer des rapports d'audit

7. Cybersécurité et Risk Management pour les communications de contenu sensible

Parvenir à un niveau de sécurité zéro trust pour le contenu est indispensable, mais ambitieux. Le rapport rappelle l'importance de se doter d'outils de sécurité avancés (chiffrement, détection des menaces et actions de sensibilisation). Sans oublier de pouvoir suivre et contrôler les accès aux contenus sensibles de manière efficace.

45%

des entreprises **n'ont pas encore atteint un niveau de sécurité zéro trust** pour leur contenu

Seuls **16%**

des entreprises sont en mesure de **suivre et contrôler l'accès** au contenu de manière systématique

56%

des personnes interrogées ont indiqué avoir besoin **d'améliorer partiellement** la sécurité des communications sensibles

8. Process opérationnels et communications de contenu sensible

La sécurité des données sensibles passe par la maîtrise des risques tiers, la consolidation des outils de communication et la résolution des problèmes liés à la réconciliation des journaux d'audit. Le rapport recommande de limiter le nombre d'outils, d'instaurer des systèmes de suivi efficaces et de veiller au respect des réglementations sur la protection de la vie privée. Voici les principales conclusions :

2/3

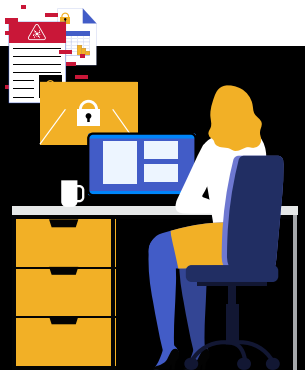
des personnes interrogées **échangent des contenus sensibles** avec plus de 1000 interlocuteurs différents

7+

Les organisations qui utilisent plus de sept outils de communication **subissent plus de violations de données**

48%

des organisations **doivent réconcilier plus de 11 journaux d'audit** et 14 % plus de 20



Améliorer la sécurité des communications de contenu sensible

Voici les points à prioriser, d'après les 8 points précédents :

1. Consolider les outils de communication :

réduire le nombre d'outils diminue directement les risques d'attaques et améliore l'efficacité

2. Appliquer les principes de sécurité du zéro trust au niveau du contenu,

avec des contrôles d'accès stricts et une surveillance continue

3. Développer des réseaux de contenu privés :

le fait de cloisonner les communications sensibles améliore la sécurité

4. Investir dans des mesures de sécurité efficaces :

chiffrement, MFA et détection des menaces

5. Faciliter la préparation des rapports d'audit,

avec des process automatisés et un suivi rigoureux

6. Classer les données par ordre de priorité

pour protéger les données les plus sensibles

Conclusion

Le rapport 2024 Kiteworks fait ressortir le besoin urgent de définir des stratégies solides de sécurité et de conformité règlementaire. En mettant en œuvre les solutions proposées, les organisations auront les moyens de protéger leur contenu sensible et d'être conformes aux règlementations en vigueur. Et surtout, de maitriser les risques dans l'environnement numérique complexe qui est le nôtre aujourd'hui.

Pour en savoir plus, nous vous invitons à consulter la page web du rapport 2024 , où vous trouverez des synthèses par région et par secteur d'activité, des infographies et un épisode de Kitecast sur le sujet.

[1] "Despite increased budgets, organizations struggle with compliance," Help Net Security, 24 mai 2024.