Kiteworks

Analyse 2024 des communications de contenu sensible pour la région APAC : les tendances en matière de sécurité et de conformité

CHIFFRES CLÉS

Outils de communication utilisés	8%	7+
	14%	6
	25%	5
	22%	4
	17%	3
	6%	2
	2%	1
Échange de contenu sensible avec des tiers	7%	Plus de 5 000
	31%	2 500 à 4 999
	39%	1 000 à 2 499
	14%	500 à 999
	10%	Moins de 499
Types de données les plus préoccupantes (top 3)	61%	Échanges juridiques
	48%	Documents financiers
	39%	PII
	37%	CUI et FCI
	36%	PI
	34%	PHI
	31%	LLMs de GenAI
	15%	Fusions & Acquisitions
Top 2 des priorités sur la confidentialité et la conformité règlementaire	43%	HIPAA
	42%	Exigences SEC
	32%	CMMC
	31%	Lois des États américains
	25%	RGPD
	18%	Lois propres à chaque pays
	11%	PCI DSS
Top 2 des validations de sécurité les plus importantes	48%	ISO 27001, 27017, 27018
	47%	NIST 800-171/CMMC 2.0
	45%	IRAP (Australie)
	38%	FedRAMP Moderate
	20%	SOC 2 Type II
	4%	Directive NIS 2
Nombre de piratages des communications de contenu sensible	3%	Plus de 10
	40%	7 à 9
	29%	4 à 6
	17%	2 à 3
	7%	1
	5%	Ne sait pas

Le rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible fournit une analyse détaillée des problématiques et des pratiques dans différentes régions, et notamment pour la région APAC (Asie-Pacifique). Ce brief reprend les principales conclusions du rapport pour la région APAC ; outils utilisés pour échanger des données sensibles, problèmes de cybersécurité, risques dans les échanges avec des tiers, menaces spécifiques et conséquences sur la conformité règlementaire.

Gestion de tous les outils de communication de contenu sensible

52 % des entreprises de la région APAC utilisent au moins cinq outils de communication différents pour envoyer et partager des informations sensibles, un chiffre proche des 53% au niveau mondial. En ce qui concerne le suivi et le contrôle des contenus sensibles, les entreprises de l'APAC se situent au même niveau que la moyenne mondiale : 61 % déclarent suivre et contrôler plus des trois quarts de ces contenus. Bien que dans la moyenne mondiale, l'APAC est nettement moins bien placée que la région Amériques (70 %).

Pas étonnant que de plus en plus d'entreprises cherchent à harmoniser et à protéger leurs échanges de données sensibles. Mais les motivations citées par les répondants de l'APAC diffèrent de celles des régions Amériques et EMEA ; 79 % ont cité le fait d'éviter l'impact négatif sur l'image de marque comme première ou deuxième raison. Tandis que les répondants de la région EMEA étaient 61 % à citer le fait de prévenir les fuites de données de propriété intellectuelle et de secrets d'entreprise en première raison, et les répondants de la région Amériques 57 % à citer le fait d'éviter les interruptions d'activité et les pertes de chiffre d'affaires. Enfin, le souci de limiter les litiges longs et coûteux (comme les recours collectifs dus à des fuites de données confidentielles) est cité en deuxième motivation pour 61 % des réponses pour l'APAC.

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques tiers est une préoccupation majeure pour les entreprises de la région APAC, qui échangent plus de données en moyenne que celles de la région EMEA et Amériques. En effet, 77 % d'entre elles partagent, envoient ou transfèrent des données avec plus de 1000 interlocuteurs différents (contre 63 % pour Amériques et EMEA). Cette situation est inquiétante, car 39 % des organisations de l'APAC ont indiqué pouvoir suivre et contrôler moins de la moitié des données sensibles qui quittent une application.

Évaluer le niveau de conformité pour les contenus sensibles

83 % des entreprises de la région APAC ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations plus ou moins importantes. Ce chiffre est légèrement inférieur à la moyenne mondiale de 88 %. Comme pour la région Amériques, 32 % ont indiqué avoir besoin d'une amélioration significative, et c'est plus que la région EMEA (25 %).

Les organisations de l'APAC ont cité les normes ISO 27001, 27017 et 27018 en tête de leurs priorités (53 % d'entre elles les ont classées en première ou deuxième position). En deuxième, on retrouve le NIST 800-171 et la CMMC 2.0, suivis de l'IRAP (33 %). Cette dernière réponse s'explique par le fait que de nombreux répondants de l'APAC sont originaires d'Australie.

Évaluer les risques liés à la sécurité des contenus sensibles

82 % des entreprises de la région APAC déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle. Cela est logique puisque 72 % des organisations de l'APAC ont subi au moins quatre violations de leurs contenus sensibles (et au moins sept dans 43 % des cas). Un chiffre nettement plus élevé que dans les régions EMEA et Amériques (respectivement 48 % et 53 %). Plus inquiétant encore, 5 % des entreprises de la zone APAC ont admis ne pas savoir.

Les outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) ne sont utilisés que partiellement dans 43 % des entreprises de l'APAC. 57 % les utilisent tout le temps, ce qui est nettement moins que les 67 % des entreprises des Amériques.

Évaluer le coût de la sécurité et de la conformité

L'enquête révèle que l'APAC est très exposée aux violations de données, 42 % des entreprises ayant indiqué avoir subi plus de sept violations de données l'année passée. Ce chiffre est nettement plus élevé que la moyenne mondiale de 32 %. Par ailleurs, 28 % des entreprises ont déclaré avoir subi entre quatre et six violations de données. Et tout aussi alarmant, 6 % ont déclaré ne pas savoir.

Du point de vue financier, 22 % des entreprises de l'APAC ont dépensé plus de 5 millions de dollars l'année dernière en frais de litiges, un peu moins que la moyenne mondiale (25 %). Par ailleurs, 26 % des répondants de l'APAC ont déclaré avoir dépensé entre 3 et 5 millions de dollars en frais de contentieux.

Connaissance et classification des types de données

24 % des organisations de l'APAC ont indiqué étiqueter et classer moins de 50 % des données non structurées. Ce chiffre est légèrement supérieur à la moyenne mondiale, où 22 % étiquettent et classent moins d'un quart des données et 30 % moins de 50 % des données.

Ces chiffres sont encore plus parlants au vu des réponses données en APAC : 20 % des personnes interrogées ont indiqué étiqueter et classer 25 % ou moins des données non structurées (et 45 % ont indiqué entre 40 et 60 %). Par rapport aux moyennes mondiales, les répondants de l'APAC sont à la traîne : 33 % d'entre eux étiquettent et classent 60 % ou plus de leurs données sensibles contre 40 % au niveau mondial

Urgence absolue à protéger les contenus sensibles dans la région APAC

Le rapport Kiteworks 2024 met en évidence les difficultés particulières auxquelles sont confrontées les entreprises de la région APAC dans la gestion de leurs communications sensibles. Avec 52 % des organisations qui utilisent au moins cinq outils de communication différents, il est évident que suivre et contrôler les contenus sensibles est complexe. Curieusement, la principale motivation pour unifier et sécuriser les communications de contenu sensible dans la région APAC est d'éviter l'impact négatif sur l'image de marque, suivie par la réduction des risques de litiges coûteux.

La grande majorité des organisations de l'APAC reconnaissent avoir besoin d'améliorer la gestion de la conformité et de la sécurité des communications de contenu sensible. La fréquence des violations de données et le manque de recours à des technologies de sécurité avancées soulignent l'urgence de remédier à ces lacunes. En travaillant sur la classification et l'étiquetage des données, et des mesures de sécurité robustes, les entreprises de l'APAC amélioreront la protection des données sensibles et la conformité règlementaire.

Accéder au rapport complet