Kiteworks

2024

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

La multiplication des outils de communication, les échanges de données avec des tiers et le manque de gouvernance augmentent les risques

Table des matières

Forew

Avant-propos

Nous sommes heureux de vous exposer les résultats de l'enquête Kiteworks 2024 sur la confidentialité et la conformité des communications sensibles. Ce rapport détaillé nous livre de précieuses informations sur l'état actuel de la protection des contenus sensibles et les défis auxquels se heurtent les organisations en la matière.

Aujourd'hui, la protection des données sensibles est une nécessité absolue. Alors que les organisations dépendent de plus en plus de la communication et de la collaboration digitales, leurs réseaux s'agrandissent et les risques de violations de données se multiplient. Notre étude révèle les tendances et les difficultés rencontrées par les entreprises pour assurer la sécurité et la conformité de leurs contenus sensibles.

Les attaques commises l'année dernière ont accentué les risques liés aux tiers et à la supply chain informatique (par exemple, les violations de données sur les transferts de fichiers MFT de MOVEit et de GoAnywhere). Dans son rapport 2024 sur les violations de données (Data Breach Investigations Report - DBIR), Verizon a constaté une progression stupéfiante de 68 % des violations de données liées à des tiers, soit 15 % de l'ensemble des incidents. En parallèle, les pirates ciblent principalement les données personnelles, obligeant les autorités à alourdir les règlementations en matière de confidentialité des données. Assurer la sécurité et la conformité des données est donc de plus en plus difficile.

En effet, l'enquête révèle que la profusion des outils de communication de contenus sensibles et la multiplication du nombre d'interlocuteurs sont des facteurs de risque majeurs. Un autre point marquant est l'incapacité à contrôler les outils de communication pour s'assurer qu'ils intègrent des mécanismes de sécurité avancés. Les chiffres sont parlants : le pourcentage de violation de données et les coûts de contentieux sont d'autant plus élevés que les organisations utilisent plus d'outils et échangent des informations critiques avec plus de tiers.

En dépit de notre parti pris, nous sommes convaincus que le réseau de contenu privé de Kiteworks est une réponse efficace. Il protège les échanges de mails et de fichiers tout en conservant les preuves que les entreprises respectent bien leurs obligations règlementaires. En espérant que cette lecture vous apporte des informations et des conseils utiles pour agir au mieux. Et comme toujours, nous accueillerons vos commentaires et suggestions avec le plus grand intérêt.

Amicalement

Patrick Spencer

Patrick Spencer, Ph.D.
VP of Corporate Marketing and Research
Kiteworks

Résumé

Le rapport sur la confidentialité et la conformité des communications de contenu sensible donne aux acteurs de l'IT, de la cybersécurité, de la gestion des risques et de la conformité, un aperçu des pratiques de leurs homologues. L'objectif est de vous éclairer sur la protection des contenus sensibles que vous envoyez et partagez via différents canaux de communication. La messagerie électronique, le partage de fichiers, le transfert de fichiers MFT, le protocole de transfert de fichiers sécurisé (SFTP) et les formulaires web sont des exemples d'outils sécurisés et conformes.

Cette année, l'enquête a été menée par Centiment entre février et mars 2024, et comportait 33 questions sur différents sujets liés à la sécurité, à la confidentialité et à la conformité des données. Certaines questions sont des «retours en arrière», qui reprennent des enquêtes menées au cours de l'une ou des deux années précédentes, tandis que d'autres ont été ajoutées pour recueillir des informations sur les nouvelles tendances. Au total, 572 répondants, dont des responsables de service IT, cybersécurité, gestion des risques et conformité d'Amérique du Nord, d'Europe, du Moyen-Orient et d'Afrique (EMEA) et de la région Asie-Pacifique.

Voici un aperçu des sujets abordés dans le but de dégager des tendances et des éléments de réflexion :

- L'impact du nombre d'outils de communication sur la gestion des risques
- L'impact réel des violations de données sur les coûts de litiges
- Quels types de données présentent le plus grand risque et pourquoi ?
- En quoi la règlementation et les normes de sécurité améliorent-elles la protection des données ?
- La réduction des risques liée à l'impact des technologies modernes sur les outils de communication
- Les raisons pour lesquelles les outils de communication traditionnels ne sont plus adaptés et génèrent des problèmes de confidentialité et de conformité.

57%

Ne parviennent pas à suivre, contrôler et tracer les envois et partages de contenus en externe

57% des répondants ont indiqué ne pas être en mesure de suivre, contrôler et tracer les envois et partages de contenus avec l'externe. Cela représente une *lacune majeure en matière de risque de gouvernance*

Deux tiers

des organisations échangent des contenus sensibles avec plus de 1000 destinataires

66% des personnes interrogées ont indiqué échanger des contenus sensibles avec *plus de 1000 interlocuteurs*. La capacité à tracer et à contrôler l'accès à ces données est d'autant plus importante une fois qu'elles quittent le périmètre de l'organisation.

x3.55

Le % d'entreprises ayant subi plus de 10 violations de données et utilisent plus de 7 outils de communication

Plus une organisation utilise d'outils de communication, plus le risque est élevé. Les répondants utilisant *plus de 7* outils de communication ont subi *au moins 10 violations de données.* C'est 3,55 fois plus que l'ensemble des répondants (ceux qui ont subi entre une et plus de 10 violations de données).

$5M

de dollars par an pour les litiges liés aux violations de données, pour la moitié des organisations

La moitié des entreprises interrogées qui échangent des contenus sensibles avec *au moins 5 000 tiers* ont versé plus de *5 millions de dollars en frais de contentieux* l'année dernière.

89%

admettent devoir améliorer la conformité de leurs communications de contenus

Seuls 11 % des répondants ont déclaré ne pas avoir besoin d'améliorer leur système de management de la conformité des communications sensibles.

62%

Consacrent plus de 1500 heures de travail par an à rédiger des rapports d'audit

62% des entreprises consacrent plus de *1500 heures par an* à la compilation des journaux des outils de communication pour les rapports d'audit.

Introduction

Voici le troisième rapport annuel de Kiteworks sur les communications de contenu sensible ! À cette occasion, nous avons mené une enquête détaillée sur les habitudes des organisations en termes de protection des contenus sensibles et de respect des normes règlementaires.

Le terme « contenu sensible » fait référence aux types de contenu ciblés par des acteurs malveillants et qui représentent un risque significatif pour une organisation en cas de fuite. Autrement dit, ce qu'on retrouve en une des journaux sous le nom de « violation de données ». Le contenu sensible peut être des informations sur les clients et les salariés : informations personnelles identifiables (PII), informations médicales protégées (PHI) et données de l'industrie des cartes de paiement (PCI). Ou encore la propriété intellectuelle (PI) d'une organisation, les communications et documents juridiques, les données financières, de fusions et acquisitions ou tout autre type d'informations confidentielles.

Risques liés à la sécurité

Du point de vue de la sécurité, le problème des contenus sensibles est qu'ils ne restent pas au même endroit. Au quotidien, il sont partagés entre les salariés, entre les salariés et les fournisseurs, les sous-traitants, les cabinets de conseil, les comptables, les auditeurs, etc. Pour fonctionner, les organisations ont besoin que ces informations circulent de manière fluide, en interne, mais aussi avec des milliers d'autres interlocuteurs. Et comme nous allons le voir, cette circulation emprunte de multiples canaux de communication.

De ce fait, les entreprises ont besoin de protéger leur contenu, non seulement là où il est stocké, mais aussi lorsqu'il transite par les différents canaux de communication vers des tiers. Et malheureusement, les cybercriminels ont découvert des vulnérabilités dans la supply chain logicielle qui leur donnent accès à des centaines, voire des milliers d'organisations et à des millions de fichiers de données sensibles. Le Data Breach Investigations Report (DBIR) de Verizon 2024 corrobore cette tendance, faisant état de 180 % d'exploitations de vulnérabilités logicielles en plus d'une année sur l'autre. On apprend également que les violations de données sur la supply chain ont bondi de 68 % d'une année sur l'autre, ce qui correspond à 15 % de toutes les violations de données. Les attaques par ransomware menées par Clop l'année dernière contre les solutions de transfert MFT de MOVEit et Forta's GoAnywhere en sont la preuve.

Risques cyber liés à l'IA

Outre la protection des canaux de communication de contenu, les entreprises et les agences gouvernementales sont confrontées à un autre problème qui prend de l'ampleur ces dix-huit derniers mois. Alors que l'intelligence artificielle (IA) explose à la fois en termes de progrès techniques et de popularité, les organisations doivent préserver leurs contenus sensibles des grands modèles de langage (LLM) désormais couramment utilisés par leurs salariés et partenaires.

Selon Gartner, ces modèles de langage GenAI comportent trois risques majeurs : l'accès à des données sensibles par des tiers (pour la moitié des responsables de la sécurité IT), les violations de données et d'applications GenAI (pour 40 % des répondants) et la prise de décisions erronées (pour plus d'un tiers des répondants).[4] Le fait que les salariés entrent des données sensibles dans les outils de GenAI représente un vrai danger. Près d'un tiers des salariés interrogés en fin d'année dernière ont admis avoir saisi des données sensibles dans des outils GenAI publics. Sans surprise, 39 % des personnes interrogées dans le cadre de la même étude ont cité la fuite potentielle de données sensibles comme l'un des principaux risques liés à l'utilisation d'outils GenAI publics par leur organisation.[5]

Dans le même temps, la chute des barrières à l'entrée a permis de démocratiser l'utilisation de l'IA, et à des cybercriminels moins expérimentés de lancer des attaques de plus en plus complexes.[6] Cela renforce le sentiment de « course à l'armement » engagée par les États-nations et les cybercriminels contre les organisations légitimes, avec des conséquences qui pourraient être existentielles.

Risques de non-conformité

À moins que votre entreprise n'exerce ses activités dans une seule et unique juridiction, la question de la conformité règlementaire est complexe et coûteuse, car les exigences varient d'un endroit à l'autre. La multiplication des règlementations et l'évolution des textes existants ont incité 93 % des entreprises à repenser leur stratégie de cybersécurité l'an passé.[7] Le Règlement général sur la protection des données (RGPD) de l'Union européenne, mis en œuvre en 2018, a harmonisé la législation de ses 27 États membres dans le cadre d'une norme unique de confidentialité des données.

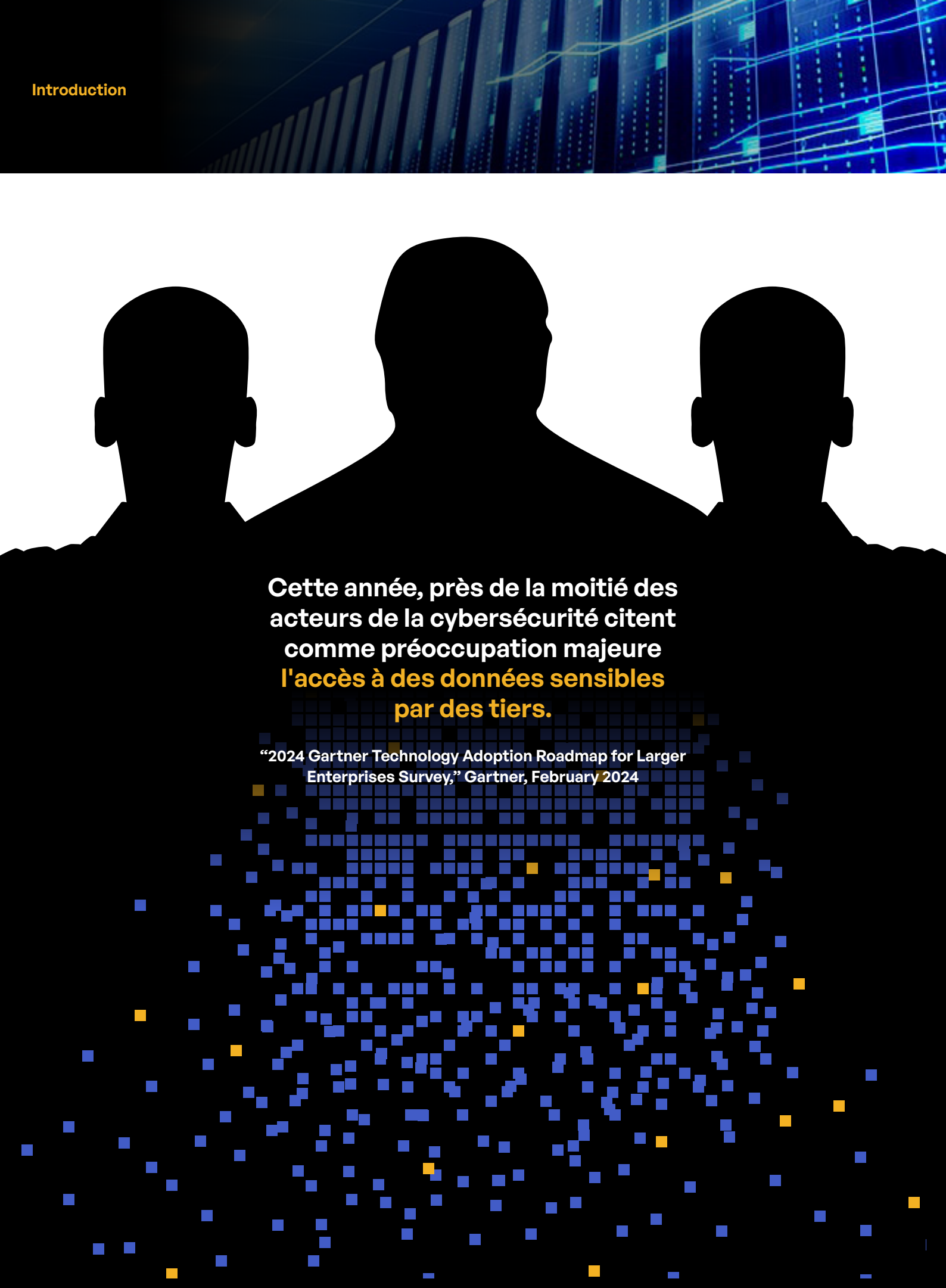
Pour le reste du monde, les choses ne sont pas aussi simples. Les données des Nations unies montrent que 137 des 194 pays du monde ont désormais des lois sur la confidentialité des données, mais toutes différentes.[8] Aux États-Unis, la législation fédérale la plus stricte est la loi HIPAA (Health Insurance Portability and Accountability Act), qui couvre les données de santé, mais pas les données personnelles. Le Congrès n'étant pas parvenu à adopter une norme nationale, certains États ont pris les devants en adoptant en 2018 la loi californienne sur la protection de la vie privée des consommateurs (California Consumer Privacy Act, CCPA). Depuis lors, 17 autres États ont adopté des lois en matière de confidentialité des données, et 10 autres sont en cours d'élaboration.[9] . S'il est louable de voir que les citoyens et résidents américains sont mieux protégés, cela ne fait qu'exacerber la situation pour ceux qui sont contraints de respecter la législation en vigueur.

Les différents organismes qui régissent la protection des données personnelles continuent de faire pression sur les organisations pour qu'elles se conforment à la règlementation. Les amendes et sanctions pour non-respect du RGPD en 2023 ont atteint 2,269 milliards de dollars (2,1 milliards d'euros), dépassant le montant combiné de 2019, 2020 et 2021. Le montant moyen par sanction a explosé : 4,75 millions de dollars (4,4 millions d'euros) par violation l'an dernier contre 540 000 dollars (500 000 euros) par violation en 2019. Les sanctions liées à l'HIPAA sont tout aussi impressionnantes avec 4,176 milliards de dollars l'année dernière.[11]

Outre les règlementations en matière de protection de la vie privée, les normes de cybersécurité préoccupent aussi les organismes publics et les autorités de surveillance. Parmi les nouvelles règlementations en la matière, citons les règles de la SEC sur la gestion des risques de cybersécurité et à la divulgation des incidents pour les marchés publics, le Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), le Cyber Resilience Act (CRA) et le Digital Operational Resilience Act (DORA) en Europe. Ou encore le Cybersecurity Framework (CSF) 2.0 du National Institute of Standards & Technology (NIST).

Risques liés à l'humain

Le facteur humain reste une source de risque important à l'origine de nombreuses violations de données sensibles. Le DBIR a constaté que les utilisateurs finaux étaient à l'origine de 68 % des erreurs conduisant à des violations.[12] Plusieurs raisons à cela : erreurs de destinataire, manque de sécurisation des données, attaques par ingénierie sociale avec par exemple la compromission des e-mails professionnels et le phishing. Le manque de visibilité et de gouvernance pour les communications de contenu sensible ajoute encore des lacunes à l'infrastructure et aux contrôles de sécurité.



Cette année, près de la moitié des acteurs de la cybersécurité citent comme préoccupation majeure l'accès à des données sensibles par des tiers.

"2024 Gartner Technology Adoption Roadmap for Larger Enterprises Survey," Gartner, February 2024

Méthodologie de l'étude

Le rapport 2024 de Kiteworks sur les communications de contenu sensible se base sur une enquête menée auprès de 572 professionnels de l'informatique, de la cybersécurité, de la gestion des risques et de la conformité au sein d'entreprises de plus de 1000 salariés. Notre analyse rend compte des commentaires des répondants pour l'ensemble de la cohorte, et les compare aux résultats des enquêtes 2023 et 2022, ainsi qu'à une analyse croisée en fonction de divers facteurs démographiques.

Diversité des répondants

Les répondants sont originaires de huit pays, avec 34 % pour la région Amérique du Nord, 18 % pour la région Asie-Pacifique et 48 % pour la région Europe-Moyen-Orient-Afrique (Figures 1 et 2). Ils sont issus d'organisations de tailles très diverses, 54 % d'entre eux comptant entre 1000 et 10 000 collaborateurs et 46 % plus de 10 000 (Figure 3).

L'échantillon provient de différents secteurs d'activité, dont les plus représentés sont la sécurité et la défense (15 %), l'industrie (12 %), la santé (12 %) et les services financiers (12 %) (Figure 4). Plus de deux participants sur dix (22 %) travaillent dans l'administration publique ou l'enseignement, tandis qu'un quart d'entre eux travaillent dans les secteurs financier, juridique et professionnel. Enfin, 10 % travaillent dans le secteur de l'énergie.

En termes de fonctions, les participants à l'enquête occupent des postes à différents niveaux hiérarchiques ; 31 % occupent des postes de direction et 69 % des postes de cadre intermédiaire (Figure 5). Ils se répartissent entre les fonctions liées au risque et à la conformité (26 %), à l'informatique (42 %) et à la sécurité (31 %).

75%

de la population mondiale verra ses données personnelles soumises à de nouvelles lois sur la protection de la vie privée d'ici fin 2024.

"Gartner Identifies Top Five Trends in Privacy Through 2024," Communiqué de presse, 31 Mai 2022.

Analyse de la confidentialité et de la conformité des communications de contenu sensible

Après la présentation du panel de répondants, nous allons passer aux résultats de l'enquête. Cette année encore, de nouveaux éléments sont ressortis concernant l'évaluation et la gestion des risques de cyberattaques et de violations de données, les types de données et leur classification, la cybersécurité, la conformité et les processus opérationnels.

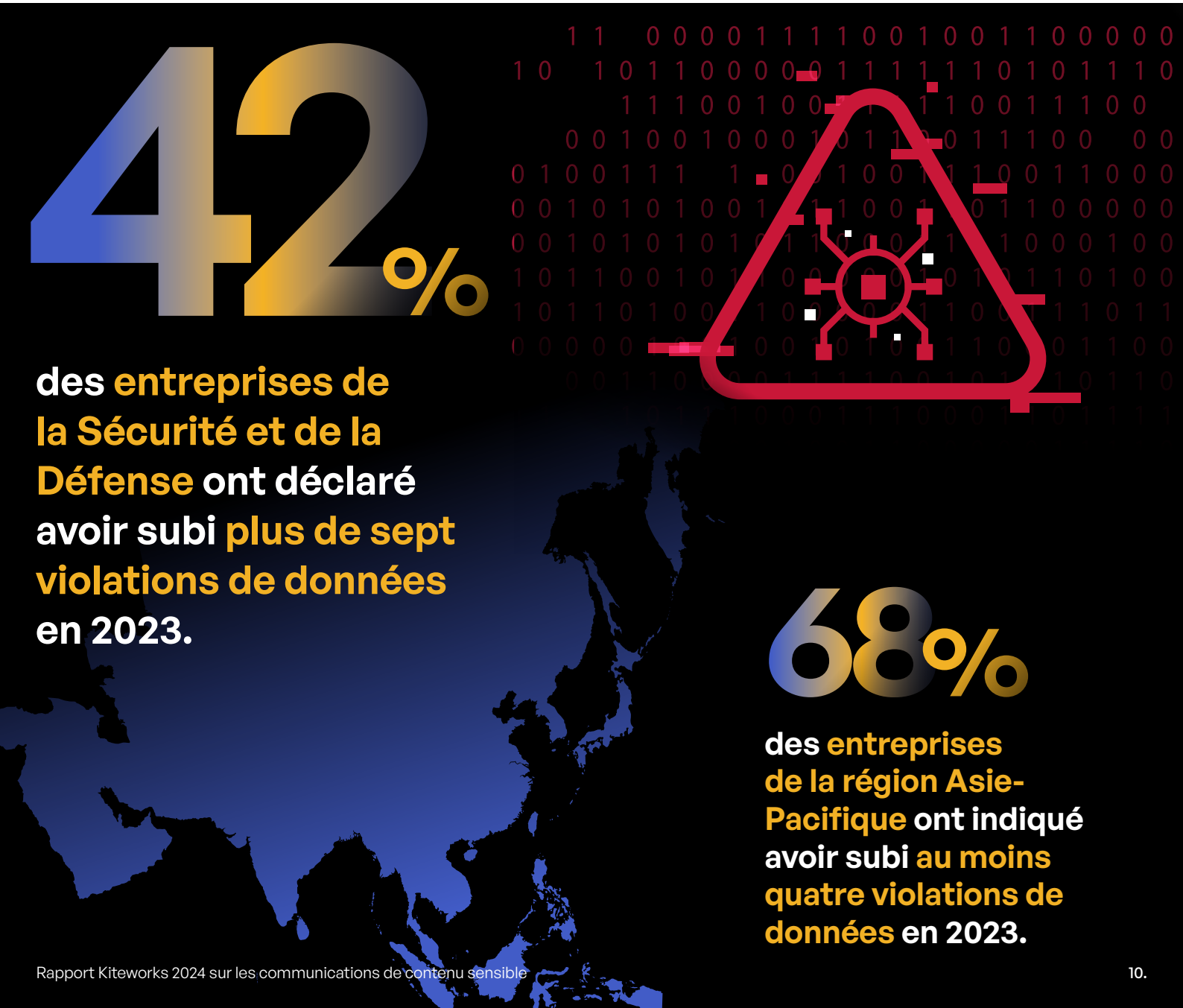
CYBERATTAQUES ET VIOLATIONS DE DONNÉES

Les communications de contenu sensible sont trop souvent la cible de violations

Les attaques malveillantes restent un problème grave pour les contenus sensibles, quel que soit le secteur d'activité. L'Identify Theft Resource Center a fait état de 3 205 **compromissions de données signalées publiquement, qui ont affecté plus de 353 millions de personnes l'année** dernière, soit 78 % de plus qu'en 2022. La bonne nouvelle, c'est que les choses vont légèrement mieux pour nos répondants en 2024. La mauvaise, c'est que les organisations subissent encore très souvent des violations graves. Près d'un tiers des personnes interrogées (32 %) ont déclaré avoir subi au moins sept piratages externes de contenus sensibles l'an dernier, contre 36 % l'année précédente (Figure 6). Et même si davantage d'entreprises (36 %) ont signalé avoir subi moins de trois violations, ces chiffres sont encore bien trop élevés pour être satisfaisants.

Le nombre de piratages subis varie considérablement d'un secteur à l'autre (Figure 7). L'enseignement supérieur, la sécurité et la défense, ainsi que les secteurs pétrolier et gazier ont connu encore plus de violations, avec 68 % ou plus déclarant quatre violations ou plus, contre 55 % pour l'ensemble du panel. L'administration fédérale a également révélé des données préoccupantes : 17 % des répondants ont indiqué avoir subi au moins 10 violations et 10 % ont déclaré en avoir subi entre sept et neuf. Plus alarmant encore, 42 % des acteurs de la sécurité et de la défense, qui échangent certains des contenus les plus critiques de tous les secteurs d'activité, ont admis avoir subi sept violations de données ou plus. En revanche, l'industrie pharmaceutique s'en sort beaucoup mieux, puisque seulement 28 % des personnes interrogées ont déclaré avoir subi quatre violations ou plus.

Dans la région Asie-Pacifique, les organisations ont également connu un nombre disproportionné de violations, 68 % des personnes interrogées ayant signalé quatre incidents ou plus (Figure 8). Les organisations de la région APAC ayant un plus grand nombre de tiers avec lesquels elles échangent des contenus sensibles (voir ci-dessous), des recherches supplémentaires pourraient mettre en évidence le lien entre les deux. Enfin, les entreprises comptant entre 20 000 et 30 000 salariés s'en sortent beaucoup moins bien que les autres, puisque 75 % d'entre elles ou plus signalent quatre violations ou plus, alors que les entreprises de plus petite et de plus grande taille maintiennent ce chiffre bien en deçà de 60 % (Figure 9).



42%

des entreprises de la Sécurité et de la Défense ont déclaré avoir subi plus de sept violations de données en 2023.

68%

des entreprises de la région Asie-Pacifique ont indiqué avoir subi au moins quatre violations de données en 2023.

32%

des organisations ont subi *plus de sept* attaques sur leur contenu sensible en 2023.

Coût des litiges liés aux violations de données

Les violations de données coûtent cher : sanctions financières pour non-respect de la règlementation, temps d'arrêt opérationnels, baisse de la productivité et perte de chiffre d'affaires. L'an dernier, le rapport annuel d'IBM et du Ponemon Institute a évalué le coût d'une violation de données à *4,45 millions de dollars américains*, un chiffre qui augmente d'année en année.[14] Et encore, ce chiffre est possiblement sous-évalué, car les coûts juridiques associés aux violations de données sont souvent ignorés ou sous-estimés. C'est pourquoi nous avons ajouté cette année une question sur les frais de contentieux, qui nous a fourni quelques informations complémentaires.

À cet égard, *six répondants sur dix* ont déclaré avoir dépensé *plus de 2 millions de dollars* chaque année pour faire face aux frais juridiques liés aux incidents de pertes de données internes et externes. 45 % ont dépensé plus de 3 millions de dollars et un quart *plus de 5 millions de dollars* (Figure 10). Plus l'organisation est grande, plus le coût des litiges est élevé : 24 % des organisations de plus de 30 000 salariés ont déclaré des frais juridiques de plus de 7 millions de dollars. Et plus de la moitié des organisations de plus de 15 000 salariés ont dépensé plus de 3 millions de dollars (Figure 11). *L'enseignement supérieur* est le secteur le plus touché, 49 % des organisations déclarant avoir déboursé plus de 5 millions de dollars l'année dernière (Figure 12). Du point de vue géographique, *l'Amérique du Nord* est en tête de liste, 27 % des entreprises ayant déclaré avoir payé plus de 5 millions de dollars. Autre point troublant, 14 % des répondants de la région EMEA ne connaissent pas le coût des litiges liés à leurs violations de données (Figure 13).

24%

des organisations de plus de 30 000 employés ont déclaré que les coûts des litiges liés aux violations de données dépassaient les 7 millions de dollars annuels.

45%

des organisations ont dépensé plus de 3 millions de dollars par an en frais de litiges, et un quart d'entre elles plus de 5 millions.

TYPES DE DONNÉES ET CLASSIFICATION

Difficulté à suivre et à contrôler tous les échanges de données

La croissance déjà exponentielle des données s'est encore accélérée au cours des 18 derniers mois avec l'adoption des grands modèles de langage (LLM) de GenAI. **Lorsque le contenu quitte une application comme la messagerie électronique, le partage de fichiers, le SFTP, le transfert de fichiers MFT ou les formulaires web, il est important que les organisations puissent suivre et contrôler les accès à ce contenu.**

Les entreprises doivent identifier leurs types de données, savoir où elles se trouvent et où elles sont envoyées et partagées. Pour déterminer quelles données non structurées doivent être contrôlées, elles doivent se doter d'un système de classification. Lorsqu'on les interroge sur la proportion de leurs données non structurées qui sont étiquetées ou classifiées, *moins de la moitié des répondants* (48 %) affirment que c'est le cas pour *75 % ou plus* de leurs données (Figure 14). Au niveau des secteurs d'activité, 66 % ont atteint ce niveau dans la santé, 56 % dans la finance et 55 % dans le secteur juridique (Figure 15).

Néanmoins, les organisations ont indiqué que toutes les données non structurées n'avaient pas besoin d'être étiquetées et classifiées. *40%* des organisations ont déclaré que *60% ou plus* des données non structurées devaient être étiquetées et classifiées. Et plus une organisation est grande, plus les données non structurées ont besoin d'étiquetage et de classification. Pour celles qui comptent plus de 30 000 salariés : 15 % ont indiqué que toutes les données devaient être étiquetées et classifiées, et 20 % plus de 80 % des données (Figure 16). Au niveau des régions, les répondants d'Amérique du Nord sont plus nombreux à déclarer que les données ont besoin d'être étiquetées et classifiées ; 10 % pour toutes leurs données non structurées et 16 % pour 80 % ou plus de leurs données (Figure 17). Les répondants du gouvernement fédéral sont les plus nombreux à déclarer que toutes les données doivent être étiquetées et classifiées (24 %), et 17 % d'entre eux déclarent que 80 % ou plus des données doivent l'être (Figure 18).

40%

des organisations déclarent que plus de 60 % de leurs données non structurées doivent être étiquetées et classées

Seuls 49% des organisations affirment que plus de 75% de leurs données non structurées ont besoin d'être étiquetées et classées.

Évaluation des risques selon les types de données

Comme indiqué ci-dessus, les contenus sensibles existent sous différentes formes, selon les organisations. Chacun d'entre eux ne présente pas le même niveau de risque. Selon l'étude d'IBM sur le coût annuel d'une violation de données, les informations personnelles identifiables *(PII)* sont les données les plus coûteuses et les plus fréquemment compromises. C'est aussi le type de données le plus touché en 2023, avec 52 % de toutes les violations de données, à l'instar des deux dernières années.[15] Les conclusions d'IBM concordent avec celles du DBIR, où 50 % de toutes les violations de données étaient liées à des PII.

Si l'on compare ces résultats à ceux de nos répondants, on constate certaines divergences. D'après les données de recherche d'IBM et de Verizon, on pourrait supposer que les répondants citent les PII comme leur première source d'inquiétude. Or, ils ont plutôt cité les *documents financiers (55%)*, la *propriété intellectuelle (44%)*, et les *communications juridiques (44%)* (Figure 19).

41% des répondants des agences fédérales déclarent que plus de 80 % de leurs données non structurées ont besoin d'être étiquetées et classées.

Les données d'IBM et de Verizon se confirment toutefois par notre analyse croisée des *PHI.* Les répondants qui les considèrent comme l'un des trois types de données les plus préoccupants ont connu un taux plus élevé de violations que les autres. Par exemple, *43%* de ceux qui ont classé les PHI parmi leurs trois principaux types de données ont déclaré avoir subi *plus de sept* violations (contrairement aux 32 % de l'ensemble des répondants qui ont signalé sept violations ou plus) (Figure 20). Le deuxième type de données pour lequel le taux de violations est le plus élevé est la *propriété intellectuelle* (35% ont déclaré avoir subi sept violations de données ou plus).

Étonnamment, la moitié des personnes interrogées en Amérique du Nord ont désigné les LLM de GenAI comme l'une des trois principales sources d'inquiétude, après les documents financiers (Figure 21). Les LLM préoccupent particulièrement les secteurs du pétrole et du gaz (62 %), l'industrie pharmaceutique (61 %), le gouvernement fédéral (61 %) et des États (58 %), ainsi que les cabinets juridiques (58 %).

Les types de données cités comme les plus à risque varient considérablement selon le secteur d'activité :

Les LLM de GenAI sont les plus préoccupantes dans les secteurs de l'énergie, des services publics, de la sécurité et de la défense, à hauteur de 50 %.

Les PII ont été citées le plus souvent par les entreprises de l'enseignement supérieur (50%).

Les PHI ont été citées le plus souvent par les établissements de santé (58%).

Les CUI et FCI ont été citées le plus souvent par les industriels (79 %).

Les échanges juridiques ont été cités le plus souvent par les sociétés pétrolières et gazières (62%) et les agences fédérales (61%).

Les informations relatives aux fusions et acquisitions ont été le plus citées par les entreprises de l'industrie pharmaceutique (40%).

Les répondants qui ont placé les PHI dans le top 3 des données les plus préoccupantes sont ceux qui ont connu un taux plus élevé de violations de données.

CONFORMITÉ ET RISK MANAGEMENT

La gestion des risques et de la conformité règlementaire sont des priorités absolues

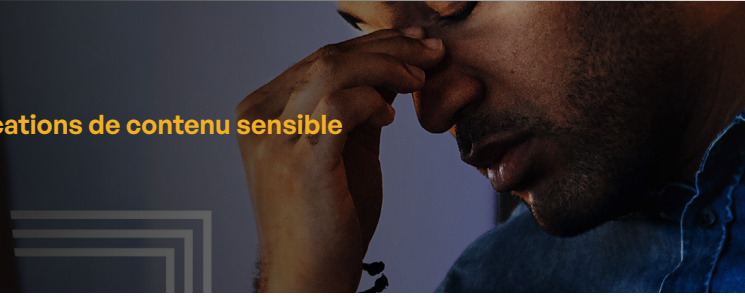
Il semblerait que la part du budget global des organisations alloué à la cybersécurité augmente chaque année. Dans son rapport annuel sur les menaces, CrowdStrike a relevé une *augmentation de 76 %, d'une année sur l'autre,* du nombre de victimes nommées sur les sites de fuites dédiés à la cybercriminalité.[16] Dans son dernier DBIR, Verizon a analysé plus de 30 000 incidents de sécurité réels au cours de l'année écoulée et a confirmé qu'environ un tiers (10 626) étaient des violations de données.[17]

Les données sensibles étant au centre de la plupart des violations de données, les agences gouvernementales et les organismes industriels ont réagi en adoptant une série de nouvelles réglementations et en renforçant celles déjà existantes. Il en résulte une mosaïque géographique qui complique la réponse aux incidents, les audits et les rapports d'audit, en particulier pour les entreprises implantées mondialement.

Comme les années précédentes, les répondants de 2024 ont fait état de difficultés persistantes en matière de conformité et de gestion des risques. Cela ressort clairement des réponses données à une question élémentaire sur l'efficacité de leur organisation à gérer les problèmes de conformité autour des outils de communication de contenus sensibles (Figure 22). *Seuls 11%* des répondants ont affirmé qu'aucune amélioration n'était nécessaire dans ce domaine, soit beaucoup moins que les cohortes 2022 et 2023. La bonne nouvelle est que *moins de répondants (32%)* déclarent qu'une amélioration *significative* est nécessaire.

Il y a peu de différences entre les régions sur cette question, contrairement à la taille de l'entreprise. Plus précisément, les grandes entreprises sont plus susceptibles de déclarer qu'une amélioration significative est nécessaire (Figure 23), *un tiers ou plus* des entreprises de chaque groupe de plus de 15 001 employés ayant répondu par l'affirmative. Néanmoins, la confiance varie quelque peu lorsqu'il s'agit de la conformité réglementaire. 29% des répondants français ont déclaré qu'*aucune amélioration* n'était nécessaire, soit un taux beaucoup plus élevé que les répondants des autres pays : 5% pour l'Allemagne, 10% pour le Royaume-Uni et 13% pour l'Arabie saoudite et les Émirats arabes unis (Figure 24). Il est intéressant, et peut-être alarmant, de constater que les *personnes interrogées au sein du gouvernement fédéral* ont déclaré qu'une amélioration significative était nécessaire (41 %), soit un taux supérieur à celui de tous les autres secteurs d'activité (le deuxième taux le plus élevé étant celui des professions libérales, avec 36 %) (Figure 25).

Seuls 11 % des organisations ont déclaré n'avoir besoin d'aucune amélioration pour le management de la conformité des communications sensibles.



Règlementations prioritaires

Pour les entreprises internationales, les réglementations en matière de confidentialité des données et les normes de sécurité à respecter sont nombreuses. À ce jour, plus de 160 lois sur la protection de la vie privée ont été adoptées au niveau international, et d'autres continuent de l'être. Tout manquement est susceptible d'entraîner une dégradation de l'image de marque, une perte de revenus, des amendes et des pénalités, ainsi que des frais de litiges. Par conséquent, 37 % des sondés du rapport de l'ISACA 2024 ont déclaré n'avoir qu'une certaine confiance (et 13 % ne pas avoir confiance) dans leur capacité à assurer la confidentialité des données conformément aux nouvelles lois.[18]

Quand on demande aux répondants de citer leur Top 2 des priorités en matière de confidentialité et de conformité, deux choix se détachent : le RGPD de l'UE et les lois sur la confidentialité des données adoptées par les États américains, comme le California Consumer Privacy Act (CCPA). Ces deux textes ont été cités par 41 % de l'ensemble des répondants (Figure 26).

Pas étonnant que le RGPD soit beaucoup plus souvent cité dans la région EMEA (57 %), de même que les lois des États américains dans la région North America (63 %) (Figure 27). Parmi les différentes fonctions, les responsables gestion des risques et de la conformité (52 %) mettent davantage l'accent sur le RGPD que les responsables IT (38 %) et cybersécurité (33 %) (Figure 28). Les responsables IT, eux, privilégient les lois propres aux États américains (52 %) par rapport aux responsables gestion des risques et de la conformité (25 %) et aux responsables de la cybersécurité (40 %). Les responsables de la cybersécurité (35 %) accordent plus d'importance au CMMC 2.0 que leurs homologues de l'informatique (22 %) et de la gestion des risques (18 %). Le Health Insurance Portability and Accountability Act (HIPAA), loi propre aux États-Unis, a été cité par 38 % des répondants nord-américains, mais ironiquement par un pourcentage plus élevé (43 %) de répondants de la région APAC.

Quelques lacunes sont à noter concernant la conformité réglementaire vue par les industriels. En particulier, seuls 38 % des prestataires de services de sécurité et de défense ont cité la conformité CMMC comme l'une de leurs deux principales préoccupations. Avec le déploiement progressif du CMMC 2.0, il y a pourtant de quoi s'inquiéter. Les sous-traitants de sécurité et de défense qui ne seront pas conformes au CMMC perdront des contrats avec le DoD (ministère de la Défense américain).

Validations et certifications de sécurité prioritaires

Au niveau des certifications de sécurité, deux normes sont les plus citées parmi les deux priorités des répondants (Figure 29) : les normes ISO à 53 % et le NIST 800-171 à 42 %. Étant donné que les 110 contrôles de la norme NIST 800-171 sont identiques à ceux du CMMC 2.0 niveau 2, ce niveau élevé de priorité est prometteur, en particulier avec le déploiement progressif du CMMC 2.0 qui a débuté. Les normes ISO 27001, 27017 et 27018 ont été les plus citées dans toutes les zones géographiques et dans la plupart des secteurs d'activité ; 59 % dans la région EMEA, 67 % dans l'industrie pharmaceutique et 69 % dans les collectivités locales (Figures 30 et 31).

59 % des personnes interrogées dans la région EMEA ont cité les normes **ISO 27001, 27017 et 27018** dans le **top 2 des validations et certifications prioritaires** (19 % de plus qu'en Asie-Pacifique et 22 % de plus qu'en Amérique du Nord).

ISO 27018 ISO 27017
ISO 27018
ISO 27001 ISO 27001

63%

des personnes interrogées dans la région North America ont cité les lois sur la confidentialité des données des États américains dans leur top 2 des priorités règlementaires.

Seuls 38% des entreprises de sécurité et de défense ont cité la CMMC 2.0 dans leur top 2 des priorités règlementaires.

Une part importante des répondants d'Asie-Pacifique étant d'Australie, il est logique que l'IRAP (Programme d'évaluateurs agréés de la sécurité de l'information) ait été davantage choisi que pour les deux autres régions (45 %). À noter que la directive NIS 2 a été choisie par seulement 20 % des organisations de la région EMEA (bien que ce soit plus qu'en Amérique du Nord avec 8 % et qu'en Asie-Pacifique, à 4 %). On aurait pu supposer qu'elle deviendrait une priorité majeure, la date limite d'entrée en vigueur étant fixée au 17 octobre 2024. Parmi les trois grandes fonctions représentées, c'est la NIS 2 qui a reçu le moins d'attention de la part des responsables gestion des risques et de la conformité (19 %) par rapport à leurs homologues de l'informatique (31 %) et de la cybersécurité (33 %). Les organisations North America ont choisi la conformité SOC 2 Type II plus souvent que les autres régions (41 %).

Au niveau des secteurs d'activité, SOC 2 Type II a été choisi le plus souvent par les professions libérales (47 %). Les normes ISO 27001, 27 017, 27 108 ont été choisies le plus souvent par l'industrie pharmaceutique (67 %). Les entreprises de sécurité et de défense ont quant à elles choisi FedRAMP Moderate (44 %), et les cabinets juridiques l'IRAP (50 %).

Les normes ISO 27001, 27017 et 27018 ont été citées le plus souvent comme les normes de cybersécurité les plus importantes.

Les difficultés à produire des rapports d'audit

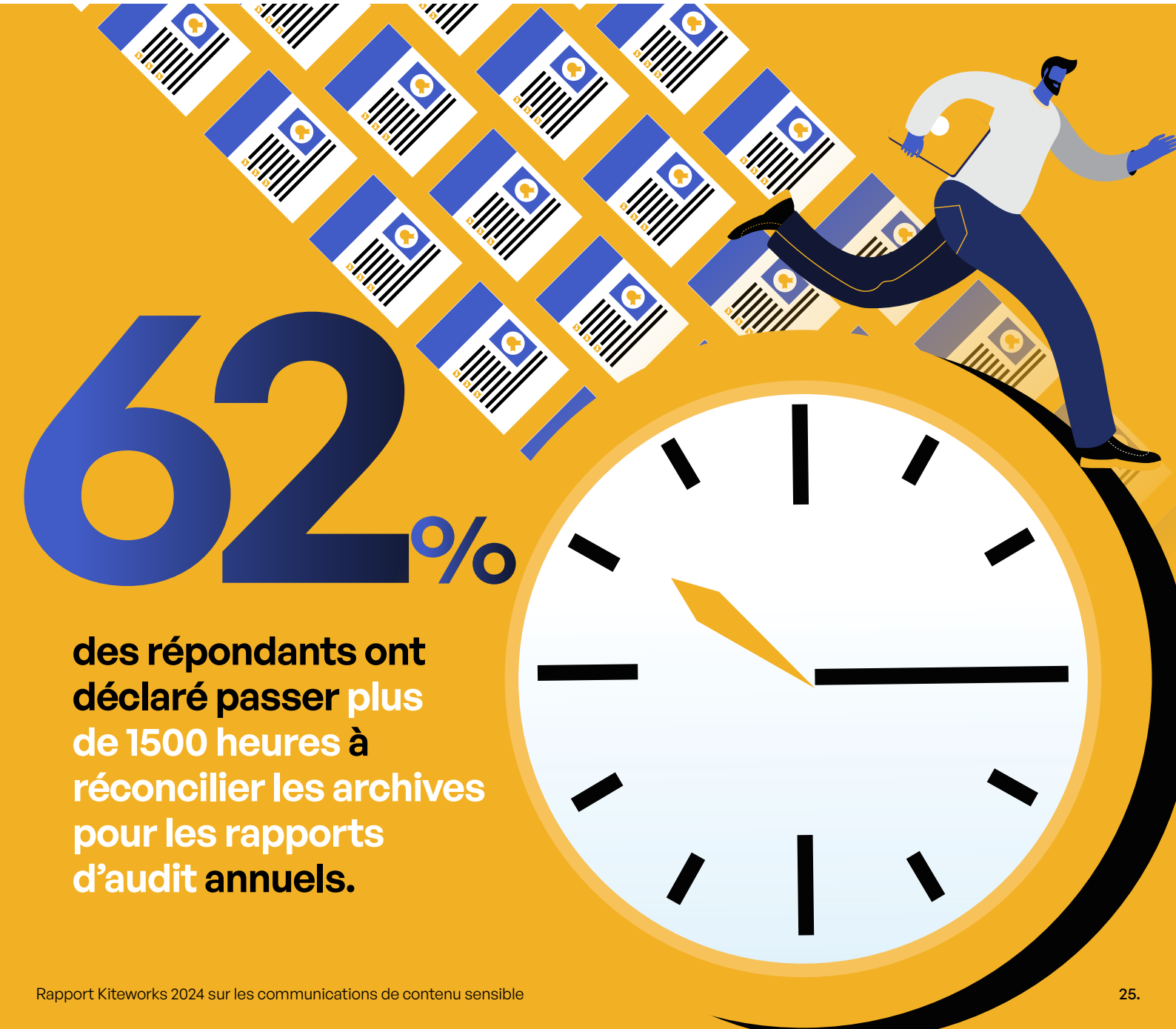
Indépendamment des règlementations et certifications particulières à respecter, la documentation sur la conformité règlementaire reste un défi de taille pour les entreprises. Confrontées à l'envoi et au partage de données sensibles en externe, 57 % d'entre elles indiquent ne pas pouvoir suivre, contrôler et consigner ces échanges (Figure 32). L'une des causes est la mosaïque d'exigences auxquelles elles se heurtent, qui crée des complexités et mobilise beaucoup de ressources humaines et de temps. Lorsqu'on leur demande à quelle fréquence elles doivent générer des journaux d'audit détaillés pour les rapports d'audit, 72 % des personnes interrogées indiquent devoir le faire au moins cinq fois par an (Figure 33). Et huit fois ou plus pour 34 % des répondants.

89%

des organisations doivent produire des rapports d'audit détaillés au moins huit fois par an.

Il n'y a pas de grandes différences entre les régions et les tailles d'entreprise sur cette question (Figures 34 et 35). Les entreprises de la région North America et les petites structures ont tendance à avoir un peu moins d'exigences en matière de traçabilité. Les organisations de plus de 30 000 salariés ont plus de journaux d'audit que les autres (19 % en ont au moins 9). Les secteurs d'activité ayant le plus grand nombre de journaux à réconcilier par an sont les professions libérales (78 %), la sécurité et la défense (77 %) et le gouvernement fédéral (72 %). Les cabinets d'avocats sont les moins impactés avec seulement 15 % des organisations ayant plus de cinq audits par an (Figure 36).

Les rapports d'audit exigent beaucoup de temps humain en raison du nombre d'archives à intégrer. Sur l'ensemble des répondants, *63 % ont déclaré que cette tâche nécessitait plus de 1500 heures de travail par an* (Figure 37). Pour les entreprises de plus de 15 000 salariés, le nombre d'heures augmente considérablement avec un tiers des organisations de plus de 30 000 salariés déclarant y consacrer plus de 2 500 heures (Figure 38). La moitié des répondants des secteurs du pétrole et du gaz et près de la moitié des répondants de l'enseignement supérieur y consacrent plus de 2 000 heures par an : ce sont de loin les secteurs d'activité les plus concernés par ce problème (Figure 39).



CYBERSÉCURITÉ ET RISK MANAGEMENT

La protection des communications de contenu sensible est toujours un vrai casse-tête

Pour les équipes sécurité, protéger le contenu sensible est la priorité des systèmes IT de l'entreprise. Et les répondants de 2024 sont beaucoup moins susceptibles d'affirmer qu'aucune amélioration n'est nécessaire en la matière qu'en 2023 (Figure 40). Seuls *11%* d'entre eux l'ont affirmé cette année. Tout comme le pourcentage de ceux qui ont déclaré qu'une amélioration significative était nécessaire a diminué aussi. Il reste donc *plus de la moitié* des répondants (56%) qui affirment qu'une *certaine amélioration est nécessaire*. Nous pouvons peut-être nous réjouir que les organisations fassent des progrès, tout en étant plus réalistes quant à la nécessité d'une amélioration supplémentaire.

Mais ces pourcentages ne sont pas uniformes dans les différents groupes. 30 % ou plus des personnes interrogées au Royaume-Uni, en Arabie saoudite, aux Émirats arabes unis, Amérique de Nord et Asie-Pacifique ont indiqué qu'une amélioration significative était nécessaire (Figure 41). Il en va de même pour les entreprises comptant entre 20 000 et 30 000 salariés, les professions libérales (47 %), la finance (43 %), le pétrole et le gaz (42 %), le gouvernement fédéral (41 %), l'industrie (36 %) et la santé (34 %) (Figures 42 et 43).

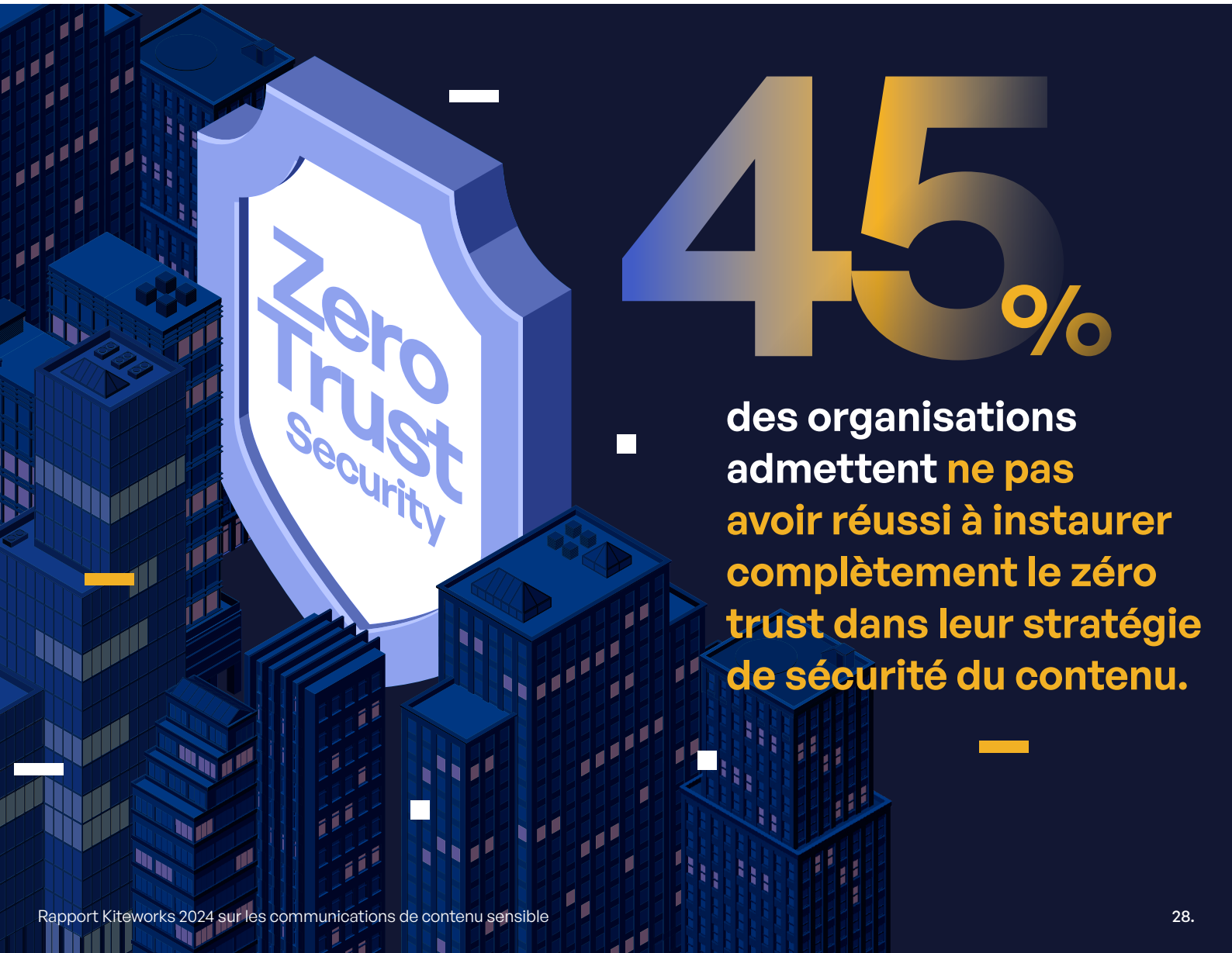
56%

des personnes interrogées ont déclaré avoir besoin d'améliorer le management de leurs communications de contenu sensible en 2024 (contre 37 % en 2023).

Progression du zéro trust

Le zéro trust dans les organisations reflète une approche et une intégration significatives à travers les différentes couches de sécurité. Les principes du zéro trust au niveau du réseau se traduisent par une microsegmentation et des contrôles d'accès stricts. Ils impliquent aussi le déploiement de solutions avancées de protection contre les menaces, et de détection et de réponse des terminaux (EDR) pour assurer l'authentification et la surveillance permanentes de tous les appareils accédant au réseau. Pour la gestion des identités et des accès, l'authentification multifactorielle (MFA) et la gestion des accès privilégiés (PAM) garantissent que l'accès des utilisateurs est strictement contrôlé et vérifié en permanence. Au niveau du contenu, les entreprises mettent en œuvre le chiffrement des données et la surveillance en temps réel pour sécuriser les informations sensibles. Bien que les entreprises privilégient le zéro trust, près de la moitié d'entre elles (48 %) déclarent avoir des difficultés à l'appliquer sur site et dans le cloud.[19]

Notre intérêt porte évidemment sur la couche de sécurité du contenu (Figure 44). Notre première observation est la regrettable proportion de 45 % d'entreprises qui *n'ont pas* encore totalement instauré le principe du zéro trust pour la sécurité du contenu. Dans certaines régions, les résultats sont encore pires. Seuls 35 % des répondants du Royaume-Uni ont atteint ce niveau de référence et 39 % au Moyen-Orient et en Asie-Pacifique (Figure 45). Par secteur d'activité, les administrations publiques (21 %), le pétrole et le gaz (33 %), ainsi que l'industrie pharmaceutique (39 %) sont à la traîne (Figure 46).



Renforcement de la protection des contenus sensibles

Parmi les organisations qui ont admis ne pas utiliser d'outils de sécurité avancés pour échanger des contenus sensibles, un pourcentage élevé (36 %) a indiqué ne pas savoir combien de violations de données les ont touchés. C'est beaucoup plus que pour celles qui ont déclaré les utiliser partiellement ou systématiquement (8 % dans les deux cas) (Figure 47). Ces chiffres montrent qu'il existe un risque important. Parmi les différents secteurs d'activité, le juridique (55 % les utilisent partiellement ou jamais), les collectivités locales (50 %), le gouvernement fédéral (48 %) et la santé (44 %) sont les plus mauvais élèves de l'étude. Ces chiffres contrastent avec l'ensemble de la cohorte (41 %). Les meilleurs élèves sont les professions libérales (71 % les utilisent systématiquement), l'administration publique (71 %) et l'enseignement supérieur (65 %) (Figure 48).

Suivi, classification et contrôle de l'accès aux contenus sensible

Lorsque le contenu quitte une application telle que la messagerie électronique, le partage de fichiers, le SFTP, le transfert de fichiers MFT ou les formulaires web, il est indispensable de suivre et de contrôler l'accès à ce contenu. Si seulement 16 % des personnes interrogées sont en mesure de le faire systématiquement, 61 % peuvent le faire au moins les trois quarts du temps (Figure 49). Ce pourcentage est plus élevé pour certains groupes ; 70 % pour l'Amérique du Nord, 79 % pour l'industrie et 75 % pour la santé (Figures 50 et 51). En revanche, l'enseignement supérieur (31 %) et les secteurs pétrolier et gazier (33 %) sont les plus mal lotis.

Pour déterminer quelles données non structurées devraient être contrôlées, encore faut-il avoir un système de classification. Lorsqu'on leur demande quelle proportion de leurs données non structurées est étiquetée ou classée, moins de la moitié des répondants (48 %) affirment que c'est le cas pour 75 % ou plus de leurs données (Figure 14). La situation est légèrement meilleure en Amérique du Nord, où 56 % des répondants y sont parvenus (Figure 52). Parmi les secteurs d'activité, 65 % ont atteint ce niveau dans la santé, 56 % dans la finance et 55 % dans le secteur juridique (Figure 53).

Seuls 16 %

des organisations sont capables de suivre et contrôler l'accès à *tous* les contenus qui quittent une application.

65%

des personnes interrogées dans le secteur de la santé déclarent étiqueter et classer plus de 75% de leurs données non structurées (c'est plus que tous les autres secteurs).

Outils de sécurité avancés pour les contenus sensibles

Toutes les entreprises disposent de plusieurs outils pour sécuriser leurs réseaux, leurs terminaux et leurs applications cloud. Pour autant, la question de savoir s'ils sont utilisés pour protéger les communications de contenus sensibles internes et externes se pose différemment.

Lorsqu'on leur demande si elles utilisent l'authentification multifactorielle, le chiffrement, le suivi et le contrôle de la gouvernance pour ces communications, les résultats sont mitigés (Figure 54). Près de six entreprises sur dix (59 %) affirment que ces protections sont systématiquement appliquées aux communications de contenu sensible externes. Presque tous les répondants affirment les utiliser de temps en temps. Les répondants d'Amérique du Nord sont les plus vigilants en matière de sécurité, 67 % d'entre eux déclarant les utiliser en permanence, contre 57 % pour les répondants de la région Asie-Pacifique et 53 % pour ceux de la région EMEA.

La capacité à évaluer et à maîtriser la sécurité des communications de contenu sensible reste un axe de progrès déterminant : seuls 11 % des entreprises ont indiqué qu'aucune amélioration n'était nécessaire, contre 26 % lors de l'enquête précédente (Figure 55). Cette année, un *pourcentage plus élevé* d'organisations a indiqué avoir besoin d'une *amélioration certaine* (56 % contre 37 % dans l'enquête de 2023).

Bien que les chiffres soient similaires pour l'ensemble de la cohorte, des différences intéressantes apparaissent en fonction des groupes. Pour les communications internes, 71 % des administrations publiques et des professions libérales ont déclaré utiliser systématiquement ces outils (Figure 56). Les deux tiers (67 %) des Nord-Américains ont déclaré la même chose, contre 53 % seulement dans la région EMEA (mais 63 % au Royaume-Uni) (Figure 57).). Il est intéressant de noter que les cabinets d'avocats (45 %) sont les moins performants en matière de communication interne. Pour les communications externes, l'industrie pharmaceutique (78 %) et l'enseignement supérieur (72 %) ont été les plus performants, tout comme les Nord-Américains (69 %) (Figure 56).

56%

des organisations ont déclaré avoir besoin d'améliorer leur façon d'évaluer et de maîtriser la sécurité des communications sensibles, soit 33 % de plus que l'an dernier.

PROCESS OPÉRATIONNELS

Il faut tout un « village » et beaucoup de temps pour maîtriser la sécurité des données et la conformité règlementaire

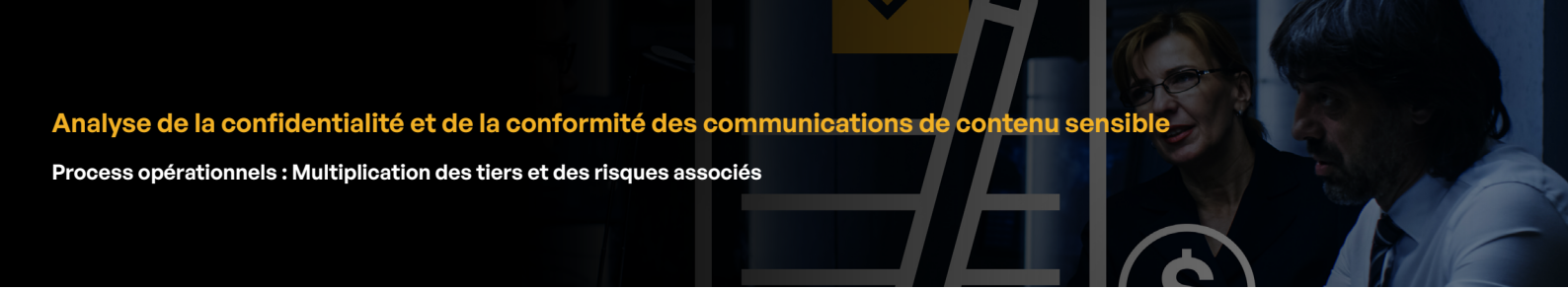
Bon nombre des difficultés évoquées jusqu'ici (violations de données, problèmes de conformité et de sécurité) sont accentuées par la complexité des processus opérationnels en général. Entre la multiplication des outils de communication et la difficulté à se passer de procédures manuelles, les problèmes de sécurité et de conformité sont inévitables et passent à travers les mailles du filet.

Multiplication des tiers et des risques associés

La plupart des organisations échangent des volumes importants de données sensibles au quotidien avec des centaines, voire des milliers d'interlocuteurs. Le risque lié aux tiers n'a jamais été aussi élevé, quel que soit le secteur d'activité. Or l'échange de contenu sensible est indispensable, ce qui accentue encore le risque.

Lorsque nous avons demandé à la cohorte 2024 d'estimer combien d'interlocuteurs recevaient des contenus sensibles de leur entreprise, *deux tiers* (66%)les ont estimés à *plus de 1 000* (Figure 58). Parmi les entreprises de plus de 30 000 salariés, 33 % échangent des contenus avec plus de 5 000 interlocuteurs (Figure 59). 77 % des répondants de l'Asie-Pacifique échangent des contenus sensibles avec plus de 1000 interlocuteurs, 66 % pour l'Amérique du Nord et 63% pour EMEA (Figure 60).

Le gouvernement fédéral échange des contenus sensibles à un rythme nettement plus élevé que la plupart des autres secteurs d'activité (28 % envoient et partagent des données avec plus de 5 000 tiers) (Figure 61). L'enseignement supérieur affiche également un taux élevé d'échange de données avec des tiers ; 47 % des personnes interrogées ont déclaré échanger des données avec plus de 2 500 personnes.

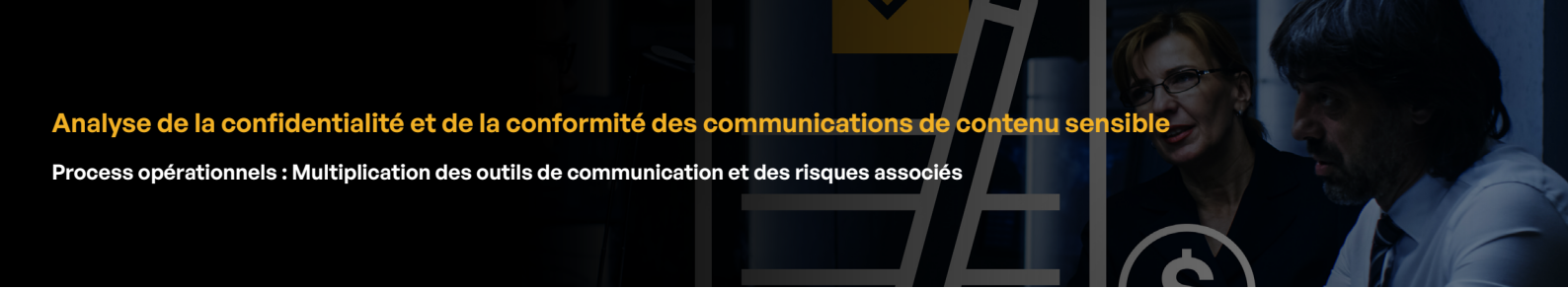


Une fois que le contenu sensible quitte l'organisation, 39 % des entreprises sont incapables de suivre et de contrôler l'accès à *plus de la moitié* de ce contenu. Les plus mauvais élèves sont dans la région EMEA avec *46%* (Figure 62). Parmi les entreprises les plus menacées par l'absence de suivi et de contrôle des communications sensibles en externe, on retrouve l'enseignement supérieur (69 %) et le pétrole et le gaz (66 %) (Figure 63). À l'inverse, les gouvernements des États s'en sortent mieux, avec 38 % des répondants indiquant être capables de suivre et de contrôler l'accès à des contenus sensibles à tout moment.

Le lien entre le nombre de violations de données subies et le nombre de tiers d'une entreprise est parlant (Figure 64). Par exemple, 35 % des organisations qui déclarent échanger des contenus sensibles avec plus de 5 000 tiers ont subi plus de 10 violations de données l'an dernier. 50 % de celles qui échangent des contenus sensibles avec 2 500 à 5 000 tiers ont subi plus de sept violations de données. Il en va de même en ce qui concerne les frais de litiges (Figure 65). Pour celles qui échangent des données sensibles avec plus de 5 000 personnes, la moitié d'entre elles ont dû payer plus de 5 millions de dollars en frais de contentieux. 44 % de celles qui échangent des contenus sensibles avec 2 500 à 5 000 tiers ont également dépensé plus de 5 millions de dollars.

35%

des entreprises qui échangent des contenus sensibles avec plus de 5 000 interlocuteurs ont subi plus de 10 violations de données l'an dernier.



Multiplication des outils de communication et des risques associés

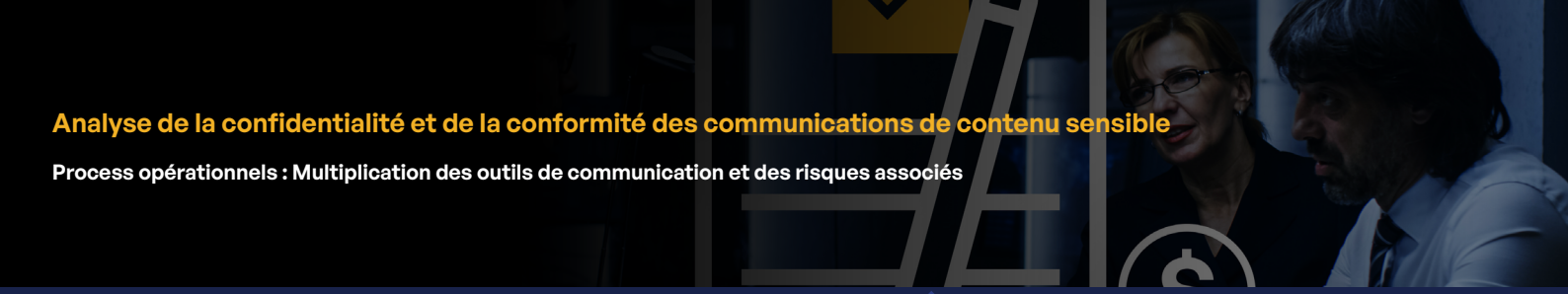
Il existe de nombreux outils de communication pour l'envoi et le partage de contenus sensibles : e-mail, partage de fichiers, transfert de fichiers MFT, SFTP, formulaires web, etc. Les mesures prises pour atténuer les risques, réduire les coûts et améliorer l'efficacité opérationnelle semblent avoir provoqué une fusion des outils de communication. En effet, la moitié des personnes interrogées en 2023 avaient le choix entre au moins six outils de communication de contenu contre 31 % cette année (Figure 66). C'est en *Amérique du Nord* que la prolifération des outils est la plus forte, 59 % des répondants utilisant cinq outils ou plus, contre 50 % pour la région EMEA et 52 % pour Asie-Pacifique (Figure 67). Un pourcentage étonnant de *77% en Amérique du Nord* utilise quatre outils ou plus, et ce chiffre est de 80 % ou plus dans les services financiers, juridiques, professions libérales, ainsi que dans le pétrole et le gaz (Figure 68).

L'analyse croisée de ces données montre que les organisations ayant un *taux élevé de violations de données* sont celles qui ont le *plus d'outils de communication* (Figure 69). 32 % des organisations ayant subi 10 violations de données ou plus disposent de plus de 7 outils de communication. Ou encore, 42 % de celles disposant de 6 outils de communication ont subi de 7 à 9 violations de données. Ces chiffres sont nettement plus élevés que le nombre moyen de violations de données pour l'ensemble des répondants : 9 % ont signalé 10 violations (par rapport aux 32 % disposant de sept outils de communication ou plus) et 23 % ont signalé de 7 à 9 violations de données (Figure 6). Cela équivaut à un taux 3,55 fois plus élevé pour ceux qui disposent de 10 outils de communication ou plus et 2 fois plus élevé pour ceux qui disposent de 7 à 9 outils de communication. Il en va de même pour les frais de contentieux liés aux violations de données : 26 % de celles qui ont déclaré avoir payé *plus de 7 millions de dollars* l'année dernière disposent de plus de sept outils de communication (3,25 fois plus que la norme de 8 %) (Figure 70).

32%

des organisations ayant subi au moins 10 violations de données ont plus de 7 outils de communication.

Plus une organisation a d'outils de communication, plus elle subit de violations de données et plus les coûts de contentieux sont élevés.



38%

des personnes interrogées en Amérique du Nord déclarent utiliser plus de six outils de communication (c'est plus que dans les autres régions).

Deux tiers des organisations échangent des contenus sensibles avec plus de 1000 interlocuteurs.

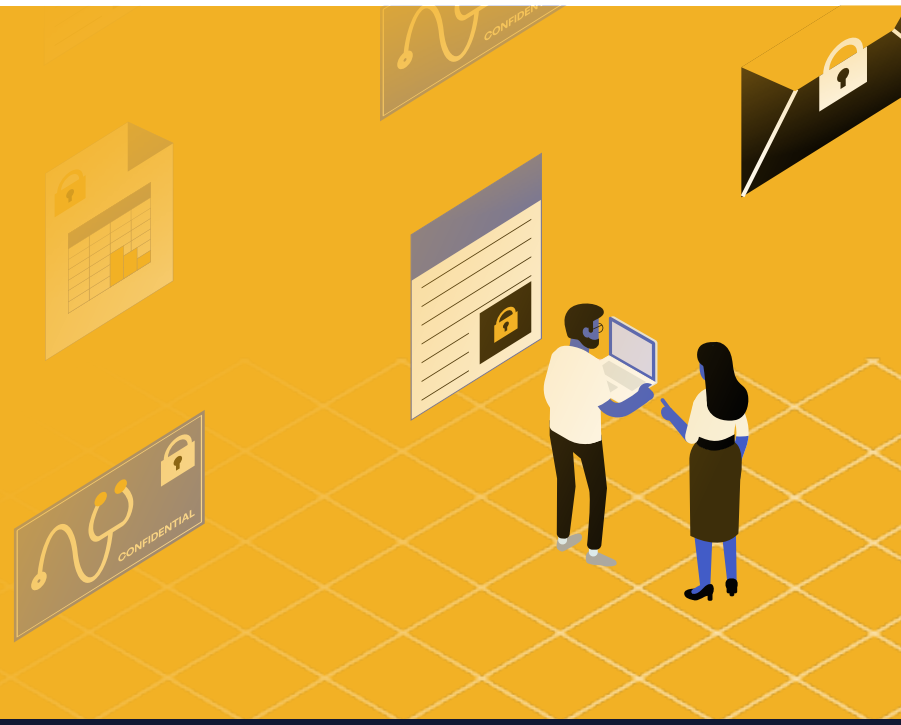
Réconciliation des journaux qui s'accumulent

Dans le cadre des rapports d'audit, beaucoup de répondants ont déclaré perdre du temps à réconcilier les journaux de communication sensibles ; *48%* ont indiqué devoir consolider *plus de 11 journaux*, et 14 % plus de 20 journaux. Le fait de ne pas savoir quels fichiers logs doivent être réconciliés constitue un risque en soi ; 8 % des personnes interrogées déclarent ne pas savoir combien elles en ont (Figure 71).

De la taille de l'organisation dépend le nombre de journaux à réconcilier ; 34 % des organisations de plus de 30 000 salariés ont admis devoir réconcilier plus de 20 journaux (contre 14 % des organisations de 20 000 à 25 000 salariés et 11 % pour celles de 25 000 à 30 000 salariés) (Figure 72).

34%

des organisations de plus de 30 000 salariés ont admis devoir réconcilier plus de 20 journaux.



Tout ce travail de réconciliation mobilise du temps et des ressources précieuses ; 20 % des personnes interrogées ont déclaré que cela prenait plus de 40 heures par mois, et 40 % plus de 25 heures par mois (Figure 73). Plus l'organisation est grande, plus la tâche est difficile : 24 % des organisations de plus de 30 000 salariés ont indiqué y consacrer *plus de 40 heures* par mois (Figure 74). En outre, 9 % des entreprises de plus de 30 000 salariés ont indiqué qu'il n'était pas possible de compiler leurs journaux, soulignant un risque important pour la sécurité et la conformité. En termes de secteur d'activité (Figure 75), les cabinets d'avocats sont les premiers à admettre ne pas savoir réconcilier leurs journaux (10 %). Les établissements d'enseignement supérieur arrivent en tête pour le temps passé à la consolidation, 30 % d'entre eux y consacrant 40 heures ou plus chaque mois.

Parmi les secteurs d'activité, les répondants du gouvernement fédéral sont les plus nombreux (34 %) à déclarer devoir consolider plus de 20 journaux d'audit.

Limitations de la taille des fichiers et risques associés

Les limites de taille de fichiers posent problème pour de nombreux outils de communication. Les salariés, frustrés, qui essaient de faire leur travail, finissent parfois par utiliser des services de partage de fichiers grand public pour contourner ces limites. Et même pour les utilisateurs qui suivent les consignes, les solutions de contournement prévues sont chronophages.

À l'exception du SFTP (27 %), *plus de trois répondants sur dix* utilisent des solutions de contournement pour les e-mails, le partage de fichiers et le transfert MFT plus de 50 fois par mois (Figure 76). Environ 10 % déclarent devoir le faire plus de 100 fois par mois (10 % pour les e-mails, 11 % pour le partage de fichiers, 8 % pour le SFTP et 11 % pour le transfert de fichiers MFT). Plus de la moitié d'entre eux le font plus de *25 fois par mois* sur ces quatre canaux de communication. Par région, la fréquence est plus élevée en Amérique du Nord que dans les régions EMEA et Asie-Pacifique ; les personnes ayant besoin de le faire plus de 100 fois par mois sont *plus de deux fois plus nombreuses* sur chacun des canaux de communication (Figure 77).

Plus de 30 %

des organisations utilisent des solutions de contournement pour des fichiers volumineux 50 fois par mois (pour contourner les e-mails, le partage de fichiers, le transfert MFT et SFTP).

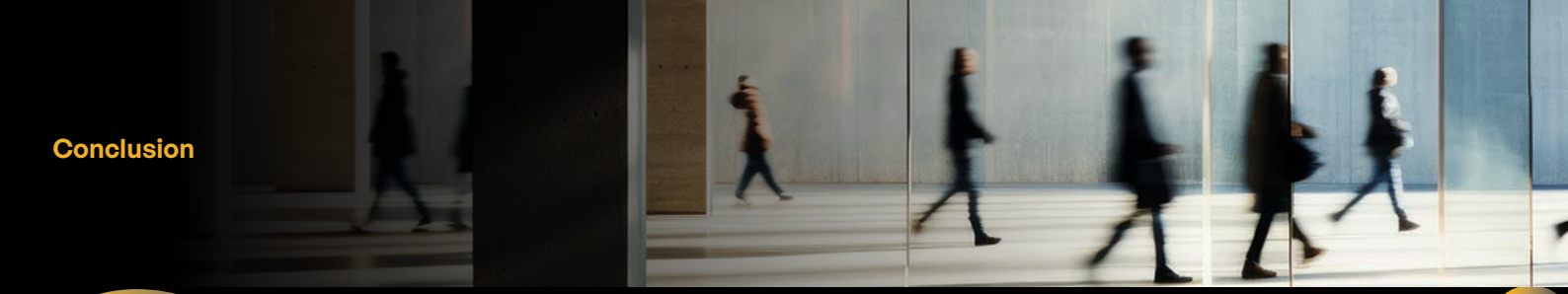
Principales motivations à unifier et à protéger les communications sensibles

Vous percevez sans doute déjà les problèmes posés par la multiplicité des outils de communication de contenus sensibles : risque pour la sécurité et à la conformité règlementaire, manque de visibilité sur les différents types de données et processus manuels inefficaces. Pour savoir comment les répondants abordent ces difficultés, nous leur avons demandé de choisir leurs deux principales motivations pour unifier et protéger leurs communications sensibles (Figure 78). La réponse la plus citée (56 %) est la *protection de la propriété intellectuelle et secrets d'entreprise*. Suivi de près par *l'atténuation des litiges* (51%) et la *prévention des non-conformités* (48%).

Selon le poste occupé, l'importance accordée aux litiges varie beaucoup (Figure 79). Cette motivation est citée par 79 % des professionnels de l'informatique et 61 % des membres de l'équipe sécurité, mais seulement par 39 % des salariés chargés de la gestion des risques et de la conformité. Les répondants des secteurs juridique (75 %), pétrolier et gazier (75 %) et du gouvernement fédéral (69 %) étaient particulièrement préoccupés par les fuites de propriété intellectuelle (Figure 80).

Il est intéressant d'observer que ces différences se répercutent également entre les régions (Figure 81). Loin devant, les répondants de la région *Asie-Pacifique* ont indiqué que le premier objectif était d'éviter de nuire à l'image de marque (79 %), suivi par l'atténuation des litiges longs et coûteux (61 %). Pour la région EMEA, le premier objectif était d'éviter les fuites de propriété intellectuelle et secrets d'entreprise (62 %), suivi par l'atténuation des litiges longs et coûteux (51 %). Les répondants d'*Amérique du Nord* ont cité le fait d'éviter les pannes opérationnelles et les pertes de revenus (57 %) et la prévention des fuites de propriété intellectuelle et secrets d'entreprise (51 %).

La protection de la propriété intellectuelle et des secrets d'entreprise (56 %), l'atténuation des litiges (51 %) et la prévention des non-conformités (48 %) sont les trois principales motivations des entreprises pour unifier et protéger leurs communications sensibles.



Conclusion

Les conclusions du rapport soulignent la nécessité pour les entreprises de prendre des *mesures proactives* pour protéger leur contenu sensible. L'une des pistes à retenir est la *consolidation des outils de communication* au sein d'une seule et même plateforme. En réduisant le nombre d'outils différents utilisés pour communiquer, les entreprises réduiront considérablement les risques et gagneront en efficacité. En particulier, les organisations ayant moins d'outils de communication subissent moins de violations de données. Donc plus une entreprise consolide ces outils, plus elle gagne en sécurité.

Le rapport souligne également les risques importants associés aux *données non étiquetées et non classées*. Les organisations qui manquent d'un système d'étiquetage et de classification s'exposent à davantage de violation des données, car elles n'ont pas la visibilité et le contrôle nécessaires sur leur contenu sensible. La croissance exponentielle des données, encore accélérée par l'adoption de GenAI, impose de prioriser la classification des données pour limiter les risques.

Pour renforcer la sécurité des communications de contenu sensible, les *principes du zéro trust et les outils de sécurité avancés* sont indispensables. Les conclusions du rapport mettent en évidence d'importantes lacunes, qui peuvent être comblées par une stratégie zéro trust basée sur le contenu. Autrement dit, comprenant des contrôles d'accès basés sur les attributs, un chiffrement complet, une surveillance en temps réel et une prévention des pertes de données. Comme le montre cette étude, les lacunes sont plus importantes dans certains secteurs d'activité, certaines régions et certains pays.

Cette enquête met également en évidence les *risques importants* liés à l'échange de contenus sensibles avec des tiers : plus les répondants envoient et partagent des contenus sensibles avec des tiers, plus ils sont confrontés à des violations de données et à des coûts de contentieux élevés. Par conséquent, les organisations doivent être en mesure de suivre et contrôler la gouvernance via des mesures de sécurité avancées.

Sur ce point, un dernier commentaire sur le *coût des violations de données*, en particulier celui lié aux *contentieux*. L'enquête a révélé que de nombreuses organisations subissaient des frais juridiques importants, rarement pris en compte dans le coût estimé des violations. L'atteinte à l'image de marque, la perte de revenus et les arrêts d'activité ne sont que quelques conséquences des violations de données. Les amendes et les sanctions pour non-conformité et les frais de contentieux supplémentaires ont souvent des conséquences à long terme. Il est donc urgent de sélectionner des outils de communication de contenus sensibles qui respectent les normes de sécurité telles que FedRAMP, ISO 27001, SOC 2 Type II ou encore NIST CSF 2.0.

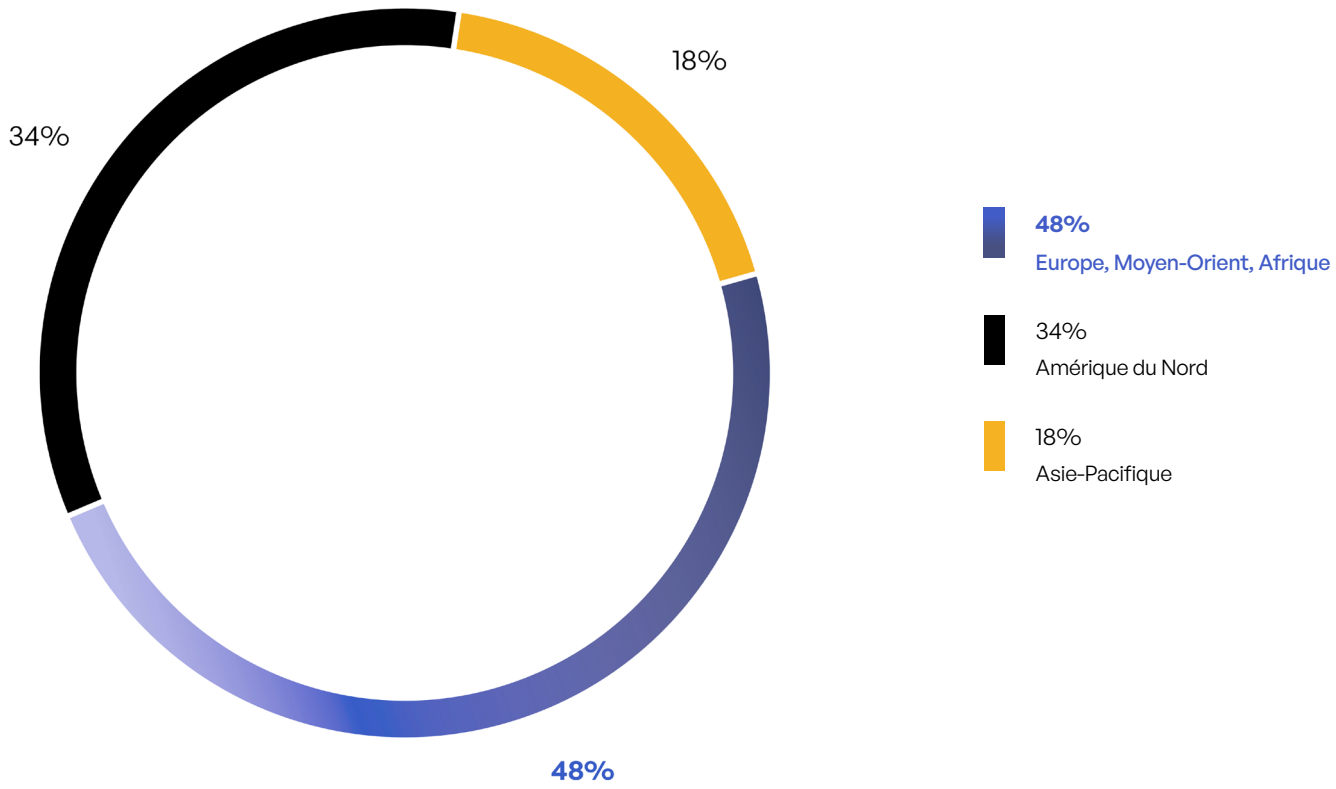


Figure 1: Répartition par région

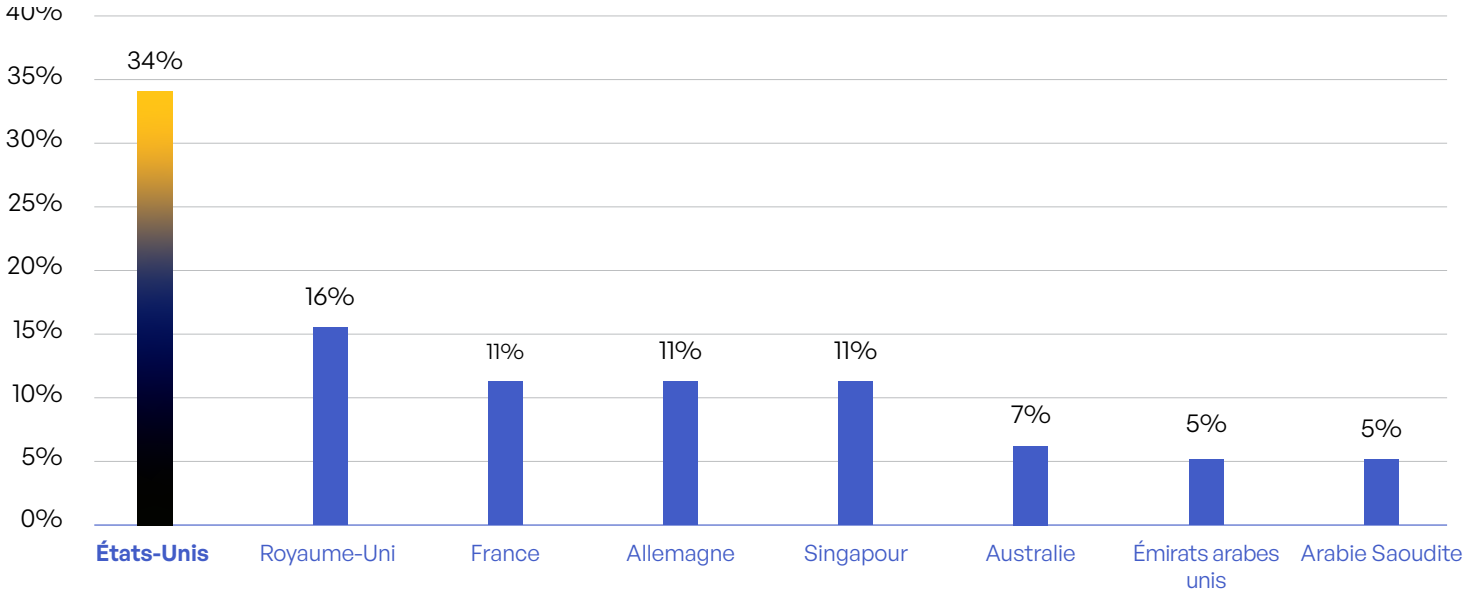


Figure 2: Répartition par pays

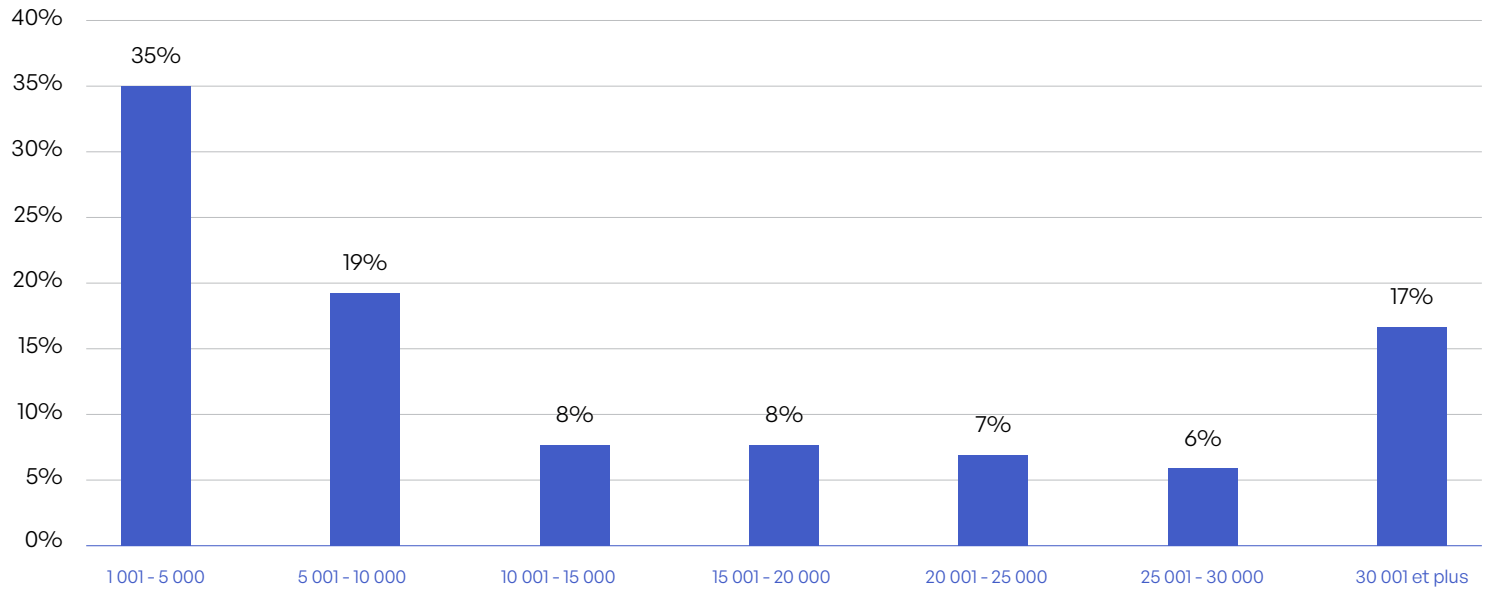


Figure 3: Taille des organisations

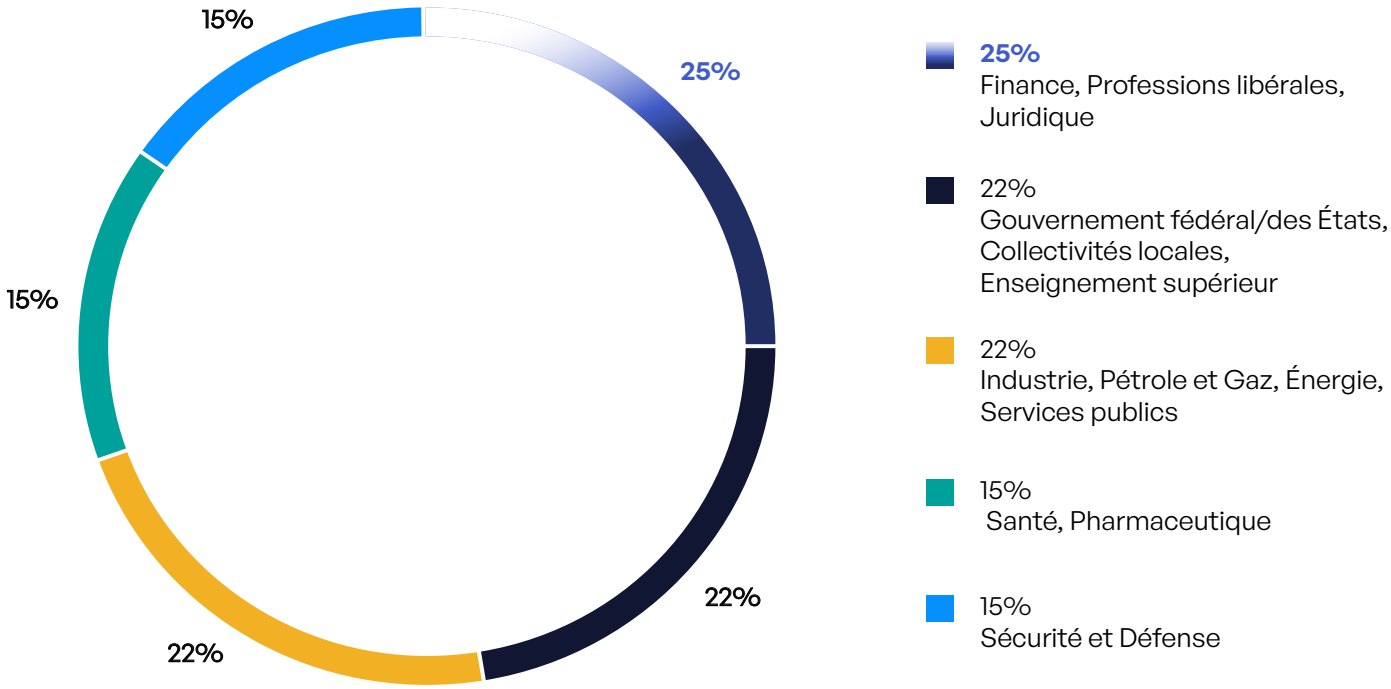


Figure 4: Répartition par secteur d'activité

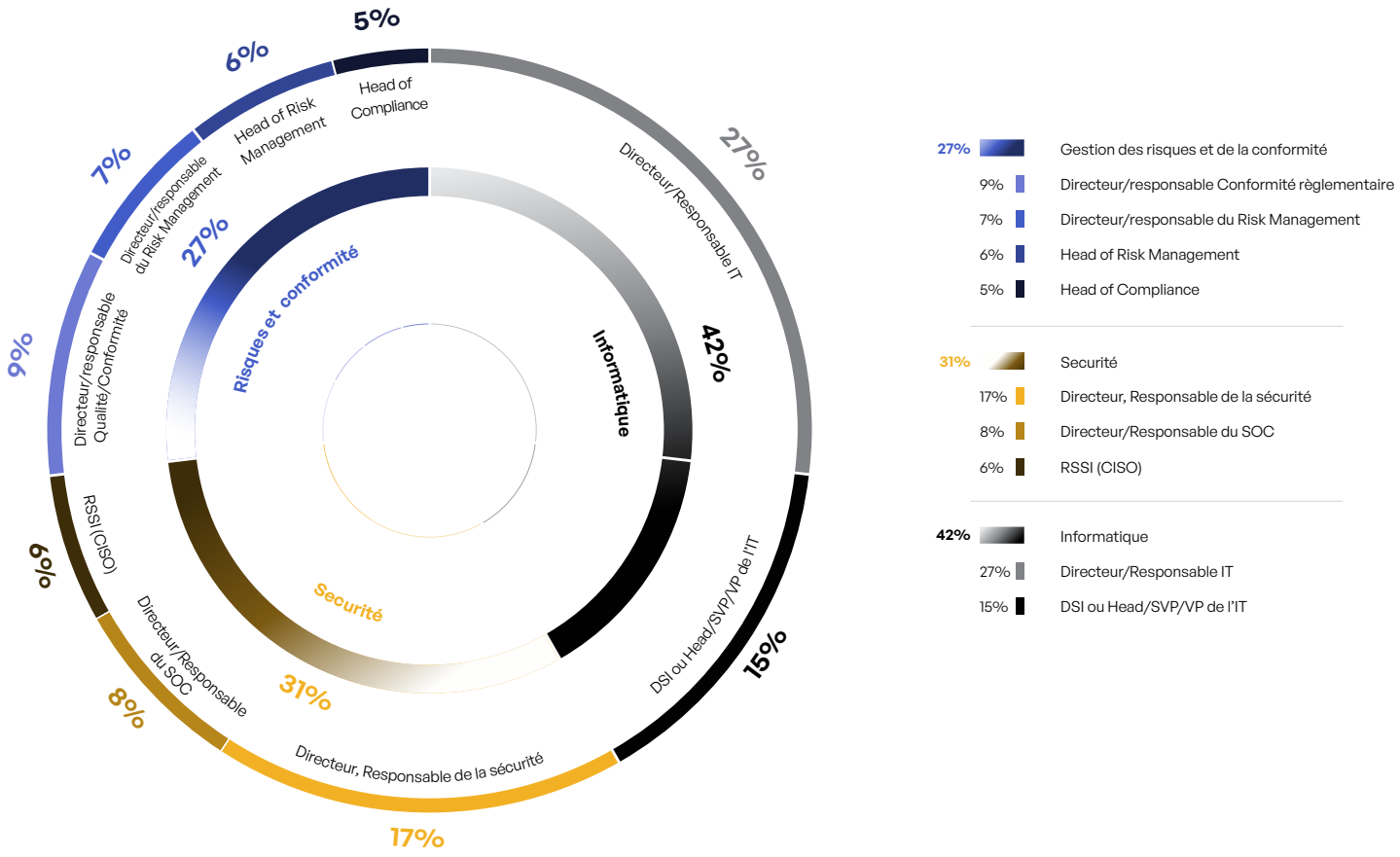


Figure 5: Responsabilités/Postes occupés

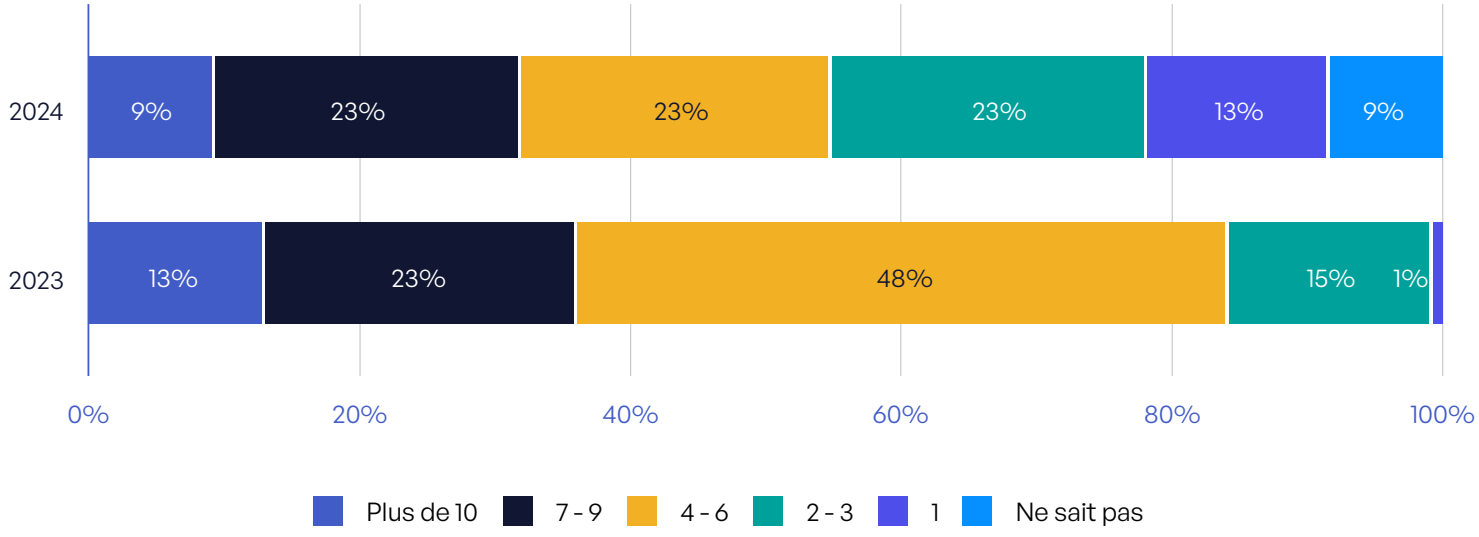


Figure 6: Nombre de piratages externes des contenus sensibles en 2023

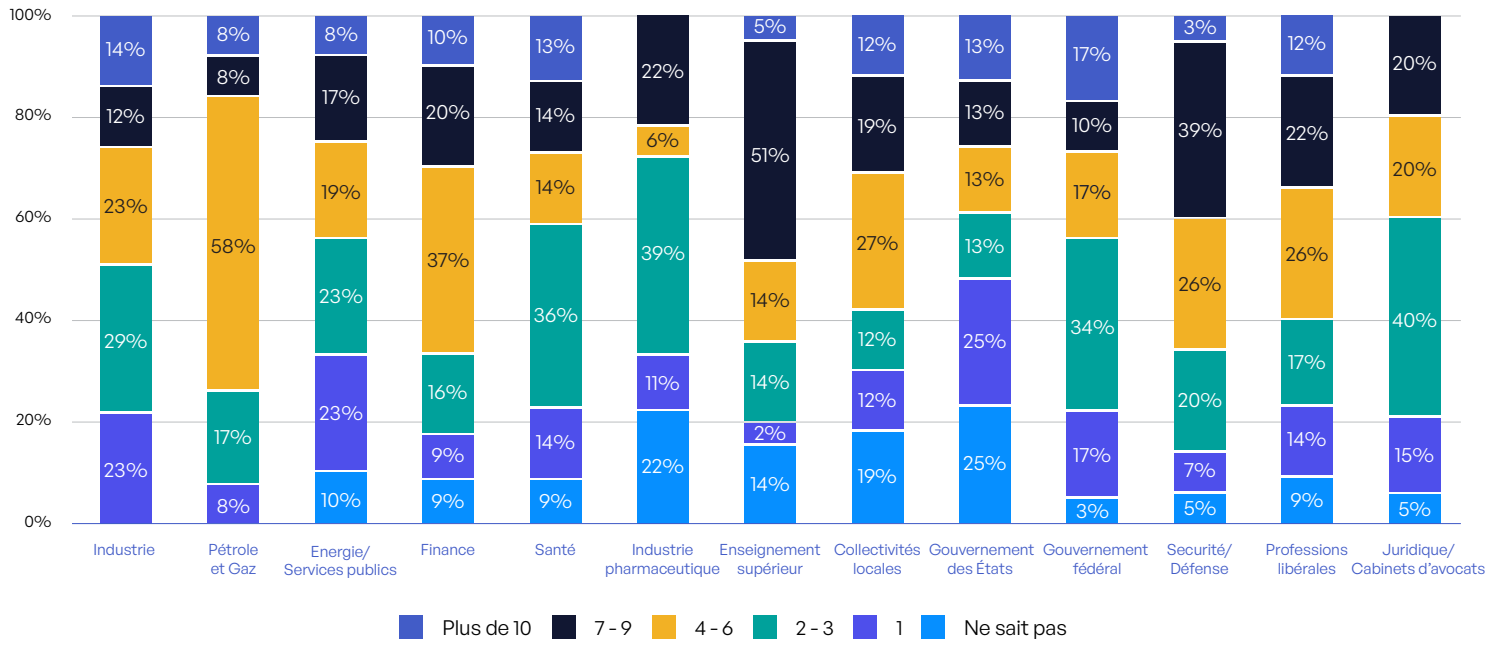


Figure 7: Nombre de piratages externes par secteur d'activité

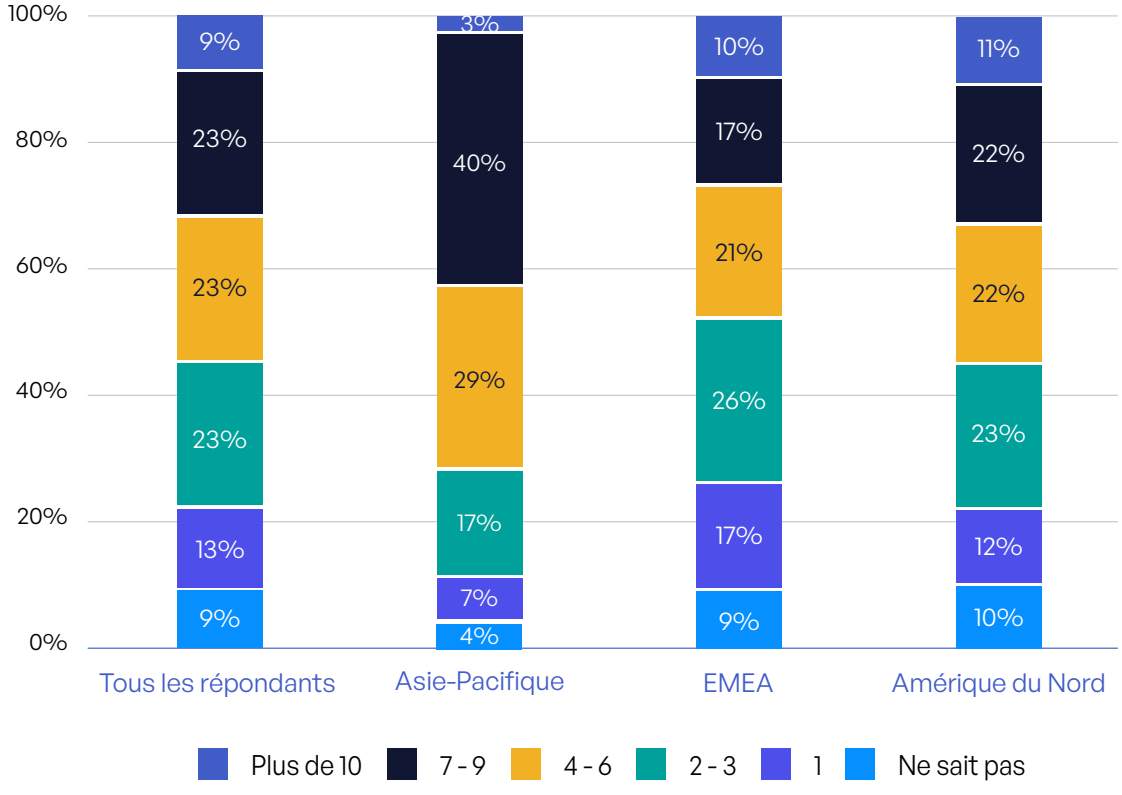


Figure 8: Nombre de piratages externes par région

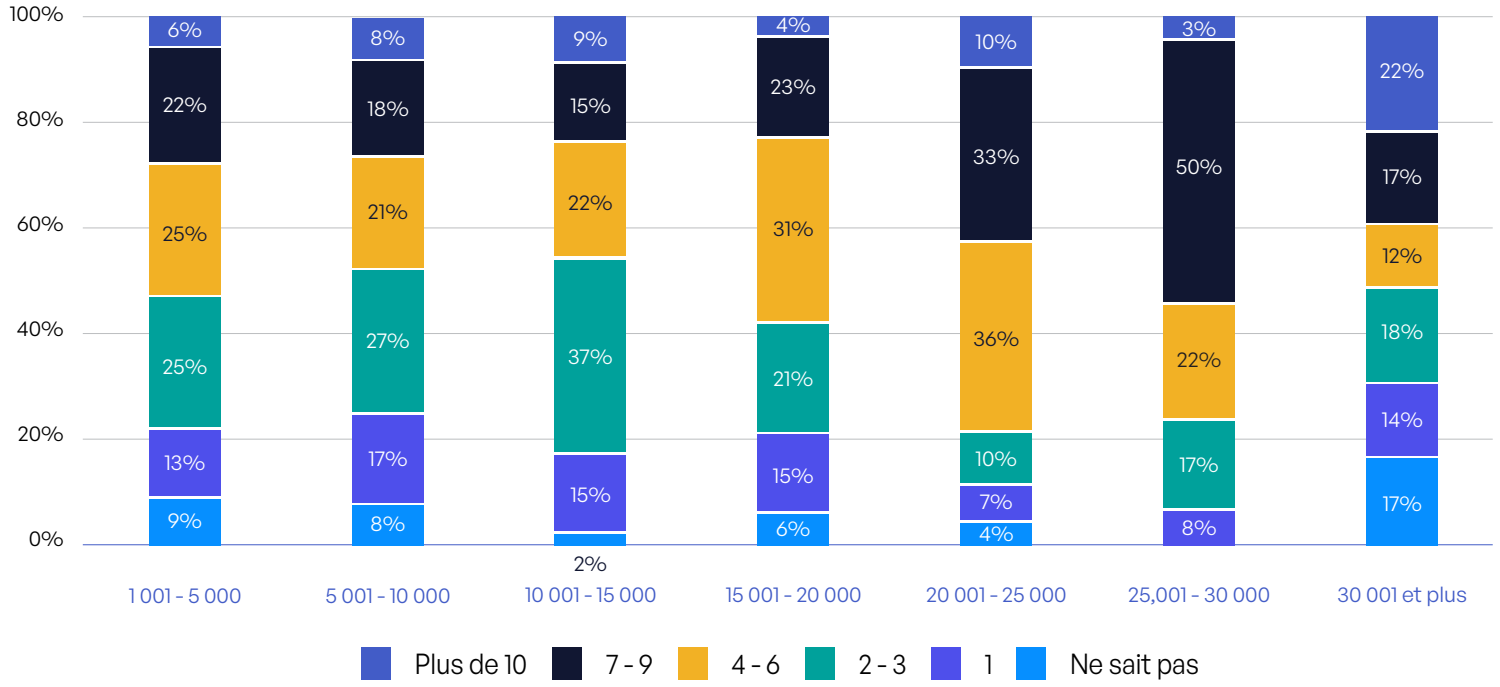


Figure 9: Nombre de piratages externes selon la taille de l'organisation

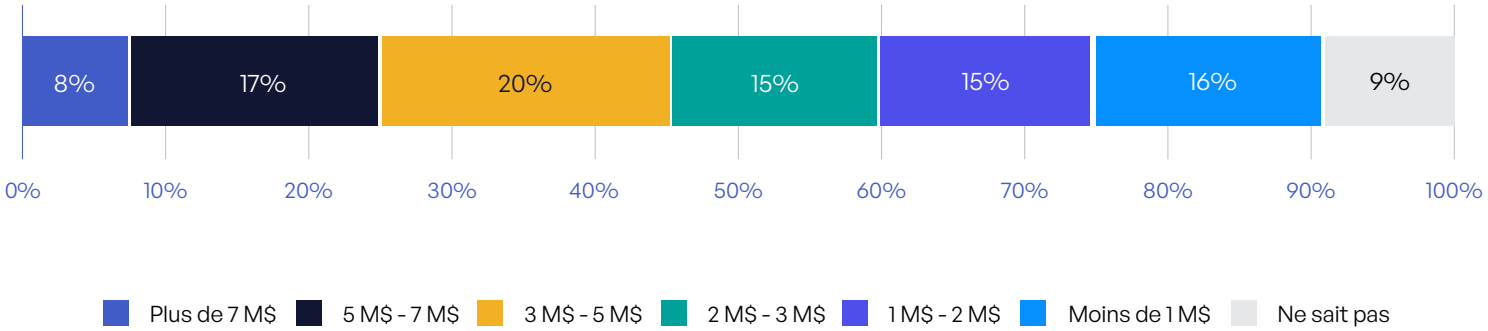


Figure 10: Coût annuel des litiges liés aux violations de données

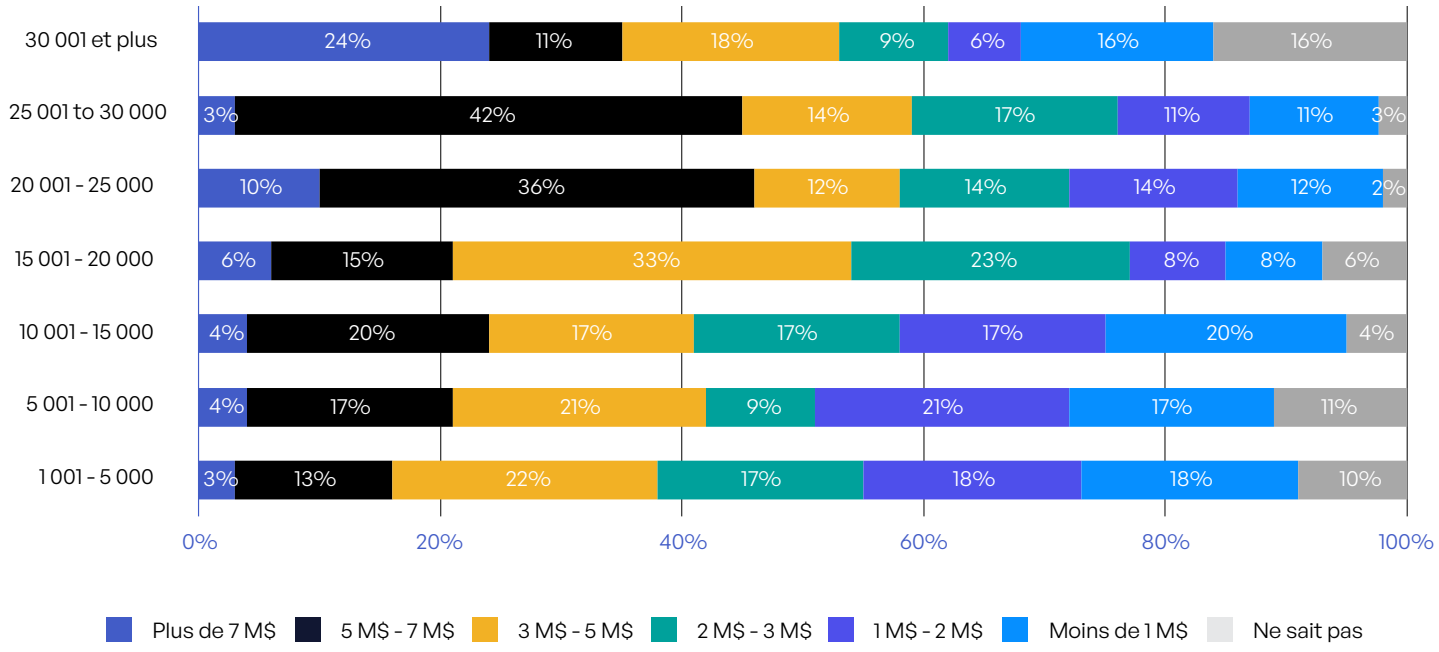


Figure 11: Coût annuel des litiges liés aux violations de données selon la taille de l'organisation

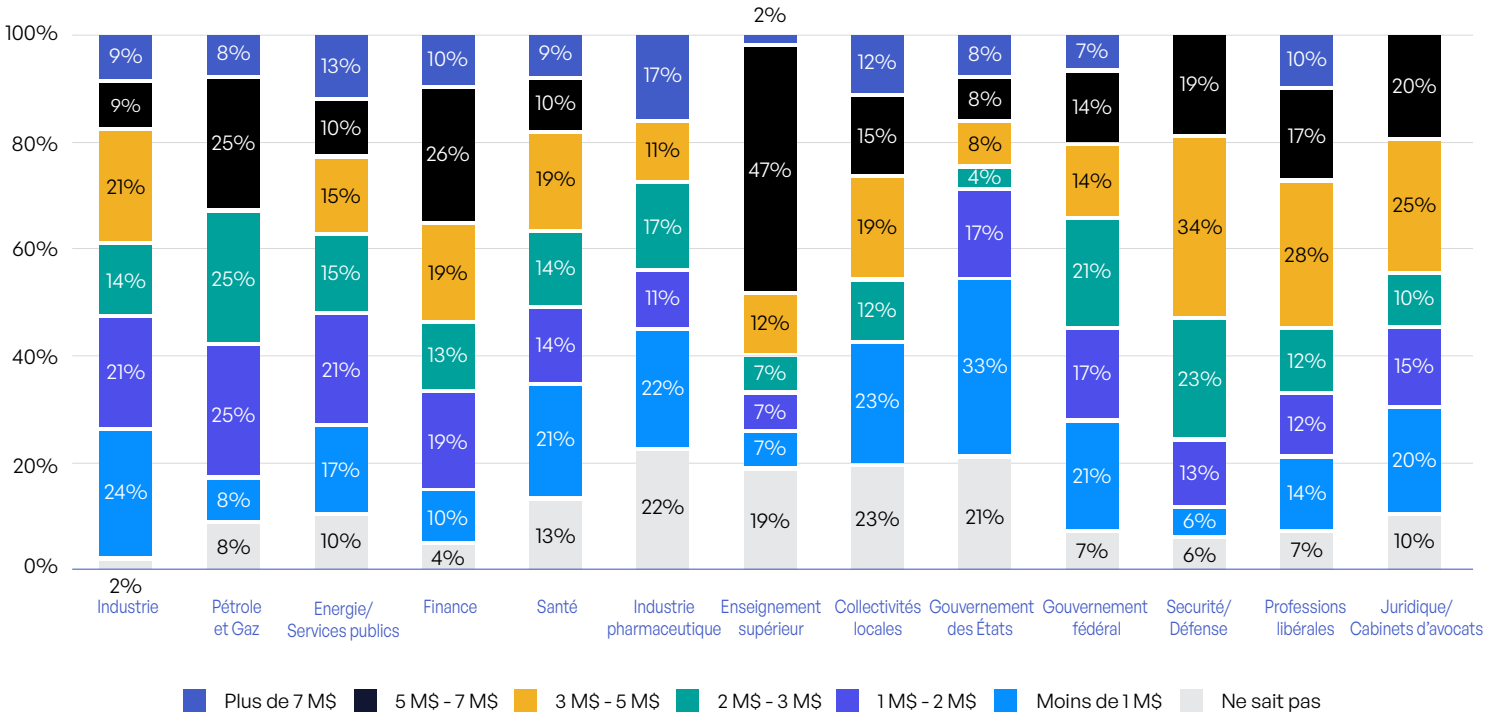


Figure 12: Coût annuel des violations de données par secteur d'activité

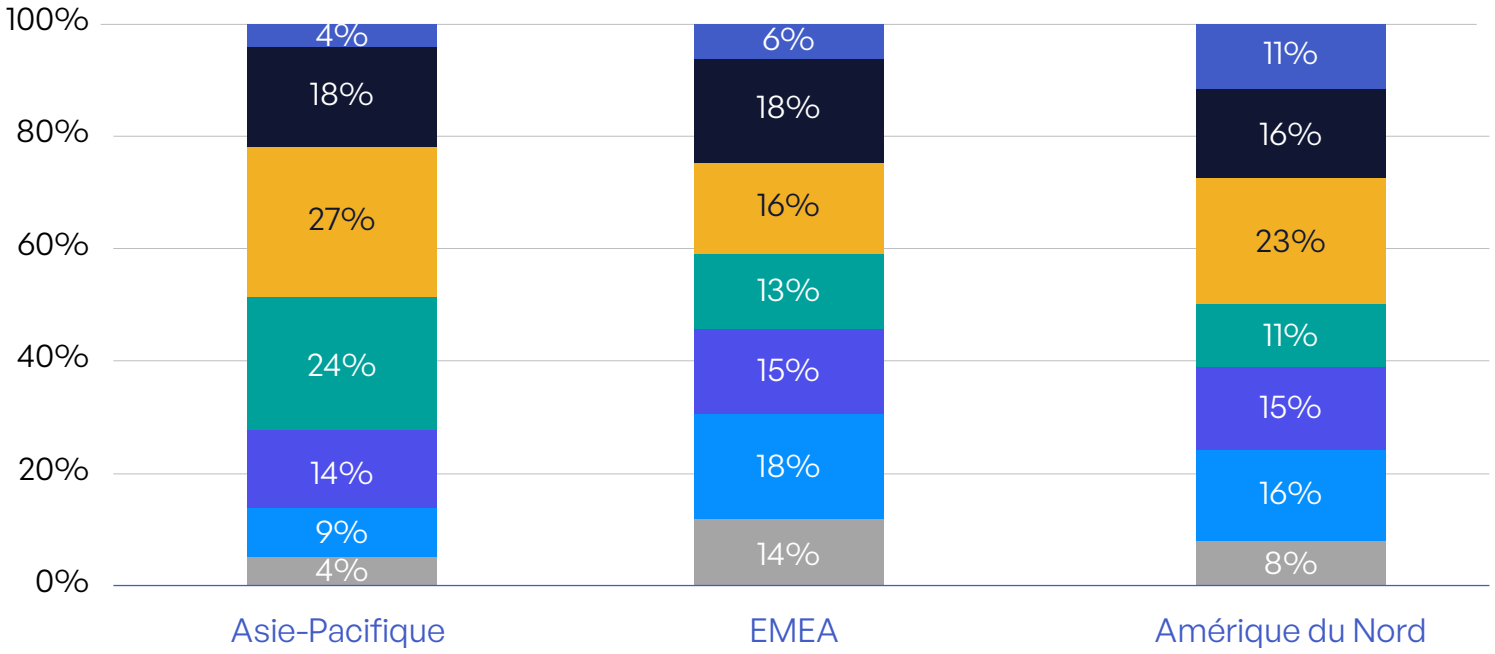


Figure 13: Coût des litiges dans les différentes régions

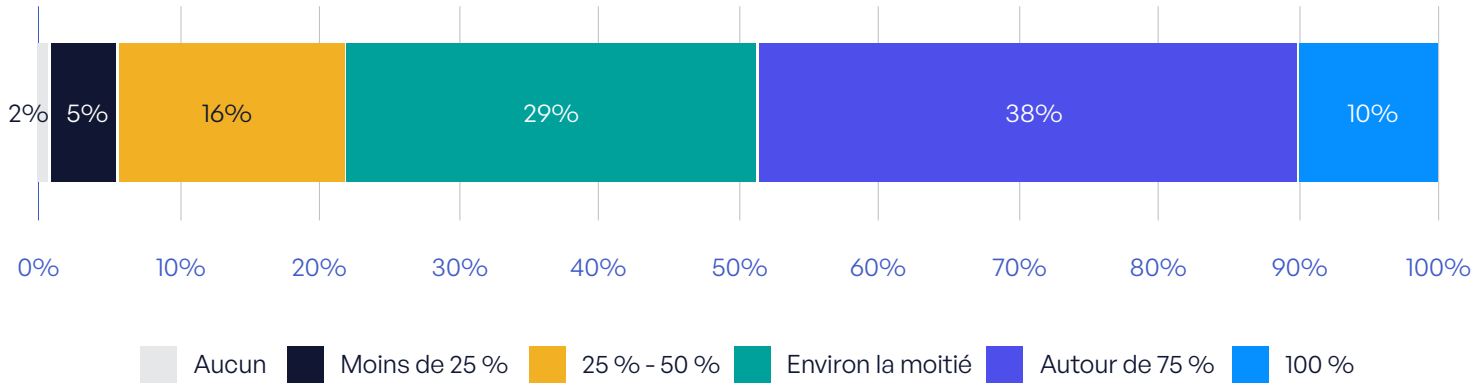


Figure 14: Pourcentage de données non structurées qui est étiqueté et classifié

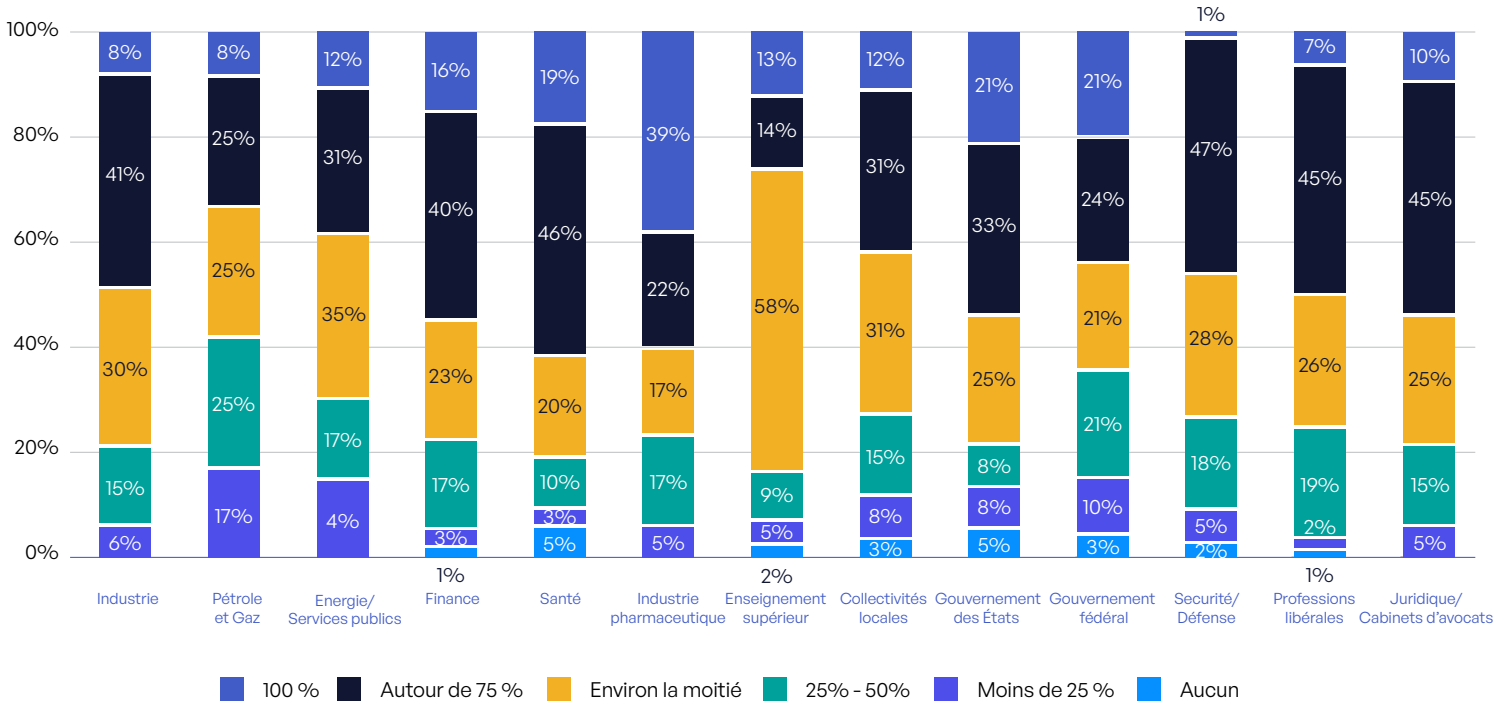


Figure 15: Classification et étiquetage des données non structurées dans les différents secteurs d'activité

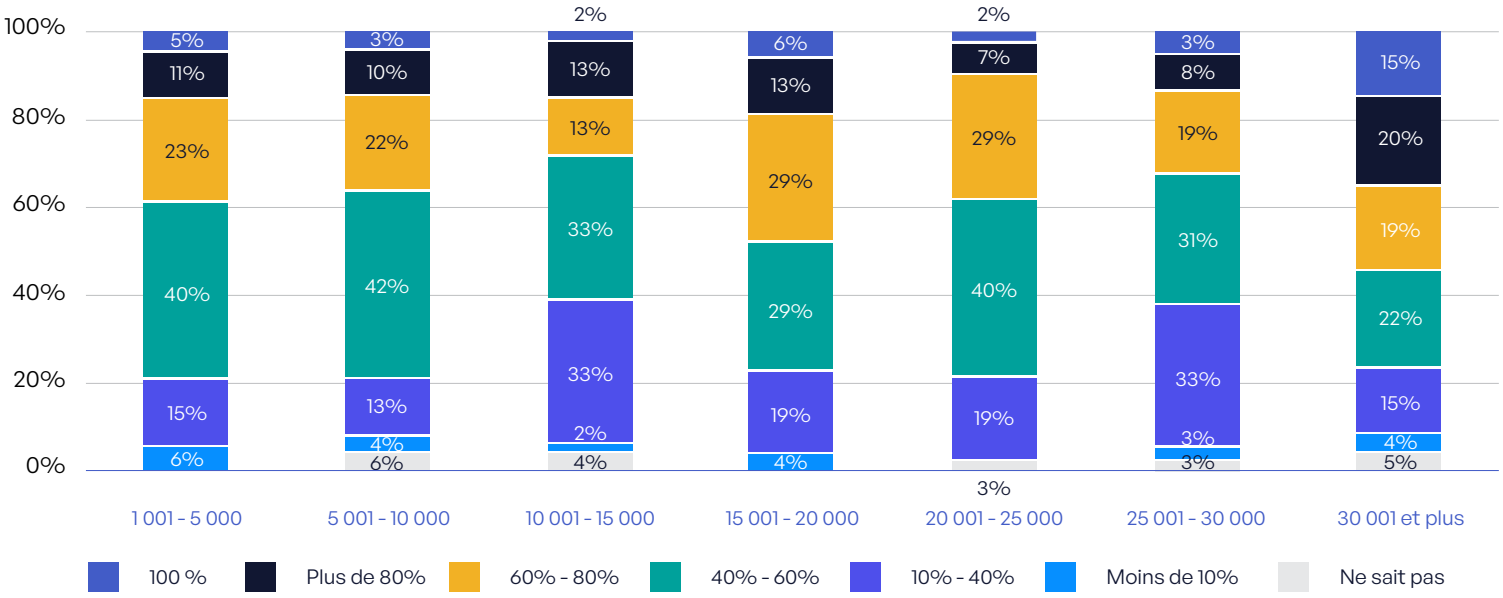


Figure 16: Pourcentage de données non structurées qui est étiqueté et classifié selon la taille de l'organisation

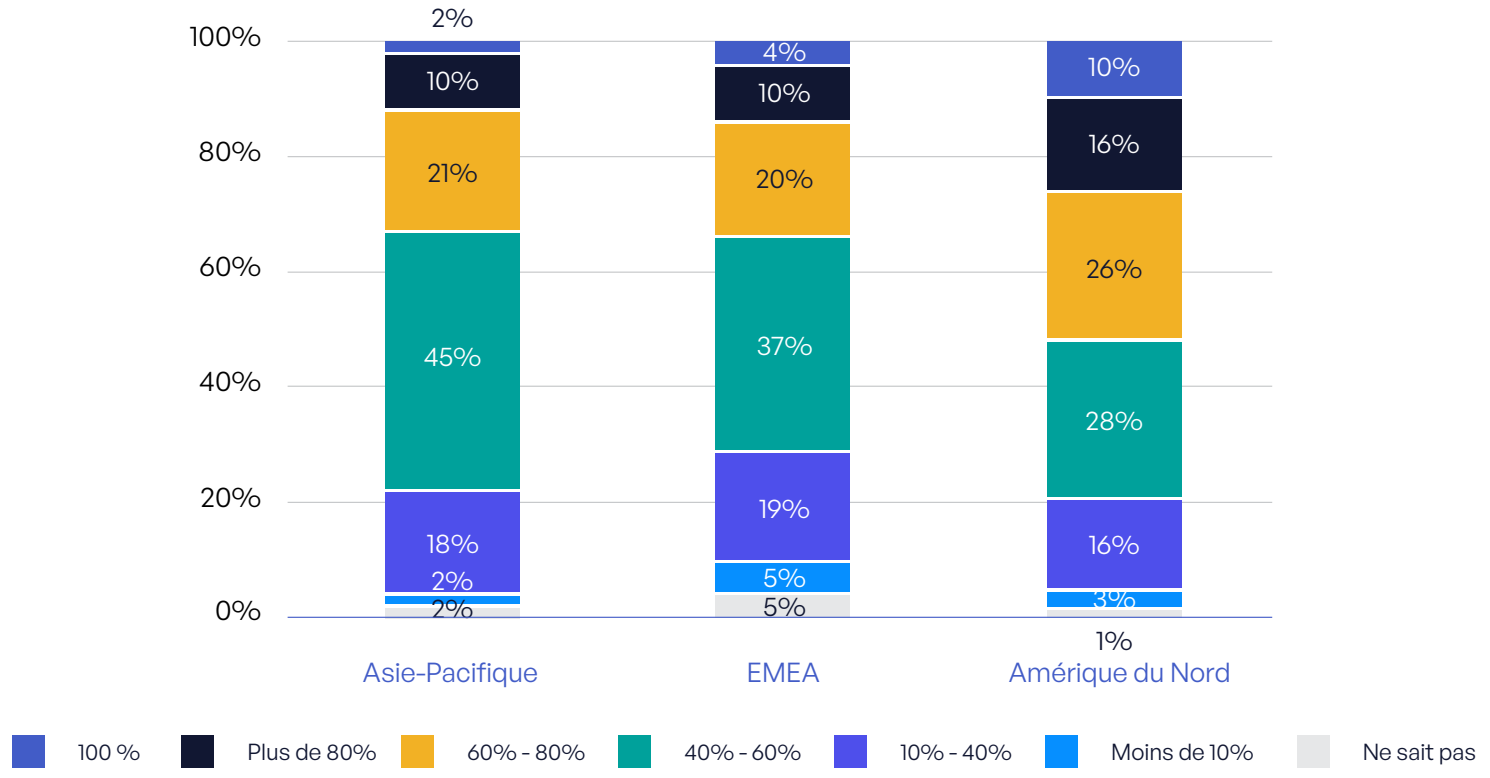


Figure 17: Pourcentage de données non structurées qui est étiqueté et classifié par région

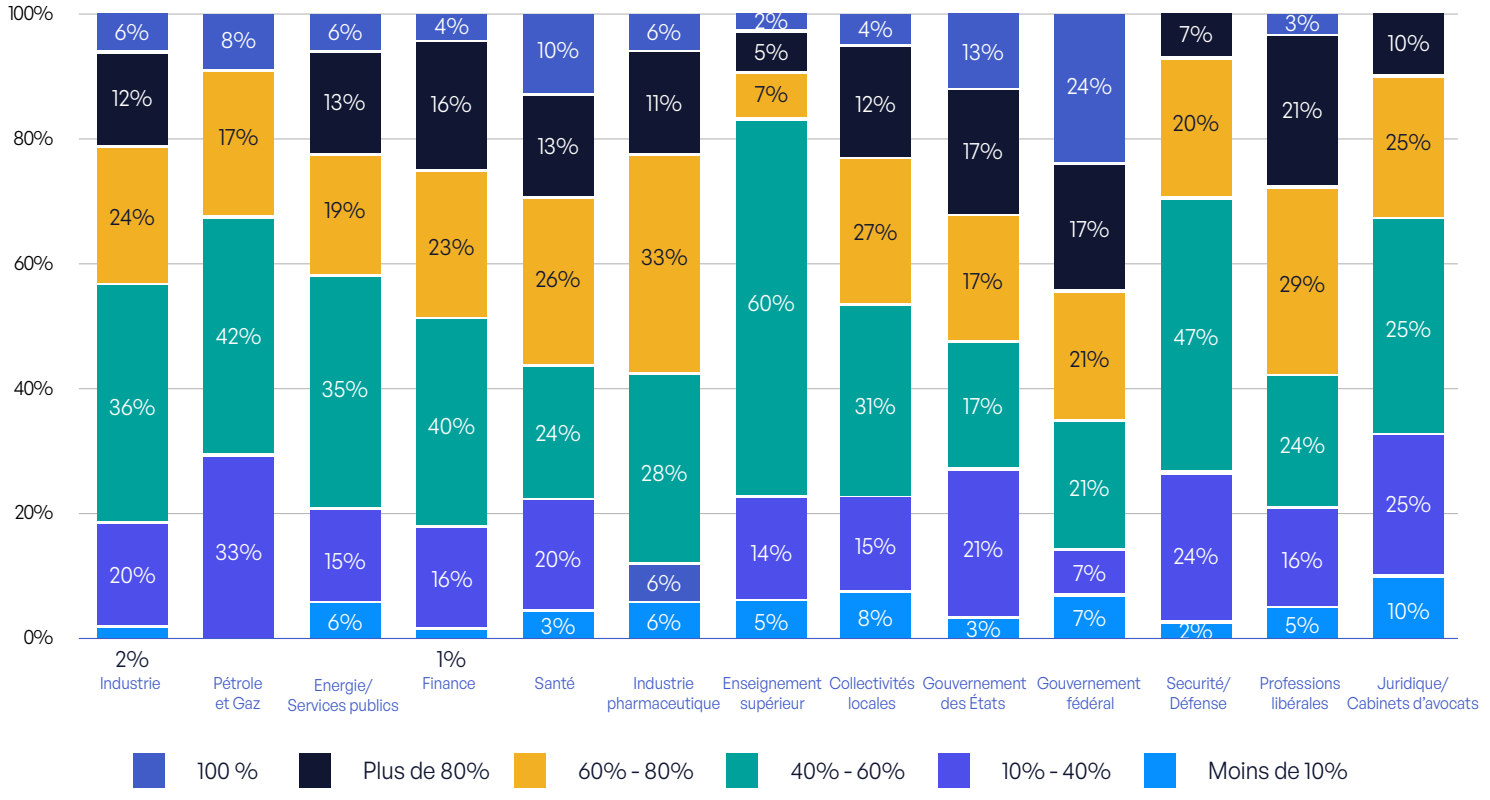


Figure 18: Pourcentage de données non structurées qui est étiqueté et classifié dans les différents secteurs d'activité

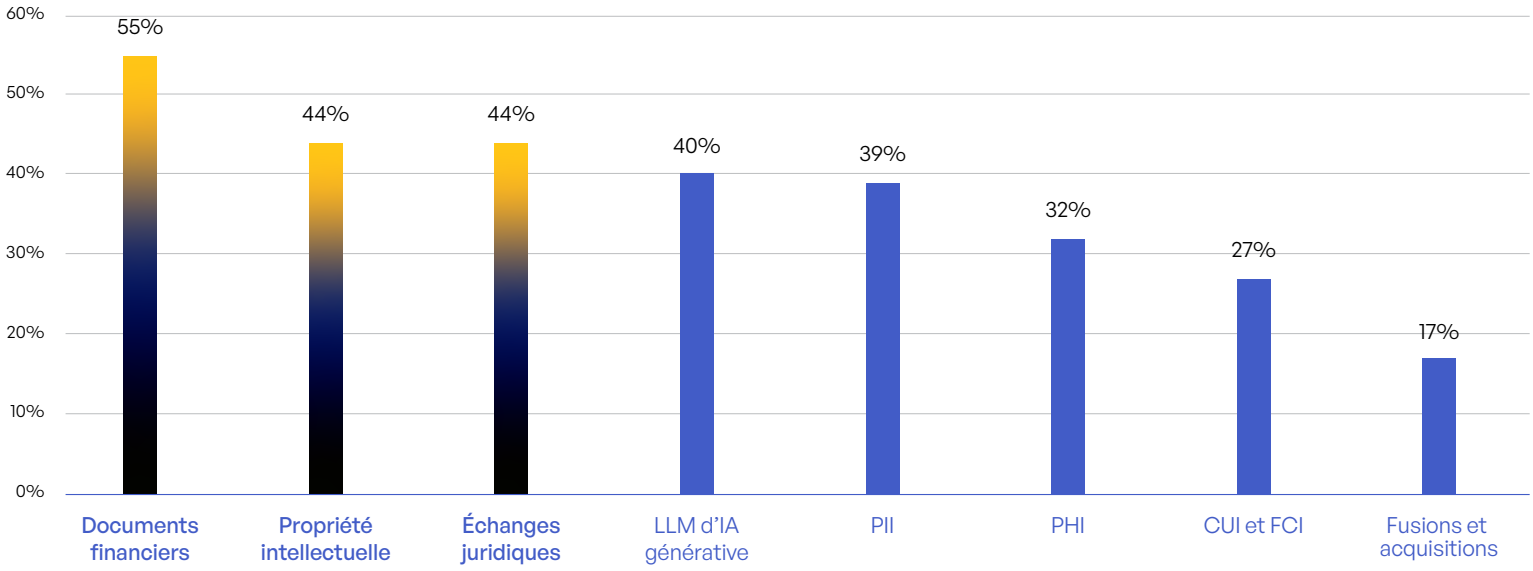


Figure 19: Types de données les plus préoccupantes

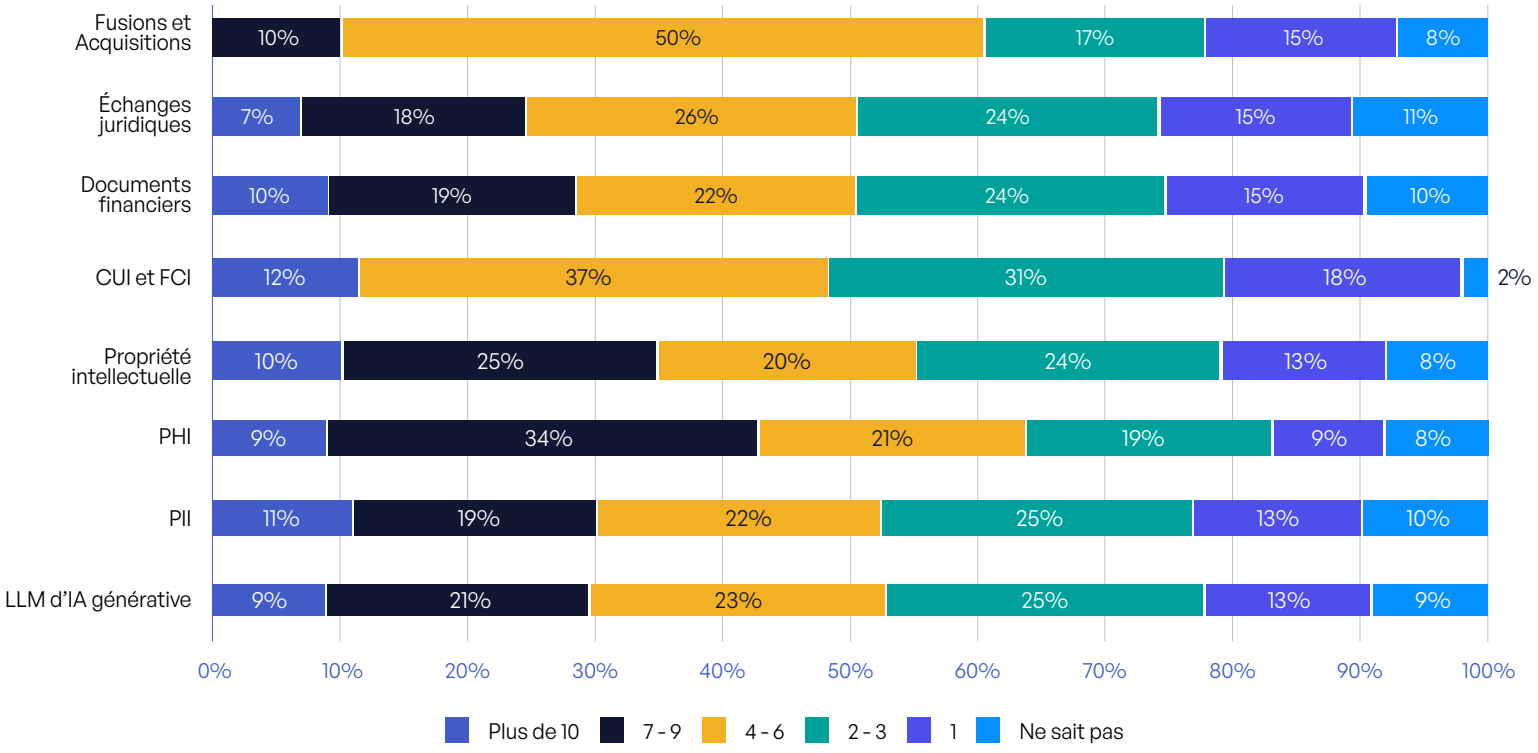


Figure 20: Le nombre de violations de données selon le type de données

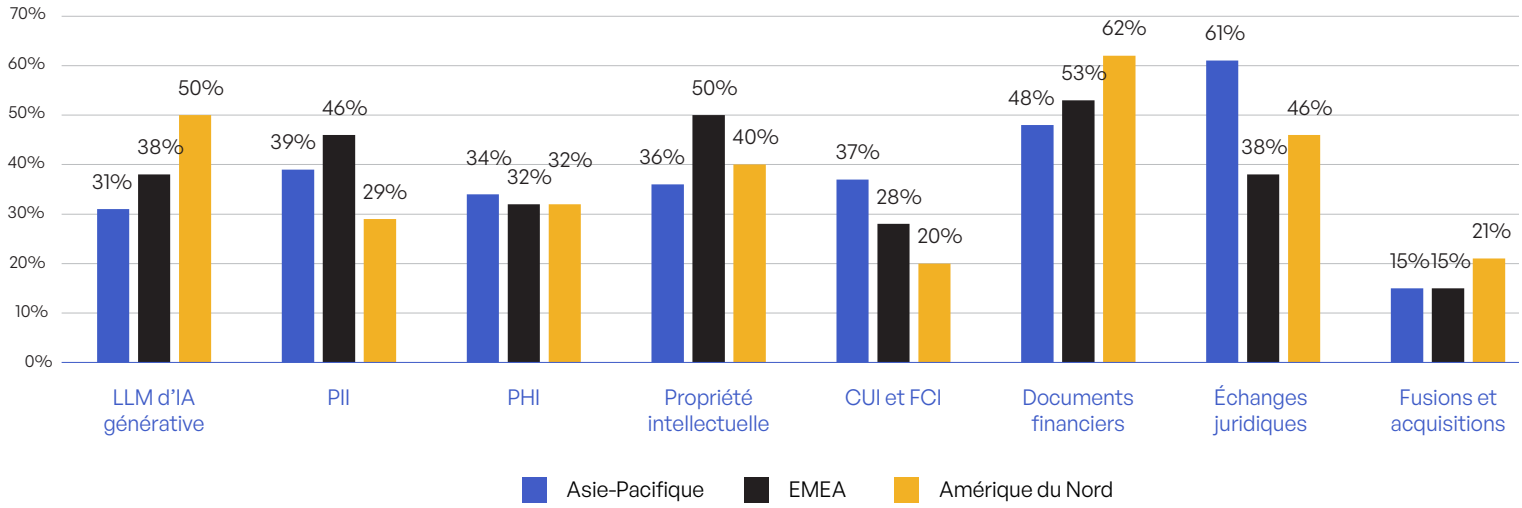


Figure 21: Types de données les plus préoccupantes dans les différentes régions

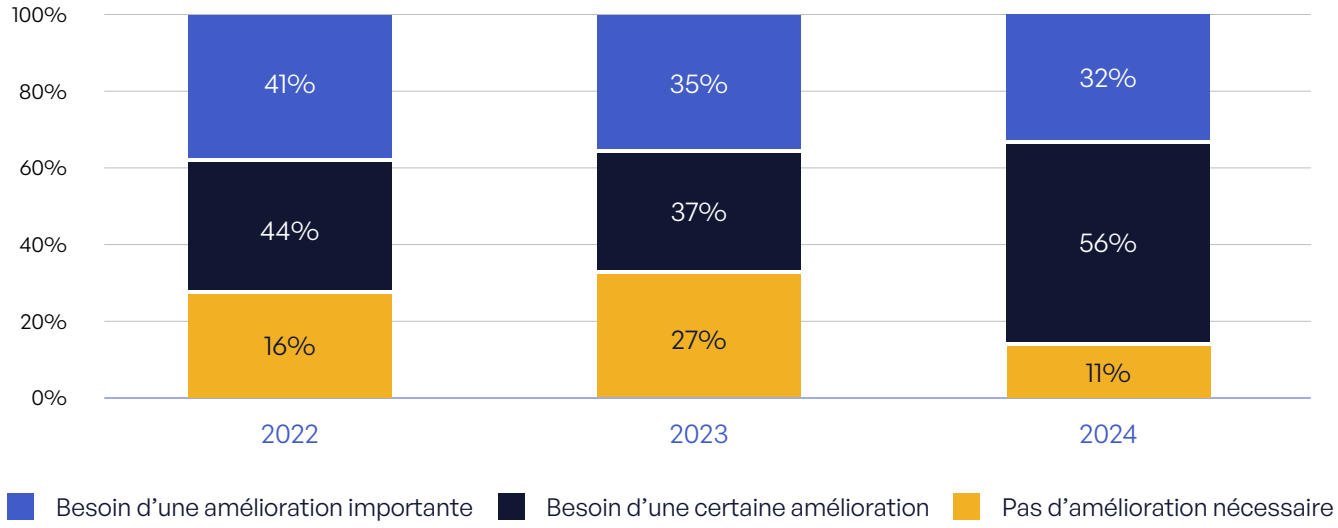


Figure 22: Besoin d'améliorer le management de la conformité des communications

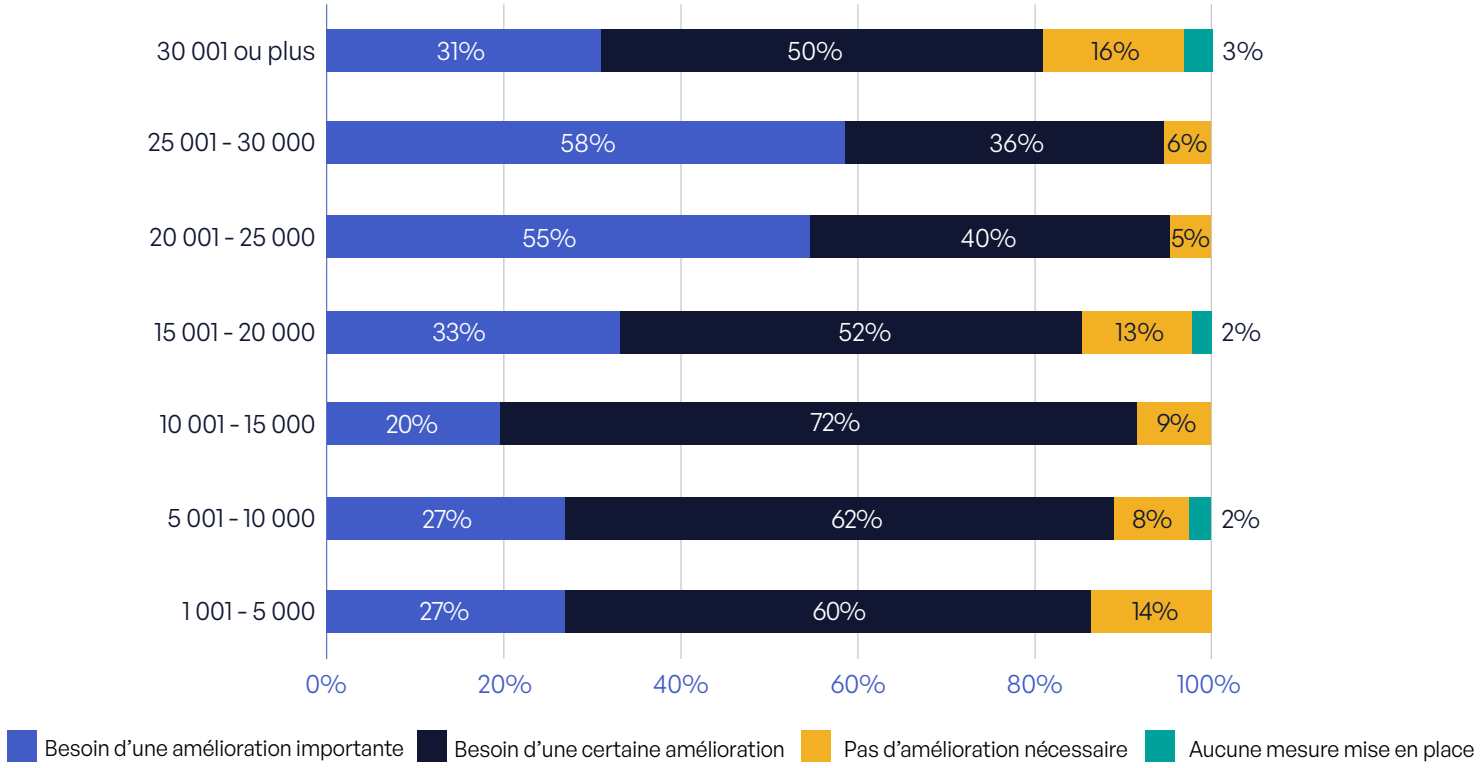


Figure 23: Besoin d'améliorer le management de la conformité des communications selon la taille de l'organisation

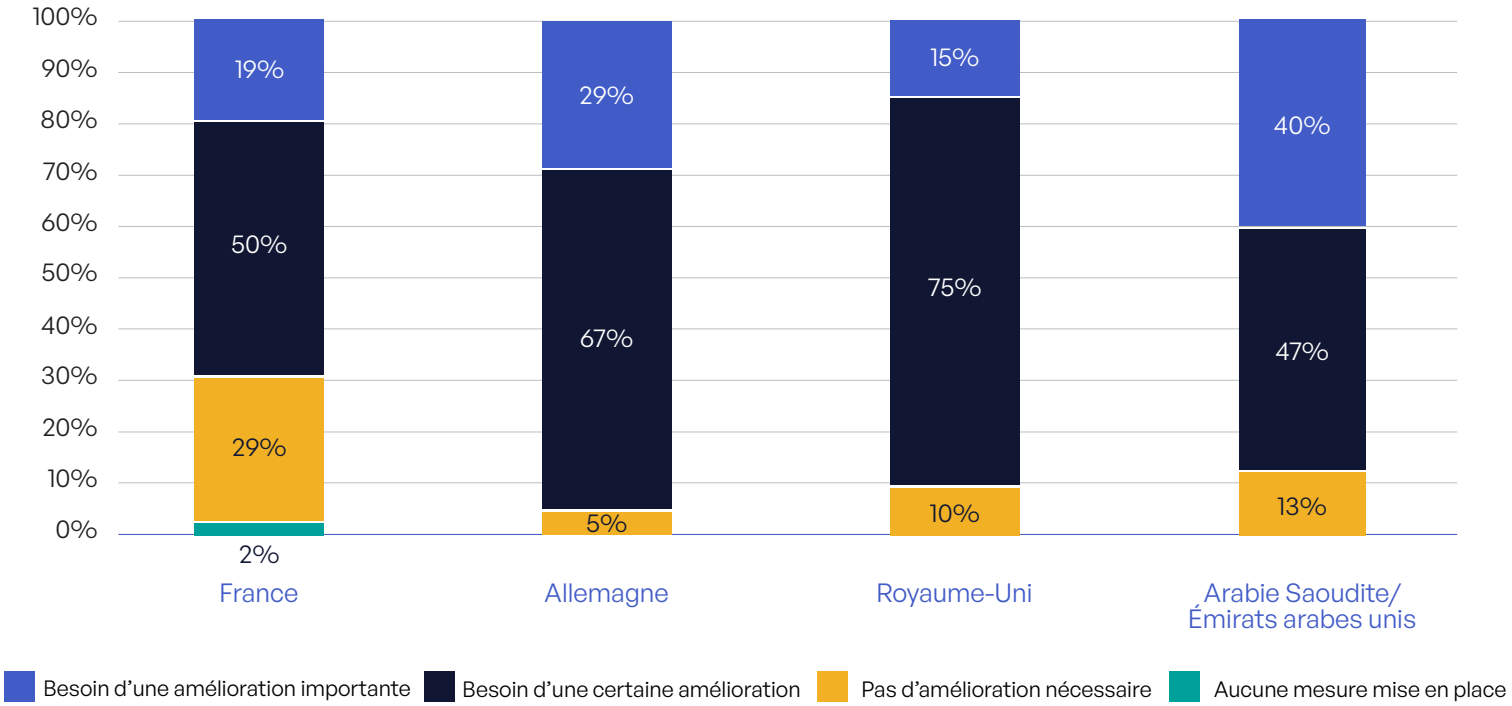


Figure 24: Besoin d'améliorer le management de la conformité des communications dans les différents pays

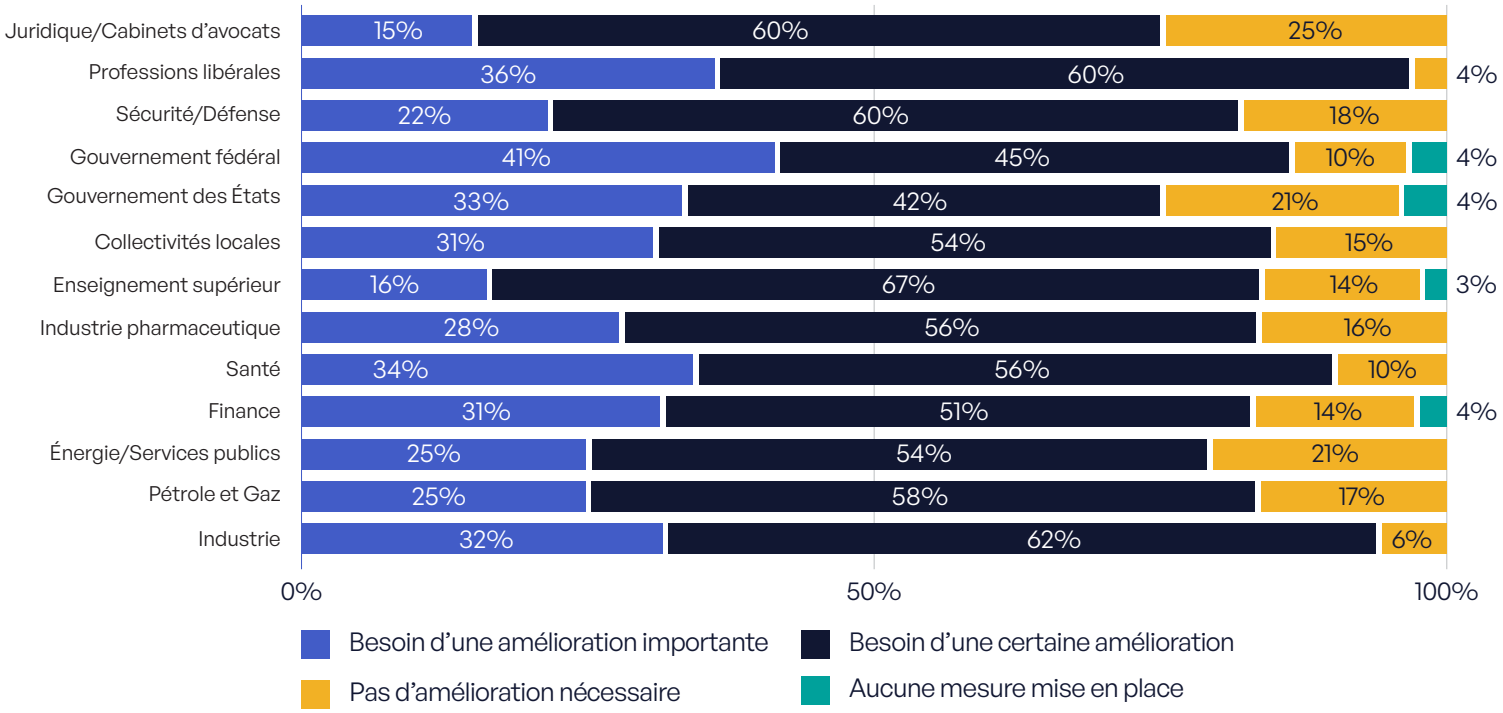


Figure 25: Besoin d'améliorer le management de la conformité des communications dans les différents secteurs d'activité

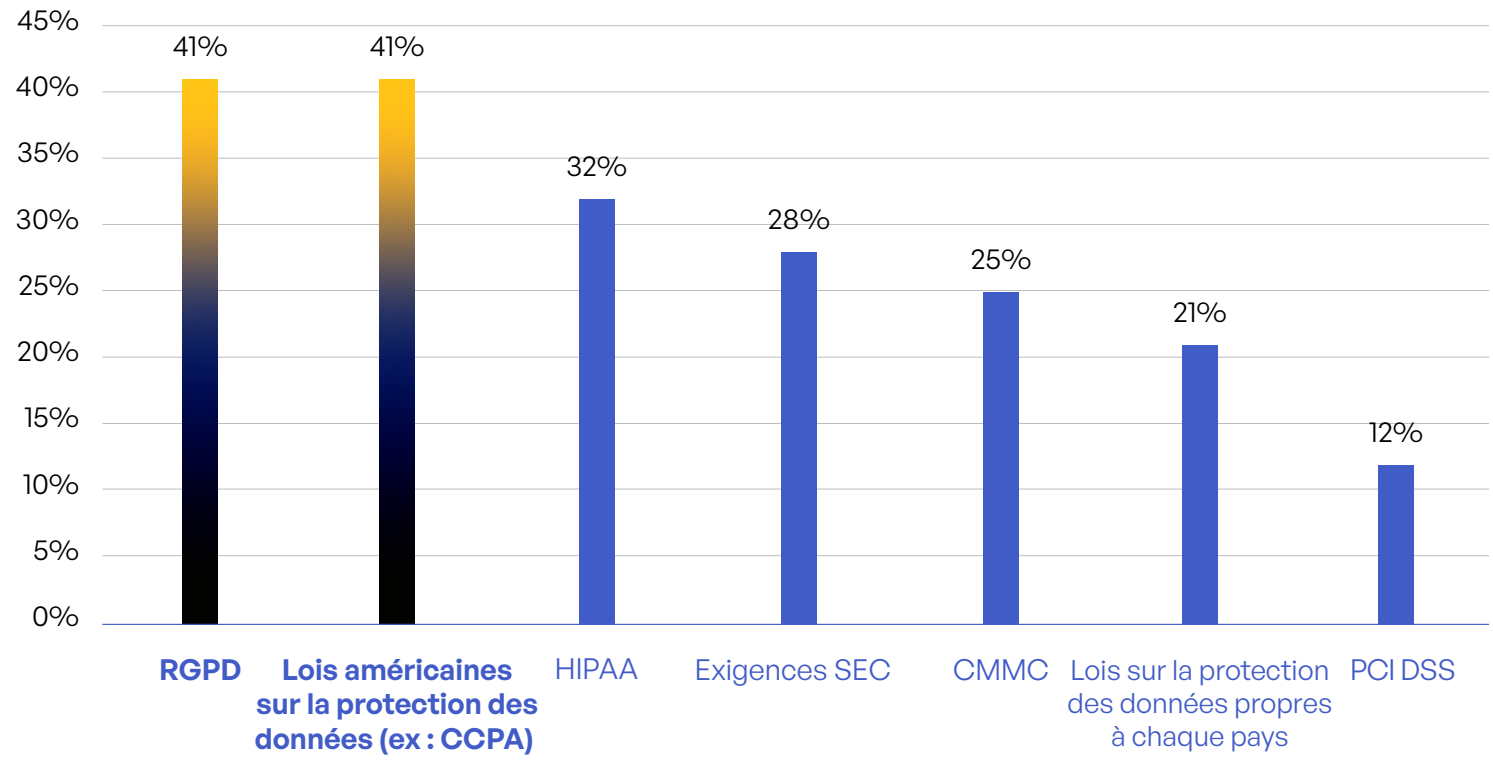


Figure 26: Priorités en termes de confidentialité et de conformité

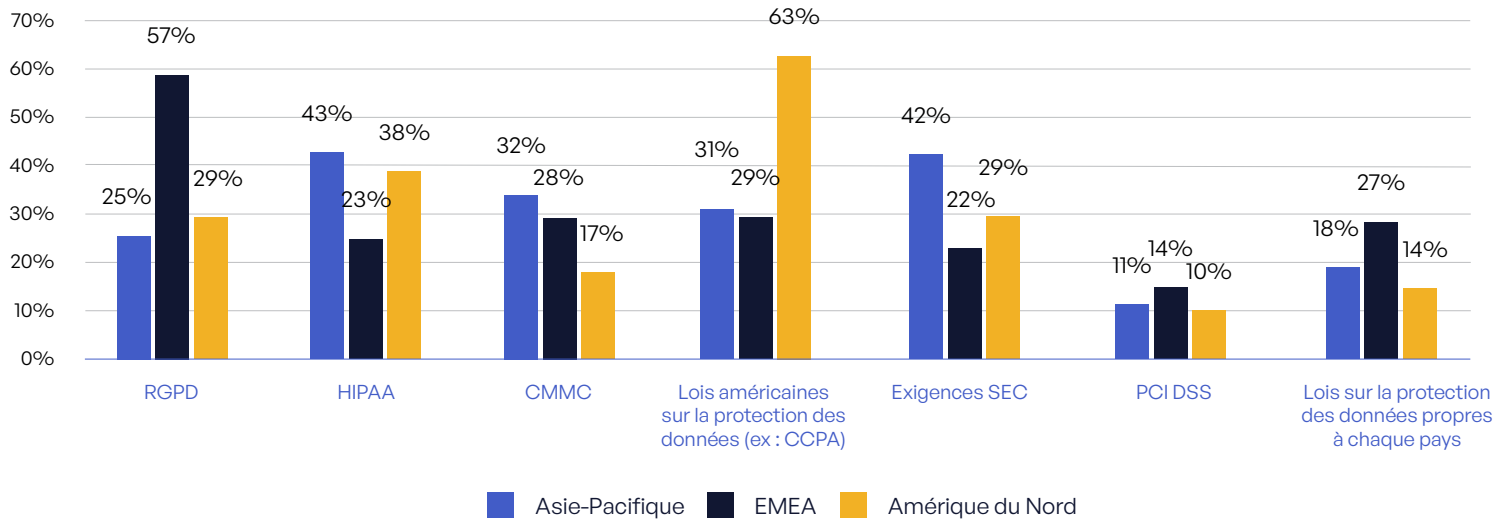


Figure 27: Priorités en termes de confidentialité et de conformité par région

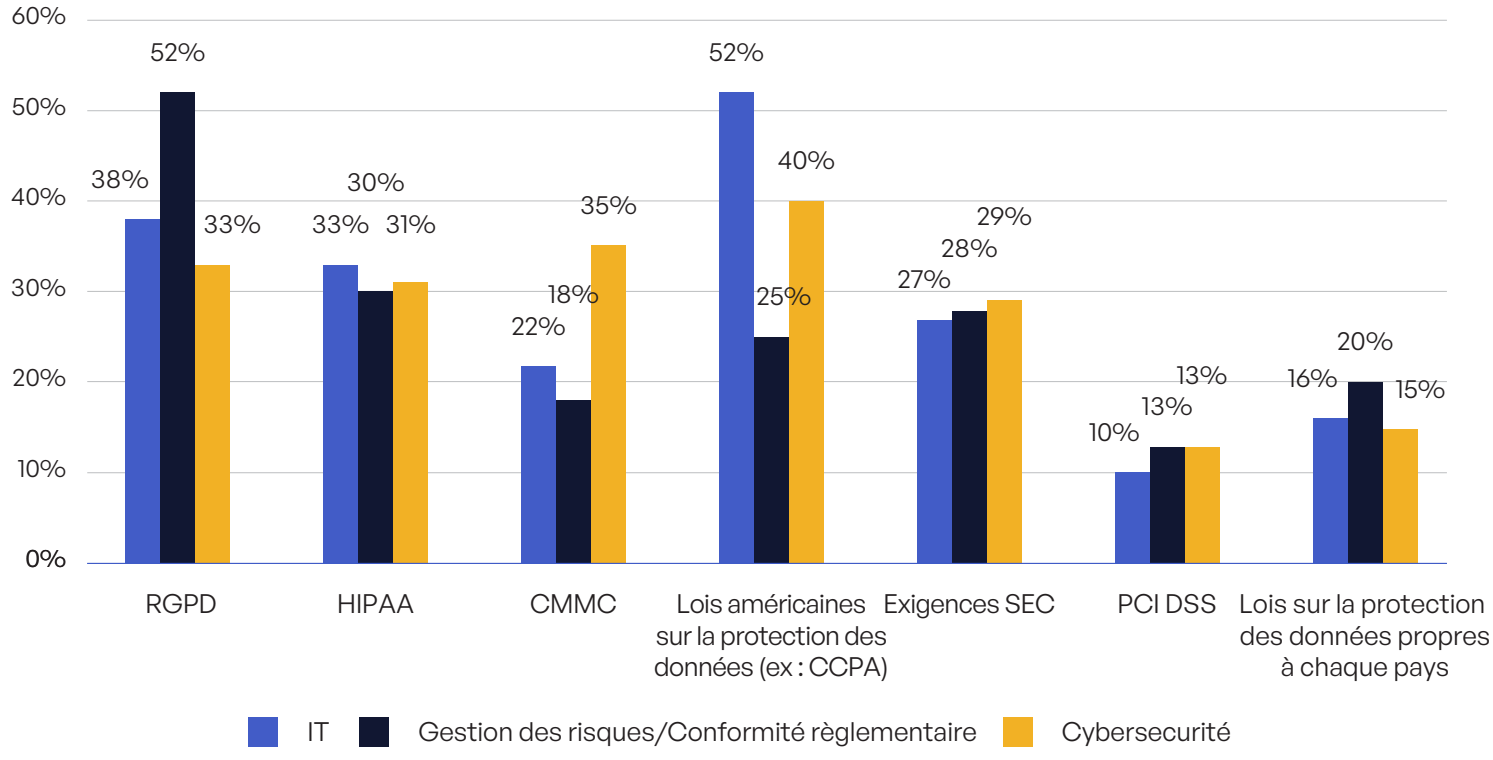


Figure 28: Priorités en termes de confidentialité et de conformité selon le poste occupé par les répondants

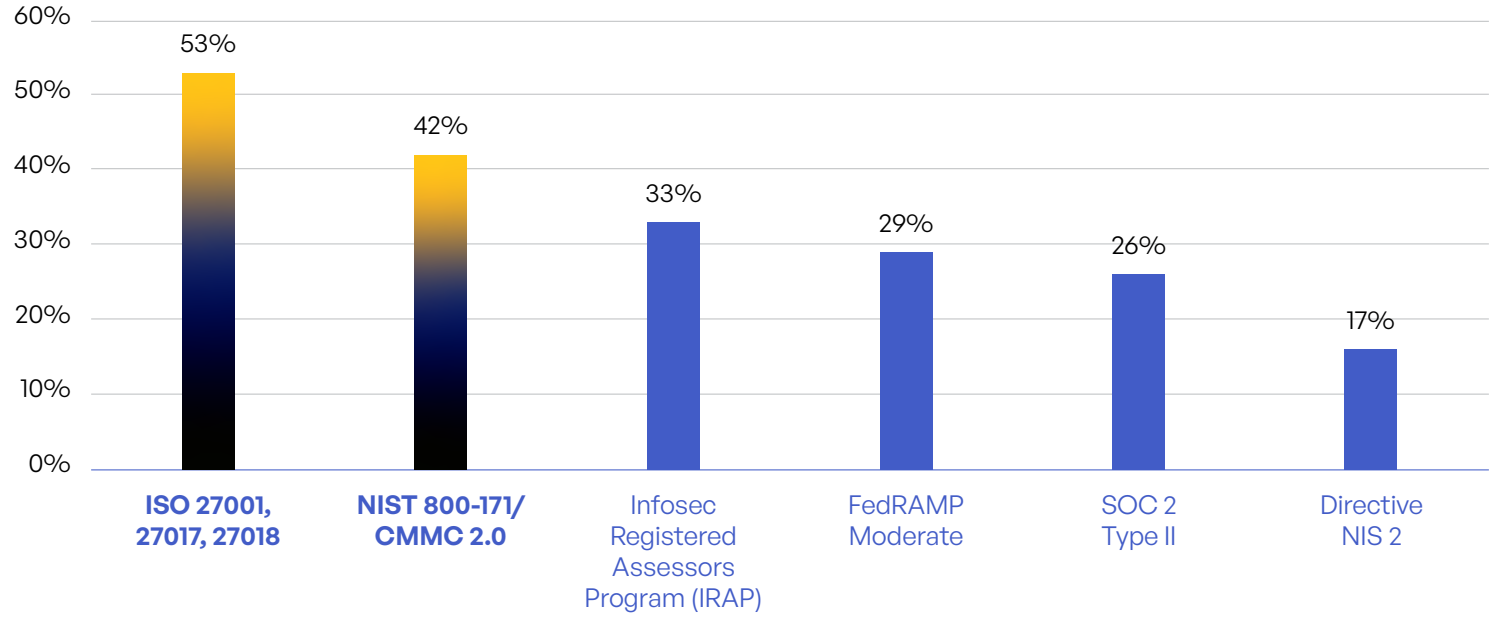


Figure 29: Top 2 des validations et certificats de sécurité les plus importants

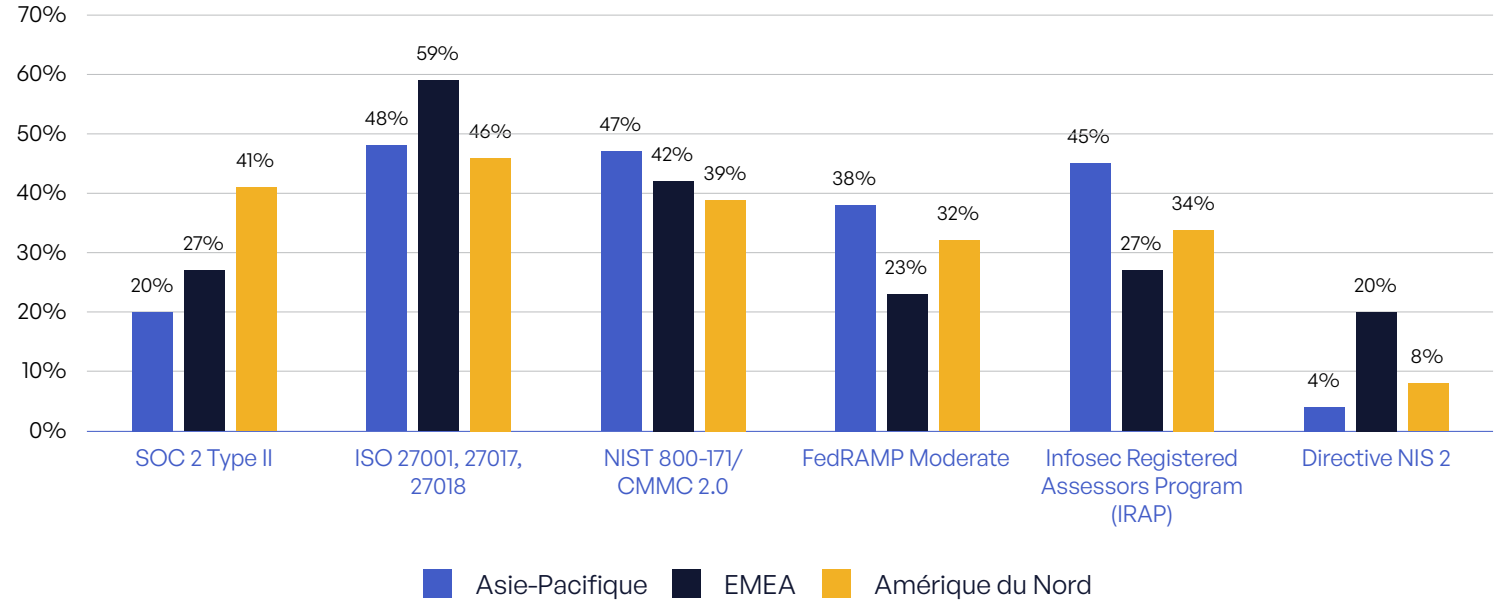


Figure 30: Priorités en termes de validations et certificats de sécurité selon la région

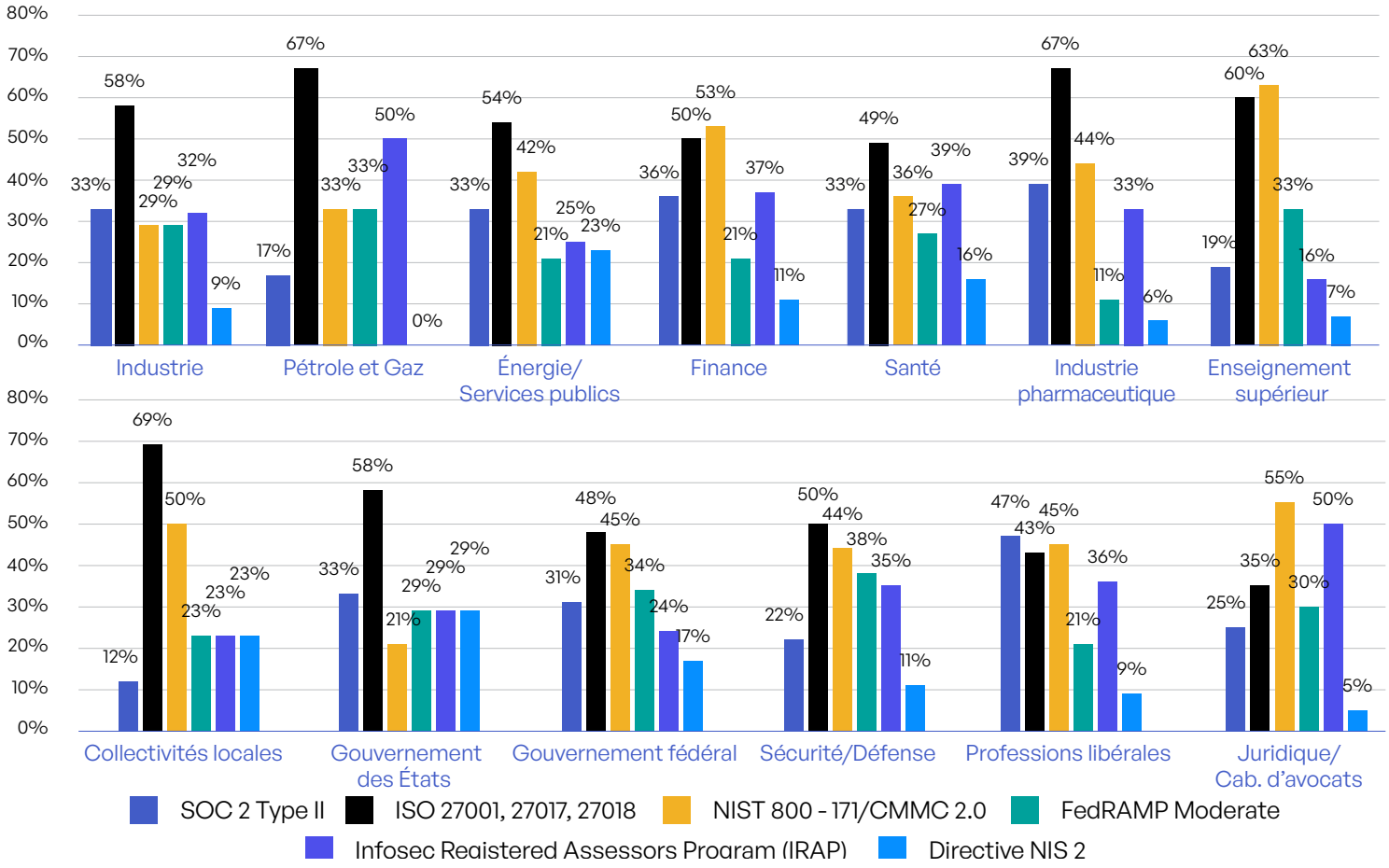


Figure 31: Priorités en termes de validations et certificats de sécurité selon le secteur d'activité

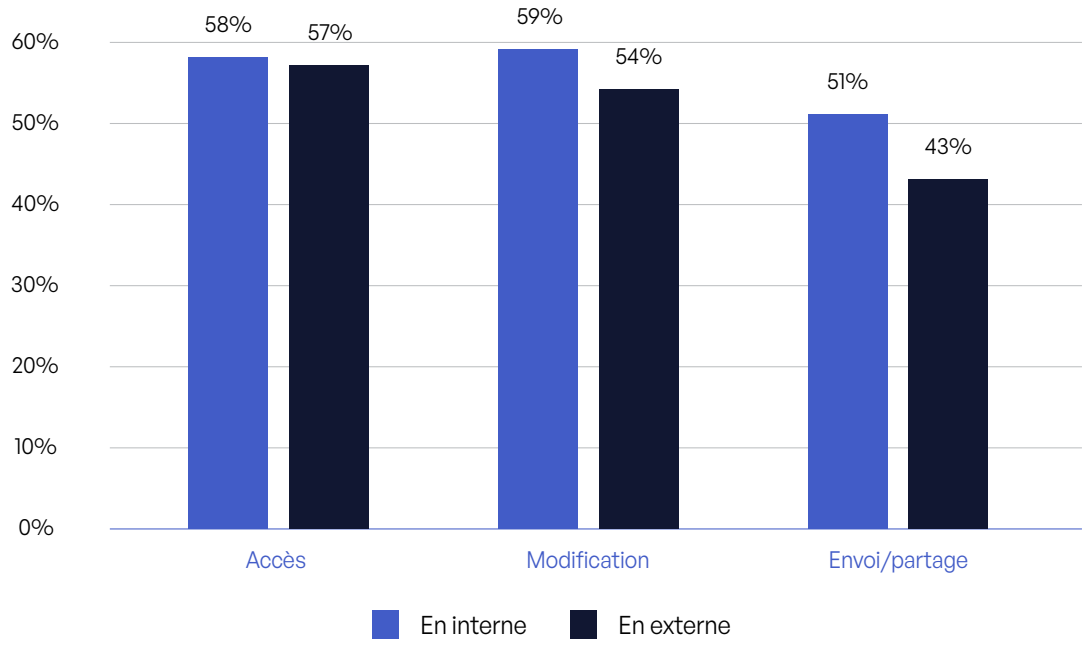


Figure 32: Capacité à suivre, contrôler et tracer les envois et partages de contenu sensible

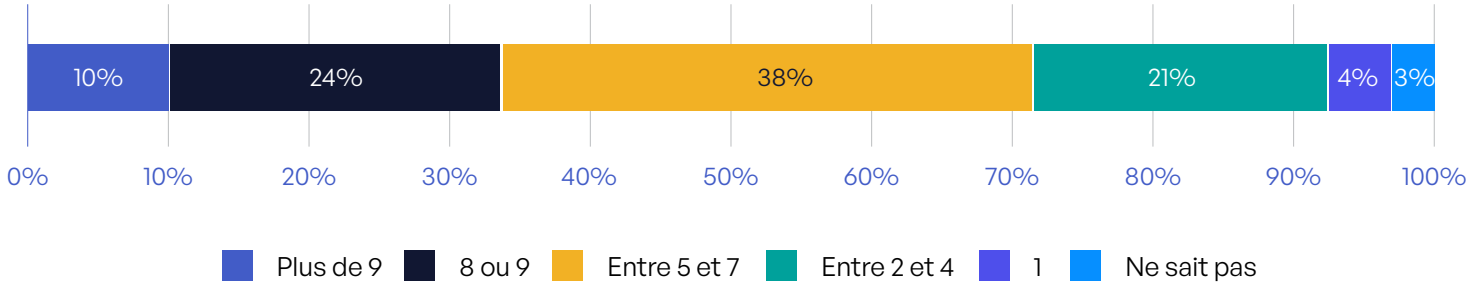


Figure 33: Nombre de rapports d'audit à réconcilier par an

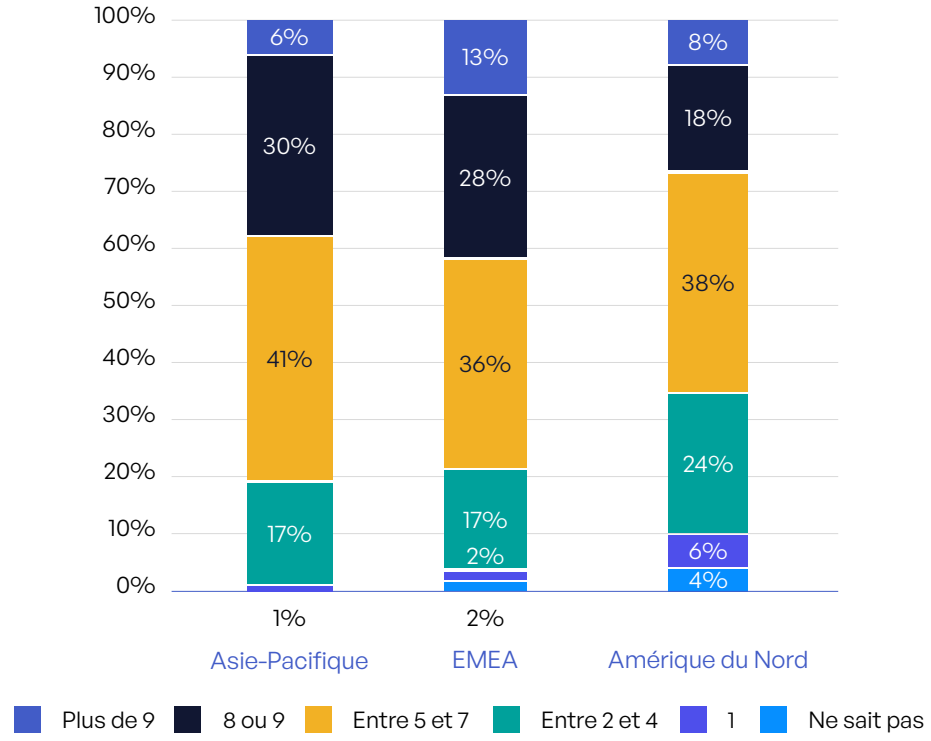


Figure 34: Nombre de rapports d'audit à réconcilier par an selon la région

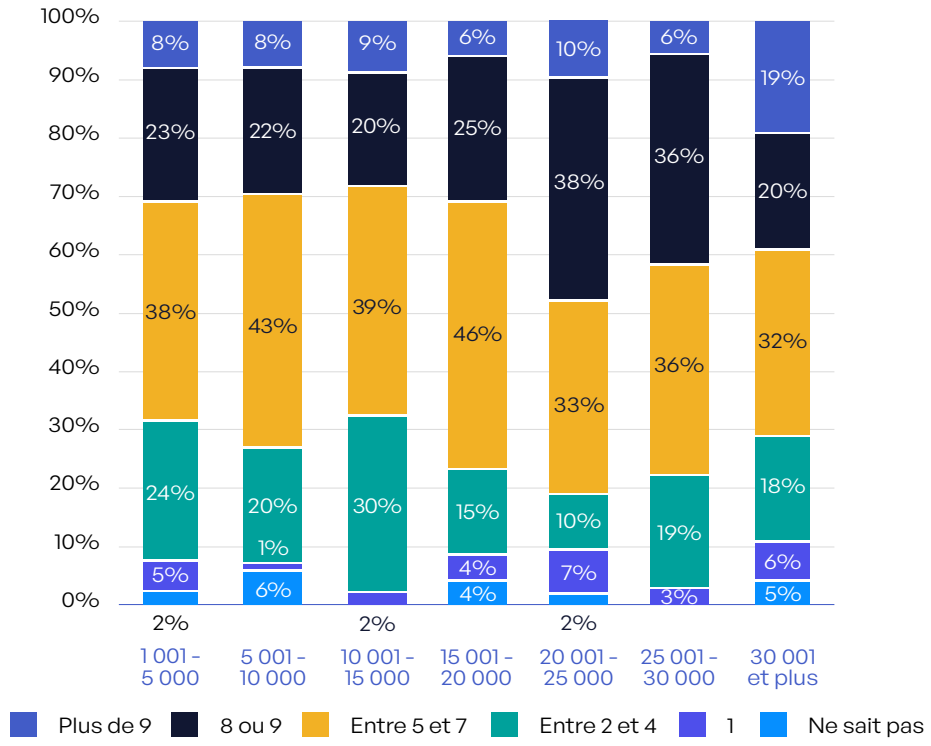


Figure 35: Nombre de rapports d'audit à réconcilier par an selon la taille de l'organisation

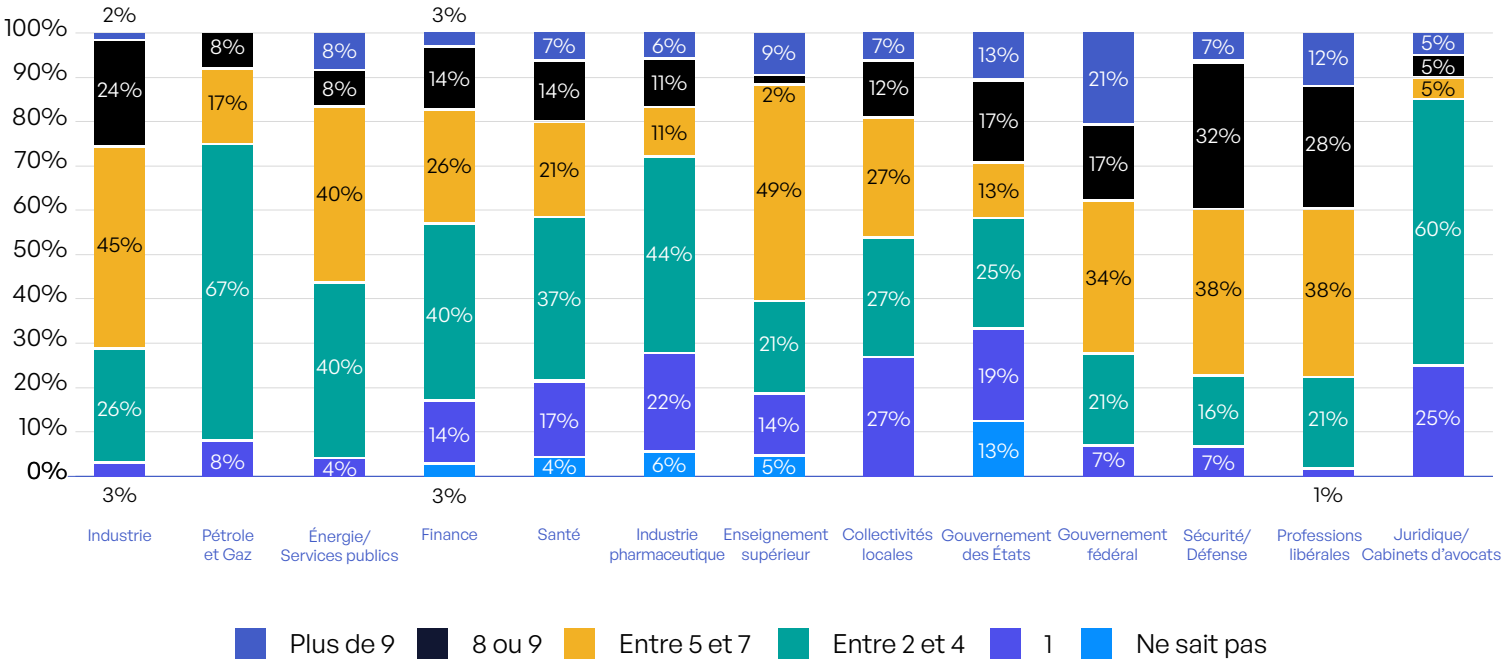


Figure 36: Nombre de rapports d'audit à réconcilier par an selon le secteur d'activité

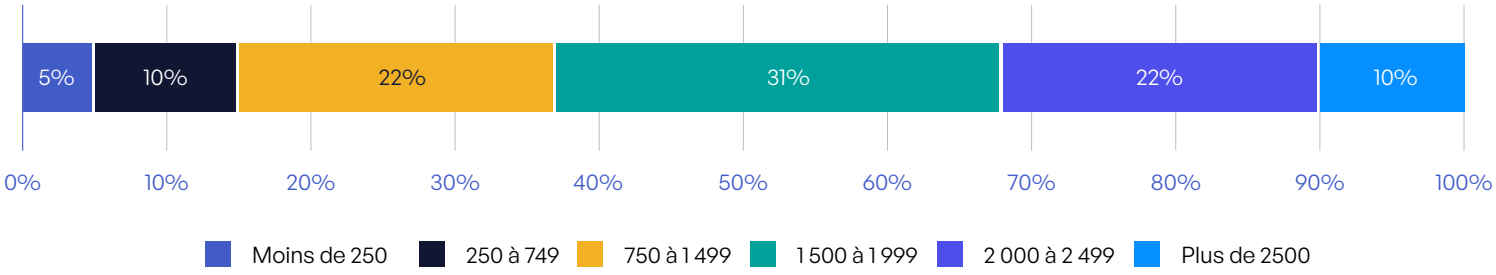


Figure 37: Nombre d'heures passées par an à compiler des rapports d'audit

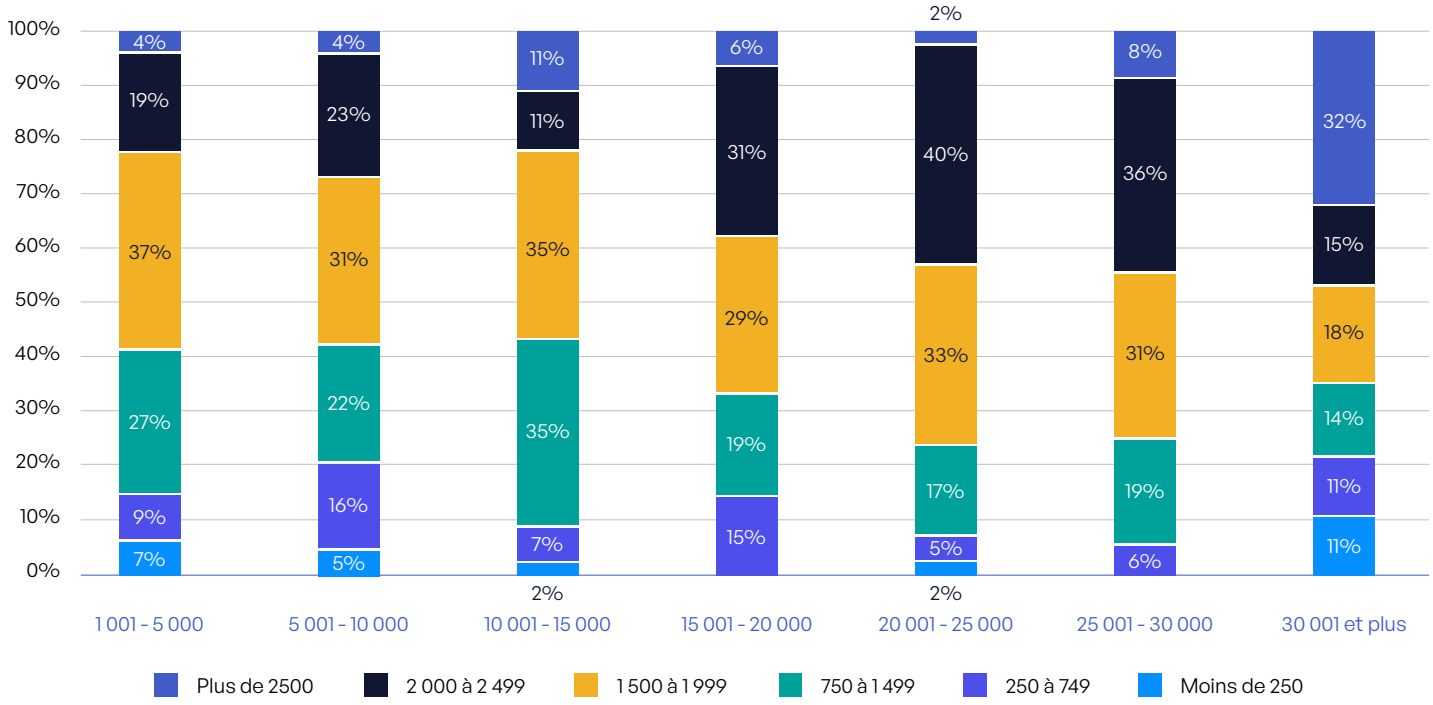


Figure 38: Nombre d'heures passées par an à compiler des rapports d'audit selon la taille de l'organisation

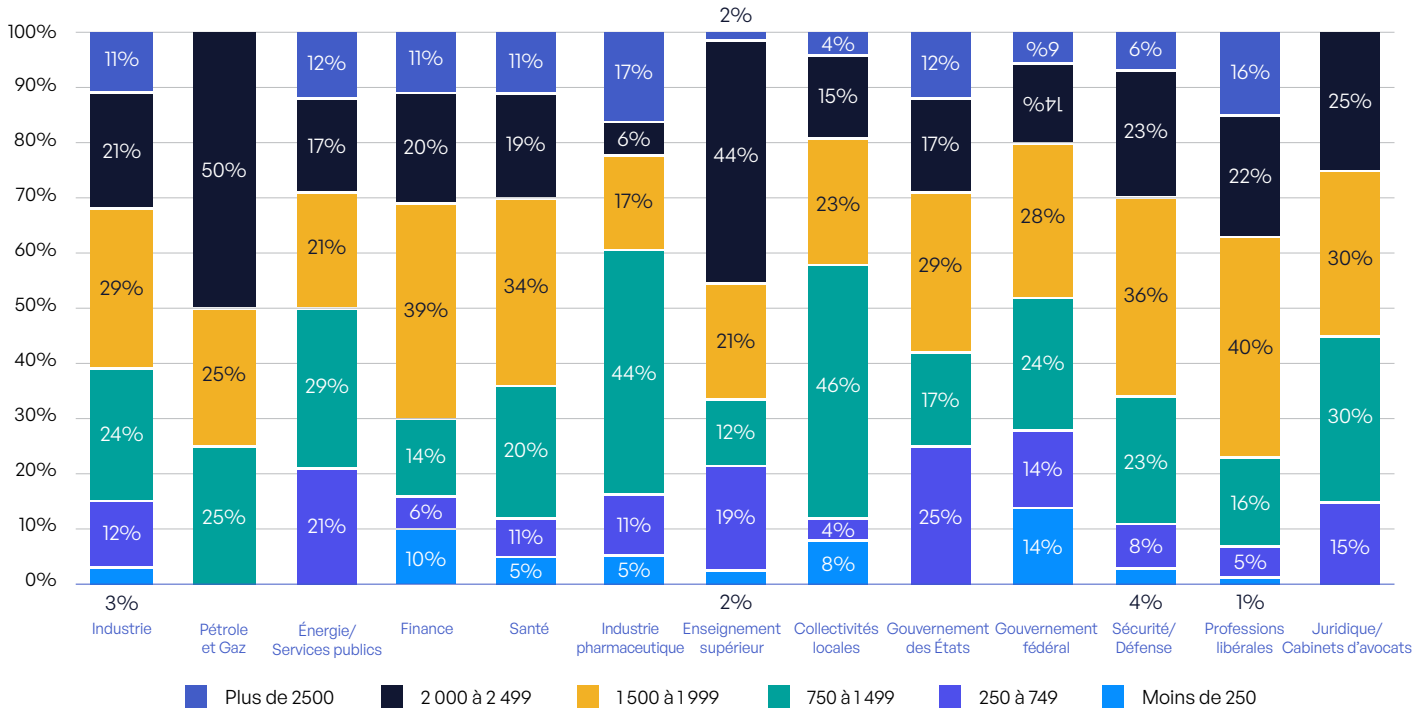


Figure 39: Nombre d'heures passées par an à compiler des rapports d'audit dans les différents secteurs d'activité

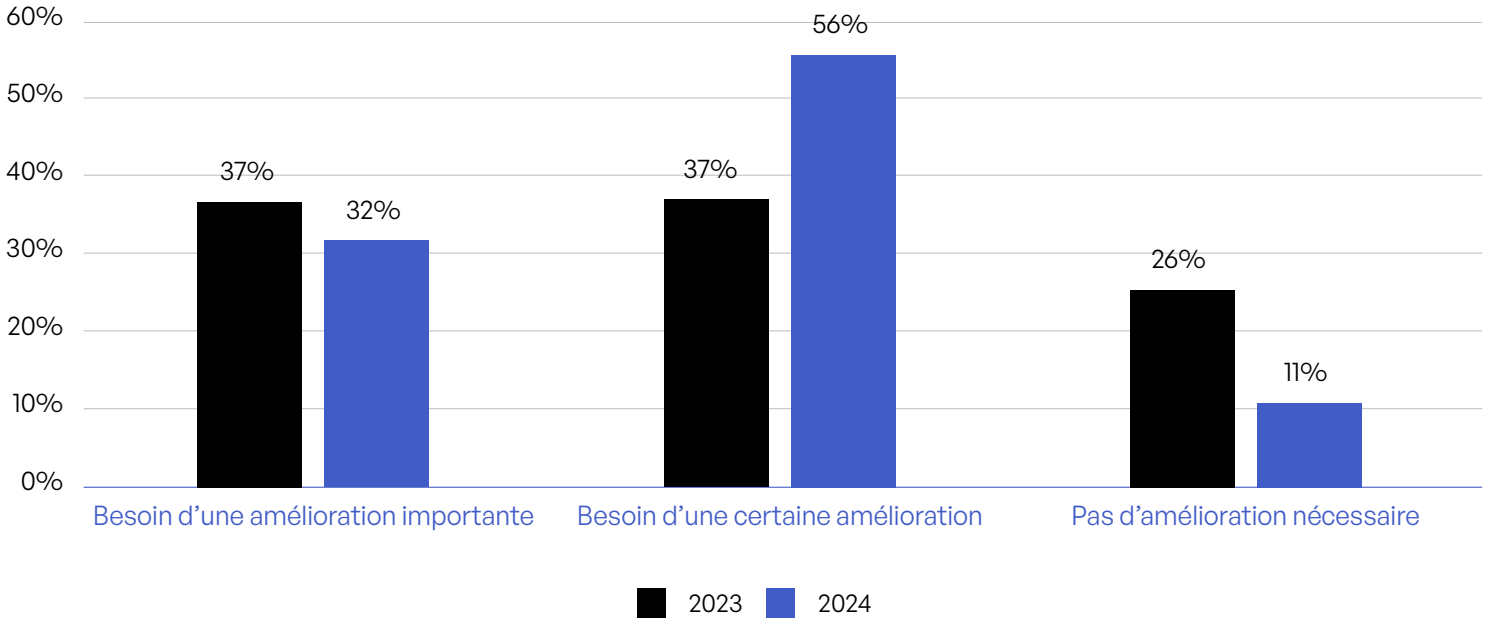


Figure 40: Besoin d'améliorer le management des risques associés aux communications sensibles

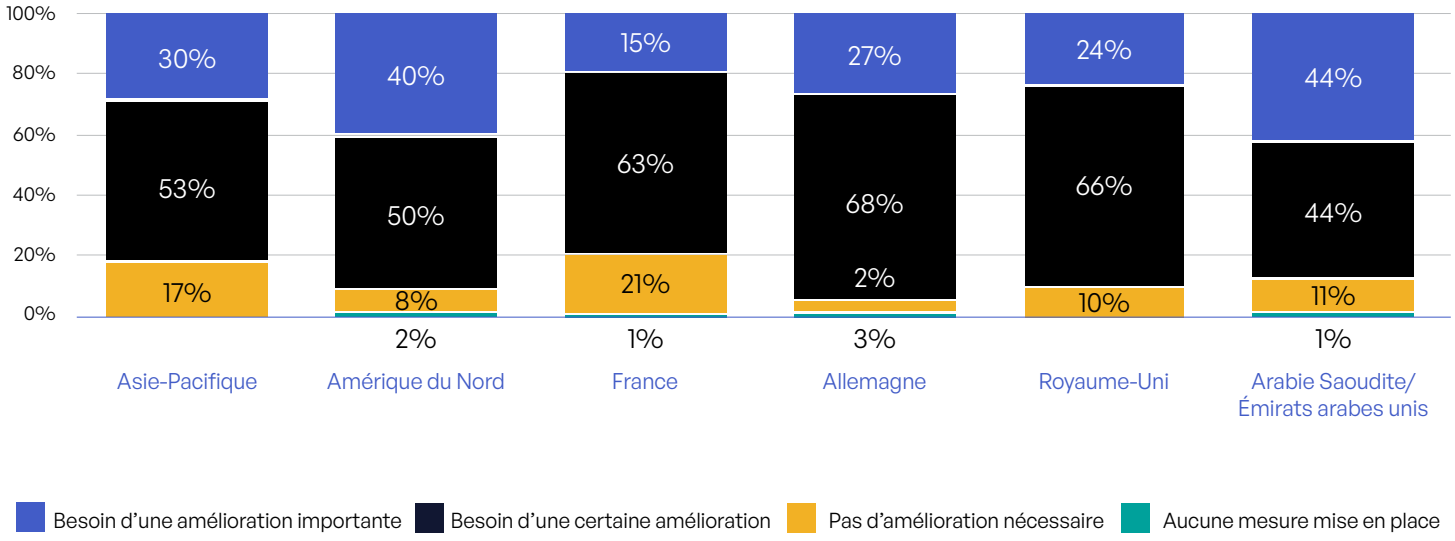


Figure 41: Besoin d'améliorer le management des risques associés aux communications sensibles dans les différentes régions et pays d'EMEA

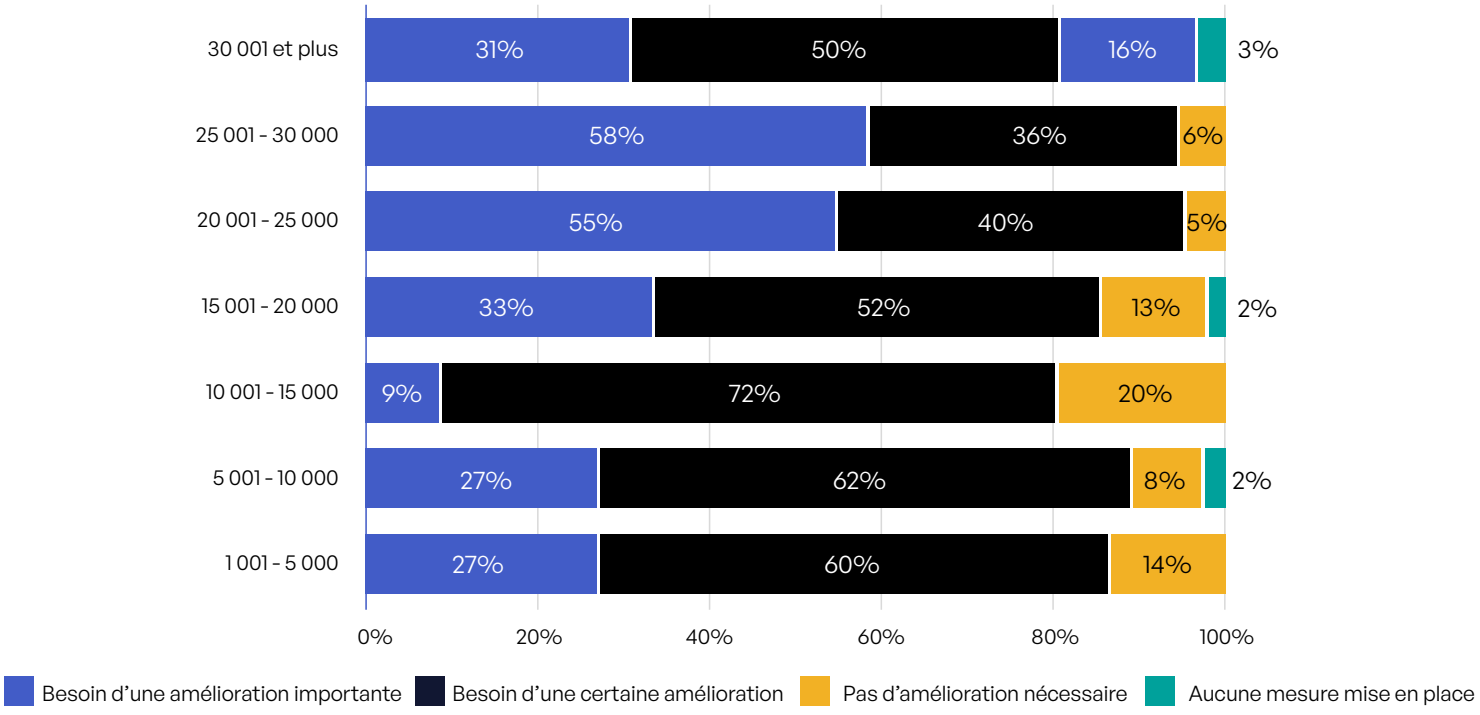


Figure 42: Besoin d'améliorer le management des risques associés aux communications sensibles selon la taille de l'organisation

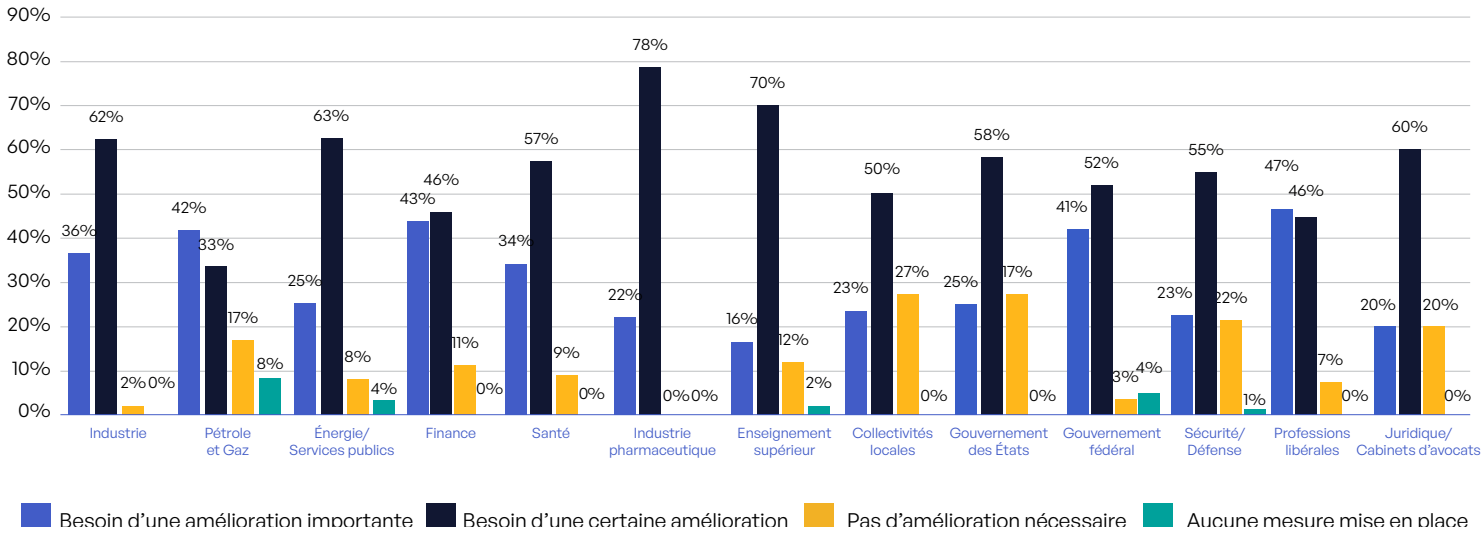


Figure 43: Besoin d'améliorer le management des risques associés aux communications sensibles dans les différents secteurs d'activité

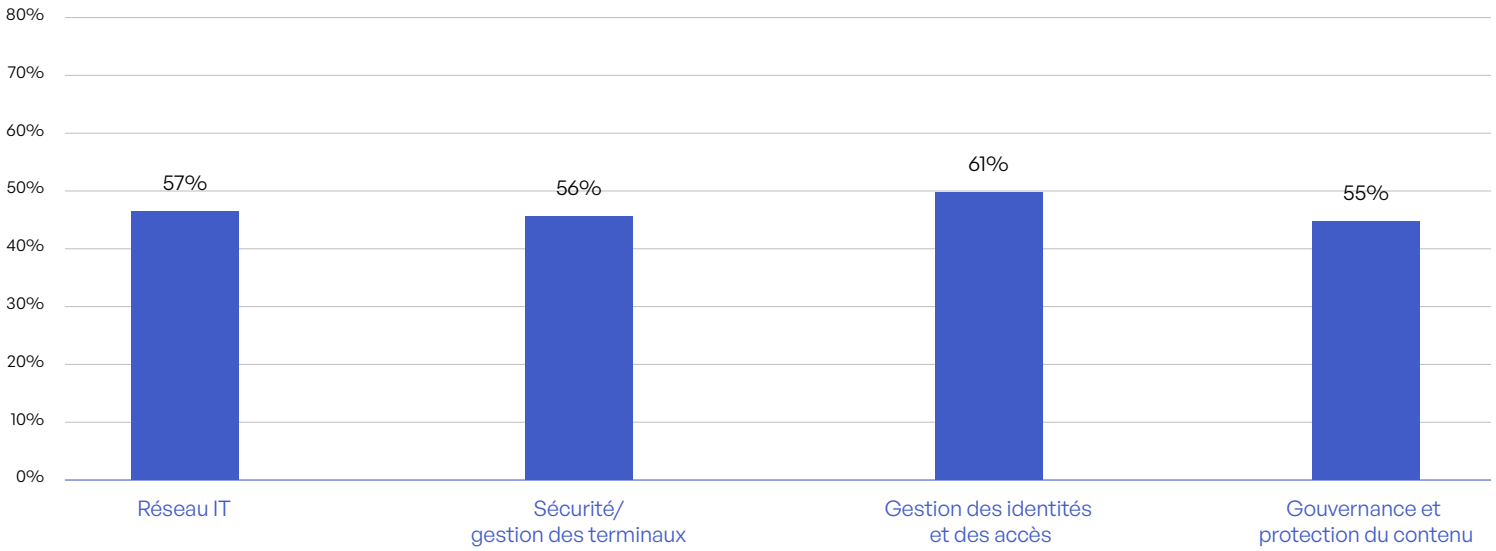


Figure 44: Périmètres pour lesquels le zéro trust est totalement instauré

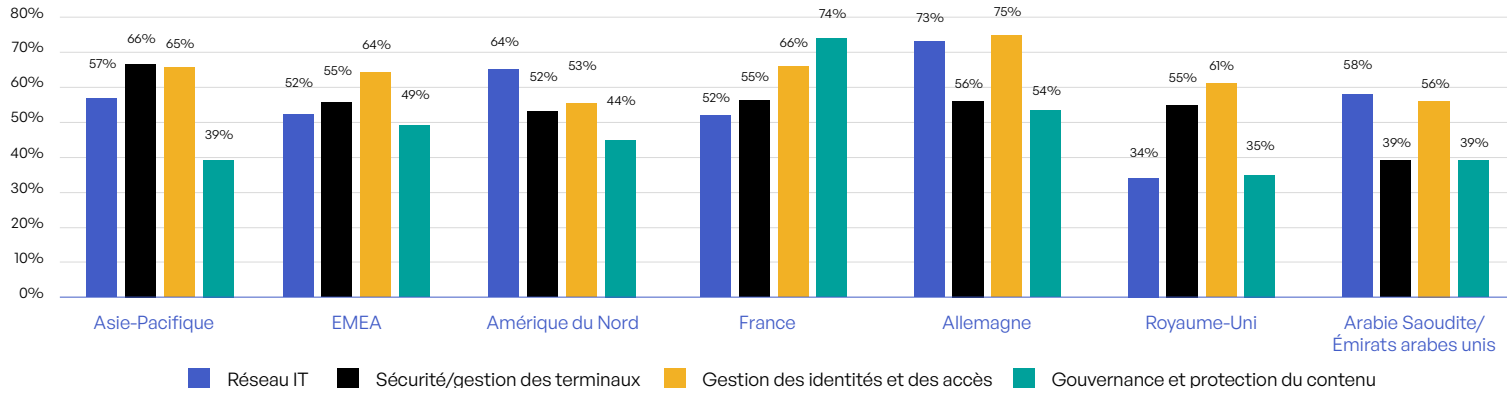


Figure 45: Zéro trust par région et pays d'EMEA

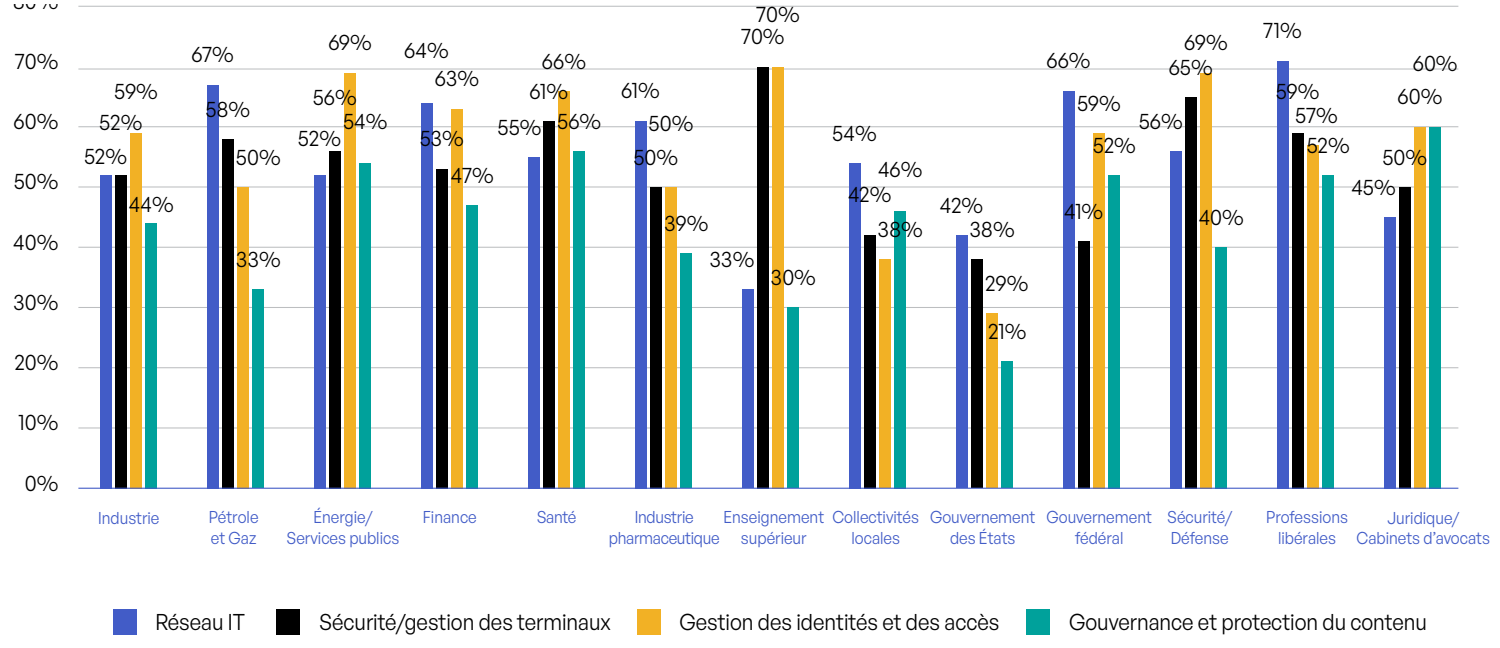


Figure 46: Périmètres pour lesquels le zéro trust est totalement instauré dans les différents secteurs d'activité

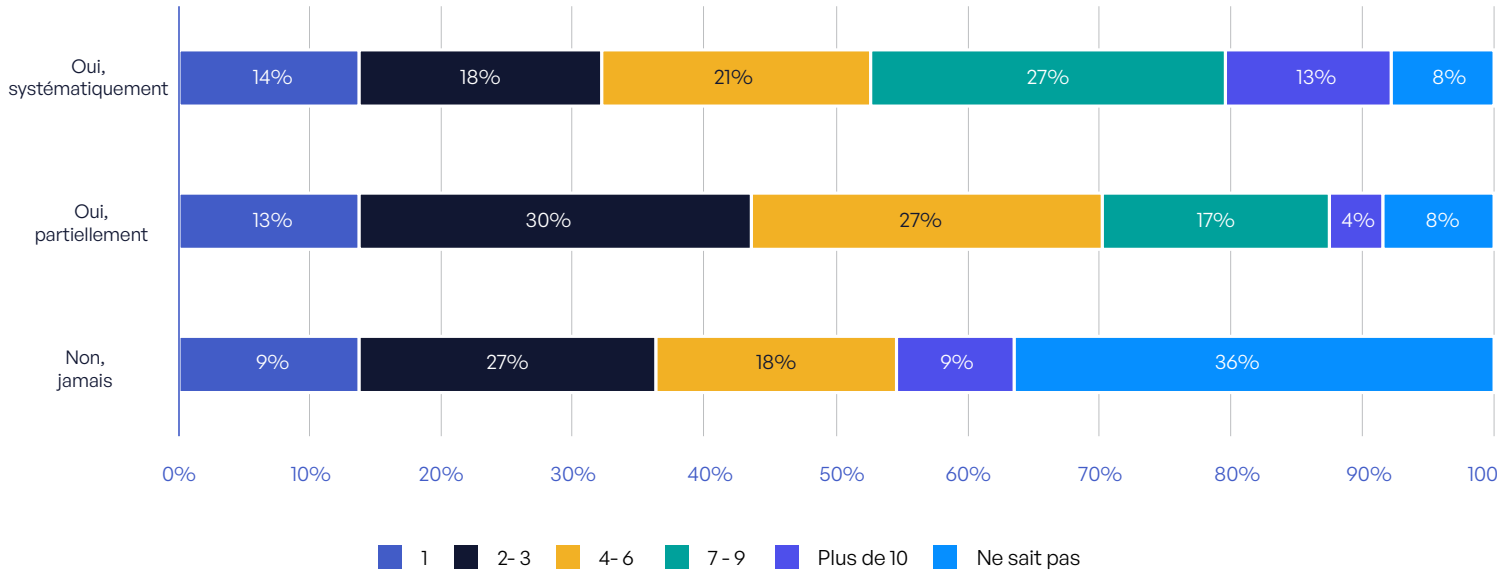


Figure 47: Nombre de violations de données en fonction de l'utilisation des outils de sécurité avancés pour les communications sensibles

	Industrie	Pétrole et Gaz	Énergie/ Services publics	Finance	Santé	Industrie pharmaceutique	Enseignement supérieur	Collectivités locales	Gouvernement des États	Gouvernement fédéral	Sécurité/ Défense	Professions libérales	Juridique/ Cabinets d'avocats
Oui, systématiquement	58%	58%	58%	60%	56%	61%	65%	50%	71%	52%	55%	71%	45%
Oui, partiellement	42%	42%	40%	36%	44%	39%	28%	50%	25%	45%	45%	28%	50%
Non, jamais	0%	0%	2%	4%	0%	0%	7%	0%	4%	3%	0%	2%	5%

Figure 48: Capacité à suivre et à contrôler les contenus sensibles une fois qu'ils ont quitté une application

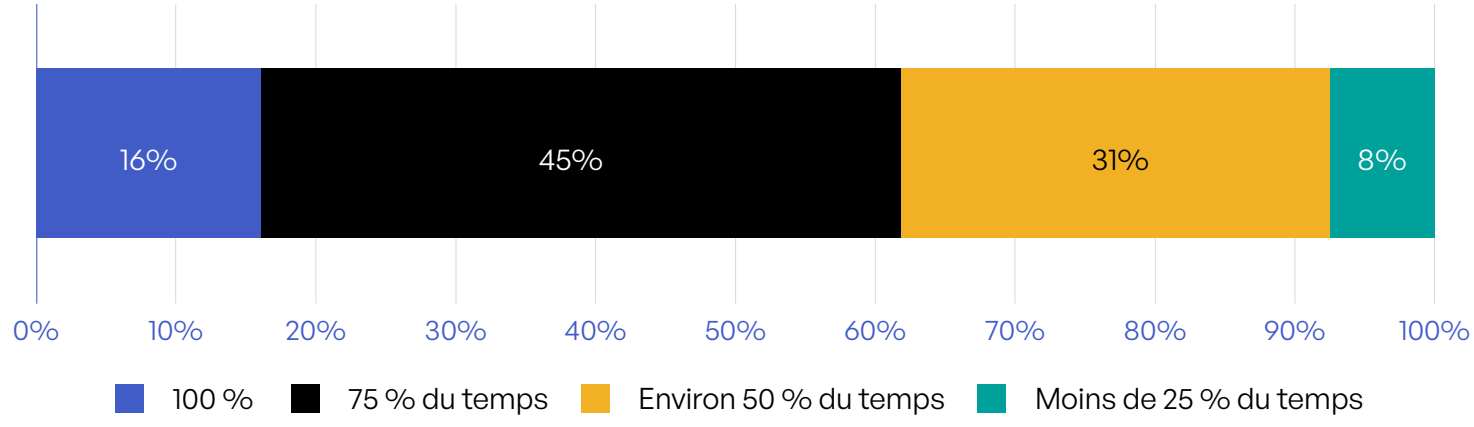


Figure 49: Capacité à suivre et à contrôler les contenus sensibles une fois qu'ils ont quitté une application

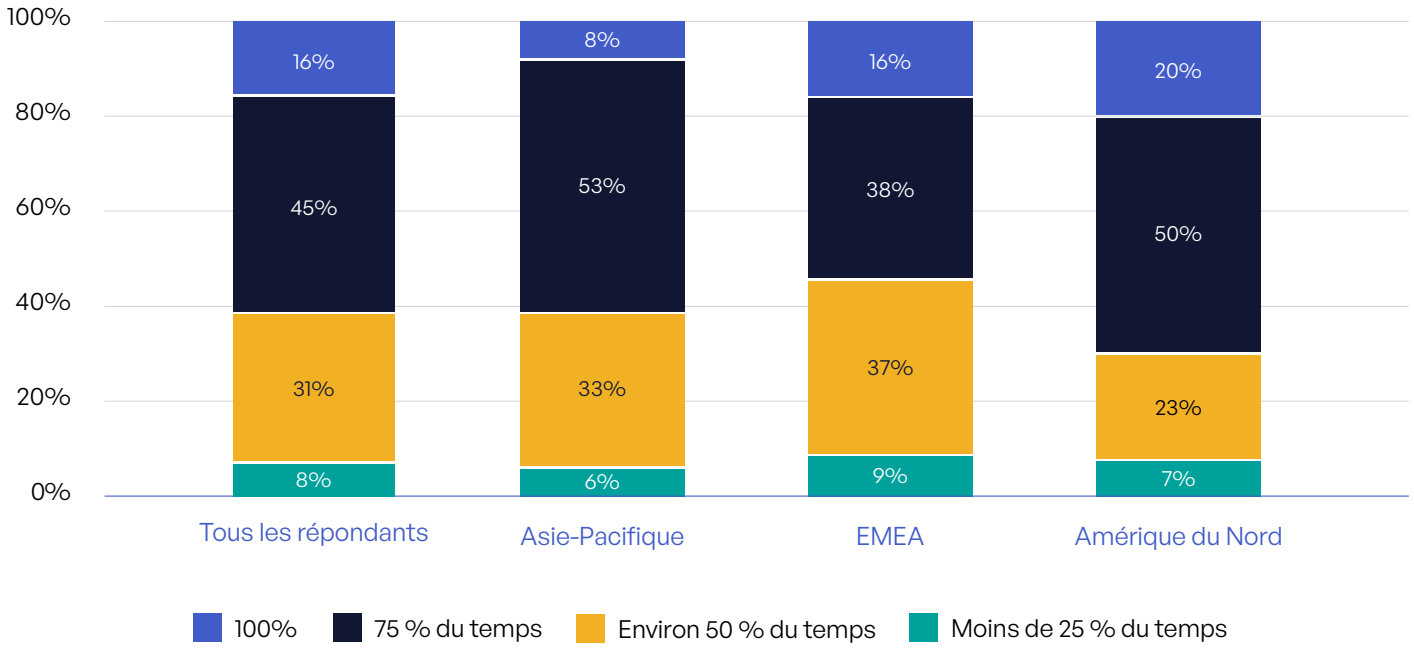


Figure 50: Capacité à suivre et à contrôler les contenus sensibles une fois qu'ils ont quitté une application selon la région

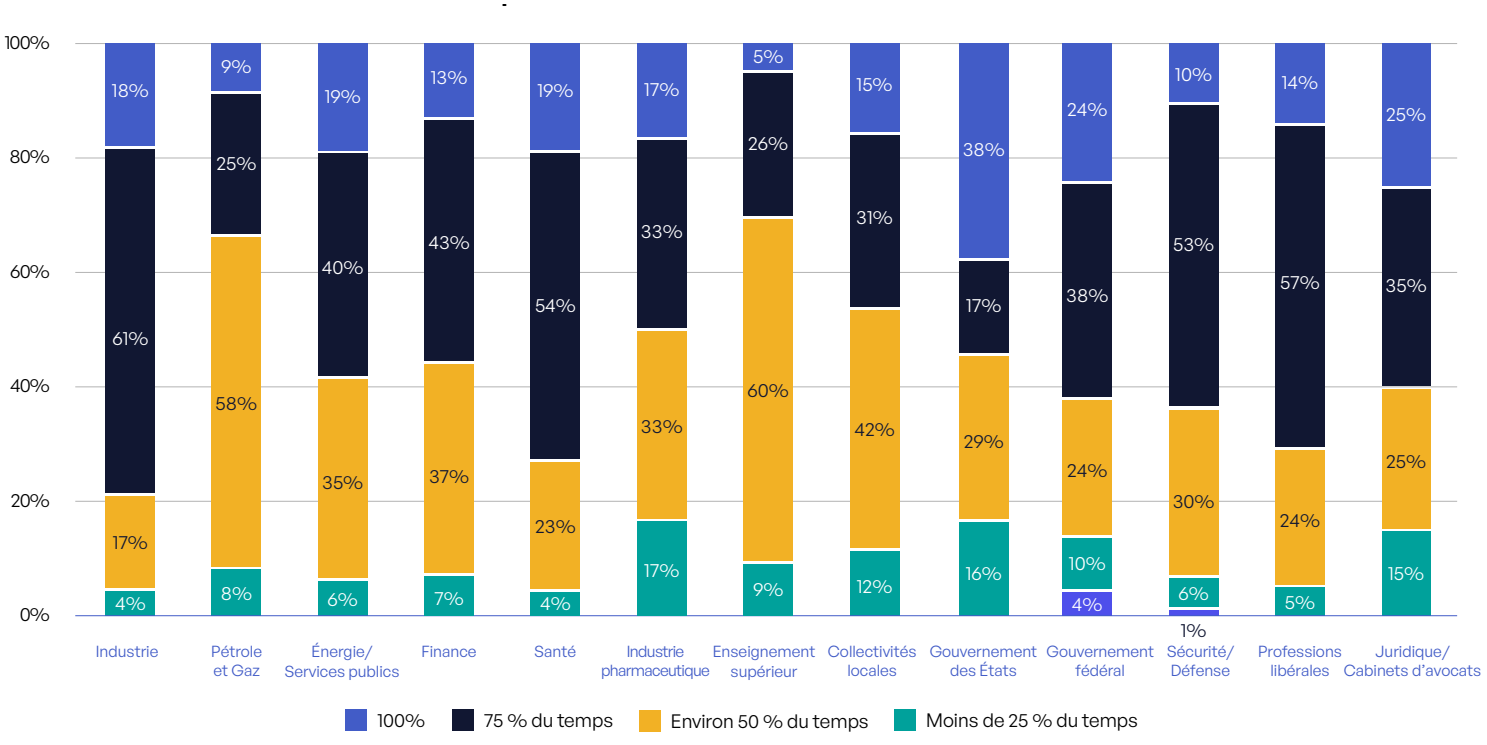


Figure 51: Capacité à suivre et à contrôler les contenus sensibles une fois qu'ils ont quitté une application, pour les différents secteurs d'activité

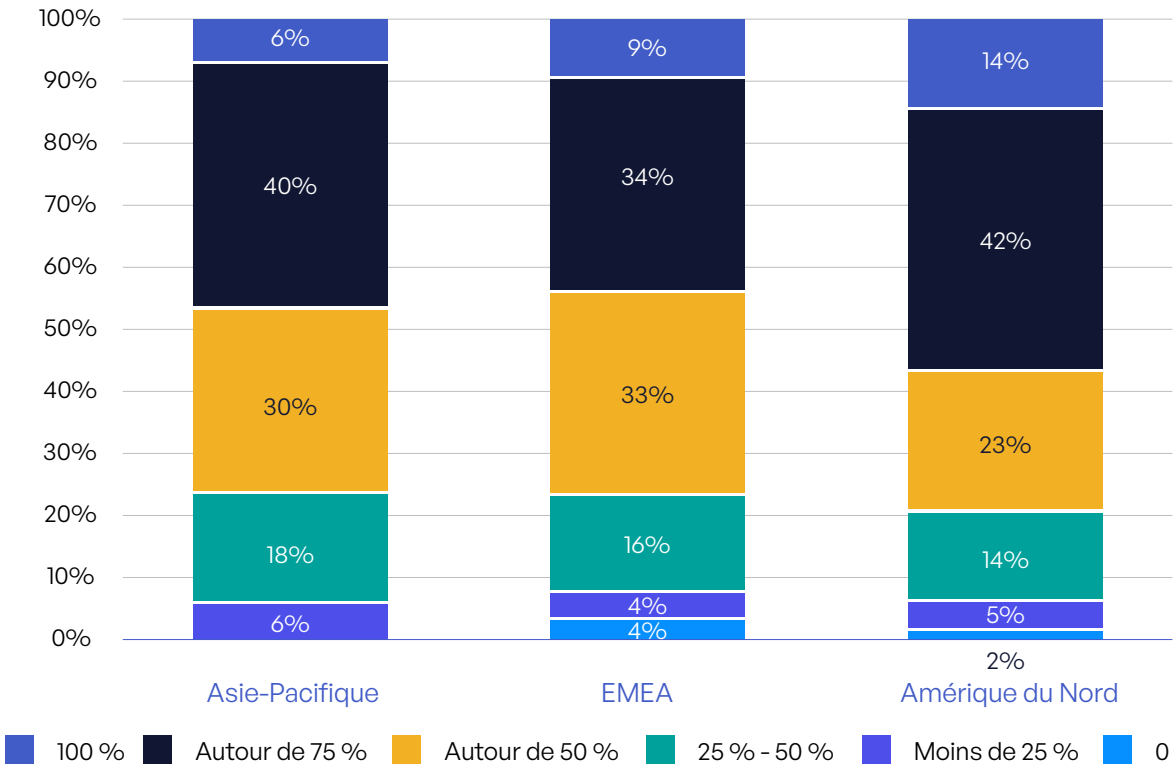


Figure 52: Part des données non structurées qui est étiquetée et classifiée dans les différentes régions

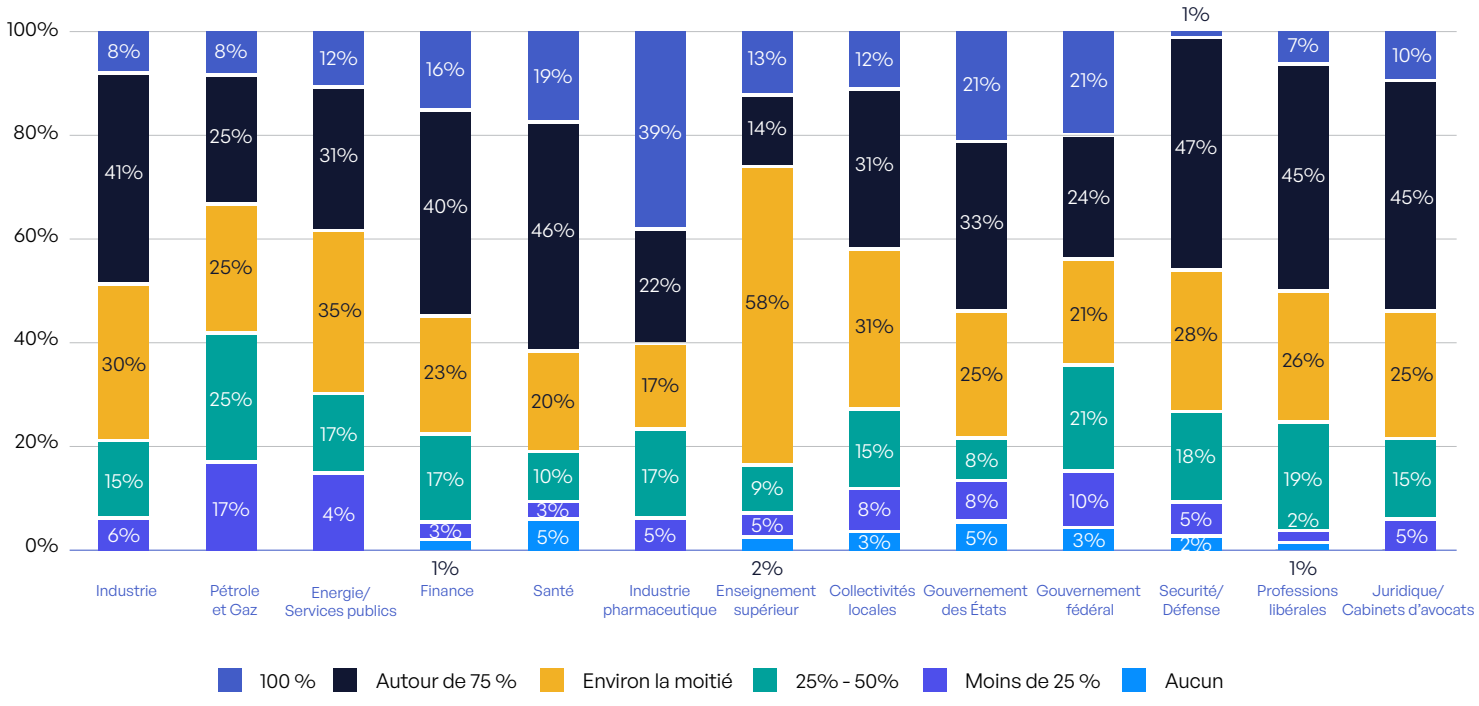


Figure 53: Part des données non structurées qui est étiquetée et classifiée dans les différents secteurs d'activité

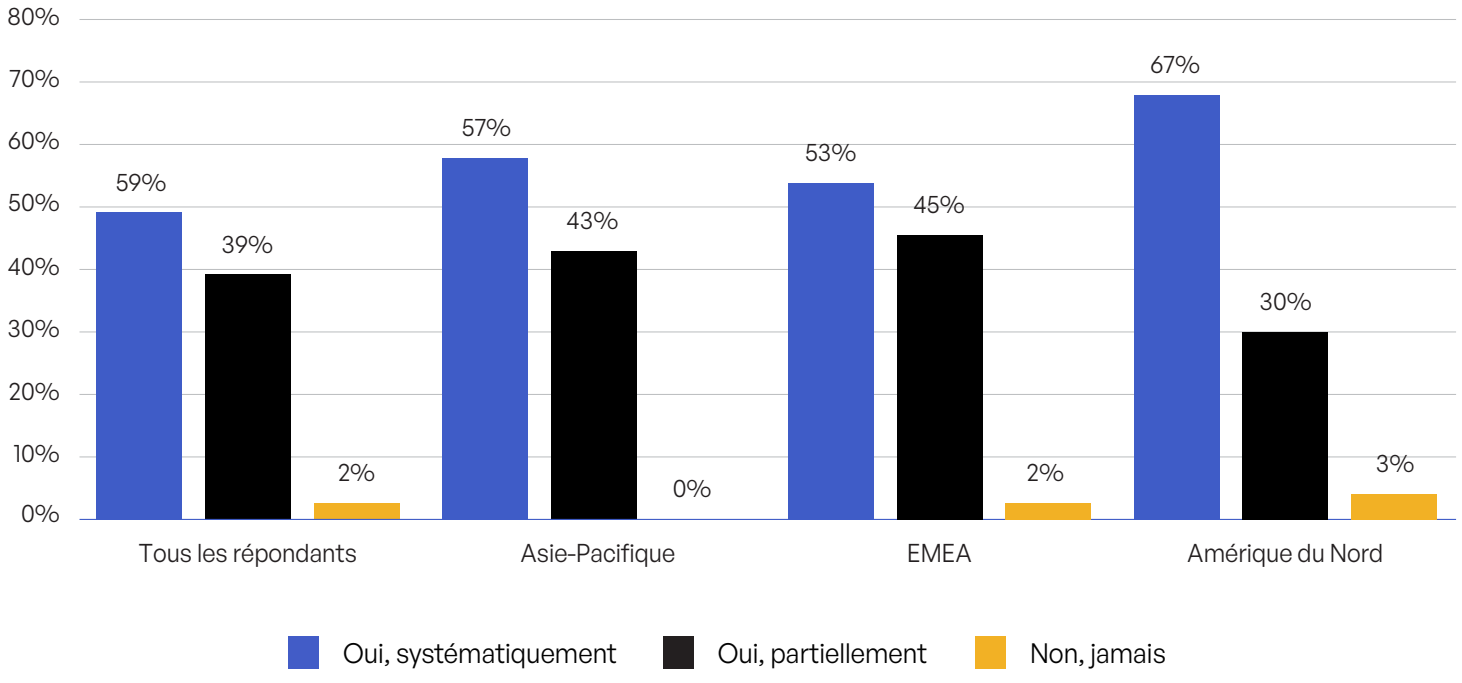


Figure 54: Utilisation des outils de sécurité avancés pour les communications sensibles dans les différentes régions

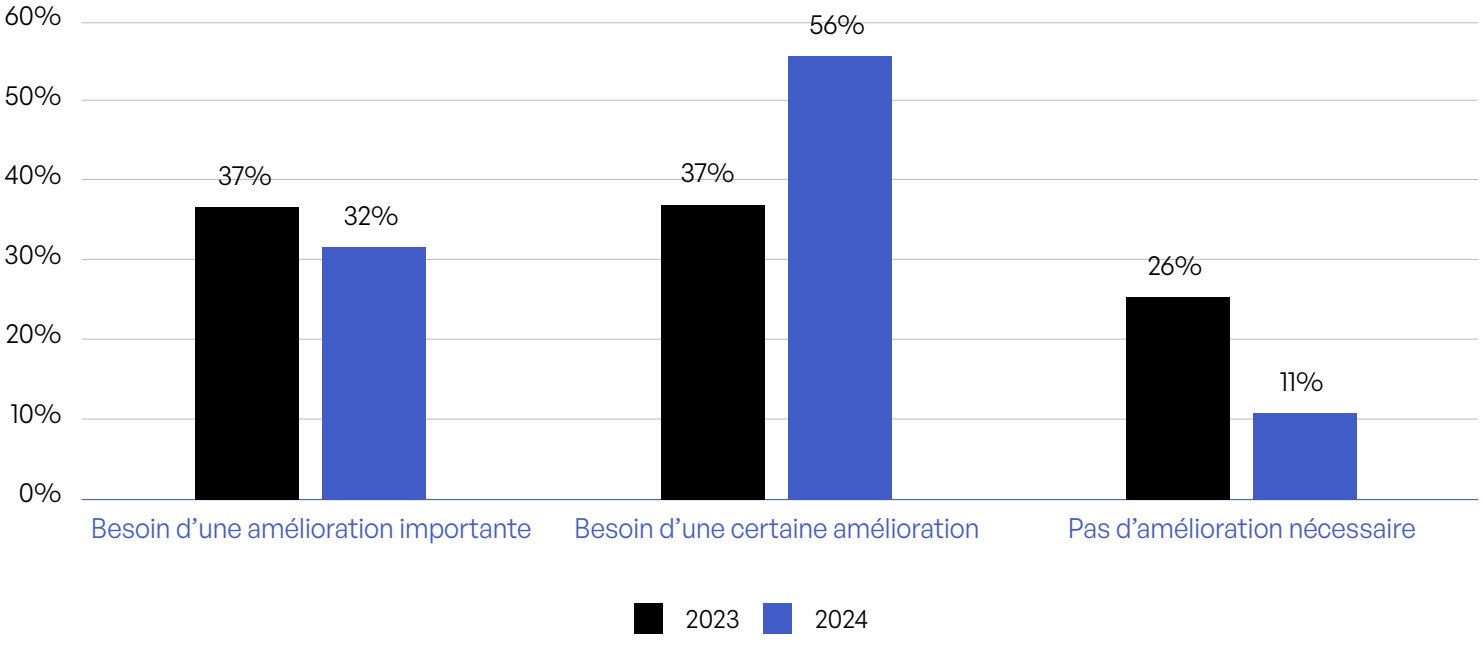


Figure 55: Besoin d'améliorer le management des risques associés aux communications sensibles

		Tous les répondants	Industrie	Pétrole et Gaz	Énergie/ Services publics	Finance	Santé	Industrie pharmaceutique	Enseignement supérieur
En interne	Oui, systématiquement	59%	58%	58%	58%	60%	56%	61%	65%
	Oui, partiellement	39%	42%	42%	40%	36%	44%	39%	28%
	Non, jamais	2%	0%	0%	2%	4%	0%	0%	7%
En externe	Oui, systématiquement	59%	62%	58%	44%	70%	56%	78%	72%
	Oui, partiellement	38%	38%	42%	52%	27%	44%	22%	21%
	Non, jamais	3%	0%	0%	4%	3%	0%	0%	7%

		Collectivités locales	Gouvernement des États	Gouvernement fédéral	Sécurité/ Défense	Professions libérales	Juridique/ Cab. d'avocats
En interne	Oui, systématiquement	50%	71%	52%	55%	71%	45%
	Oui, partiellement	50%	25%	45%	45%	28%	50%
	Non, jamais	0%	4%	3%	0%	2%	5%
En externe	Oui, systématiquement	50%	67%	48%	51%	60%	50%
	Oui, partiellement	38%	29%	45%	48%	40%	45%
	Non, jamais	12%	4%	7%	1%	0%	5%

Figure 56: Utilisation des outils de sécurité avancés pour les communications sensibles dans les différents secteurs d'activité

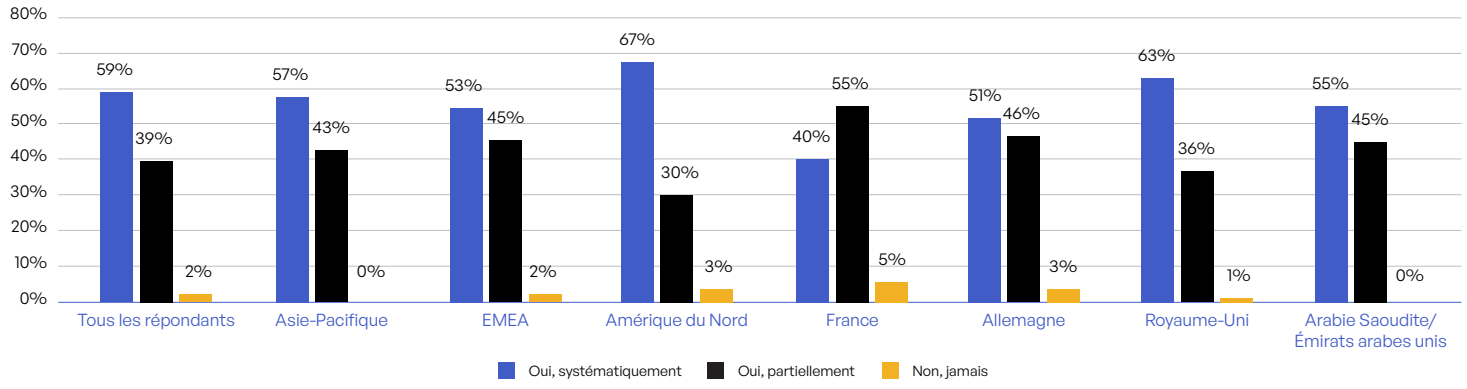


Figure 57: Utilisation des outils de sécurité avancés pour les communications sensibles dans les différentes régions

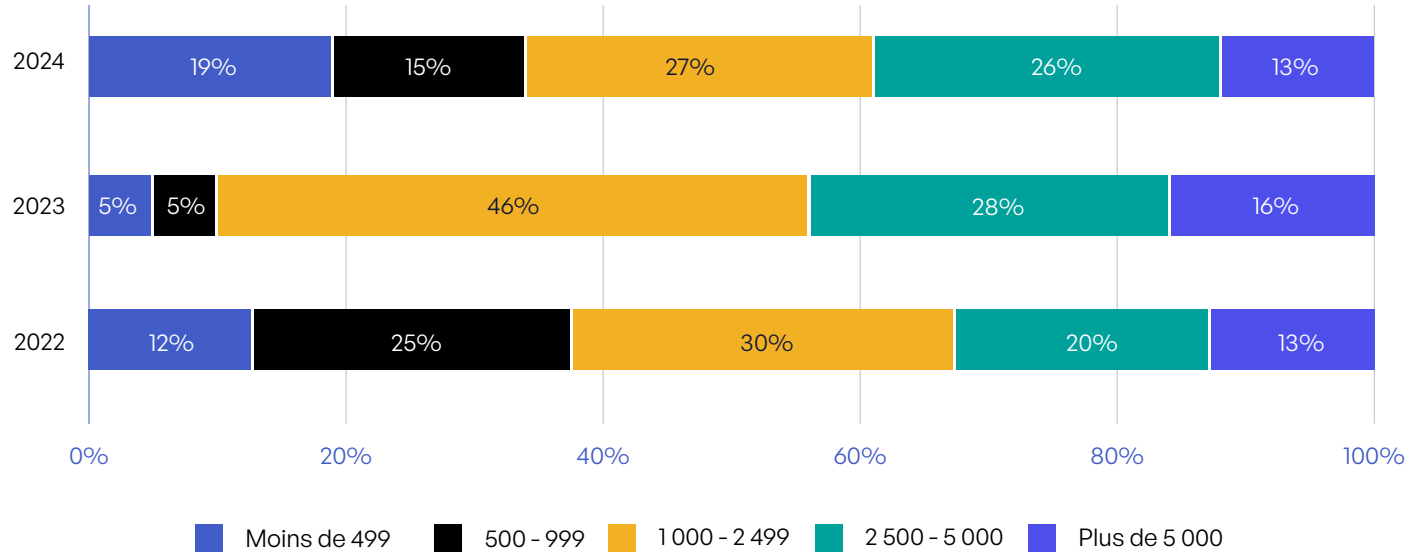


Figure 58: Estimation par les répondants du nombre d'interlocuteurs pour les communications de contenu sensible

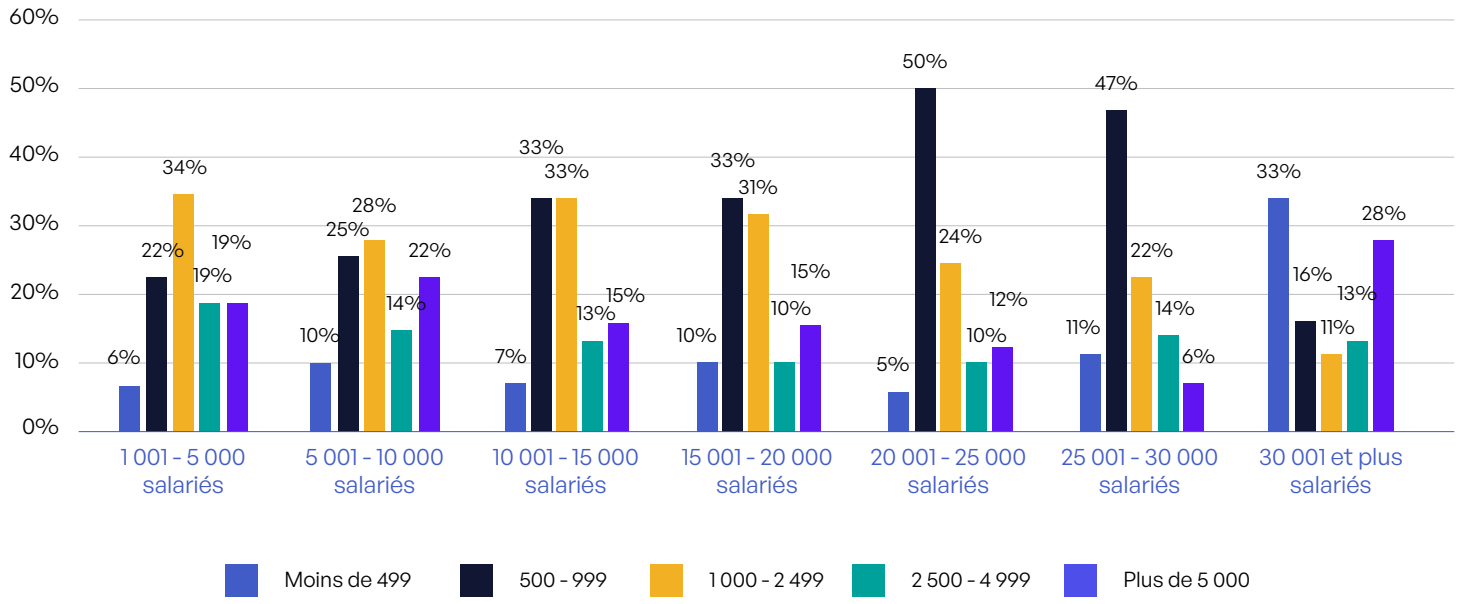


Figure 59: Nombre d'interlocuteurs pour les communications de contenu sensible selon la taille de l'organisation

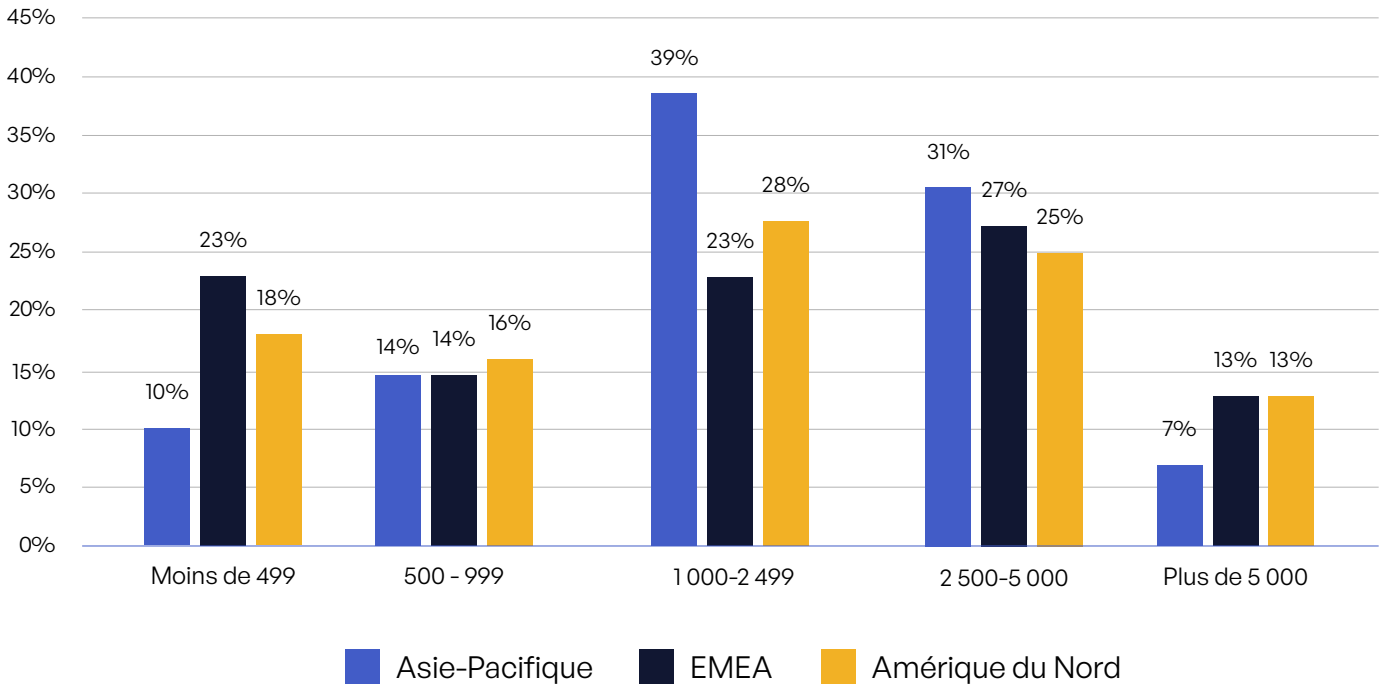


Figure 60: Nombre d'interlocuteurs pour les communications de contenu sensible dans les différentes régions

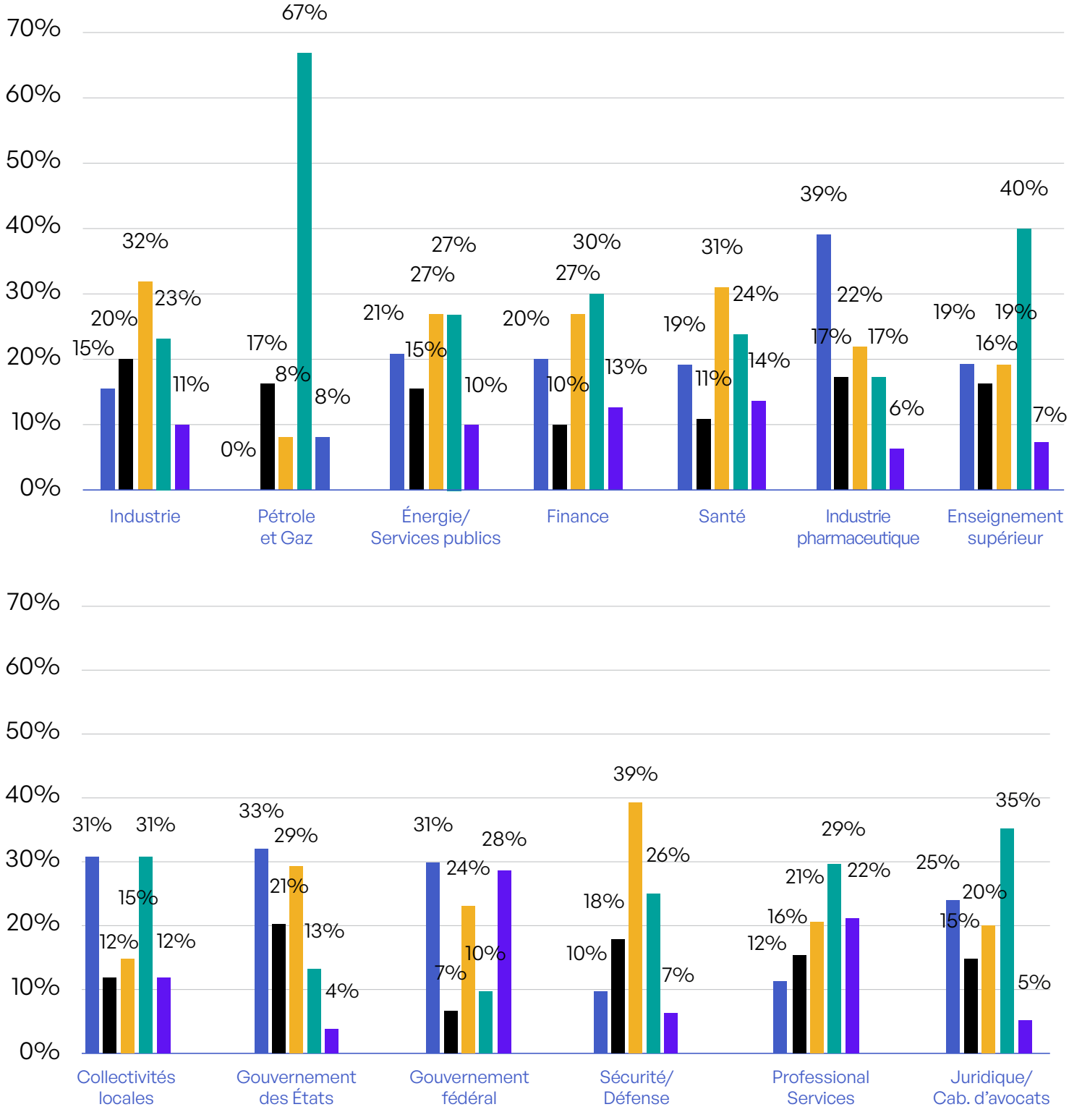


Figure 61: Nombre d'interlocuteurs pour les communications de contenu sensible dans les différents secteurs d'activité

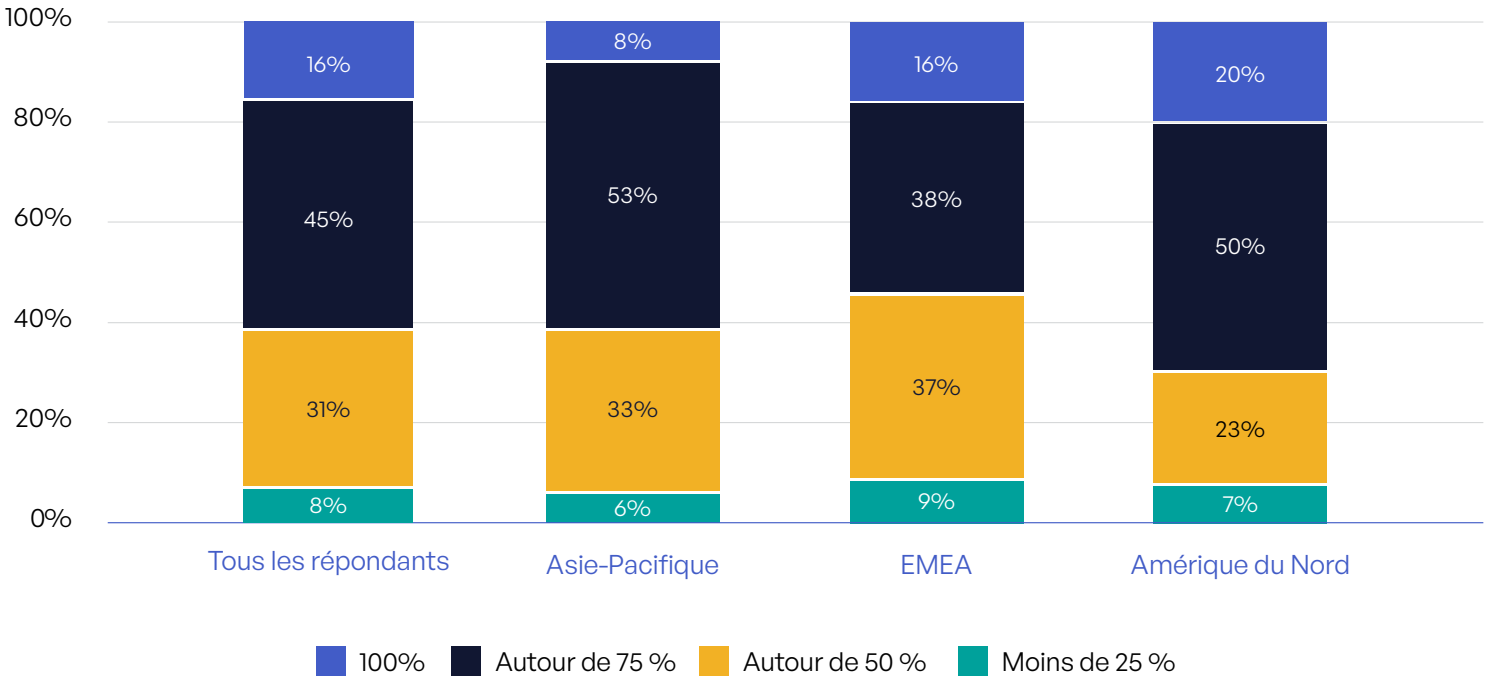


Figure 62: Part des communications de contenu sensible qui sont suivies et contrôlées, dans les différentes régions

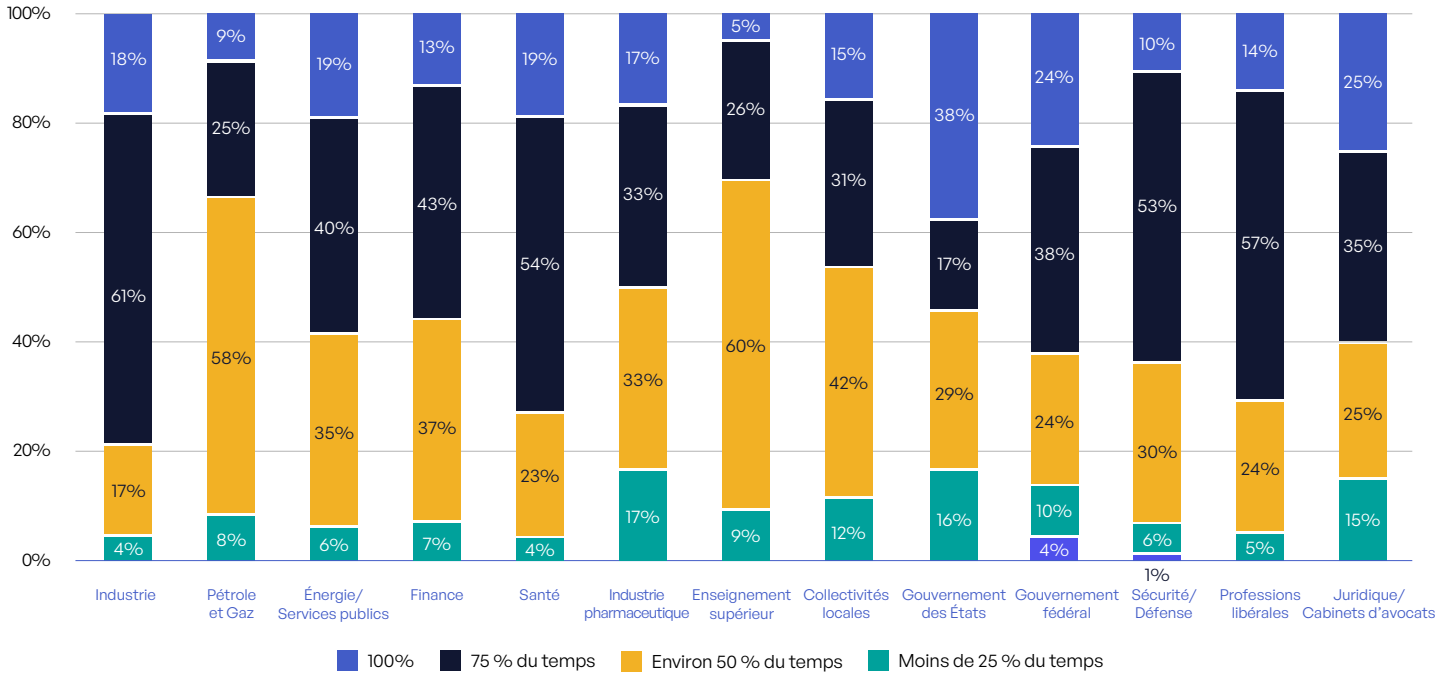


Figure 63: Capacité à suivre et à contrôler les contenus sensibles une fois qu'ils ont quitté une application, pour les différents secteurs d'activité

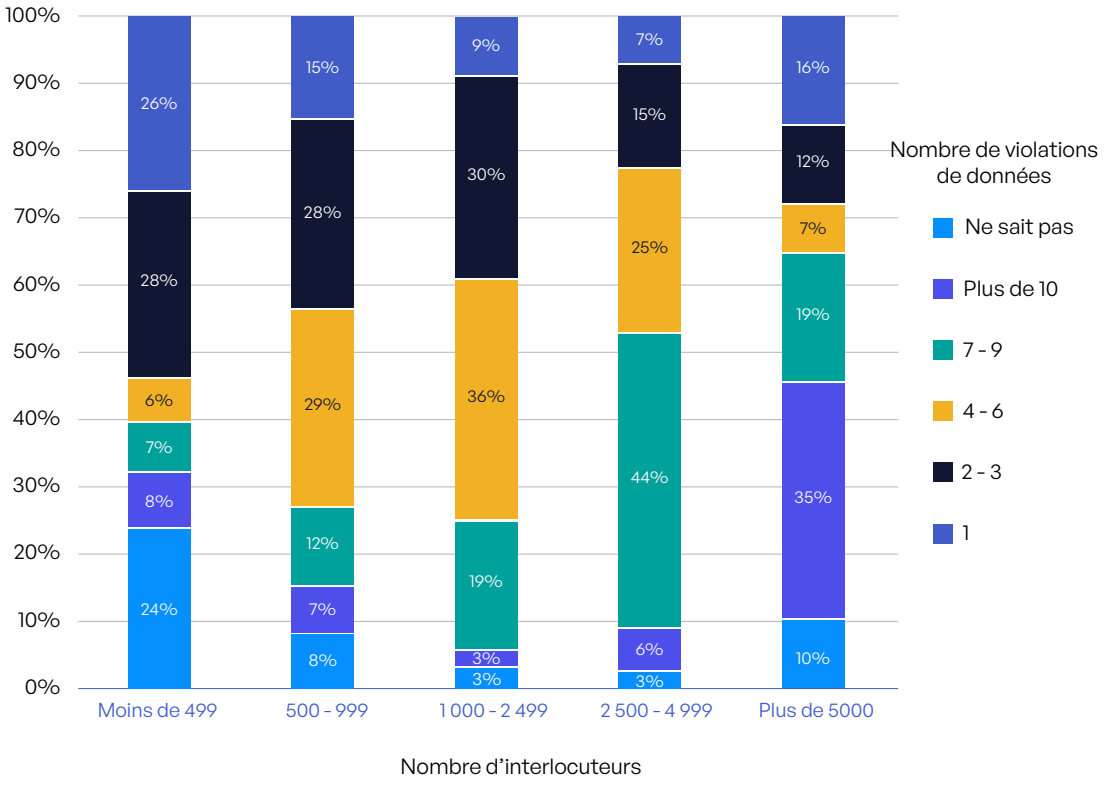


Figure 64: Nombre de violations de données en fonction du nombre d'interlocuteurs

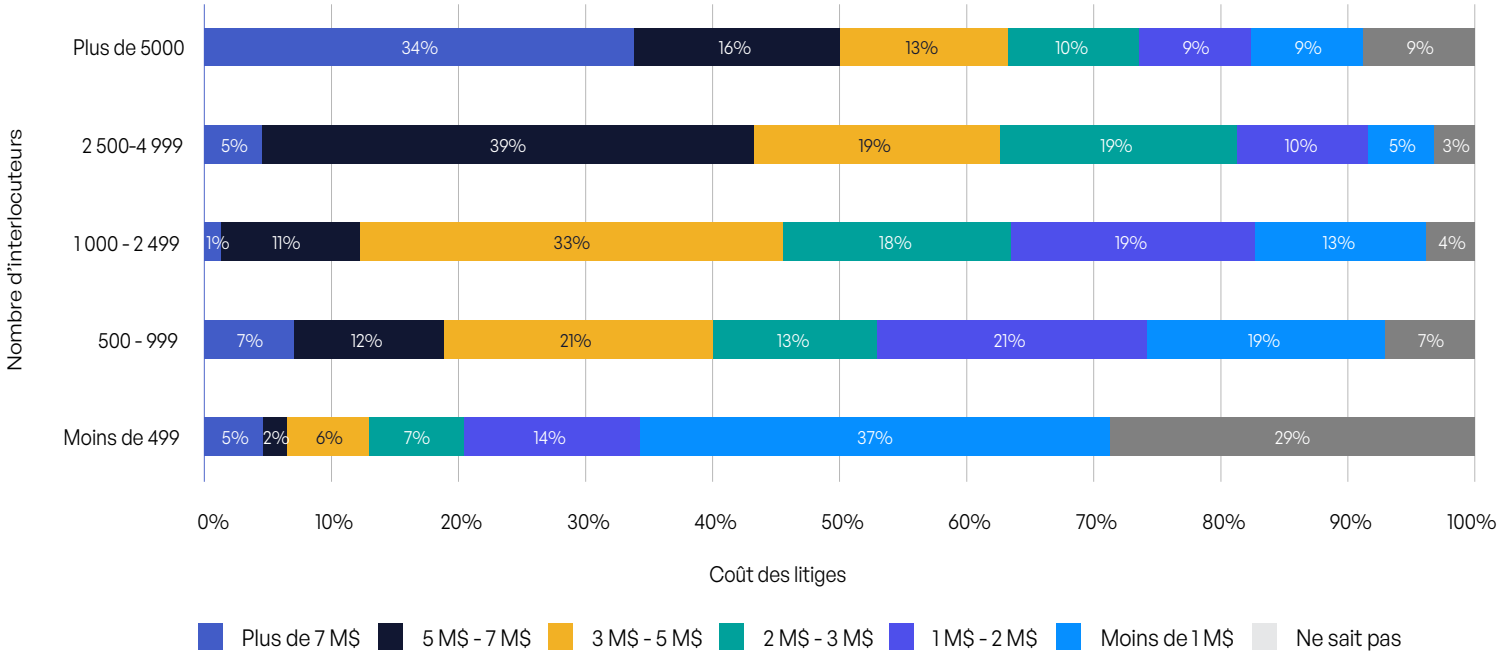


Figure 65: Coût des litiges en fonction du nombre d'interlocuteurs

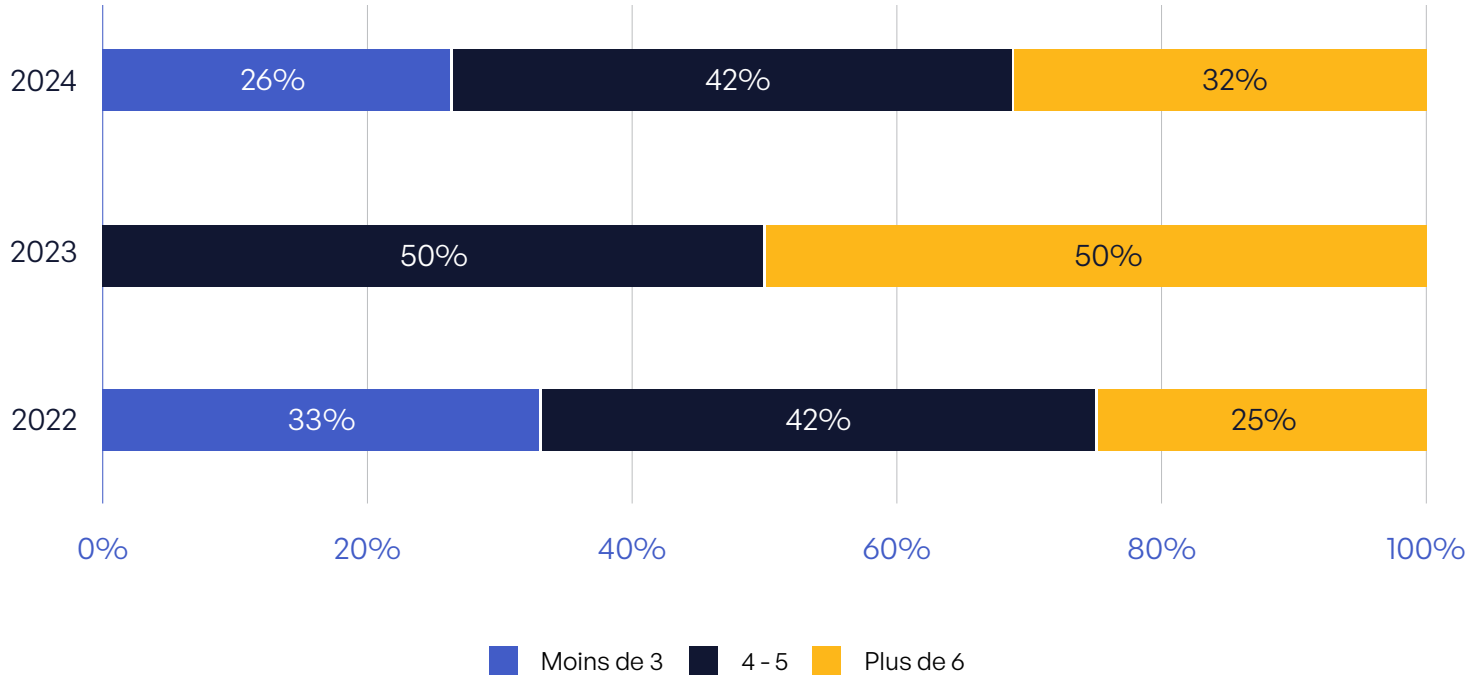


Figure 66: Nombre d'outils/Systèmes différents utilisés pour échanger des contenus sensibles

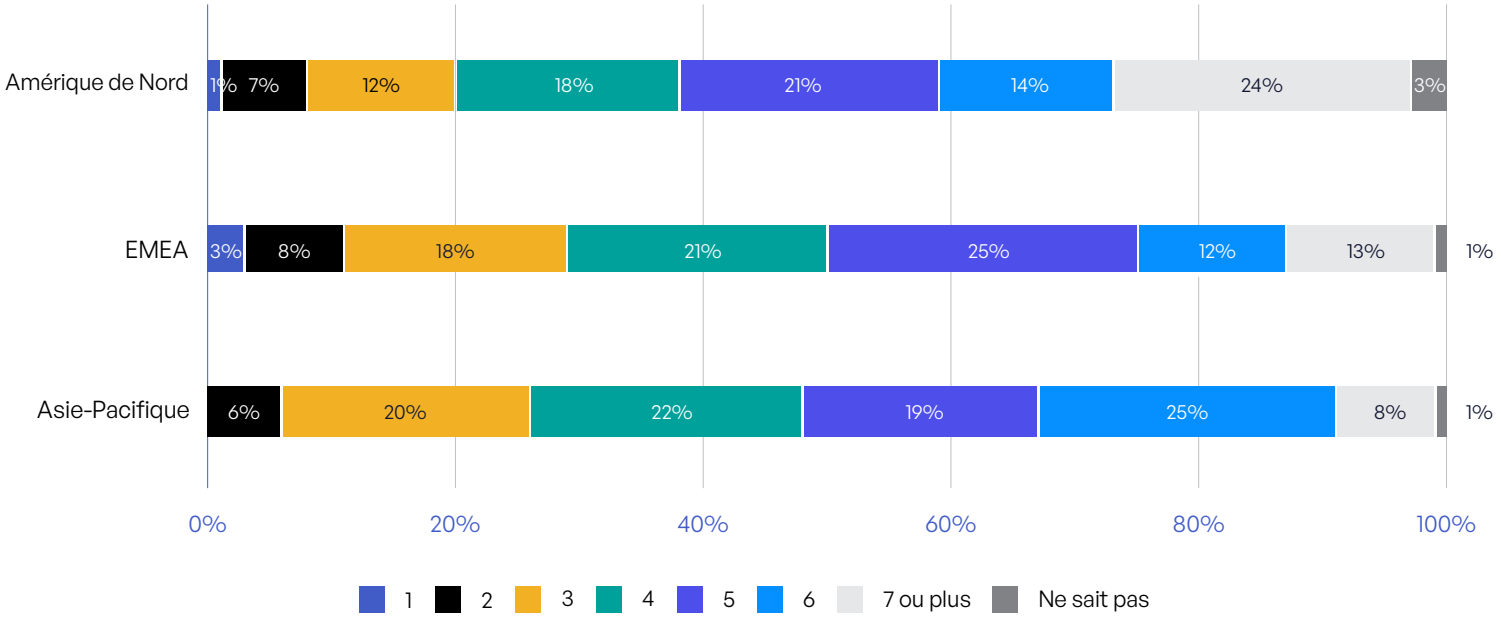


Figure 67: Nombre d'outils de communication différents dans les différentes régions

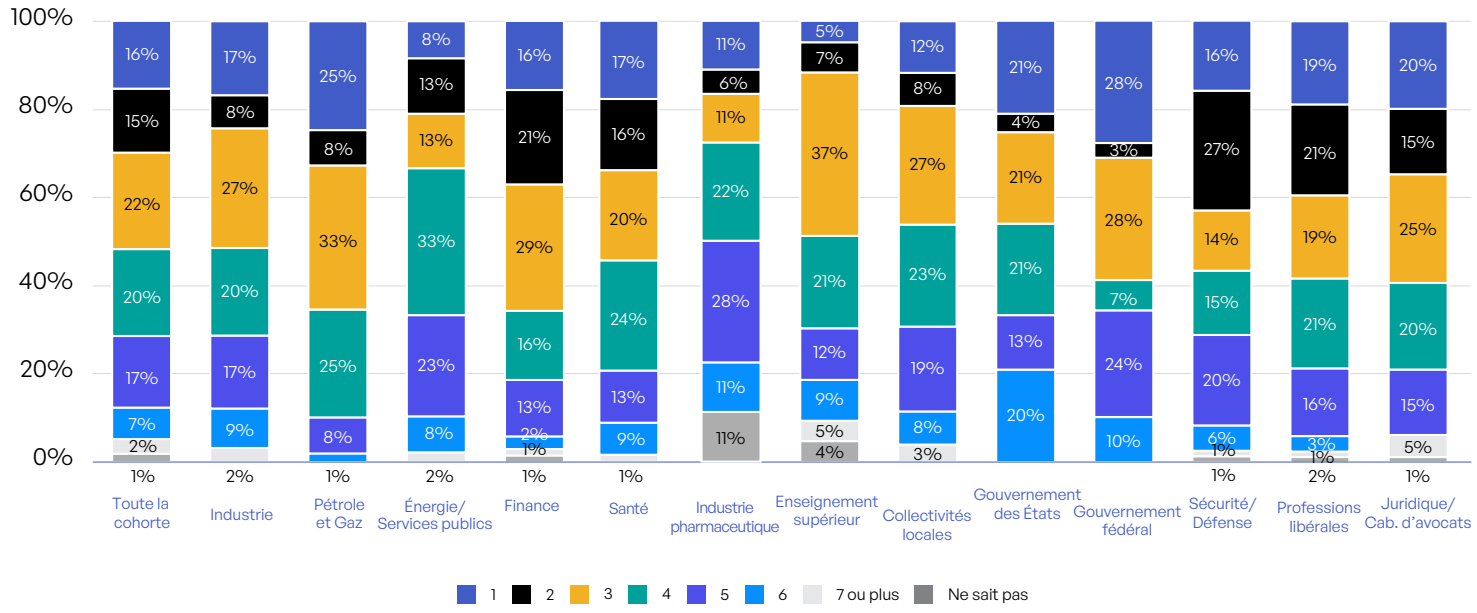


Figure 68: Nombre d'outils de communication différents dans les différents secteurs d'activité

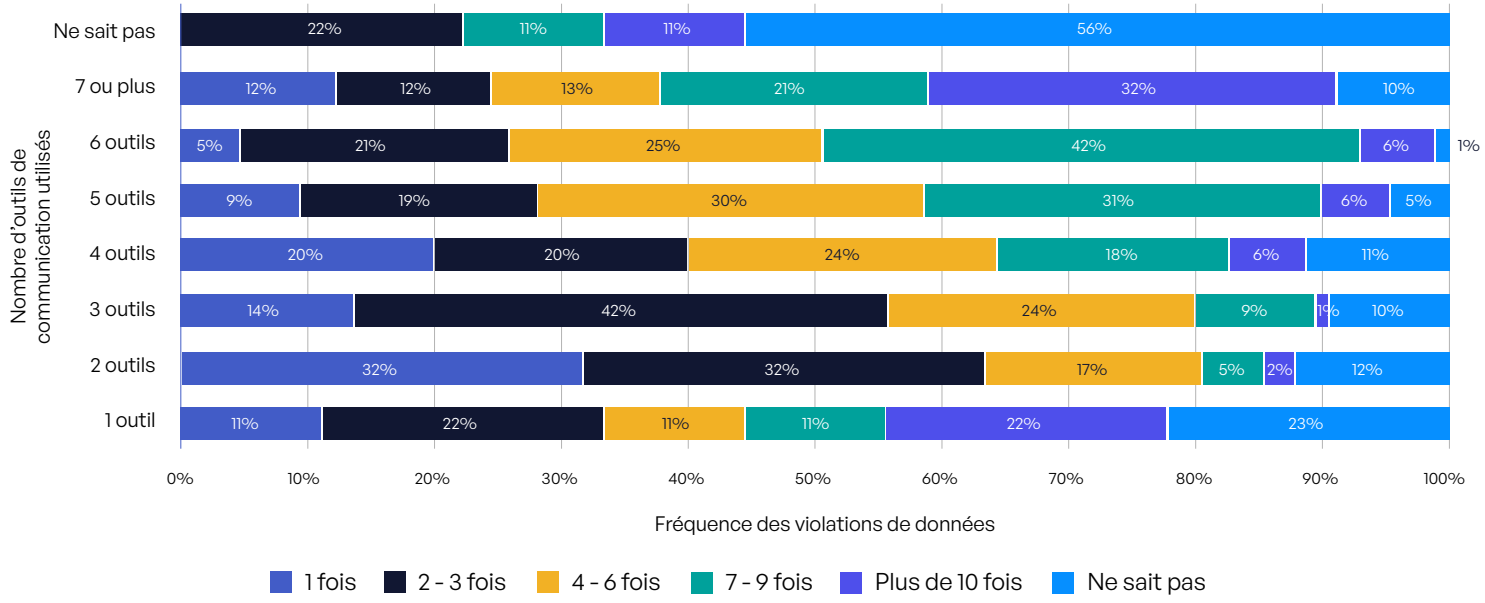


Figure 69: Fréquence des violations de données en fonction du nombre d'outils de communication utilisés

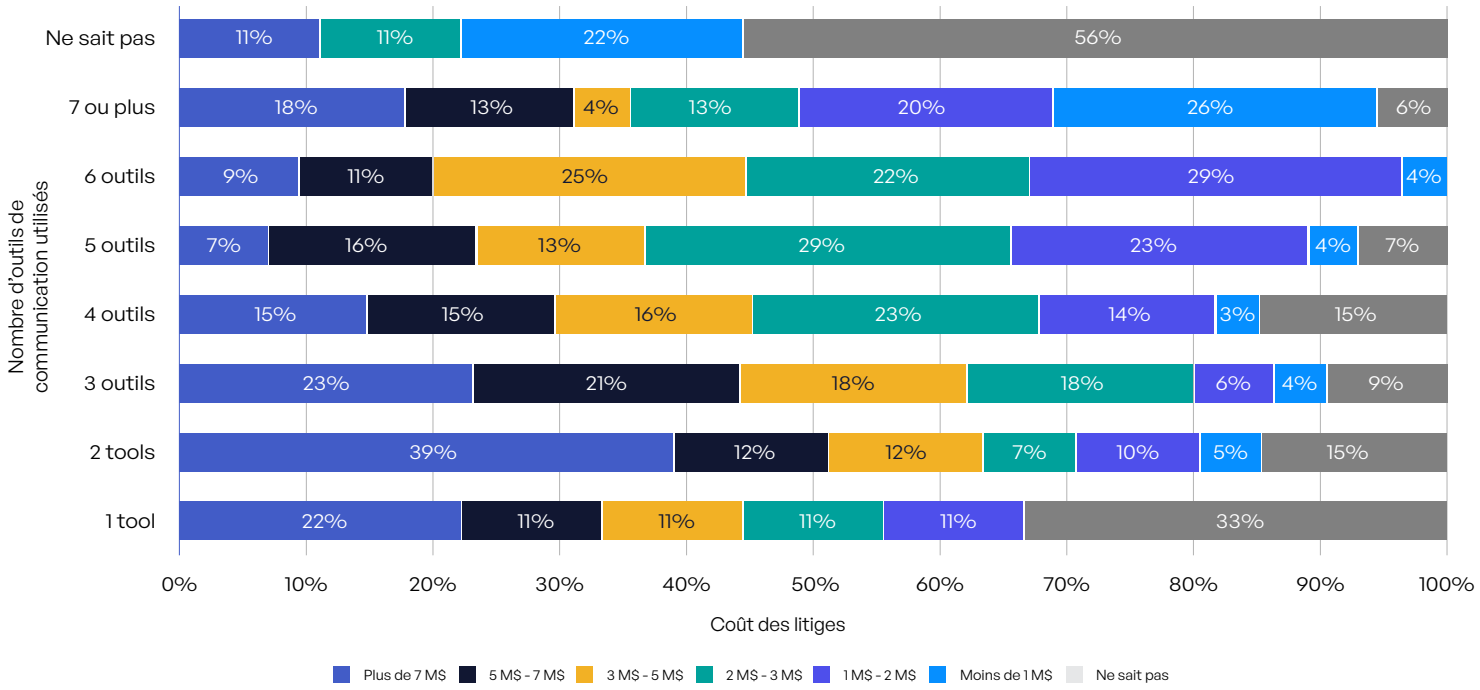


Figure 70: Coût des litiges liés aux violations de données en fonction du nombre d'outils de communication utilisés

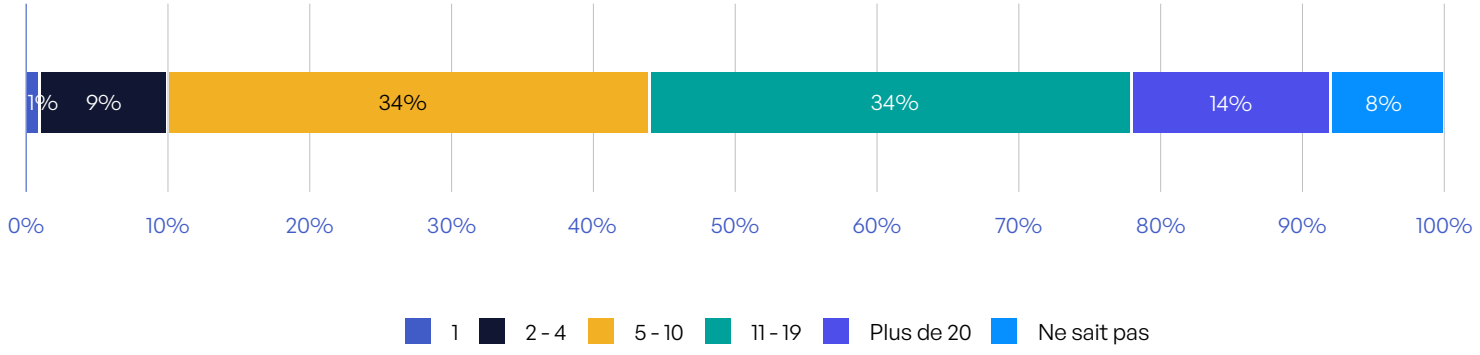


Figure 71: Nombre de journaux d'audit à réconcilier

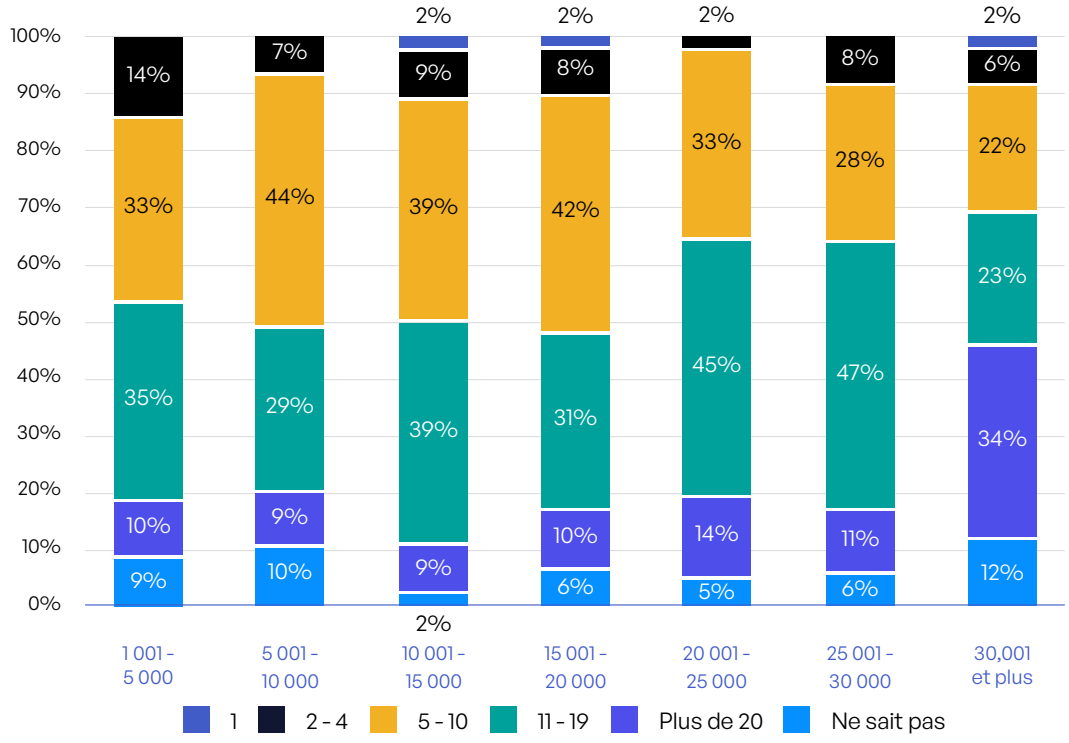


Figure 72: Nombre de journaux d'audit à réconcilier selon la taille de l'organisation

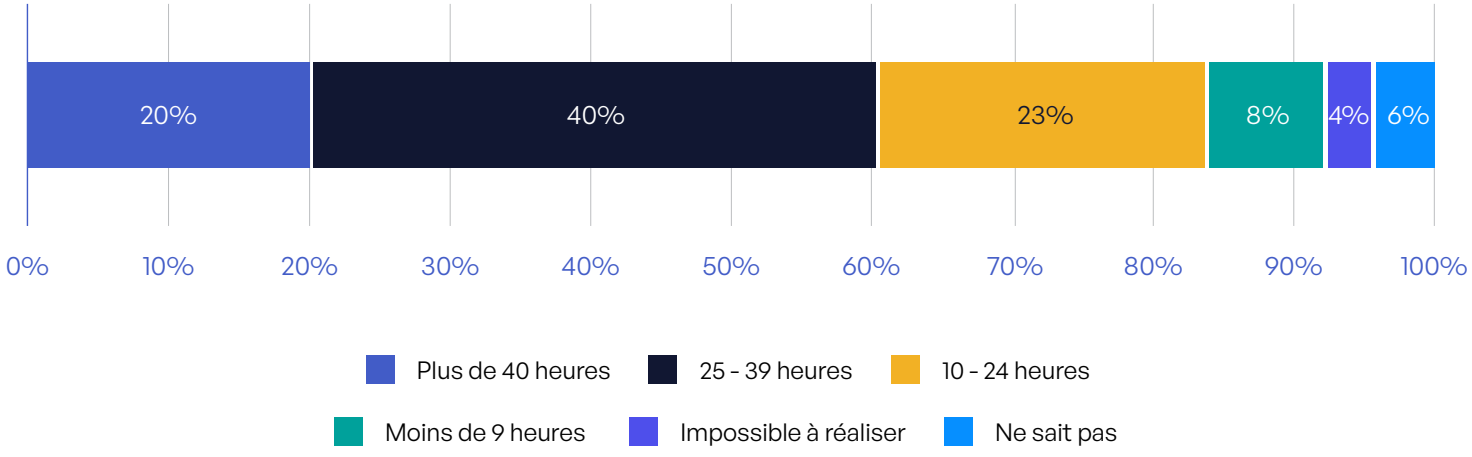


Figure 73: Temps passé à compiler les journaux d'audit par mois

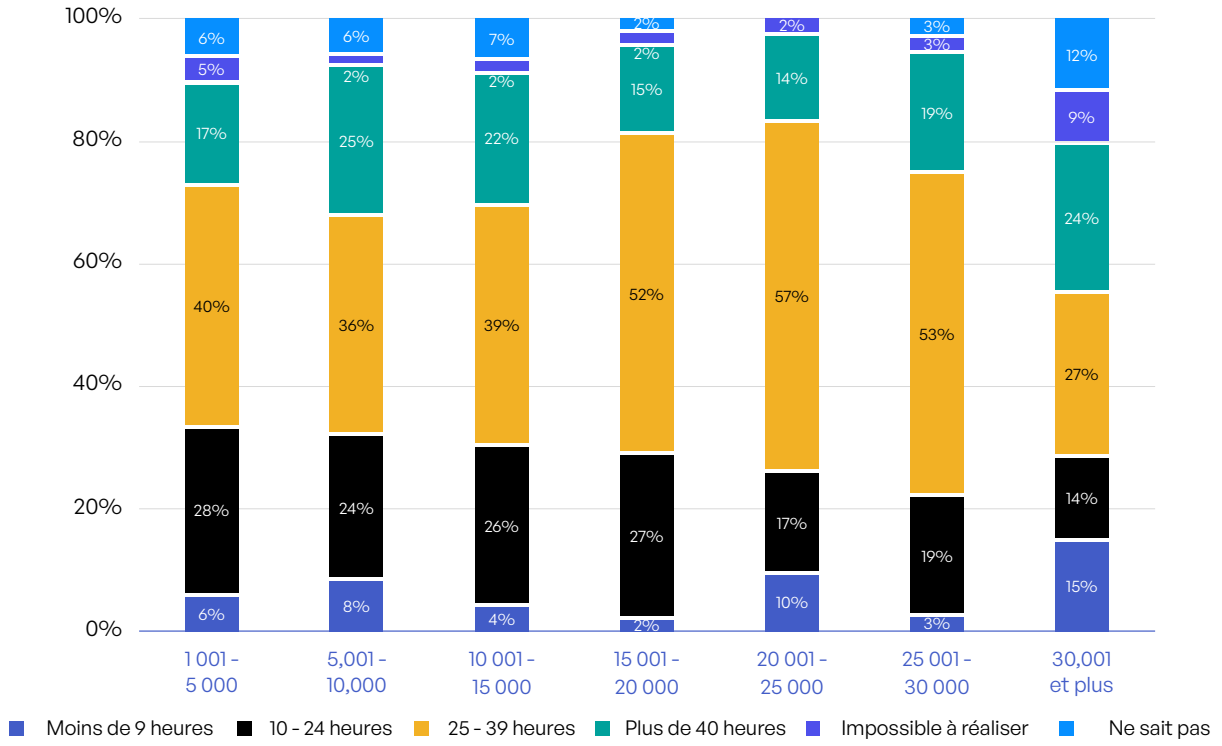


Figure 74: Temps passé pas mois à compiler les journaux d'audit de communications sensibles selon la taille de l'organisation

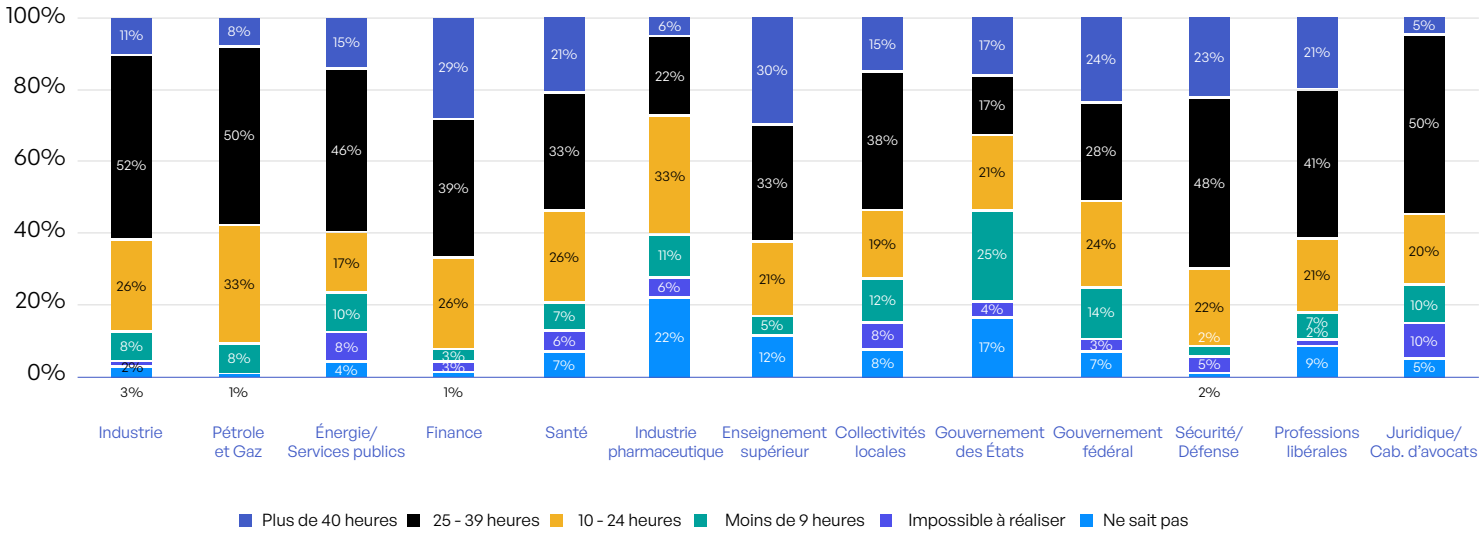


Figure 75: Temps passé pas mois à compiler à la main des journaux d'audit dans les différents secteurs d'activité

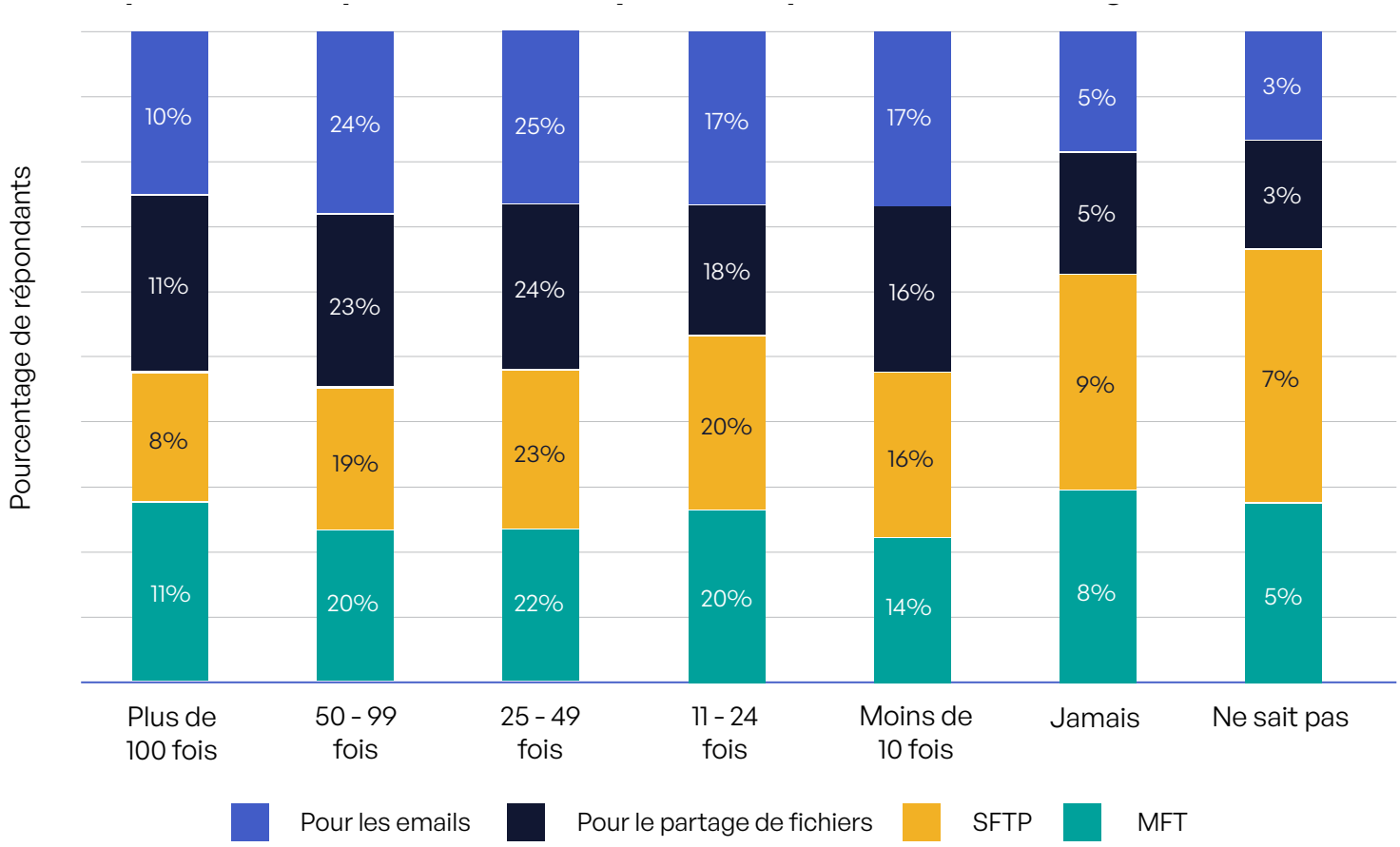


Figure 76: Nombre de fois par mois où les répondants utilisent une solution de contournement à cause de fichiers trop volumineux

	Asie-Pacifique				Amérique du Nord				EMEA			
	Email	Partage de fichiers	SFTP	MFT	Email	Partage de fichiers	SFTP	MFT	Email	Partage de fichiers	SFTP	MFT
Jamais	0%	2%	3%	2%	4%	4%	8%	16%	5%	6%	10%	11%
Moins de 10 fois	9%	14%	9%	9%	14%	13%	14%	10%	21%	17%	18%	17%
10 à 24 fois	27%	17%	27%	27%	11%	18%	18%	17%	14%	17%	17%	18%
25 à 49 fois	32%	24%	24%	25%	20%	23%	22%	21%	24%	24%	21%	20%
50 à 99 fois	17%	26%	18%	19%	30%	24%	21%	25%	22%	21%	18%	17%
Plus de 100 fois	6%	8%	6%	9%	15%	14%	11%	15%	7%	8%	5%	9%
Ne sait pas	3%	3%	7%	3%	1%	1%	3%	3%	2%	3%	8%	5%

Figure 77: Nombre de fois par mois où les répondants utilisent une solution de contournement à cause de fichiers trop volumineux, pour les différentes régions

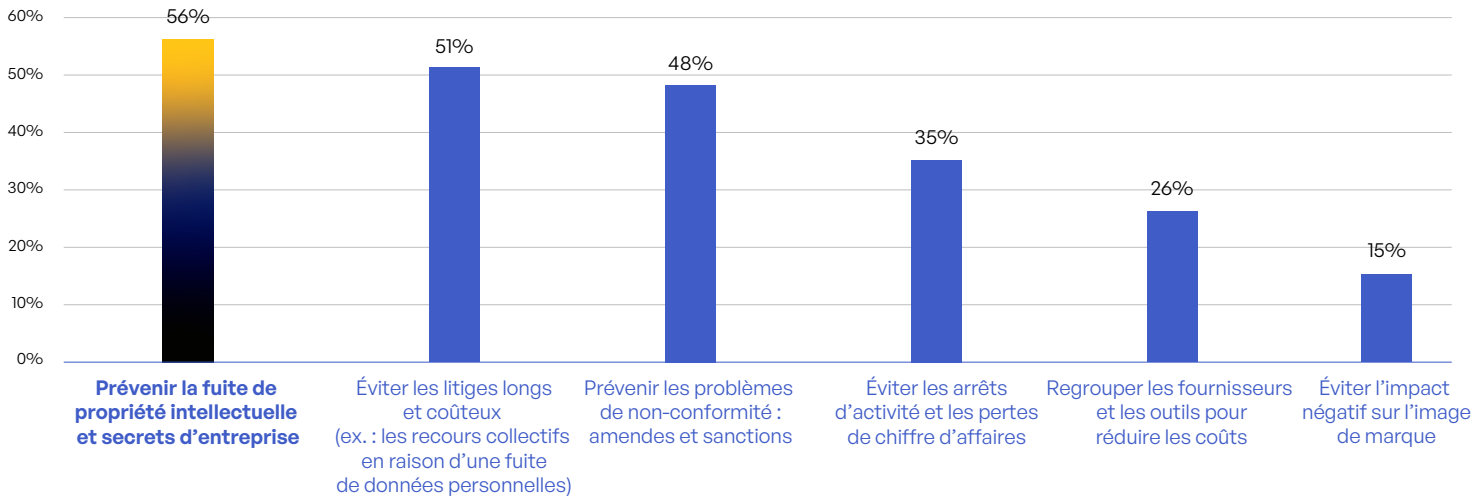


Figure 78: Principales motivations à unifier et à protéger les communications sensibles

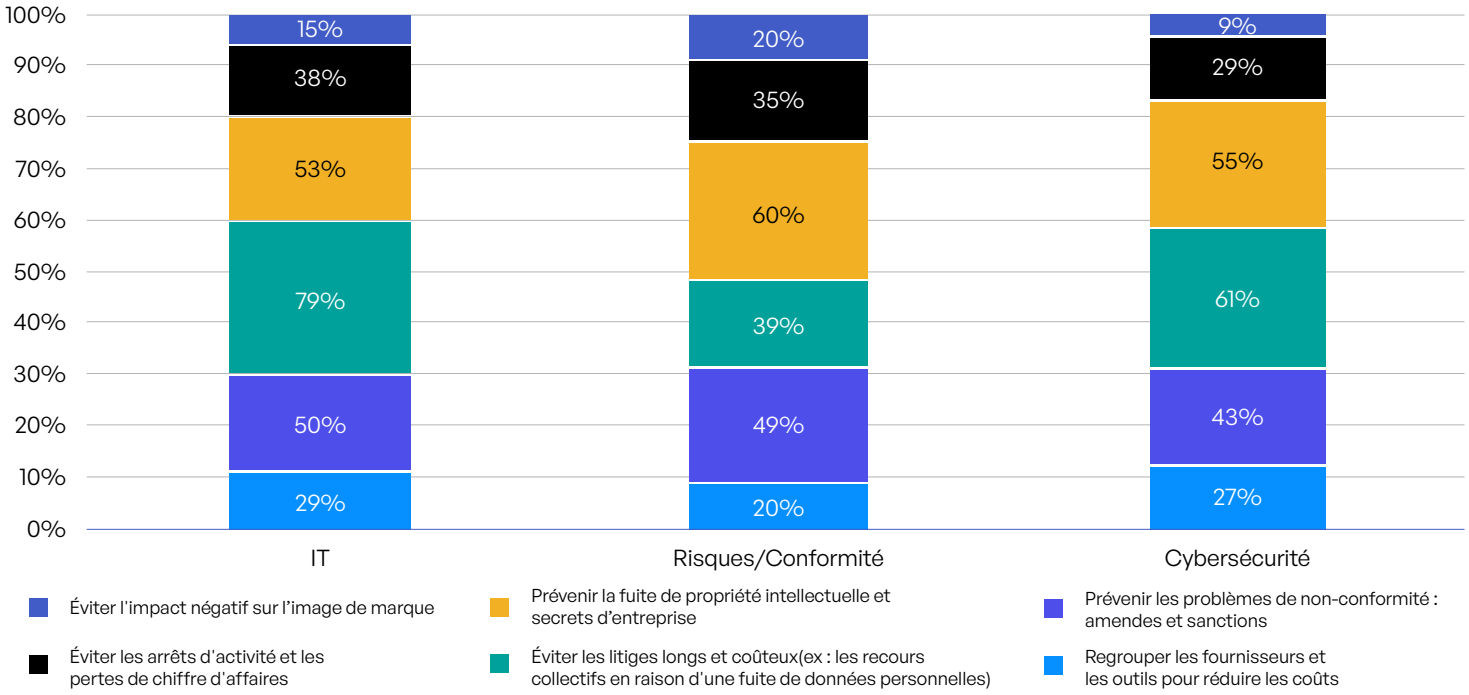


Figure 79: Principales motivations à unifier et à protéger les communications sensibles selon le poste occupé par les répondants

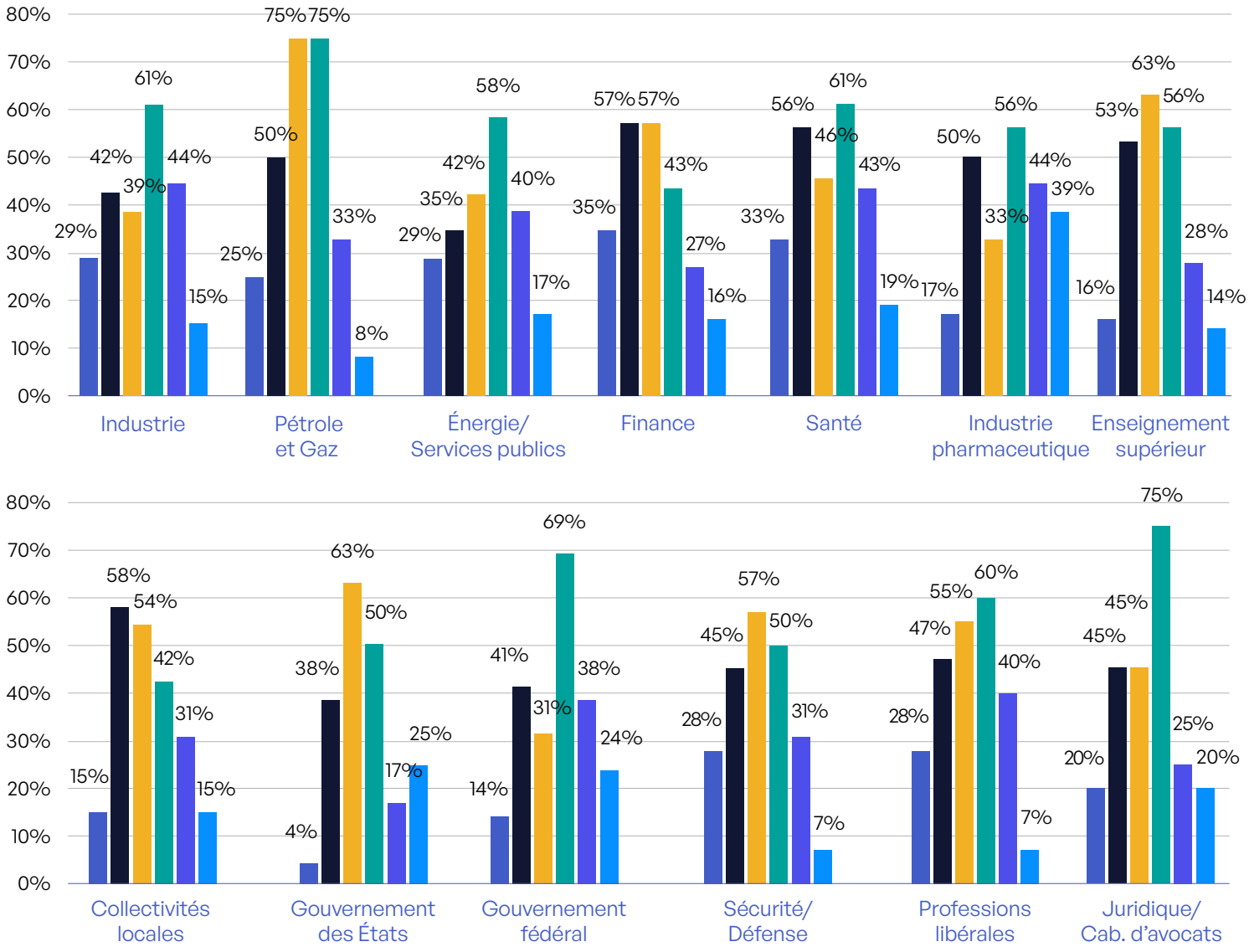


Figure 80: Principales motivations à unifier et à protéger les communications sensibles selon le secteur d'activité

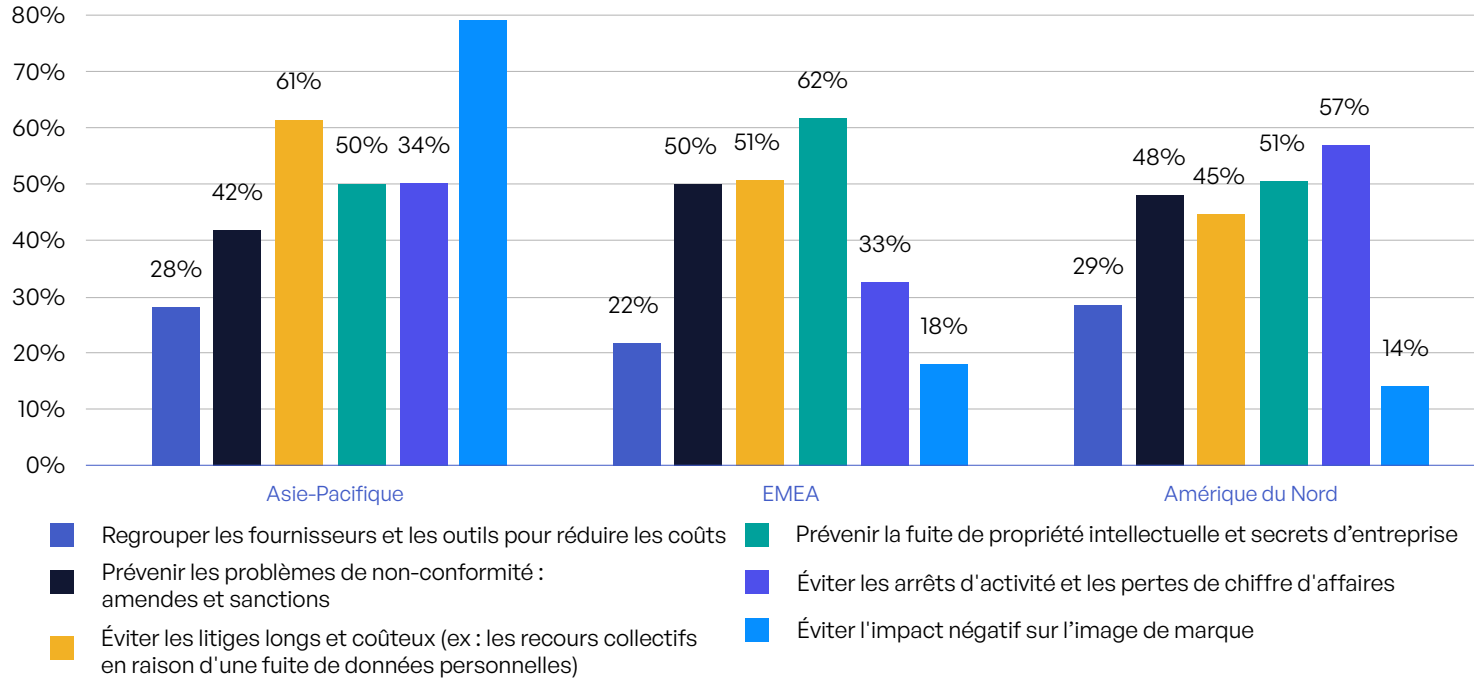


Figure 81: Principales motivations à unifier et à protéger les communications sensibles dans les différentes régions

Bibliographie

1. “2024 Data Breach Investigations Report,” Verizon, Avril 2024.
2. Matt Kapko, “Progress Software’s MOVEit meltdown: uncovering the fallout,” Cybersecurity Dive, 16 janvier 2024.
3. Bill Toulas, “Fortra shares findings on GoAnywhere MFT zero-day attacks,” BleepingComputer, 1 Avril 2023.
4. “2024 Gartner Technology Adoption Roadmap for Larger Enterprises Survey,” Février 2024.
5. Eileen Yu, “Employees input sensitive data into generative AI tools despite the risks,” ZDNet, 22 février 2024.
6. “2024 Global Threat Report,” CrowdStrike, Février 2024.
7. “Despite increased budgets, organizations struggle with compliance,” Help Net Security, 24 mai 2024.
8. “Data Protection and Privacy Legislation Worldwide,” U.N. Trade & Development, accessed 7 juin 2024.
9. “U.S. State Privacy Legislation Tracker,” IAPP, dernière mise à jour le 28 mai 2024.
10. Martin Armstrong, “EU Data Protection Fines Hit Record High in 2023,” Statistica, 8 janvier 2024.
11. “Health Information Privacy: Enforcement Highlights,” U.S. Health and Human Services, consulté le 30 avril 2024.
12. “2024 Data Breach Investigations Report,” Verizon, Avril 2024.
13. “2023 Data Breach Report,” ID Theft Center, Janvier 2024.
14. “Cost of a Data Breach Report 2023,” IBM Security, Juillet 2023.
15. Ibid.
16. “2024 Global Threat Report,” CrowdStrike, Février 2024.
17. “2024 Data Breach Investigations Report,” Verizon, Mai 2024.
18. “Privacy in Practice 2024,” ISACA, Janvier 2024.
19. “Fortinet Global Zero Trust Report Finds Majority of Organizations Are Actively Implementing Zero Trust But Many Still Face Integration Challenges,” Fortinet Press Release, 20 juin 2023.

Kiteworks

Juin 2024

www.kiteworks.com