Microsoft

hypothesis

Indice de sécurité des données

Tendances, perspectives et stratégies de sécurisation des données

Avant-propos

À notre époque caractérisée par l'essor des données, il est devenu incontestable que les données d'une organisation ne sont rien de moins que sa force vitale. La grande quantité de données créée et utilisée par les entreprises alimente les opérations critiques, éclaire la prise de décisions stratégiques et globales, et façonne leurs possibilités d'avenir. Les données ne sont pas simplement une ressource; elles sont le cœur battant des entreprises modernes.

Pourtant, cette dépendance accrue aux données s'accompagne d'une dure réalité : les vulnérabilités cachées dans l'ombre de l'univers numérique sont réelles et se développent rapidement. Les cybermenaces, les violations de données et les incidents liés aux délits d'initié ne sont plus rares; elles sont omniprésentes et s'intensifient, ce qui fait courir des risques aux organisations qui dépendent des données. Parmi les décideurs que nous avons interrogés récemment, 89 % ont déclaré qu'ils considéraient que la sécurité des données était essentielle à leur prospérité en général.

Dans ce livre blanc, nous partons à l'exploration de cet impératif fondamental : la protection des données de votre organisation. Mon équipe et moi-même sommes ravis de partager nos conclusions avec vous et, je l'espère, d'entamer un dialogue portant sur la manière d'avancer collectivement vers une sécurité des données d'excellence. Nos découvertes illustrent à quel point la sécurité des données se trouve à un tournant critique. Bien que les décideurs s'accordent à dire qu'elle est essentielle à la sécurité de leurs données, et que la plupart se disent confiants dans ce qu'ils font, ils se trouvent simultanément confrontés à une multitude d'incidents et de défis liés à la sécurité des données. Et bien que 80 % des dirigeants à qui nous avons parlé concèdent qu'une approche intégrée « best-in-suite » est préférable aux solutions ponctuelles, la plupart des entreprises utilisent encore un système fragmenté et composé de nombreux outils pour protéger leurs données, ce qui est souvent cause d'une augmentation plutôt que d'une diminution du nombre des incidents de sécurité.

Nous vous invitons à lire et partager ce dernier rapport et à le considérer comme le point de départ de nouvelles conversations avec nos équipes sur la meilleure façon d'assurer notre avenir collectif.

Rudra Mitra
Vice-président
Sécurité et conformité des données, Microsoft

Présentation

La prévention des violations de données et autres incidents de sécurité continue de préoccuper les décideurs en matière de sécurité et de risque. C'est aussi la pierre angulaire de tout programme de cybersécurité, car une seule violation peut causer des dommages importants aux finances et à la réputation de l'entreprise. Les entreprises doivent protéger un large éventail de données sensibles, notamment les informations concernant les employés et les clients, la propriété intellectuelle, les prévisions financières et les données opérationnelles.

Pour comprendre les pratiques et les tendances actuelles en matière de sécurité des données et reconnaître les occasions d'amélioration, Microsoft a chargé une agence de recherche indépendante, Hypothesis Group, de mener une enquête multinationale auprès de plus de 800 professionnels de la sécurité des données. Ce rapport présente cinq conclusions clés de l'étude, parmi lesquelles les tendances, les perspectives et les stratégies de sécurisation des données.

Principaux résultats

1

Les décideurs pensent être protégés, mais la réalité ne correspond pas à leurs perceptions.

Bien que la plupart des décideurs se disent satisfaits et confiants quant à leurs solutions de sécurité des données, ils subissent encore en moyenne 59 incidents de sécurité par an, avec des conséquences coûteuses.

2

Disposer de davantage d'outils n'implique pas une meilleur efficacité ou une meilleure sécurité des données, bien au contraire.

80 % des décideurs conviennent que les solutions complètes et intégrées sont supérieures aux meilleures solutions manuelles. Et pourtant, les entreprises continuent d'utiliser des outils disparates, disposant en moyenne de plus de 10 outils de sécurité des données. Mais ceux qui possèdent le plus d'outils subissent également plus d'incidents de sécurité, ce qui suggère que plus la prolifération des outils est importante, plus la sécurité est faible.

3

Les entreprises sont toujours livrées au stress des incidents de sécurité de provenance externe et interne, en particulier en ce qui concerne les données d'affaires.

50 % des entreprises interrogées ont déjà fait l'expérience d'une attaque par rançongiciel ou de logiciel malveillant au cours de l'année écoulée, et de nombreux décideurs pensent que leur organisation n'est pas entièrement préparée pour prévenir et traiter de futures attaques. En interne, les initiés malveillants constituent une préoccupation majeure. De plus, les entreprises sont très préoccupées par la vulnérabilité de leurs données d'affaires. Cela souligne une fois de plus la nécessité d'une plateforme de sécurité qui traite les risques de manière exhaustive.

Principaux résultats

4

Les entreprises ont besoin du nuage et de l'IA pour mener à bien leur transformation numérique, mais ils constituent aussi les emplacements de données les plus vulnérables.

Les applications infonuagiques et la technologie de l'IA sont devenues essentielles pour la collaboration et la productivité des entreprises; toutefois, cette évolution a également engendré des risques plus dynamiques et protéiformes. À mesure que les entreprises adoptent l'IA, il devient essentiel d'améliorer la sécurité des données pour en permettre une utilisation responsable et sûre.

5

L'automatisation et l'IA sont des voies prometteuses pour une meilleure protection.

Les entreprises souhaitent que leurs équipes consacrent moins de temps à la détection et plus de temps à la prévention. L'automatisation peut permettre aux équipes de se concentrer davantage sur les mesures proactives, tandis que l'emploi de l'IA pour la sécurité des données aide les entreprises à se positionner de manière plus stratégique et à mieux anticiper les menaces futures.

1

Les décideurs pensent être protégés, mais la réalité ne correspond pas à leurs perceptions.

Les décideurs pensent être protégés, mais la réalité ne correspond pas à leurs perceptions.

En apparence, les décideurs perçoivent de leurs solutions de sécurité des données de hauts niveaux de satisfaction et de confiance. La majorité des entreprises conviennent que leurs contrôles de sécurité des données sont suffisants pour empêcher les violations, estiment savoir où résident la plupart de leurs données et pensent pouvoir détecter la majorité des risques qui les concernent.

Dans le même temps, les entreprises continuent de connaître d'importants volumes d'incidents de sécurité des données : 59 en moyenne au cours des 12 derniers mois, dont un cinquième sont considérés comme « graves ». Ces incidents ont un impact notable car, en moyenne, les organisations estiment que le coût financier total de leur plus grave incident de sécurité de données est d'environ 244 000 dollars (ce qui signifie que les incidents annuels peuvent coûter jusqu'à 15 millions de dollars). En plus de ces coûts, quatre décideurs sur 10 affirment également qu'en cas d'incident de sécurité des données, les coûts opérationnels liés à la récupération et la perte d'activité consécutive à une réputation entachée sont une source d'inquiétude.

De plus, 92 % d'entre eux sont confrontés à des difficultés qui entravent leur capacité à investir davantage dans la sécurité des données, principalement dans les domaines des coûts, de l'intégration et du délai de mise en œuvre, d'où la nécessité de solutions moins coûteuses et plus économes en main-d'œuvre.

Entre le sentiment de confiance en l'état de préparation à la sécurité des données et la réalité des incidents auxquels les entreprises sont confrontées, il y a une différence. Même s'il est important pour les organisations de savoir où se trouvent leurs données et de détecter les risques, ces mesures, individuellement ou séparément, ne sont pas suffisantes pour permettre aux entreprises de prévenir les incidents qui empêchent les responsables de la sécurité des données et les décideurs de dormir la nuit.

Comme le dit un DSI (Directeur de la sécurité de l'information), des services financiers : « Je ne peux pas déclarer à mon comité d'administration que j'ai sécurisé les données, mais que je ne les ai pas protégées... la dernière chose que nous voulons voir, c'est un gros titre en première page du Wall Street Journal disant que notre banque ne tient pas ses promesses. »

59

Nombre moyen d'incidents de sécurité des données au cours des 12 derniers mois

JUSQU'À

15 millions de dollars

Coût annuel d'un incident de sécurité grave

2

Disposer de davantage d'outils n'implique pas une meilleur efficacité ou une meilleure sécurité des données, bien au contraire.

Disposer de davantage d'outils n'implique pas une meilleur efficacité ou une meilleure sécurité des données, bien au contraire.

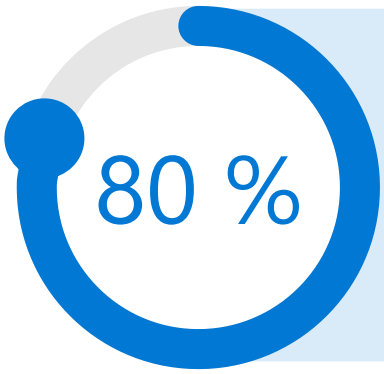
Les entreprises se rendent compte qu'après des années d'utilisation de solutions ponctuelles, des lacunes sont apparues en termes de visibilité et d'efficacité, en raison du cloisonnement des différents outils de sécurité. Cette tendance cède maintenant la place au désir de disposer d'une solution intégrée pour la sécurité des données; 80 % des personnes interrogées conviennent qu'une plateforme de sécurité des données complète, avec des solutions intégrées, est supérieure à plusieurs solutions de pointe conjointes devant être intégrées et gérées manuellement.

Pourtant, même si la grande majorité considère que les solutions intégrées sont préférables, les outils de sécurité des données demeurent nombreux et fragmentés.

En conséquence, les entreprises déclarent utiliser en moyenne 10 outils pour gérer les risques de sécurité des données, notamment des outils de protection contre la perte de données,de protection des informations, de gestion des risques internes, de gestion des événements et des informations de sécurité (SIEM), des courtiers en sécurité d'accès au nuage, et d'autres encore. Pour les entreprises comptant plus de 5 000 employés, le nombre moyen d'outils est encore plus important.

Multiplier les outils peut créer une fausse impression de sécurité, car ceux qui en utilisent davantage (plus de 16) sont plus confiants dans leur niveau de sécurité des données que ceux qui en utilisent moins (61 % contre 56 %).

Cependant, les recherches contredisent ce sentiment de sécurité, car les entreprises disposant de 16 outils ou plus ont rencontré davantage d'incidents de sécurité des données au cours de l'année écoulée (133 en moyenne), contre 48 dans les entreprises ayant moins d'outils.

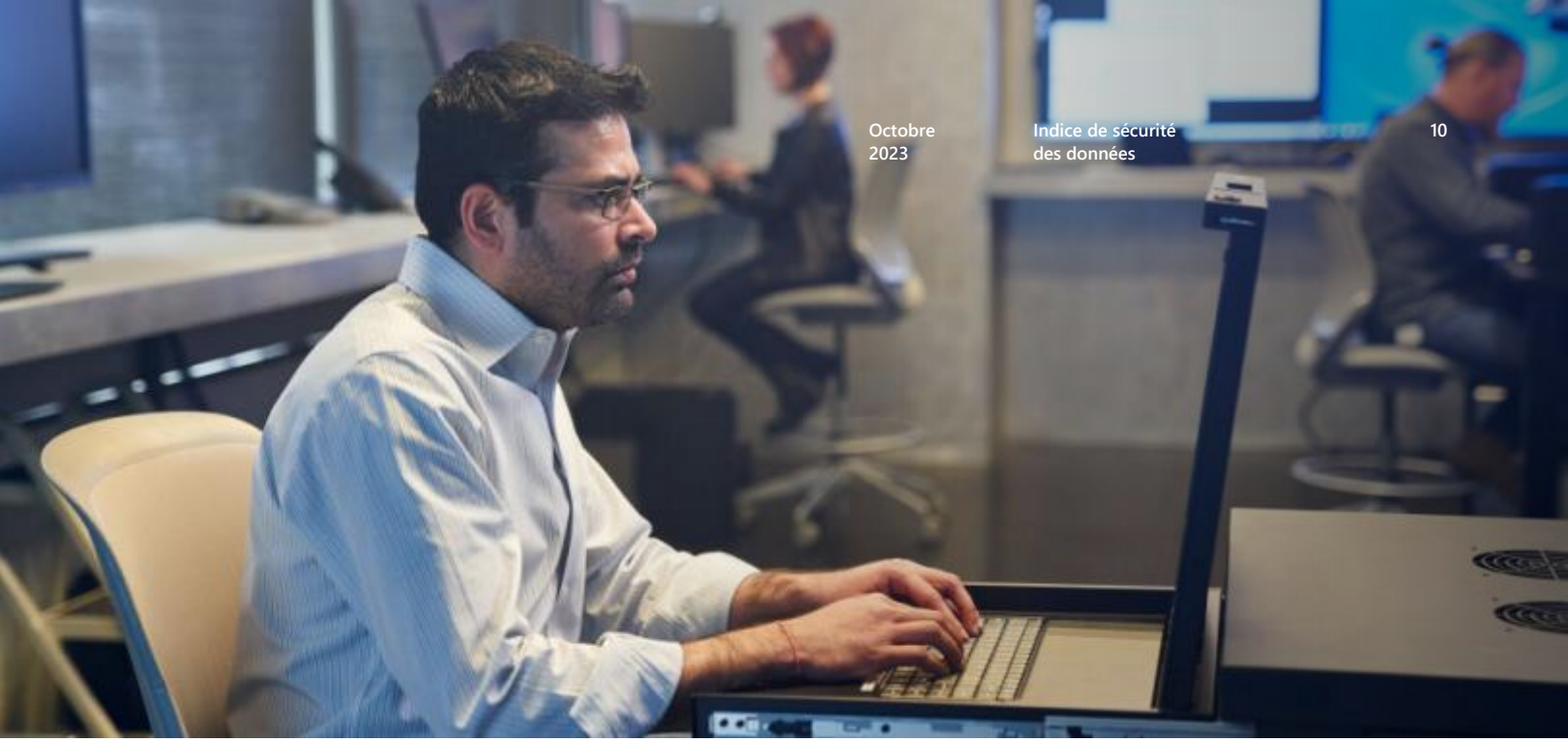


conviennent qu'une plateforme de sécurité des données complète, avec des solutions intégrées, est supérieure à plusieurs solutions de pointe conjointes devant être intégrées et gérées manuellement.

2,8 fois

plus d'incidents de sécurité des données au cours de l'année écoulée

pour les entreprises disposant de 16 outils ou plus (par rapport aux entreprises disposant de moins d'outils)



Les arguments en faveur de solutions plus intégrées et d'un moindre nombre d'outils pour renforcer la sécurité des données deviennent encore plus convaincants si l'on examine les sentiments et les pratiques de ceux qui privilégient les solutions de pointe ou la prolifération des outils.

« Comment les données vont-elles être recueillies, agrégées et utilisées à partir de plusieurs systèmes? De nombreux points de données différents doivent être rassemblés dans un écosystème pour que cela fonctionne vraiment. Sinon, vous obtenez une sécurité des données qui ressemble à du gruyère. »

Vice-président des TI, Fabrication et Production

Tout d'abord, la disparité de nombreux outils de sécurité des données peut entraîner des lacunes de visibilité et davantage de données cachées. En fait, ceux qui se préoccupent des données cachées sont plus susceptibles de préférer les solutions de pointe. Cela est très probablement dû au fait que les entreprises ayant adopté cette approche doivent redoubler d'efforts pour obtenir une visibilité complète du niveau de sécurité de leurs données.

Deuxièmement, la gestion de solutions cloisonnées est plus complexe pour les équipes de sécurité des données, car chaque solution distincte nécessite un personnel dédié, l'installation et la maintenance d'un agent de point de terminaison et diverses nouvelles procédures. Prenez pour exemple le contrôle et le tri des alertes, l'une des tâches qui nécessitent du personnel et des ressources. Les équipes de sécurité des données doivent redoubler d'efforts lorsqu'elles gèrent des solutions isolées, car le nombre des alertes augmente. Les entreprises disposant de plus d'outils reçoivent en moyenne 96 alertes de sécurité des données par jour, tandis que les équipes qui disposent de moins d'outils en reçoivent moins de la moitié (44). De plus, elles ne peuvent pas examiner autant de ces alertes que les équipes disposant de moins d'outils (61 % contre 68 %). Il en résulte souvent aussi que les entreprises disposant de plus d'outils sont plus dans la réaction que les entreprises qui utilisent moins d'outils.

Enfin, un grand nombre d'outils implique également que les entreprises doivent déployer des efforts considérables pour intégrer les informations obtenues et les plans de correction, et que des informations peuvent se perdre. Quand on pose la question des principaux défis en matière de sécurité des données, le coût de mise en œuvre ou de maintenance, puis les difficultés d'intégration des solutions de sécurité des données prennent les deux premières places.

Cela se traduit par des processus plus longs et plus lents : 37 % des personnes qui utilisent 16 outils ou plus déclarent avoir besoin d'un mois ou plus pour mener à bien une enquête sur la sécurité des données, contre seulement 21 % de celles qui ont moins d'outils.

« En ce moment, nous faisons du sur-place. Chacun de nos systèmes a son propre portail, ses propres outils, ses propres façons de faire les choses. Chacun suit son propre chemin dans son domaine d'expertise. Ensuite, ils se réunissent et décident de ce qui se passe, et nous abordons la question à partir de là. Il y a donc un peu un travail manuel à ce stade », déclare un Directeur de l'infrastructure et des opérations dans la fabrication et la production.

En fin de compte, en choisissant de continuer avec plusieurs solutions, les entreprises ignorent leur propre discours sur l'intérêt des solutions intégrées et marchent dans la direction opposée, ce qui leur coûte du temps et de l'argent.

RÉSULTATS DE CEUX QUI UTILISENT MOINS D'OUTILS (<16) PAR RAPPORT À CEUX QUI EN UTILISENT PLUS (>16)	Faible volume d'outils	Grand volume d'outils
Nombre **d'incidents de sécurité des données** au cours des 12 derniers mois	48	133
Proportion d'incidents **graves** de sécurité des données	19 %	26 %
Notre stratégie actuelle de sécurité des données est plus **réactive**	31 %	40 %
Difficulté à **intégrer** des solutions	24 %	39 %
L'équipe de sécurité des données consacre plus de temps à la **réponse**	19 %	26 %
Nous sommes **confiants** en notre niveau de sécurité des données	56 %	61 %
Nombre d'alertes **reçues** par jour en moyenne	44	96
Proportion d'alertes que nous pouvons **examiner** par jour	68 %	61 %
Un mois ou plus nécessaire pour mener à bien une enquête sur la sécurité des données	21 %	37 %

3

Les entreprises sont toujours livrées au stress des incidents de sécurité de provenance externe et interne, en particulier en ce qui concerne les données d'affaires.

Les entreprises sont toujours livrées au stress des incidents de sécurité de provenance externe et interne, en particulier en ce qui concerne les données d'affaires.

Étant donné que les facteurs liés aux données (y compris les personnes qui interagissent avec les données, les activités concernant les données et les appareils et applications utilisés pour traiter les données), évoluent constamment, des incidents de sécurité des données et des violations peuvent se produire à tout moment et n'importe où. De plus, ces menaces proviennent à la fois de pirates externes et de membres du personnel dignes de confiance, notamment d'employés, de sous-traitants et de partenaires. Que ce soit par malveillance ou par inadvertance, tous les acteurs peuvent provoquer des incidents de sécurité des données. Cela signifie que le besoin de protection est constant dans une multitude de domaines.

Un vice-président des TI dans les services financiers a déclaré : « Ce contre quoi vous essayez de vous protéger est en constante évolution. C'est une cible mouvante. Elle sera toujours évolutive, changeante et flexible. Les choses à protéger et leur lieu de résidence ne feront que devenir plus variés. »

Bien que les incidents de sécurité des données proviennent de diverses sources, la menace externe par les logiciels malveillants ou les rançongiciels (incidents où un logiciel malveillant s'infiltre dans un système, fournissant aux pirates un accès non autorisé aux systèmes ou aux réseaux) est de loin la plus courante, 50 % des entreprises interrogées ayant connu au moins un incident de ce type au cours de l'année passée.

De plus, ces attaques portent là où les entreprises se sentent les plus vulnérables : 41 % d'entre elles déclarent se sentir moins bien préparées à faire face à de futures attaques de logiciels malveillants ou de rançongiciel au cours de l'année à venir. Ce sentiment de vulnérabilité est encore plus élevé chez ceux qui préfèrent une approche de pointe : 44 % ne se sentent pas préparés à une attaque de cette nature, contre seulement 36 % parmi ceux qui ont privilégié une solution intégrée.

La protection et la prévention contre les risques internes constituent également une préoccupation majeure pour les décideurs. 35 % disent avoir besoin de renforcer leurs défenses contre les initiés malveillants et les comptes compromis, et un tiers s'inquiètent des incidents internes involontaires. Bien que les incidents internes malveillants ne soient pas la principale source des violations de sécurité des données, ils représentent le deuxième type d'incident auquel les décideurs se sentent le moins préparés.

« Au moins une fois par mois, je reçois un appel d'un responsable paniqué... « Un événement s'est produit, j'ai découvert un événement, ou l'équipe de lutte contre les menaces a découvert un événement. » Certains de ces événements sont involontaires, d'autres viennent de personnes qui ne savent pas ou ne comprennent pas ce que leurs privilèges leur permettent. »

Directeur de la sécurité informatique d'une administration des États-Unis

Les initiés sont des personnes de confiance qui ont obtenu un accès aux ressources, aux données ou aux systèmes de l'entreprise qui ne sont généralement pas accessibles au public, ou qui en ont connaissance. Par conséquent, les risques pour la sécurité des données associés aux initiés ont tendance à être plus insaisissables et difficiles à détecter. Comme l'a relevé Bret Arsenault, le DSI de Microsoft; « En fin de compte, peu importe que la violation soit intentionnelle ou accidentelle. La stratégie de la sécurité de chaque entreprise doit intégrer la gestion des risques internes. »

RÉSUMÉ DES INCIDENTS DE SÉCURITÉ DES DONNÉES

Causes des incidents de sécurité des données	Incidents les plus courants au cours des 12 derniers mois	Moindre préparation à la prévention au cours des 12 prochains mois
Logiciel malveillant ou rançongiciel	**50 %**	**41 %**
Comptes compromis	**38 %**	**35 %**
Attaques par déni de service (DoS)	**35 %**	**33 %**
Utilisateurs internes par négligence	**32 %**	**29 %**
Utilisateurs internes par inadvertance	**31 %**	**32 %**
Initiés malveillants	**31 %**	**35 %**
Propriété physique	**29 %**	**29 %**

Les solutions de sécurité des données choisies par les entreprises doivent également prendre en charge diverses données sensibles, notamment les données d'affaires de grande valeur, les données opérationnelles et les données personnelles. Lors des incidents de sécurité des données des 12 derniers mois, 74 % des entreprises ont vu leurs données d'affaires exposées, 65 % ont vu leurs données opérationnelles compromises et 58 % ont vu leurs données personnelles vulnérables. Parmi les différents types de données, les données de propriété intellectuelle, de conception TI et réseau et les données à caractère personnel sont celles qui ont été le plus souvent exposées ou compromises.

Pour l'avenir, 77 % des entreprises perçoivent leurs données d'affaires, comme la propriété intellectuelle et le code source, comme les plus vulnérables. Cela est principalement dû au fait que les données d'affaires jouent un rôle crucial dans le gain d'avantages concurrentiels et la génération de revenus. Cependant, l'identification et le classement de ces données peuvent être difficiles, car les technologies classiques de reconnaissance de schémas, d'expressions régulières et de fonctions peuvent ne pas identifier efficacement les contenus dépourvus de formats de chaîne ou de mots clés spécifiques. Les entreprises ont donc besoin de technologies plus avancées pour découvrir et protéger leurs données sensibles vulnérables.

TYPES DE DONNÉES LES PLUS EXPOSÉS AU COURS DES 12 PROCHAINS MOIS

77 % **données d'affaires**		64 % **Données opérationnelles**		63 % **Données à caractère personnel**	
Propriété intellectuelle	**30 %**	Conception des TI et réseau	**29 %**	Informations personnelles et identifiables (PII)	**31 %**
Code source	**28 %**	États financiers	**18 %**	Informations des Ressources humaines (salaires, curriculum vitae, etc.)	**21 %**
Plans d'affaires	**27 %**	États de ventes et recettes	**15 %**	Données de l'industrie des cartes de paiement (PCI)	**18 %**
Secrets d'affaires	**24 %**	Approvisionnement et factures	**12 %**	Informations médicales protégées (PHI)	**18 %**
Fichiers de fusion et d'acquisition	**20 %**	Documents juridiques et contrats	**12 %**	Informations d'identification	**17 %**
Spécifications de construction	**18 %**	Procédés de fabrication et fichiers de commandes	**11 %**		

4

Les entreprises ont besoin du nuage et de l'IA pour mener à bien leur transformation numérique, mais ils constituent aussi les emplacements de données les plus vulnérables.

Les entreprises ont besoin du nuage et de l'IA pour mener à bien leur transformation numérique, mais ils constituent aussi les emplacements de données les plus vulnérables.

La collaboration au travers d'applications et de plateformes infonuagiques, associée aux nouvelles technologies IA, améliore considérablement la productivité des employés et permet des modalités de travail flexibles. Cela rend les applications infonuagiques et la technologie IA essentielles pour les organisations. En moyenne, les entreprises utilisent aujourd'hui 147 services de nuage public, aussi bien SaaS, PaaS et IaaS[1]. Et 66 % des entreprises ont élaboré une stratégie IA (et 36 % l'ont déjà mise en œuvre)[2]. Cependant, cette évolution a engendré des risques plus dynamiques et polymorphes en raison de la difficulté de définir clairement les frontières des données dans divers environnements.

1. Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022
2. Microsoft data security AI research, Hypothesis, mars 2023

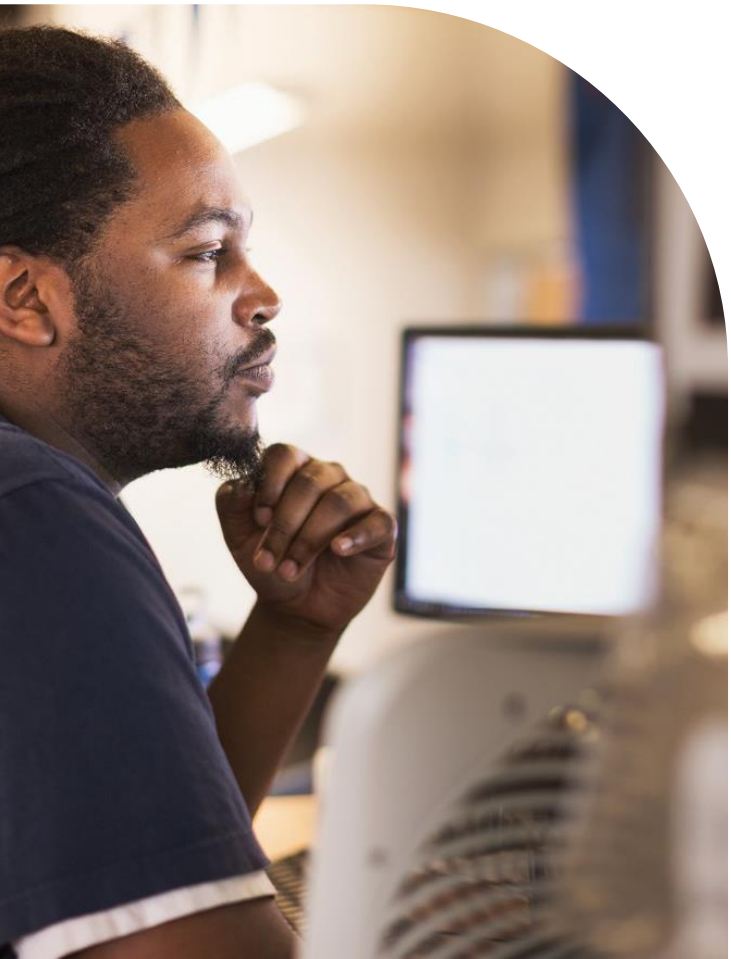
Il est encore plus crucial de disposer de la solution de sécurité des données adaptée à ces emplacements de données à haute productivité. Au cours des 12 derniers mois, 42 % des entreprises ont signalé des incidents de sécurité dans le stockage infonuagique et 31 % dans les courriels, la messagerie instantanée ou les outils de réunion en ligne. Les incidents semblent plus courants là où la productivité et la collaboration prévalent.

La gestion de ces types d'incidents mobilise des ressources, et 79 % des entreprises indiquent que leur équipe de sécurité des données a besoin d'un effectif accru pour assumer efficacement les responsabilités critiques en matière de sécurité des données. Cependant, parmi les entreprises qui affirment avoir besoin de plus de personnel, la majorité (57 %) privilégient une approche de pointe. Cette préférence souligne que les entreprises qui utilisent un plus grand nombre de solutions ont plus de difficultés à identifier les risques réels parmi la myriade d'activités des utilisateurs.

RÉSUMÉ DE L'EMPLACEMENT DES DONNÉES

Emplacement des données	Compromis au cours des 12 derniers mois	Les plus à risque
Stockage dans le nuage (par exemple, Box, OneDrive, Google Drive)	42 %	54 %
Courriels, messagerie instantanée et outils de réunion en ligne	31 %	39 %
Plateforme en tant que service (PaaS)	29 %	34 %
Infrastructure en tant que service (IaaS)	28 %	36 %
IA (par exemple, ChatGPT, Bard, etc.)	27 %	38 %
Bases de données et lacs de données SaaS	27 %	41 %
Points de terminaison et appareils	25 %	36 %
Référentiels sur place, partages de fichiers et bases de données	24 %	28 %
Données cachées	21 %	23 %
Applications sectorielles	17 %	25 %
Outils de développement	16 %	23 %

Avec plus d'un tiers des entreprises qui mettent en œuvre leur stratégie IA et plus encore qui se lancent dans cette démarche, l'adoption de l'IA se fait à un rythme sans précédent, beaucoup plus rapide que celui de l'adoption du nuage et du courrier électronique par le passé. À mesure que les entreprises adoptent l'IA, il devient essentiel d'améliorer la sécurité des données pour en permettre une utilisation responsable et prévenir les risques. L'IA est considérée comme l'un des emplacements les plus à risque pour les données, comparativement aux autres emplacements. Et 27 % des entreprises ont rencontré une violation de la sécurité des données IA. Les inquiétudes des entreprises par rapport à l'IA concernent le faible de contrôle des données partagées avec l'IA, l'absence de contrôles pour détecter et atténuer les utilisations risquées de l'IA, le manque de transparence sur l'entraînement des modèles d'IA générative et les fuites d'informations confidentielles par l'IA.



« L'IA est bénéfique pour la productivité et l'efficacité, mais elle comporte des risques potentiels pour la sécurité et les données. » déclare le responsable de la sécurité d'une entreprise.

Bien que l'IA suscite des inquiétudes, les décideurs peuvent également en percevoir le potentiel, d'autant plus que les fournisseurs du marché développent des innovations pour aider les entreprises utiliser l'IA de manière responsable. Toutefois, pour poursuivre l'utilisation de l'IA, les entreprises indiquent que les contrôles dont elles ont besoin viseraient à détecter les contenus malveillants ou à risque dans l'IA, à chiffrer, masquer ou anonymiser les données avant leur chargement dans l'IA et à identifier les données sensibles générées par l'IA.

5 PRINCIPAUX CONTRÔLES DE SÉCURITÉ DES DONNÉES NÉCESSAIRES POUR L'IA

1. **Détecter les contenus malveillants ou** à risque dans l'IA
2. **Chiffrer, masquer ou anonymiser les données** avant de les charger dans l'IA
3. **Identifier les données sensibles** générées par l'IA
4. **Empêcher le transfert de données** sensibles vers l'IA
5. **Détecter la manipulation des modèles ou des données** dans l'IA

5

L'automatisation et l'IA sont des voies prometteuses pour une meilleure protection.

L'automatisation et l'IA sont des voies prometteuses pour une meilleure protection.

Dans un monde idéal, exempt de contraintes de priorités organisationnelles ou de budget, la moitié des entreprises aimeraient être plus proactives dans leur gestion de la sécurité des données, en consacrant plus de temps à des choses comme la détection des données sensibles et des risques associés, ou la prévention des incidents de sécurité des données. Actuellement, cependant, plus de la moitié des entreprises consacrent la majeure partie de leur temps à des mesures réactives comme la détection des incidents, la réponse et les enquêtes. Or, la détection et la réponse aux incidents de sécurité des données prennent beaucoup de temps : la résolution d'un incident de sécurité prend environ un mois à la plupart des organisations. Pour certaines, la résolution peut prendre jusqu'à six mois.

L'avantage d'adopter une stratégie plus proactive est évident : les entreprises interrogées qui sont plus proactives subissent déjà des incidents de sécurité des données moins coûteux, sont mieux en mesure d'enquêter sur ces incidents en moins d'un mois et sont plus enclines à croire que leurs contrôles de défense sont suffisants pour empêcher les violations de données.

Bien que les entreprises soient conscientes que des mesures proactives de sécurité des données peuvent réduire les risques, elles ne progressent pas dans la mise en œuvre de ces mesures. Par exemple, celles qui cherchent à être plus proactives en allouant plus de temps à la prévention sont plus susceptibles de choisir des solutions de pointe qui exigent en réalité plus d'efforts de gestion des mesures de réactions lorsque les signaux de détection et les contrôles de réponse sont appelés conjointement.

COMPARAISON DES RÉSULTATS ENTRE ENTREPRISES PROACTIVES ET RÉACTIVES

	Plus proactive	Plus réactive
Coût moyen d'un incident de sécurité des données au cours des 12 derniers mois	**207 000 $ US**	**330 000 $ US**
Conclure une enquête sur la sécurité des données en moins d'un mois en moyenne	**80 %**	**68 %**
Nos contrôles de défense sont suffisants pour prévenir les violations de données	**77 %**	**68 %**

Étant donné que les ressources et le personnel sont limités et que la répartition des efforts entre les activités n'est pas forcément idéale, les entreprises sont à la recherche de technologies leur permettant de consacrer davantage de temps aux activités proactives. L'automatisation est une façon pour les entreprises d'épargner du temps pour une approche plus proactive de la sécurité des données. 74 % des entreprises interrogées préféreraient une atténuation des risques semi-automatisée ou entièrement automatisée, qui permettrait aux équipes de sécurité de minimiser à l'avance l'impact des incidents de sécurité des données potentiels plutôt que de devoir les examiner manuellement. De plus, les entreprises reconnaissent que de nombreuses autres tâches pourraient bénéficier de l'automatisation, comme la création de rapports de sécurité des données, les flux de travail de gestion des incidents, l'enquête sur les incidents et la réponse à y apporter. Pour la plupart, les principales tâches que les équipes de sécurité souhaitent automatiser sont les mesures réactives. En automatisant ces tâches, les entreprises peuvent alléger la charge de travail de leurs équipes de sécurité des données, ce qui leur permet d'adopter une approche plus proactive.

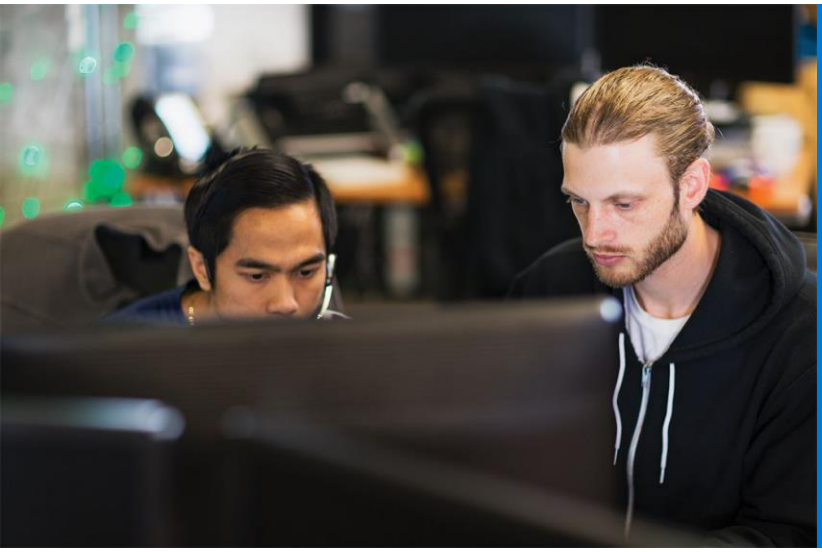
5 PRINCIPAUX DOMAINES QUE LES ÉQUIPES DE SÉCURITÉ DES DONNÉES PRÉFÈRENT AUTOMATISER OU FACILITER

Réaction

1. Création de flux de travail automatisés pour la gestion et la réponse aux incidents
2. Création de rapports sur la sécurité des données

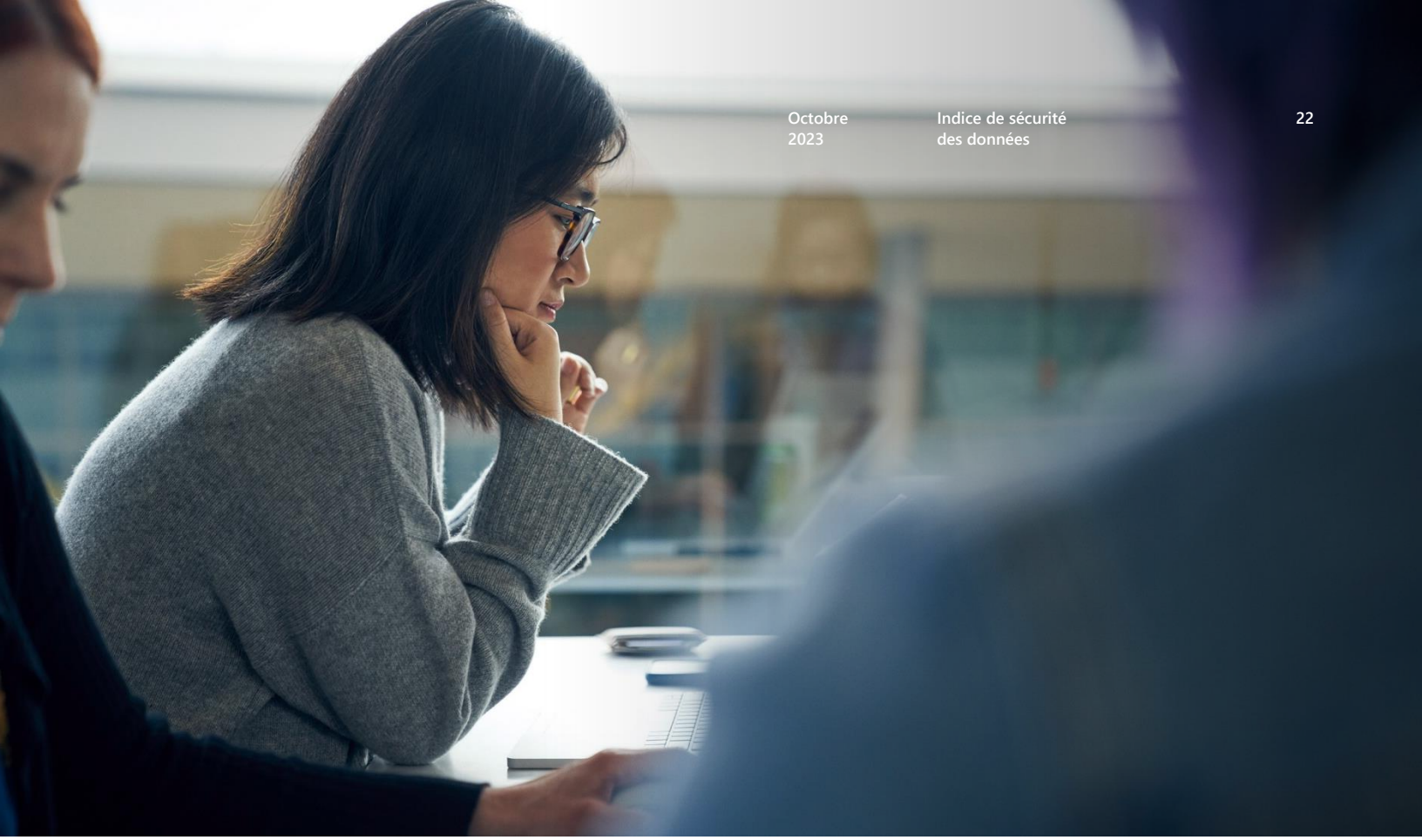
Réaction

3. Réponse et confinement des incidents de sécurité des données
4. Transfert des incidents aux équipes appropriées (p. ex. équipe SOC, juridique, RH) au cours des enquêtes
5. Enquêtes sur les incidents de sécurité des données



« Il y a tellement de données exposées à évaluer manuellement. L'IA permet d'accélérer les temps de réponse de notre équipe et de protéger les données lorsque nous manquons de ressources. »

Un décideur en sécurité au Royaume-Uni



L'utilisation de l'IA pour la sécurité des données peut également aider les organisations à être plus stratégiques et à mieux faire face aux menaces futures. La technologie accélère la réponse aux incidents détectés, ce qui permet aux professionnels de la sécurité des données de mieux les étudier. Comme pour l'automatisation, les entreprises citent de nombreux scénarios dans lesquels l'IA peut contribuer à renforcer la sécurité, **faisant ainsi gagner du temps à leur équipe.** Les principaux scénarios d'utilisation de l'IA incluent le blocage automatique du partage inapproprié de données, la détection des risques critiques pour la sécurité des données et des activités anormales sur les données, et l'étude des incidents de sécurité des données potentiels.

En tirant parti des avantages de l'IA et de l'automatisation et en s'orientant vers des solutions plus intégrées, les entreprises peuvent adopter une stratégie de sécurité des données plus proactive et se ménager un avenir plus sécurisé.

PRINCIPAUX SCÉNARIOS D'UTILISATION DE L'IA

Blocage automatique des partages de données inappropriés

Détection des risques critiques pour la sécurité des données et des activités anormales sur les données

Recommandations pour mieux sécuriser votre environnement de données

Enquête sur les incidents de sécurité des données potentiels

Ajustement des stratégies de sécurité des données

Recommandations finales

- Adopter une plateforme intégrée pour renforcer la sécurité des données
- Se protéger contre les incidents de sécurité des données provenant de l'extérieur et de l'intérieur avec une approche de défense en profondeur
- Améliorer vos stratégies de sécurité des données grâce à l'IA et à l'automatisation

Adopter une plateforme intégrée pour renforcer la sécurité des données

Selon les résultats de cette étude, un moindre nombre de solutions peut être source d'une sécurité accrue. Cela peut sembler contre-intuitif, mais les entreprises doivent combattre le faux sentiment de confiance qu'inspire la prolifération de solutions isolées. Le regroupement des fournisseurs constitue une approche stratégique qui permet non seulement de réduire les coûts, mais aussi d'améliorer la sécurité.

Les décideurs en matière de sécurité des données peuvent initier cette transformation en donnant à leurs équipes les moyens de consacrer plus de temps aux tâches stratégiques que sont la recherche et la planification de nouveaux contrôles de sécurité ou l'optimisation des stratégies de sécurité. 84 % des décideurs déclarent que c'est ce qu'ils souhaitent faire. Ce processus implique de remplacer les solutions cloisonnées existantes, qui sont souvent considérées comme les « meilleures de leur catégorie », mais qui ne s'intègrent pas efficacement avec d'autres outils.

Les décideurs peuvent favoriser une collaboration étroite avec leurs équipes pour établir les objectifs du programme de sécurité des données et les indicateurs de performance clés (KPI). Ils peuvent ensuite progresser en définissant les exigences de la solution et en identifiant ses caractéristiques non négociables. Cette approche leur permet d'identifier les fournisseurs capables de mettre à leur disposition les outils correspondant à leurs objectifs primordiaux. Fondamentalement, cela favorise un état d'esprit avant-gardiste et aide les équipes à éviter de faire une fixation sur les pratiques existantes ou des cas d'utilisation isolés. Cela leur permet de mettre en œuvre les changements nécessaires vers une approche plus intégrée.

Une plateforme de sécurité des données intégrée doit permettre aux équipes de sécurité d'effectuer toutes ces tâches critiques de manière transparente :

1. Découvrir et protéger les données sensibles au sein de leur environnement numérique.
2. Détecter les risques critiques associés à ces données.
3. Empêcher l'utilisation non autorisée de données sensibles sans nuire aux activités légitimes de l'entreprise.

En mettant en œuvre une stratégie de sécurité des données intégrée, les entreprises peuvent atteindre un niveau de protection plus élevé tout en simplifiant leur infrastructure de sécurité.

Se protéger contre les incidents de sécurité des données provenant de l'extérieur et de l'intérieur avec une approche de défense en profondeur

Les incidents de sécurité des données proviennent généralement de pirates externes, d'initiés malveillants ou d'acteurs internes négligents. Les entreprises doivent faire le nécessaire pour protéger leurs données, à la fois en empêchant l'accès non autorisé par les acteurs malveillants externes et en atténuant le risque de vol interne ou d'exposition accidentelle des données.

Pour relever ces défis, les entreprises peuvent adopter une approche de défense en profondeur pour la sécurité de leurs données. Cette stratégie est analogue à la protection des œuvres inestimables d'un musée : des caméras de sécurité de pointe, équipées de renseignements sur les menaces, surveillent les visiteurs; les systèmes de billetterie gèrent l'identité et l'accès au musée, et les strictes mesures de sécurité qui entourent les œuvres assurent le même rôle que les contrôles de sécurité des données qui protègent vos précieuses données. Ces mesures découragent les incidents potentiels, qu'ils proviennent d'acteurs malveillants externes ou de personnes qui se trouvent déjà dans l'environnement de l'entreprise.

La lutte contre les risques de sécurité des données en constante évolution nécessite un effort concerté à l'échelle de l'entreprise pour mettre en œuvre cette stratégie de défense en profondeur. La collaboration de l'équipe de sécurité des données avec d'autres départements, comme le Centre des opérations de sécurité (SOC), permet d'optimiser les investissements dans la sécurité des données. Il est à noter que 66 % des entreprises qui se considèrent proactives interagissent avec leur équipe SOC, contre 54 % pour celles qui ne le font pas.

À l'instar des différentes équipes de sécurité qui doivent travailler ensemble, les solutions de sécurité des données doivent s'intégrer harmonieusement aux autres systèmes, comme les solutions de détection et de réponse étendues (XDR) ou de gestion des identités et des accès (IAM), afin de prévenir efficacement les incidents de sécurité des données provenant de sources internes et externes. Ces intégrations permettent aux entreprises d'enquêter de manière approfondie sur les incidents de sécurité et d'y répondre convenablement, de comprendre finement quels sont les données, les acteurs et les activités concernés, et de réagir par de nombreuses mesures d'atténuation. Par conséquent, cela leur permet de réagir de manière éclairée, précise et rapide afin de minimiser l'impact des incidents de sécurité potentiels.

Améliorer vos stratégies de sécurité des données grâce à l'IA et à l'automatisation

L'automatisation et l'IA peuvent aider les entreprises à être plus proactives en matière de sécurité des données. Voici quelques recommandations pour votre entreprise qui se lance dans l'automatisation et l'IA :

- Découvrir les données sensibles : utilisez l'IA pour identifier les données sensibles et y appliquer des stratégies de protection, notamment le chiffrement et la gestion des droits. Ceci est particulièrement utile pour les données d'affaires qui peuvent être difficiles à détecter par les technologies classiques de reconnaissance de schémas. Les entreprises peuvent tirer parti des technologies de classification, comme les classificateurs assistés par l'intelligence artificielle ou l'apprentissage automatique, reconnus pour leur intelligence et leur capacité à localiser rapidement les contenus sensibles en fonction du contexte ou de la catégorie d'activité des données. Par ailleurs, les entreprises peuvent utiliser une technologie de correspondance exacte des données pour découvrir les données opérationnelles ou personnelles.

  De plus, à mesure que les réglementations sectorielles évoluent (par exemple, le RGPD, la loi HIPAA ou la norme PCI DSS) et que le paysage des données devient de plus en plus dynamique, il est crucial de posséder une technologie de classification avancée, personnalisable et facilement adaptable pour identifier de nouvelles catégories de données sensibles.

- Détecter les risques critiques pour la sécurité des données : exploitez la puissance de l'IA pour identifier les risques critiques associés à vos données sensibles et allouer stratégiquement les ressources de manière à affronter les incidents potentiels à haut risque. Les technologies d'intelligence artificielle peuvent générer des alertes de haute fidélité, qui font gagner un temps précieux aux équipes de sécurité qui devraient autrement passer au crible de longues listes de faux positifs. De plus, l'IA peut aider les organisations à identifier les risques furtifs, en particulier lorsque des acteurs malveillants tentent d'échapper à la détection. Il est impératif d'exploiter la vitesse de la machine pour devancer ces acteurs.

- Prévenir les incidents de sécurité des données de façon dynamique : utilisez l'IA et l'automatisation pour adapter automatiquement vos contrôles de prévention et d'atténuation en fonction des risques estimés, pour mettre en place une stratégie de sécurité des données plus adaptable et plus proactive. Lorsque des solutions assistées par l'IA détectent et évaluent les risques, les contrôles de prévention automatisés peuvent rapidement s'enclencher pour protéger les données et appliquer précisément les mesures d'atténuation aux zones à haut risque. Par exemple, dans les cas où les premiers indicateurs d'une intention d'exfiltration de données sont détectés par des utilisateurs à haut risque, les entreprises peuvent appliquer des stratégies de protection contre la perte de données (DLP) plus strictes, anticipant ainsi les incidents de sécurité des données potentiels.

Nous espérons que vous aurez trouvé les informations et recommandations contenues dans ce rapport utiles pour améliorer vos mesures de sécurité des données et fortifier votre entreprise face aux dangers en constate évolution.

Pour en savoir plus sur la sécurité des données Microsoft, consultez la page https://aka.ms/DataSecurityNews

Objectifs détaillés, méthodologie et recrutement du panel de l'étude

Les objectifs de la recherche étaient les suivants :

1. Comprendre le paysage de la sécurité des données, notamment les priorités, les mentalités et les difficultés

2. Relier les causes et les effets des incidents de sécurité des données et identifier les actions que les équipes de sécurité peuvent entreprendre pour améliorer le niveau de sécurité des données

3. Explorer l'avenir de la sécurité des données, y compris les stratégies émergentes et les innovations relatives à l'IA pour la sécurité des données

Méthodologie :

Une enquête internationale en ligne de 15 minutes, menée du 28 juillet au 9 août 2023 auprès de 822 décideurs en matière de sécurité des données.

Les questions portaient sur le paysage de la sécurité des données, la façon dont les équipes de sécurité des données affectent leurs ressources, les incidents de sécurité des données, ainsi que le positionnement à l'égard de l'intelligence artificielle (IA) et de son utilisation pour la sécurité des données.

Pour répondre aux critères de sélection, les décideurs de sécurité des données devaient être :

RSI et décideurs adjoints (C-2 et au-dessus) ayant compétence en matière de sécurité des données

Travailler dans de grandes entreprises (plus de 500 employés; plage de taille)

Mélange de secteurs réglementés et non réglementés (sans les secteurs de l'enseignement, de l'administration ou du non-lucratif)

Sur les 822 décideurs en matière de sécurité des données interrogés dans le cadre de l'étude, le décompte par pays est le suivant :

États-Unis	329
Royaume-Uni	322
Australie	171