Kiteworks

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

CHIFFRES CLÉS

Outils de communication utilisés	24%	7+
	14%	6
	21%	5
	18%	4
	12%	3
	7%	2
	1%	1
Échange de contenu sensible avec des tiers	13%	Plus de 5 000
	25%	2 500 à 4 999
	28%	1 000 à 2 499
	16%	500 à 999
	18%	Moins de 499
Types de données les plus préoccupantes (Top 3)	62%	Documents financiers
	46%	Échanges juridiques
	50%	LLMs de GenAI
	40%	PI
	34%	PHI
	29%	PII
	20%	CUI et FCI
	21%	Fusions & Acquisitions
Top 2 des priorités sur la confidentialité et la conformité règlementaire	63%	Lois des États américains
	38%	HIPAA
	29%	Exigences SEC
	29%	RGPD
	17%	CMMC
	14%	Lois propres à chaque pays
	10%	PCI DSS
Top 2 des validations de sécurité les plus importantes	46%	ISO 27001, 27017, 27018
	41%	SOC 2 Type II
	39%	NIST 800-171/CMMC 2.0
	34%	IRAP (Australie)
	32%	FedRAMP Moderate
	8%	Directive NIS 2
Nombre de piratages des communications de contenu sensible	11%	Plus de 10
	22%	7 à 9
	22%	4 à 6
	23%	2 à 3
	12%	1
	10%	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 en Amérique du Nord. Ce brief reprend les principales conclusions du rapport pour la région North America ; 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

Près de 6 organisations sur 10 (59 %) en Amérique du Nord utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, plus que les 53 % des entreprises au niveau mondial. 70 % d'entre elles affirment pouvoir suivre et contrôler plus des trois quarts de ces contenus (contre 61 % à l'échelle mondiale).

Pas étonnant que de plus en plus d'organisations cherchent à harmoniser et à protéger leurs communications sensibles. Le top 2 des priorités citées par les entreprises nord-américaines était d'éviter les pannes opérationnelles et les pertes de revenus (57 %) et de prévenir les fuites de propriété intellectuelle et de secrets d'entreprise (51 %). Cela diffère des autres régions où la motivation la plus citée est de limiter les litiges longs et coûteux.

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques tiers est une préoccupation majeure pour les entreprises d'Amérique du Nord. 63 % d'entre elles échangent des contenus sensibles avec plus de 1000 interlocuteurs, soit un peu moins qu'au niveau mondial (66 %). Cette situation est inquiétante dans la mesure où seuls 31 % des entreprises nord-américaines ont indiqué pouvoir suivre et contrôler environ la moitié des données sensibles qui quittent une application.

Évaluer le niveau de conformité pour les contenus sensibles

87 % des entreprises de la région North America ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations plus ou moins importantes. Ce chiffre correspond à la moyenne mondiale de 88 %.

Les organisations d'Amérique du Nord ont cité les lois sur la protection des données de chaque État américain en tête de leurs priorités (63 % les ont classés en première ou deuxième position). L'HIPAA arrive loin derrière, avec 38 % des organisations qui la citent comme étant leur priorité. Pour ce qui est des certifications de sécurité, les répondants de la région North America ont cité les normes ISO 27001, 27 017 et 27 018 (46 %) comme étant les plus importantes, suivies de SOC 2 Type II (41 %). Ces chiffres contrastent avec les moyennes mondiales de 53 % pour ISO 27001, 27017 et 27018 (15 % de plus qu'en Amérique du Nord) et de 26 % pour SOC 2 Type II (45 % de moins qu'en Amérique du Nord).

Évaluer les risques liés à la sécurité des contenus sensibles

88 % des entreprises de la région North America déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle. 55 % ont indiqué avoir subi au moins quatre violations de leur contenu sensible (33 % déclarent en avoir subi plus de sept). Plus inquiétant encore, 10 % 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 29 % des entreprises d'Amérique du Nord, dont 2 % indiquant n'en utiliser aucun. 69 % déclarent y avoir recours de façon systématique. Si les entreprises nord-américaines sont plus nombreuses à utiliser des outils sécurisés que celles des régions EMEA et APAC, le risque n'en est pas moindre.

Évaluer le coût de la sécurité et de la conformité

33 % des répondants de la région North America ont indiqué avoir subi plus de sept violations de données l'année passée. Ce chiffre est légèrement supérieur à la moyenne mondiale, où 32 % des répondants ont déclaré avoir subi plus de sept violations de données. Par ailleurs, 22 % des répondants ont déclaré avoir subi entre quatre et six violations de données. Tout aussi préoccupant, 10 % ont déclaré ne pas savoir.

Du point de vue financier, 27 % des entreprises interrogées en Amérique du Nord ont déclaré avoir subi des frais de litige de plus de 5 millions de dollars. Ce chiffre est supérieur à la moyenne mondiale de 25 %. En outre, 49 % des répondants nord-américains ont déclaré avoir dépensé plus de 3 millions de dollars, contre seulement 45 % au niveau mondial.

Connaissance et classification des types de données

20 % des organisations nord-américaines ont indiqué étiqueter et classer moins de 25 % des données non structurées ; 23 % ont admis étiqueter et classer moins de la moitié des données. Ces pourcentages correspondent aux moyennes mondiales : 20 % étiquettent et classent moins d'un quart des données. L'Amérique du Nord est cependant en retard par rapport à la moyenne mondiale, où 29 % des répondants indiquent étiqueter et classer moins de la moitié des données.

Ces chiffres sont encore plus parlants si l'on en croit les réponses données en Amérique du Nord sur le pourcentage de données non structurées à classifier : 19 % ont indiqué devoir étiqueter et classifier 40 % ou moins des données non structurées (et 28 % ont indiqué entre 40 et 60 %). Ces chiffres révèlent un écart, surtout si on les compare aux moyennes mondiales, où 22 % des répondants étiquettent et classifient moins d'un quart des données et 35 % entre 40 et 60 %.

Urgence absolue à protéger les contenus sensibles en Amérique du Nord

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible. Près de 60 % des organisations de la région North America utilisent des outils de communication multiples, bien plus que la moyenne mondiale. Néanmoins, 70 % d'entre elles affirment être capables de suivre et de contrôler une grande partie de leur contenu sensible, soit un niveau de contrôle plus élevé que le reste du monde. Elles cherchent en priorité à éviter les arrêts d'activité et les fuites de données confidentielles, en privilégiant l'unification et la protection de leurs outils de communication.

Il est impératif d'adopter une approche globale et proactive pour protéger les contenus sensibles des entreprises. 87 % des organisations nord-américaines reconnaissent la nécessité d'améliorer leur stratégie de gestion des risques, et 78 % ont subi de multiples violations. On ne saurait donc trop insister sur l'importance d'utiliser des technologies de sécurité avancées. Bien que l'Amérique du Nord applique davantage le chiffrement, l'authentification multifactorielle et le suivi de la gouvernance que les autres régions du monde, les risques restent importants. Il n'y a plus qu'à renforcer les mesures de sécurité et la classification des données pour maintenir l'intégrité des données et assurer la conformité règlementaire.

Accéder au rapport complet