RAPPORT

L'état de la sécurité des données, 2024

1er juillet 2024 • 14 min de lecture

Heidi Shey
Analyste principal

Avec Amy DeMartine, Danielle Chittem et Peter Harrison

Résumé

Les données sont partout et ce qui constitue des données sensibles pour les organisations s'est considérablement élargi aujourd'hui. Les professionnels de la sécurité et de la confidentialité doivent aligner leurs préoccupations sur les causes réelles des violations, comprendre quels types de données sont compromises, reconnaître les effets

et l'impact post-violation et comparer les approches de sécurité des données pour leurs programmes de cybersécurité et de conformité à la confidentialité. Utilisez ce rapport pour comprendre les tendances actuelles et modifier vos programmes en conséquence.

de propriété intellectuelle. Il s'agit d'emojis, de communications des employés, de données de capteurs IoT, d'algorithmes et de modèles d'IA. Il s'agit des données de vos bases de données et des fichiers enregistrés sur les terminaux, des conversations numériques stockées dans des environnements cloud et des données structurées et non structurées dans les lacs de données. Il s'agit du code source des référentiels de code et des secrets (identifiants numériques) comme les clés de chiffrement. En bref, les données sensibles sont plus que des données réglementées, et elles sont partout car c'est là qu'elles doivent se trouver pour permettre les opérations de votre organisation. Pour sécuriser ces sources de données nouvelles et familières, les professionnels de la sécurité et des risques doivent rester au courant des préoccupations et des approches en matière de sécurité des données, ainsi que des tendances en matière de violation de données, afin de modifier correctement leurs pratiques.

Le travail hybride et à distance constitue une part importante de votre surface d'attaque

L'enquête de Forrester sur la sécurité en 2023 montre que 21 % des violations de données survenues au cours des 12 derniers mois dans les entreprises étaient dues à une attaque externe ciblant l'environnement de travail à

domicile ou à distance d'un employé (voir la figure 1). Il s'agit d'environnements que les organisations ne contrôlent pas, du réseau au cadre de travail physique, et qui peuvent inclure l'utilisation d'appareils non gérés, qui créent tous des problèmes de sécurité et des failles que les attaquants peuvent exploiter. Ces environnements domestiques incluent des appareils périphériques , comme les routeurs , que les groupes d'acteurs malveillants ciblent et utilisent comme rampes de lancement. Les attaques externes ciblant l'organisation ont été à l'origine de 28 % des violations ; 22 % étaient des incidents internes et 19 % étaient des attaques ou des incidents impliquant l'écosystème externe. Parallèlement, 10 % des violations étaient dues à des actifs perdus ou volés. Ces actifs peuvent inclure des smartphones, des tablettes, des ordinateurs portables, des disques durs externes et des clés USB.

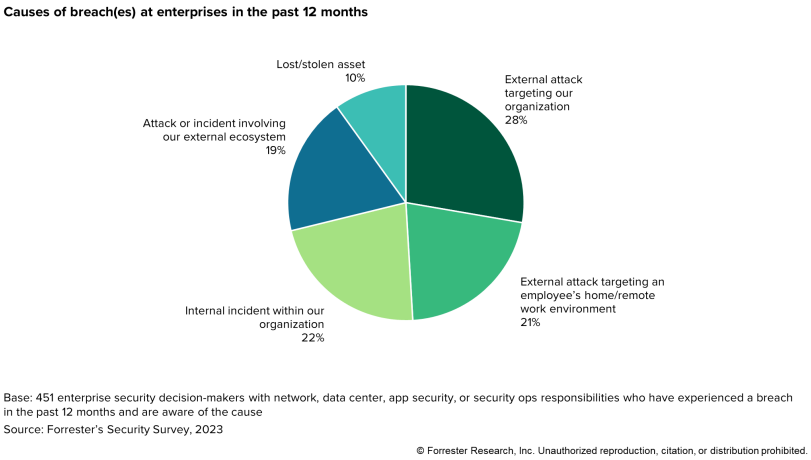


Figure 1 – Causes courantes des violations de sécurité dans les entreprises

Différents types de données ont une probabilité de compromission variable selon la région

À l'échelle mondiale, les données personnelles, les identifiants d'authentification et les PHI sont les trois principaux types de données personnelles compromises. Ce phénomène est particulièrement marqué en Asie-

Pacifique : environ la moitié des décideurs en matière de sécurité des entreprises qui ont subi une violation au cours des 12 derniers mois ont déclaré que les données personnelles, les identifiants d'authentification ou les PHI ont été potentiellement compromis ou violés (voir la figure 2). Il convient de noter que près d'un tiers des répondants en Asie-Pacifique ont signalé une compromission des numéros de compte, contre 23 % en Amérique du Nord et 21 % en Europe. Le rapport Verizon Business DBIR 2023 met en évidence le déplacement des modèles d'attaque de l'Amérique du Nord vers l'Europe et l'Asie-Pacifique, et la manière dont l'Asie-Pacifique a été fortement ciblée et touchée par une multitude de types d'attaques, allant de l'ingénierie sociale et des ransomwares à l'espionnage des États-nations motivé par des alliances politiques découlant d'événements géopolitiques en Russie, en Ukraine, en Chine et à Taïwan. Dans l'analyse de Forrester sur les principales violations de 2023 , l'Indonésie, l'Inde, le Bangladesh et l'Australie figurent en bonne place, avec des violations majeures dans le secteur public, l'éducation et la santé.

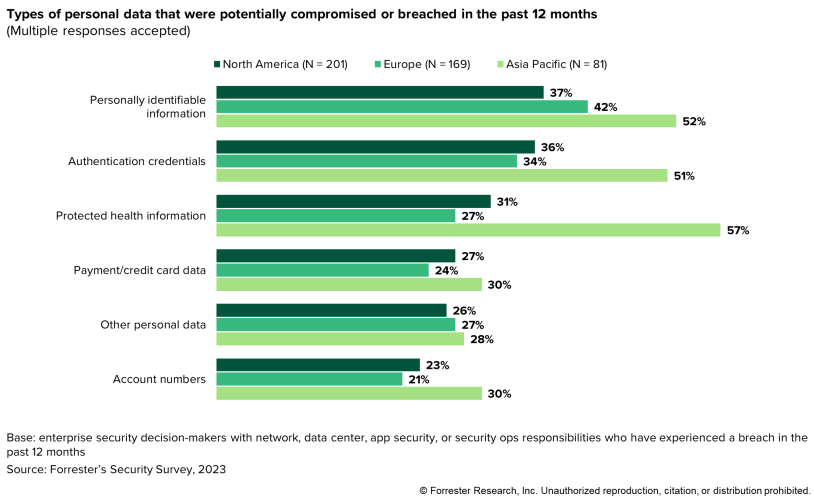


Figure 2 – Types de données personnelles potentiellement compromises ou violées par région

Les données financières sont les données d'entreprise les plus fréquemment perdues et celles qui varient le

plus selon les régions

En ce qui concerne les violations de données d'entreprise, les données financières ont été signalées par 31 % des décideurs en matière de sécurité des entreprises en Amérique du Nord et 38 % en Asie-Pacifique (voir la figure 3). Les données financières peuvent avoir de multiples avantages, allant de la révélation d'informations sur la santé des opérations commerciales à l'identification de cibles lucratives pour l'extorsion, en passant par l'utilisation pour des délits d'initiés. En Europe, les répondants étaient plus susceptibles de signaler une violation d'autres données d'entreprise sensibles (33 %) que de données financières (25 %). La propriété intellectuelle d'entreprise a été compromise par seulement 18 % des répondants en Europe, 28 % en Asie-Pacifique et 26 % en Amérique du Nord au cours des 12 derniers mois. En fin de compte, les attaquants sont motivés par des incitations financières. L'évolution des tendances en matière de ransomware, comme la menace de divulguer des données au public ou d'extorquer davantage les victimes pour la restitution des données volées, peut être un facteur déterminant pour cibler à la fois les informations personnelles et les données d'entreprise comme la propriété intellectuelle.

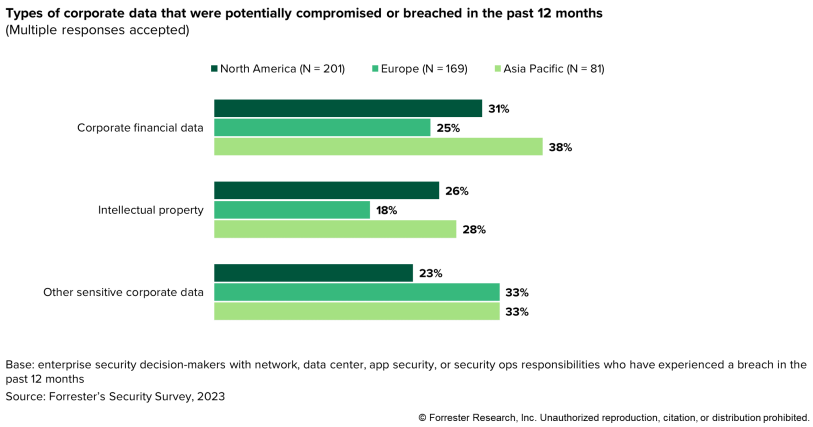


Figure 3 – Types de données d'entreprise compromises par région

Les mesures prises après une violation de données vont des interruptions d'activité aux nouvelles dépenses technologiques

Les mesures prises par les organisations après une violation peuvent varier considérablement en fonction de différents facteurs. L'un des facteurs déterminants est le fait que la violation ait concerné des données personnelles ou des données d'entreprise.

Les répercussions après une violation commencent à être similaires, quel que soit le type de données compromises

Dans l'enquête Forrester Security Survey 2022 , que la violation impliquait des données personnelles ou professionnelles, les répercussions sur l'assurance cybernétique figuraient parmi les principaux effets. Les répercussions sur l'assurance cybernétique figurent toujours parmi les cinq principaux effets des violations d'entreprise au cours des 12 derniers mois dans l' enquête Forrester Security Survey 2023. L'interruption d'un processus commercial d'entreprise était un effet fréquemment sélectionné, que le type de données compromises soit des données personnelles (32 %) ou des données d'entreprise (36 %) (voir la figure 4). Cela reflète la nature changeante des attaques de ransomware et de l'extorsion aujourd'hui. L'impact sur les données elles-mêmes est également plus important ; les décideurs en matière de sécurité des entreprises qui ont signalé des violations au cours des 12 derniers mois ont également signalé les effets d'une violation de données personnelles, notamment la manipulation de données (29 %), l'extorsion de données (27 %) et le vol de données (26 %). Les violations de données d'entreprise ont des effets similaires, et les répondants évoquent également la manipulation de données (33 %), l'extorsion de données (32 %) et le vol de données (30 %).

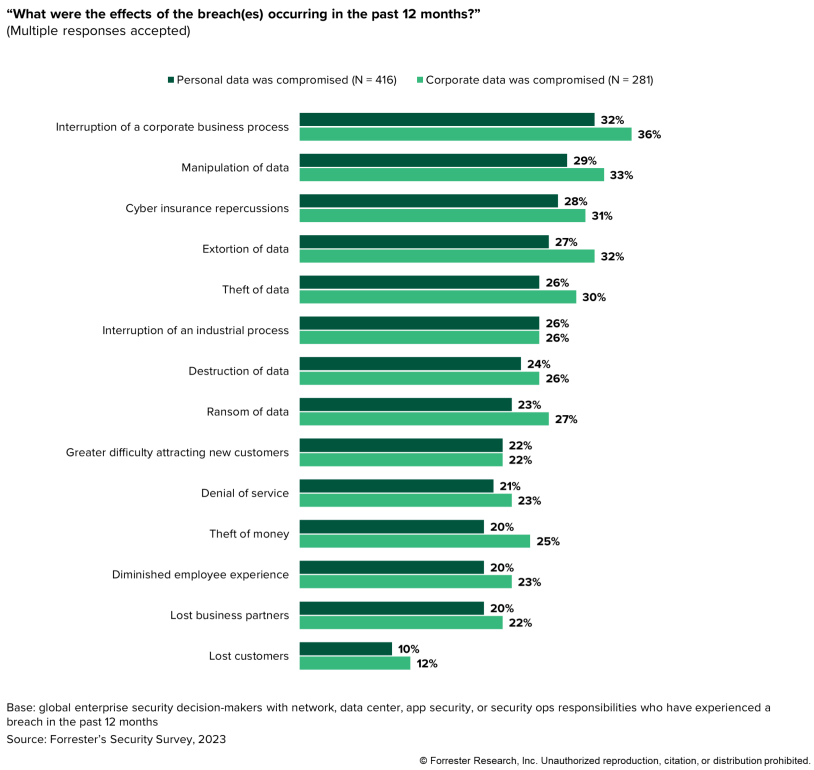


Figure 4 – L'interruption d'un processus opérationnel d'entreprise arrive en tête de liste des effets d'une violation

Après une violation, les organisations dépensent principalement de l'argent dans la réponse aux incidents et d'autres technologies

Les entreprises interrogées qui ont subi une violation au cours des 12 derniers mois ont indiqué avoir dépensé davantage en nouvelles technologies ou services pour répondre aux incidents lorsque les données personnelles ont été compromises (42 %) ainsi que lorsque les données de l'entreprise ont été compromises (46 %). C'est un bon signe – car les entreprises se tournent vers des professionnels pour un aspect aussi essentiel de la réponse et de la récupération – et cela reflète l'impact de l'assurance cyber et des assureurs sur la préparation à la réponse aux incidents. Les entreprises augmentent également généralement leurs dépenses en nouvelles technologies après une violation, y compris les technologies couvrant la détection, la protection, la récupération et la collecte et la conservation des journaux (voir la figure 5). Malheureusement, il faut parfois une violation pour débloquer les budgets de sécurité.

Notamment, 40 % des personnes ayant déclaré avoir subi une violation de données personnelles et 44 % de celles ayant déclaré avoir subi une violation de données d'entreprise ont investi dans de nouvelles technologies de détection. Les investissements dans de nouvelles technologies de protection sont également fréquents parmi les décideurs en matière de sécurité qui ont subi une violation de données d'entreprise (43 %) et ceux qui ont subi une violation de données personnelles (39 %).

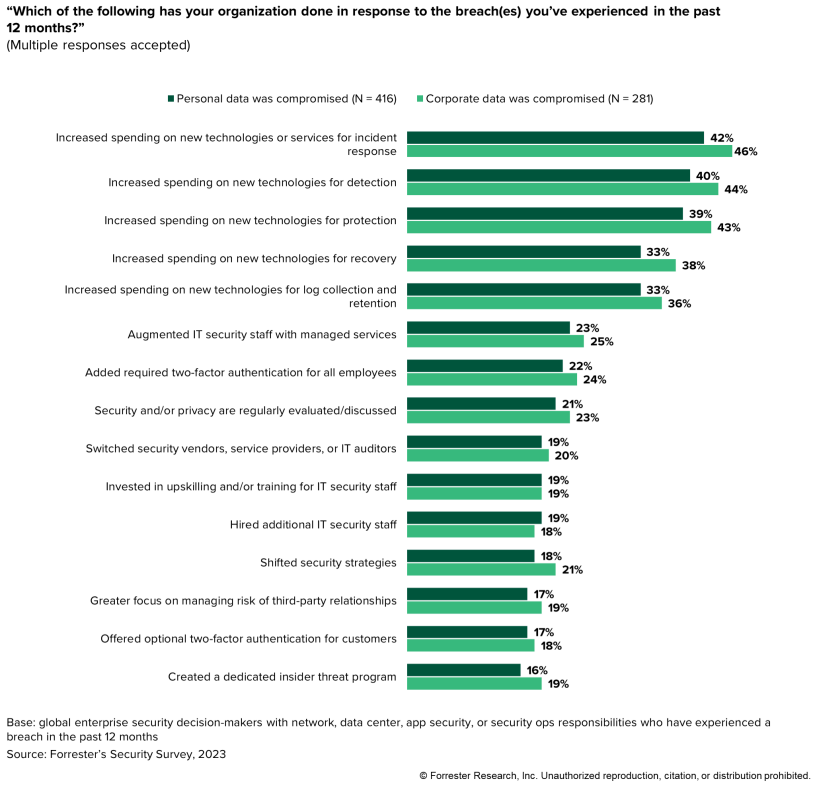


Figure 5 – Les violations de données stimulent les dépenses en nouveaux services et technologies

Les entreprises s'approvisionnent différemment en technologies de sécurité des données

Les fonctionnalités de sécurité des données sont de plus en plus intégrées aux principales plateformes technologiques de productivité de Microsoft et de Google, ainsi qu'aux référentiels de données tels que Snowflake, Databricks et MongoDB. Les organisations disposent également d'une multitude d'autres options,

allant des solutions tierces autonomes et des solutions ponctuelles aux plateformes de sécurité des données de fournisseurs tels qu'IBM, Immuta et Varonis. Il ne s'agit pas d'une option mutuellement exclusive ; il est courant que les entreprises utilisent à la fois des fonctionnalités intégrées et des solutions autonomes pour la sécurité des données, y compris plusieurs types de plateformes de sécurité des données au sein de leur environnement d'entreprise. Cependant, les préférences régionales varient.

Les entreprises de la région Asie-Pacifique sont plus susceptibles de s'appuyer sur Microsoft, tandis que Google a du succès en Amérique du Nord

Microsoft (Microsoft 365 et Azure) et Google (Workspace et Google Cloud Platform) sont les principaux centres de gravité des contrôles de données au sein d'une organisation, avec des fonctionnalités intégrées que les entreprises peuvent activer et utiliser. De nombreuses entreprises trouvent une proposition intéressante dans l'utilisation des fonctionnalités intégrées de ces plateformes plutôt que d'investir séparément dans des solutions autonomes supplémentaires à gérer. Cependant, il existe souvent des compromis entre l'utilisation de fonctionnalités intégrées et d'autres solutions autonomes. Par exemple, une solution autonome peut inclure des fonctionnalités plus robustes pour les besoins d'une organisation et permettre la gestion de politiques cohérentes sur plusieurs référentiels de données. 41 % des décideurs en matière de sécurité des entreprises en Asie-Pacifique ont déclaré qu'ils utilisaient les fonctionnalités intégrées de Microsoft, contre 36 % en Amérique du Nord et 34 % en Europe (voir la figure 6). 41 % des répondants nord-américains ont déclaré qu'ils s'appuyaient principalement sur les fonctionnalités intégrées de Google plutôt que sur des solutions tierces, contre 35 % en Europe et 37 % en Asie-

Pacifique. Dans l'ensemble, les répondants étaient moins susceptibles de répondre qu'ils s'appuyaient principalement sur les contrôles intégrés des référentiels de données qu'ils utilisent plutôt que sur une solution tierce.

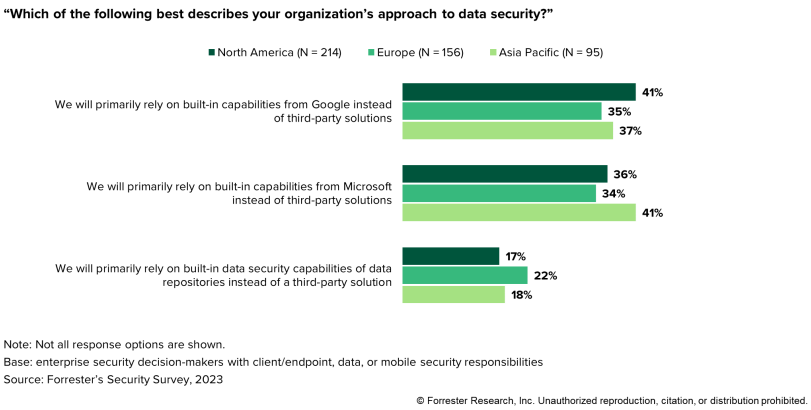


Figure 6 – Les entreprises s'appuient principalement sur des capacités intégrées pour la sécurité des données

La prévention des pertes de données (DLP) est largement répandue, avec la plus grande traction et utilisation en Amérique du Nord

L'utilisation de la DLP par les entreprises est courante dans le monde entier. La fonctionnalité de surveillance et de blocage de la DLP permet d'appliquer des politiques qui peuvent répondre à divers besoins. Elle peut répondre aux exigences des auditeurs, démontrer des capacités d'application pour les exigences de conformité telles que le RGPD et fonctionner comme une capacité technologique clé pour un programme de gestion des risques internes . La popularité de la DLP est particulièrement évidente pour la DLP des terminaux : 83 % des décideurs mondiaux en matière de sécurité des entreprises ont déclaré que leur organisation avait adopté cette capacité. Cependant, les entreprises interrogées en Amérique du Nord (82 %) et en Asie-Pacifique (84 %) adoptent la DLP par e-mail, contre 72 % en Europe (voir la figure 7). Les fonctionnalités DLP font également partie des solutions de passerelle de sécurité cloud (CSG)/de

courtier en sécurité d'accès cloud (CASB) aujourd'hui, bien que toutes les entreprises qui utilisent une CSG/CASB ne s'appuient pas sur les fonctionnalités DLP pour activer le blocage. L'adoption de la CSG/CASB est relativement élevée dans toutes les régions : les trois quarts des entreprises en Europe, 79 % en Asie-Pacifique et 83 % en Amérique du Nord ont adopté la CSG/CASB.

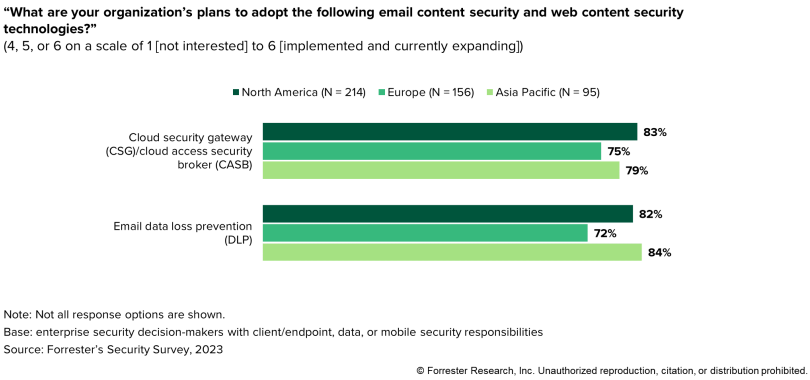


Figure 7 – L'adoption de la DLP et de la CSG/CASB par courrier électronique est élevée dans toutes les régions

La confidentialité et l'utilisation des données entraîneront des investissements supplémentaires dans les contrôles de sécurité des données

Les décideurs en matière de sécurité des entreprises prévoient d'accroître leurs investissements dans de nouveaux contrôles de sécurité des données afin de se conformer aux exigences de confidentialité au cours des 12 prochains mois : 80 % des répondants en Amérique du Nord, 78 % en Asie-Pacifique et 72 % en Europe ont déclaré que c'était le cas pour leur entreprise (voir la figure 8). À l'échelle mondiale, 75 % des entreprises interrogées indiquent préférer travailler avec des startups pour identifier de nouvelles approches en matière de sécurité des données. Les technologies de préservation de la confidentialité sont un exemple de contrôles et d'approches centrés sur les données disponibles aujourd'hui . Cela décrit une variété d'approches plutôt qu'une seule technique. Cela peut inclure des techniques de dépersonnalisation telles que le masquage et la

tokenisation, des approches telles que le cryptage homomorphe et l'informatique confidentielle. L'intérêt pour les technologies de préservation de la confidentialité est croissant, en particulier en Asie-Pacifique, où 84 % des entreprises interrogées ont indiqué qu'elles prévoyaient d'augmenter leurs dépenses dans ce pays pour protéger les données en cours d'utilisation. L'intérêt va également probablement s'intensifier en Europe, car la loi européenne sur la résilience opérationnelle numérique impose la confidentialité des données au repos, en cours d'utilisation ou en transit, en particulier lorsque les données sont utilisées pour soutenir des fonctions critiques ou importantes.

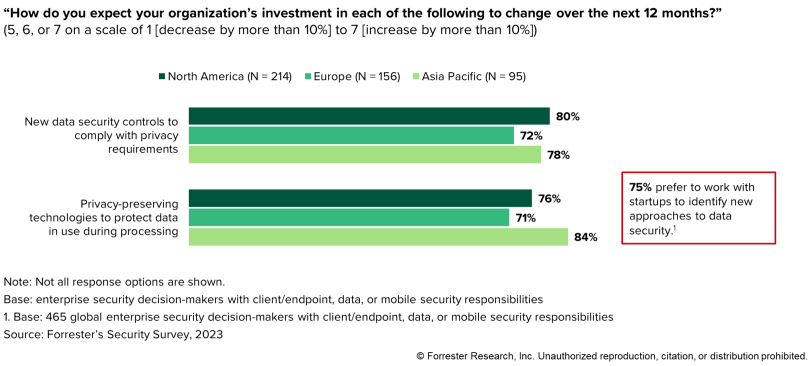


Figure 8 – Les initiatives en matière de confidentialité et de données stimulent les attentes d'augmentation des dépenses en Asie-Pacifique

Peu d'organisations déploient toutes leurs capacités de sécurité des données via le cloud

Seuls 13 % des décideurs mondiaux en matière de technologies de sécurité des entreprises ont déclaré que leur organisation avait déployé 100 % de ses capacités de sécurité des données dans le cloud (voir la figure 9). Plus d'un tiers d'entre eux en ont déployé moins de la moitié, tandis que 2 % disposent de capacités de sécurité des données qui restent entièrement déployées sur site. Ceux qui doivent déployer des solutions sur site ont généralement des exigences spécifiques pour le faire,

qu’elles soient motivées par la conformité, l’infrastructure ou un niveau élevé d’aversion au risque. La réalité pour de nombreuses organisations est qu’elles doivent fonctionner dans un monde hybride. Même si elles s’engagent à migrer vers le cloud, les entreprises ne déplaceront pas l’intégralité de leurs données et de leur environnement informatique en une seule fois. Elles peuvent donner la priorité à des systèmes, des données et des cas d’utilisation particuliers. C’est un parcours, et la décision de déployer également des capacités de sécurité des données via le cloud suit un chemin similaire.

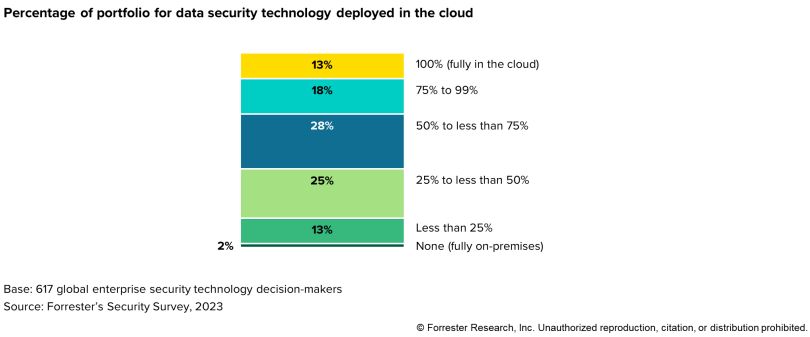
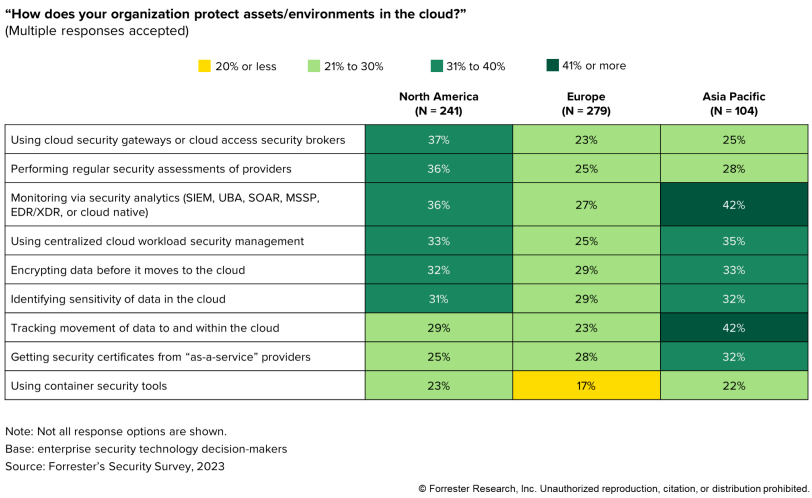


Figure 9 – La plupart des organisations ont déployé des capacités de sécurité des données de manière hybride

Les entreprises utilisent plusieurs approches pour protéger les données dans les environnements cloud

Français Les entreprises nord-américaines interrogées se tournent vers l'utilisation de passerelles de sécurité cloud ou de courtiers en sécurité d'accès au cloud (37 %), effectuent des évaluations de sécurité régulières des fournisseurs (36 %) et surveillent via des analyses de sécurité (36 %) pour protéger les actifs et les environnements cloud (voir Figure 10). Les entreprises européennes interrogées identifient la sensibilité des données dans le cloud (29 %) et chiffrent les données avant qu'elles ne soient transférées vers le cloud (29 %) pour protéger les actifs. Pour protéger les actifs, les entreprises d'Asie-Pacifique interrogées surveillent via

des analyses de sécurité (42 %), suivent les mouvements de données vers et au sein du cloud (42 %) et utilisent une gestion centralisée de la sécurité des charges de travail cloud (35 %). Les différences par région sont influencées par un certain nombre de facteurs, tels que la popularité des environnements cloud, y compris le cloud public, et les problèmes de sécurité qu'ils génèrent ; les types de données transférées dans divers environnements cloud préoccupants, comme les applications SaaS ; et l'environnement réglementaire.



"How does your organization protect assets/environments in the cloud?"
(Multiple responses accepted)

20% or less | 21% to 30% | 31% to 40% | 41% or more

	North America (N = 241)	Europe (N = 279)	Asia Pacific (N = 104)
Using cloud security gateways or cloud access security brokers	37%	23%	25%
Performing regular security assessments of providers	36%	25%	28%
Monitoring via security analytics (SIEM, UBA, SOAR, MSSP, EDR/XDR, or cloud native)	36%	27%	42%
Using centralized cloud workload security management	33%	25%	35%
Encrypting data before it moves to the cloud	32%	29%	33%
Identifying sensitivity of data in the cloud	31%	29%	32%
Tracking movement of data to and within the cloud	29%	23%	42%
Getting security certificates from "as-a-service" providers	25%	28%	32%
Using container security tools	23%	17%	22%

Note: Not all response options are shown.
Base: enterprise security technology decision-makers
Source: Forrester's Security Survey, 2023

Figure 10 – Les principales approches de protection des actifs dans le cloud varient selon la région

Matériel supplémentaire

Méthodologies d'enquête

Enquête de Forrester sur la sécurité, 2023