Kiteworks

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

CHIFFRES CLÉS

Outils de communications utilisés	**13 %**	7+
	12 %	6
	25 %	5
	21 %	4
	18 %	3
	8 %	2
	3 %	1
Échange de contenu sensible avec des tiers	**13 %**	Plus de 5 000
	27 %	2 500 à 4 999
	23 %	1 000 à 2 499
	14 %	500 à 999
	23 %	Moins de 499
Types de données les plus préoccupantes (Top 3)	**53 %**	Documents financiers
	50 %	PI
	46 %	PII
	38 %	LLMs de GenAI
	38 %	Échanges juridiques
	32 %	PHI
	28 %	CUI et FCI
	15 %	Fusions & Acquisitions
Top 2 des priorités sur la confidentialité et la conformité règlementaire	**57 %**	RGPD
	29 %	Lois des États américains
	28 %	CMMC
	27 %	Lois propres à chaque pays
	23 %	HIPAA
	22 %	Exigences SEC
	14 %	PCI DSS
Top 2 des validations de sécurité les plus importantes	**59 %**	ISO 27001, 27017, 27018
	42 %	NIST 800-171/CMMC 2.0
	27 %	SOC 2 Type II
	27 %	IRAP (Australie)
	20 %	Directive NIS 2
Nombre de piratages des communications de contenu sensible	**10 %**	Plus de 10
	17 %	7 à 9
	21 %	4 à 6
	26 %	2 à 3
	17 %	1
	9 %	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 EMEA (Europe, Moyen-Orient et Afrique). Ce brief reprend les principales conclusions du rapport pour la région EMEA ; 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

La moitié des entreprises de la région EMEA utilisent au moins cinq outils de communication différents pour envoyer et partager des informations sensibles, un peu moins que les 53 % des entreprises au niveau mondial. À l'échelle du monde, 39 % des organisations interrogées ne sont pas capables de suivre et de contrôler plus de la moitié de leurs communications sensibles une fois envoyées, partagées ou transférées. Et le problème est plus grave encore en EMEA, avec 45 % des répondants concernés.

Pour autant, de plus en plus d'entreprises cherchent à harmoniser et la protéger leurs échanges de données sensibles. En tête des priorités citées par les entreprises en EMEA : prévenir les fuites de données de propriété intellectuelle et de secrets d'entreprise (62 % en première ou deuxième intention). Vient ensuite le souci de limiter des litiges longs et coûteux (51 %), comme les recours collectifs dus à des fuites de données confidentielles). Ces chiffres illustrent l'importance de consolider les outils de communication de contenu sensible pour réduire les risques et gagner en efficacité opérationnelle.

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques tiers est une préoccupation majeure pour les entreprises de la région EMEA. 63 % d'entre elles échangent des contenus sensibles avec plus de 1000 interlocuteurs différents, soit un peu moins qu'au niveau mondial (66 %). Cette situation est inquiétante dans la mesure où seuls 45 % des entreprises en EMEA 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

86 % des entreprises de la région EMEA 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 %.

Sans surprise, les organisations de la région EMEA ont cité le RGPD en tête de leurs priorités, devant d'autres règlementations sur la protection des données (57 % en première ou deuxième position). En deuxième, on retrouve les lois sur la confidentialité des données de certains États américains (29 %) et la CMMC 2.0 (28 %). Quant aux entreprises de l'EMEA implantées aux États-Unis, elles sont soumises aux lois fédérales et de chaque État américain. Pour ce qui est des certifications de sécurité, les répondants de la région EMEA ont cité les normes ISO 27001, 27017 et 27018 à un taux plus élevé (59 %) que ceux de la région APAC (48 %) et Amériques (46 %). Étonnamment, la directive NIS 2 n'est citée que dans 20 % des cas.

Évaluer les risques liés à la sécurité des contenus sensibles

88 % des entreprises de la région EMEA déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle. 48 % des entreprises de la région EMEA ont indiqué avoir subi au moins quatre violations de leur contenu sensible (27 % déclarent en avoir subi plus de sept). Plus inquiétant encore, 9 % des entreprises de la zone EMEA 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'EMEA, dont 4 % indiquant n'en utiliser aucun. 53 % déclarent y avoir recours de façon systématique. Par rapport aux moyennes mondiales, la région EMEA est à la traîne dans ce domaine (59 % au niveau mondial).

Évaluer le coût de la sécurité et de la conformité

27 % des répondants de la région EMEA ont indiqué avoir subi plus de sept violations de données pour des communications sensibles l'année passée. 21 % ont déclaré en avoir subi entre quatre et six. Ce chiffre est légèrement inférieur à la moyenne mondiale de 32 %, qui compte plus de sept violations de données. Tout aussi alarmant, 9 % des répondants ont déclaré ne pas être certains du nombre de violations de données subies.

Du point de vue financier, 25 % des entreprises de la région EMEA ont déclaré avoir subi des frais de litige de plus de 5 millions de dollars, ce qui correspond à la moyenne mondiale. 16 % ont déclaré avoir dépensé entre 3 et 5 millions de dollars, et 41 % ont déclaré plus de 3 millions de dollars en 2023. Bien que ces chiffres soient moins élevés qu'en Amérique, ils sont considérables.

Connaissance et classification des types de données

21 % des organisations de la région EMEA ont indiqué étiqueter et classer moins de 25 % des données non structurées ; 33 % ont admis étiqueter et classer moins de la moitié des données. Ces pourcentages correspondent aux moyennes mondiales : 21 % étiquettent et classent moins d'un quart des données, tandis que 29 % déclarent qu'ils en classent la moitié ou moins.

Ces chiffres sont encore plus parlants, si l'on en croit les réponses données en EMEA sur le pourcentage de données non structurées à classifier : 24 % des personnes interrogées ont indiqué devoir étiqueter et classifier 40 % ou moins des données non structurées (et 37 % ont indiqué entre 40 et 60 %). Ces chiffres sont révélateurs d'une lacune : des données non structurées qui ne sont pas étiquetées et classées, mais qui devraient l'être.

Urgence absolue à protéger les contenus sensibles dans la région EMEA

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible. Rien de tel que des outils de communication avancés, la maîtrise des risques tiers, le respect de normes strictes et la compréhension des types de données traitées pour mener une stratégie de cybersécurité efficace. En outre, les organisations de l'EMEA ont intérêt à se servir de la gestion des droits numériques (DRM) dernière génération pour atteindre un niveau de gouvernance avancée de leurs contenus sensibles.

Alors que les menaces évoluent, il est impératif d'adopter une approche proactive et globale pour protéger les contenus sensibles et maintenir l'intégrité des données de l'organisation. Les organisations de la région EMEA, légèrement mieux positionnées sur certains points par rapport aux tendances mondiales, ont la capacité à relever ces défis avec succès.

Accéder au rapport complet