L'ÉTAT DE LA SÉCURITÉ DES DONNÉES

LE PARCOURS

POUR SE PROTÉGER DE

L'IMPRÉVISIBLE

Rubrik Zero Labs

SOMMAIRE

Sources de données

(RT) TÉLÉMÉTRIE DE RUBRIK (WR) WAKEFIELD RESEARCH

C’est une histoire de data

Quels sont nos volumes de données actuels ?
Quels seront les volumes à l’avenir ?
Comment cette croissance impactera-t-elle notre capacité à protéger ces données ?

Mais c'est aussi l'histoire d'un mot :

optïmïsme

Comment trop d'optimisme mène à l'échec.
Et comment il nous aide à nous accommoder
d'un avenir incertain.

À PROPOS DE LA DATA

PRENDRE LA BONNE DIRECTION

Le Rubrik Zero Labs s'est fixé pour mission d'analyser les données sur tous les types d'environnements et de fournir des informations exploitables sur les risques auxquels elles sont exposées. Pour cela, nous avons compilé les résultats obtenus auprès de deux sources différentes.

Télémétrie de Rubrik®

Les données télémétriques de Rubrik nous ont permis d'illustrer au maximum la réalité des environnements d'une organisation type, mais aussi les menaces réelles auxquelles ils sont exposés. Grâce à cette approche, nous avons pu également créer des modèles de projection à terme sur la base de données concrètes. Pour plus de transparence, nous vous présentons ci-après les sources constituant le jeu de données ayant servi de base à notre analyse. Les données télémétriques de Rubrik, c'est :

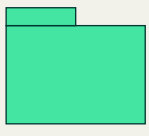
Plus de 5 000
clients

22
secteurs d'activité

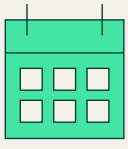
Plus de 35 Eo SÉCURISÉS
avec plus de 24 milliards d'enregistrements de données sensibles

67 pays dans 3 régions du globe

Volume total de données sécurisées :
Plus de 35 exaoctets (Eo) de stockage logique
817 pétaoctets (Po) de stockage back-end physique



Plus de 24 milliards d'enregistrements de données sensibles



Données couvrant la période de janvier 2022 à juillet 2023

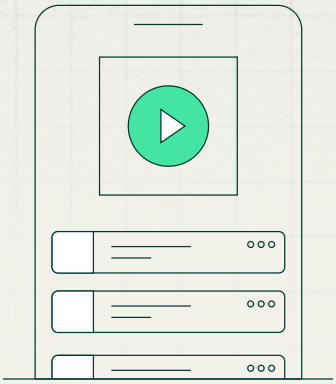
Avis aux geeks

Quand le commun des mortels entend le mot « données », il pense au stockage logique, autrement dit au stockage front-end. Nous qui évoluons dans le monde de la data, nous préférons nous concentrer sur le stockage back-end.

Rubrik prend l'intégralité des données d'une organisation et applique différentes techniques (notamment la déduplication et la compression) pour réduire le volume de données stockées en back-end. C'est pourquoi nous nous appuierons sur les données de stockage en back-end dans ce rapport.

Tout est question d'échelle
Que représentent 35 Eo de données ?

Un bon voyage commence par une bonne playlist. Sachant qu'une chanson type de bonne qualité audio fait en moyenne 4,8 Mo, notre playlist #2023DataJourneyJamz de 35 Eo contiendrait 7 300 milliards de titres, pour une durée d'écoute totale de plus de 48 millions d'années[1][2][3]. Au moins, vous ne risquez pas de vous lasser d'écouter toujours le même morceau !



Wakefield Research (WR)

Points de vue de plus de 1 600 responsables IT et sécurité

10
pays

49 %
de DSI ou RSSI

Nous avons demandé à Wakefield Research de réaliser une étude visant à compléter notre propre télémétrie et à brosser un tableau plus large de la sécurité des données. Nous avons choisi d'interroger des responsables IT et sécurité afin d'étudier d'éventuelles divergences entre leurs points de vue et ce que nous avons pu observer sur le terrain.

Plus de 1 600
responsables IT et sécurité

49 %
de DSI et RSSI

16 %
de vice-présidents

38 %
de directeurs

Trois régions
(États-Unis, EMEA et APAC)

10 pays
(États-Unis, Royaume-Uni, France, Allemagne, Italie, Pays-Bas, Japon, Australie, Singapour, Inde)

Période de l'étude
du 1er juin 2022 au 1er juin 2023

1 https://math.ucr.edu/home/baez/timeline.html#:~:text=50%20million%20years%20ago%20%2D%20India,of%20all%20species%20died%20out!
2 https://ucmp.berkeley.edu/tertiary/eocene.php
3 https://www.whistleout.ca/CellPhones/Guides/How-Much-Data-Does-Spotify-Use-Canada

COMPRENDRE LES RISQUES

ENTRE RÉACTION ET RÉFLEXION

Avant d'entamer notre parcours vers la protection des données, étudions d'abord les mécanismes de la prise de décisions. Histoire de vous aider à orienter vos choix futurs.

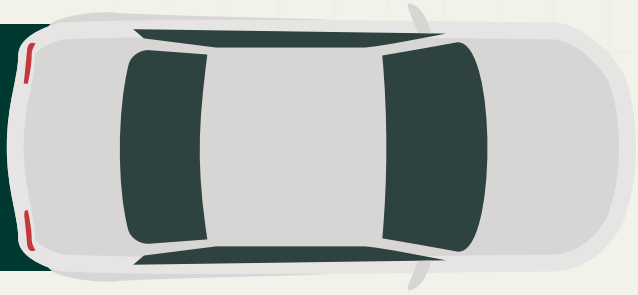
L'être humain est optimiste par nature.

Il le faut. Si nous devions porter sur nos épaules toute la misère du monde, beaucoup d'entre nous n'arriveraient même pas à se lever le matin. L'optimisme, c'est la survie.

Toutefois, cet optimisme peut aussi nous faire perdre de vue des réalités importantes.

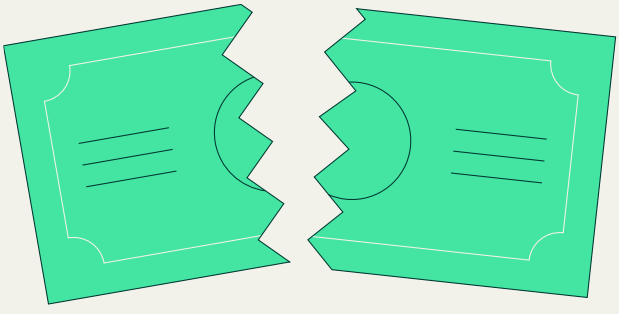
Au fond de nous, nous savons que nous prenons un risque chaque fois que nous prenons le volant. Les compagnies d'assurance estiment qu'un conducteur lambda sera impliqué dans un accident…

une fois tous les 18 ans



Pourtant, nous surestimons presque tous notre capacité à déjouer les pronostics. Nous envoyons des SMS, passons des appels, mangeons, parlons, lisons, nous recoiffons… tout en conduisant.

Nous savons qu'un danger se profile à l'horizon. Mais avons tendance à penser que ces choses n'arrivent qu'aux autres.



2007

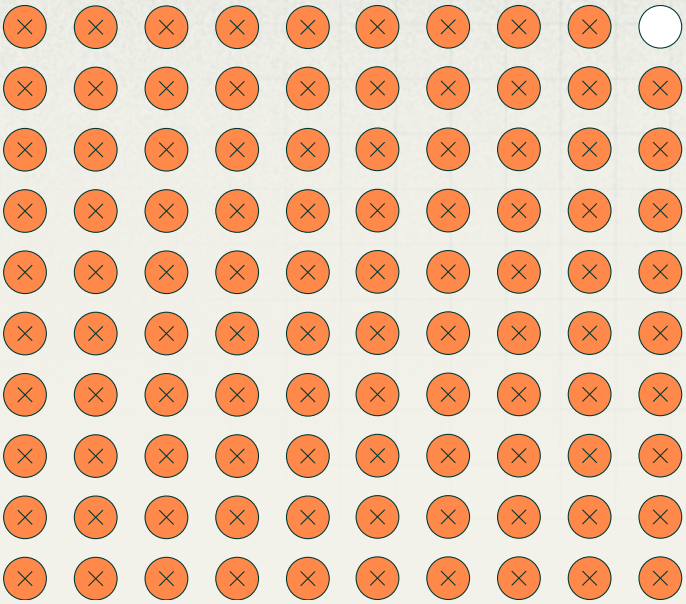
Notre optimisme influence également notre vision des choses à plus grande échelle. En 2007, les signaux faibles d'une crise économique mondiale étaient visibles. Certains les ont vus.

Michael Burry, fondateur du fonds spéculatif Scion Capital, a expliqué comment il a suivi les signes avant-coureurs de l'effondrement du marché immobilier à partir de 2003, dans une tribune du New York Times, intitulée « I Saw the Crisis Coming. Why Didn't the Fed? »[1]

La plupart des grands experts n'ont pas vu ces symptômes ou les ont ignorés.

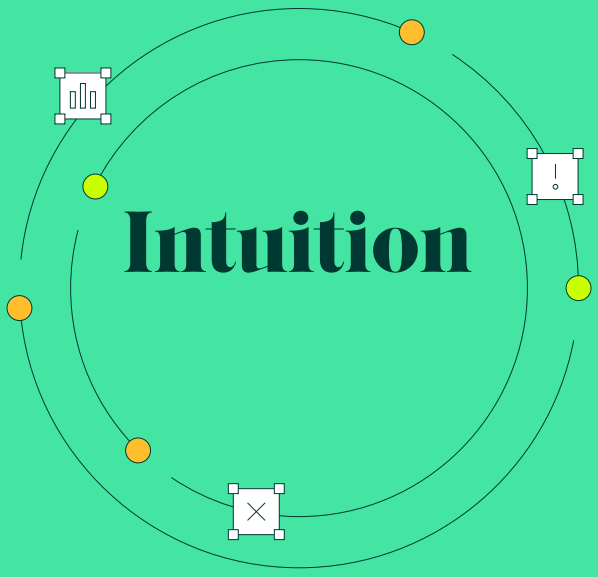
Paradoxalement, les organisations abordent souvent la cybersécurité – sujet ô combien associé à la peur, à l'incertitude et au doute – avec plus d'optimisme qu'on ne pourrait le croire.

99 %



Le rapport Rubrik Zero Labs paru au printemps[2] révèle que 99 % des responsables IT et sécurité ont eu connaissance d'au moins une attaque en 2022, pour 52 occurrences traitées en moyenne. Or, ces dirigeants sont à la tête d'équipes qui manquent souvent de ressources et sont mal préparées à combattre et récupérer de ces mêmes attaques.

Les organisations savent qu'elles vivent sous une menace permanente. Pourtant, elles conservent un certain optimisme en se persuadant que « ça n'arrive qu'aux autres ».



Chaque fois que nous montons dans une voiture, que nous contractons un emprunt ou que nous prenons l'une des 35 000 autres décisions du quotidien, grandes ou petites,[3] nous prenons un risque calculé.

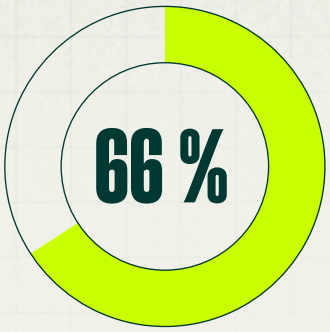
Selon les chercheurs, cette évaluation du risque se fait de deux manières : **par l'intuition ou par l'analyse.**

Les économistes et les psychologues débattent de l'utilité et de la précision de chaque type de raisonnement, mais en règle générale, l'intuition permet une prise de décision rapide avec peu d'efforts[4]. L'analyse guide quant à elle les décisions plus complexes[5], mais nécessite plus de temps et de réflexion.

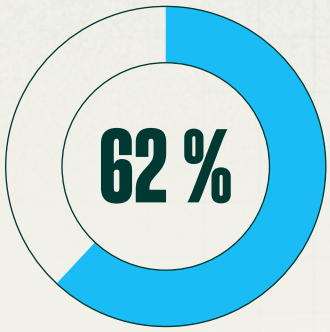
Des erreurs sont possibles dans les deux cas, mais le raisonnement intuitif est considéré comme moins précis. Toutefois, l'expérience permet d'améliorer la précision de certains types de raisonnement intuitif. C'est pourquoi les secouristes les plus chevronnés peut « sentir » le danger avant même qu'il n'apparaisse.

En matière de cybersécurité, nous savons déjà que les organisations se montrent pour le moins optimistes, du moins dans leurs actions.

Quelques précisions sur la notion d'intuition :



des organisations estiment être dépassées par le rythme de croissance des volumes de données, au point de n'être plus capables d'en garantir la sécurité et d'en gérer les risques. [W]



La majorité des organisations externes pensent que les employés accèdent aux données en contrevenant aux politiques établies en la matière. [W]

Il existe une dissonance profonde entre l'attitude des organisations et le sentiment de leurs experts vis-à-vis de la sécurité de leurs données.

Cette disparité se vérifie-t-elle dans les données de terrain ? Ces experts s'appuient-ils sur des éléments concrets ou suivent-ils simplement leur intuition ? *Découvrons-le !*

1 https://www.nytimes.com/2010/04/04/opinion/04burry.html?searchResultPosition=3
2 https://www.rubrik.com/zero-labs#hero
3 https://edition.cnn.com/2022/04/21/health/decision-fatigue-solutions-wellness/index.html#:~:text=Whether%20you're%20making%20breakfast,put%20your%20finger%20on%20why.
4 https://thedecisionlab.com/reference-guide/neuroscience/automatic-thinking
5 https://thedecisionlab.com/reference-guide/philosophy/system-1-and-system-2-thinking?utm_campaign=TDL+Dynamic&utm_medium=ppc&utm_source=adwords&utm_term=&hsa_mt=&hsa net=adwords&hsa_ad=564666141034&hsa_src=g&hsa_cam=14567061057&hsa_kw=&hsa_grp=127713121155&hsa_tgt=dsa-19959388920&hsa_ver=3&hsa_acc=8441935193&gad=1&gclid=Cj0K CQjw2qKmBhCfARIsAFy8buJQVuDOqwKnaCjbZ1gPhagxEBoYo6z8q6VxIf0_thil3IfcDPUDozcaAknUEALw_wcB

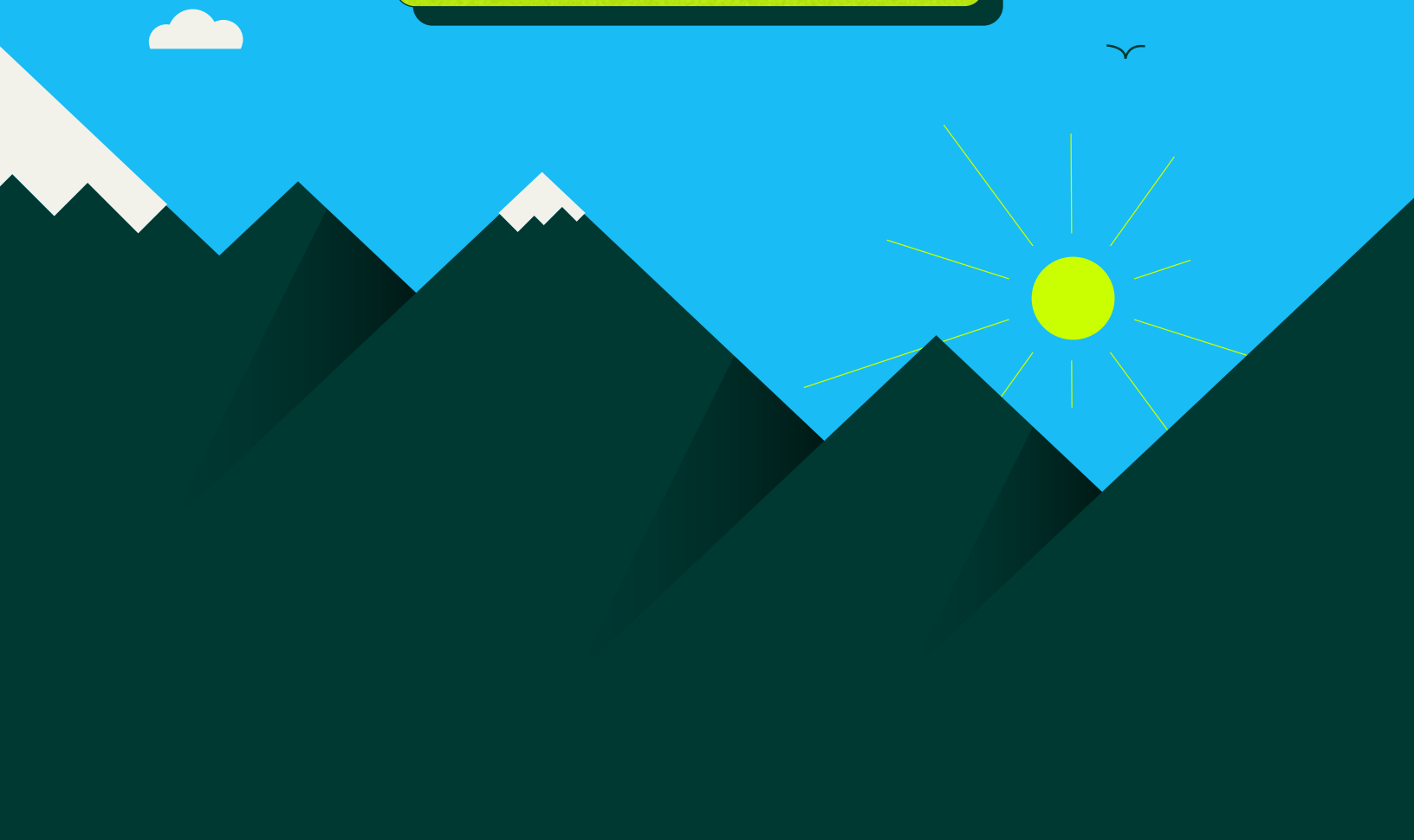
LES RÉALITÉS DE LA DONNÉE

INDICATEURS ACTUELS

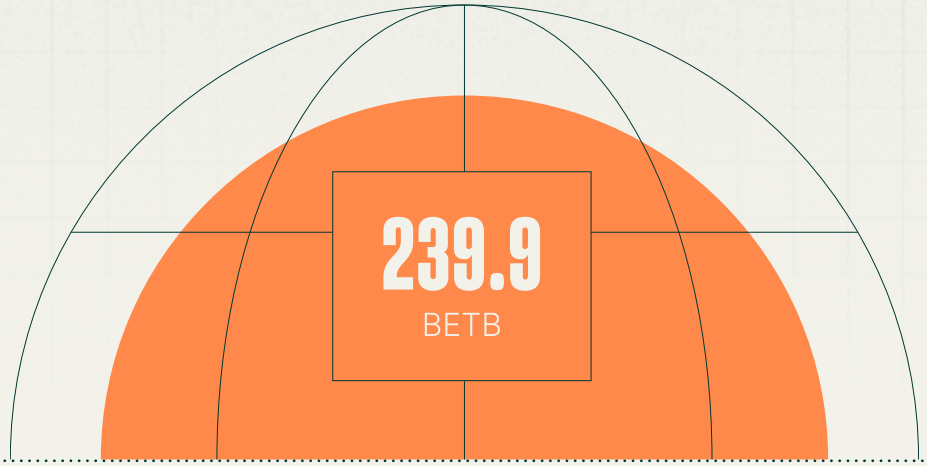
Passons de l'intuition à l'analyse. Aux chiffres en dur et aux leçons concrètes à en tirer. Sans analyse solide, nous ne faisons que brasser du vent.

Brasser du vent : expression.

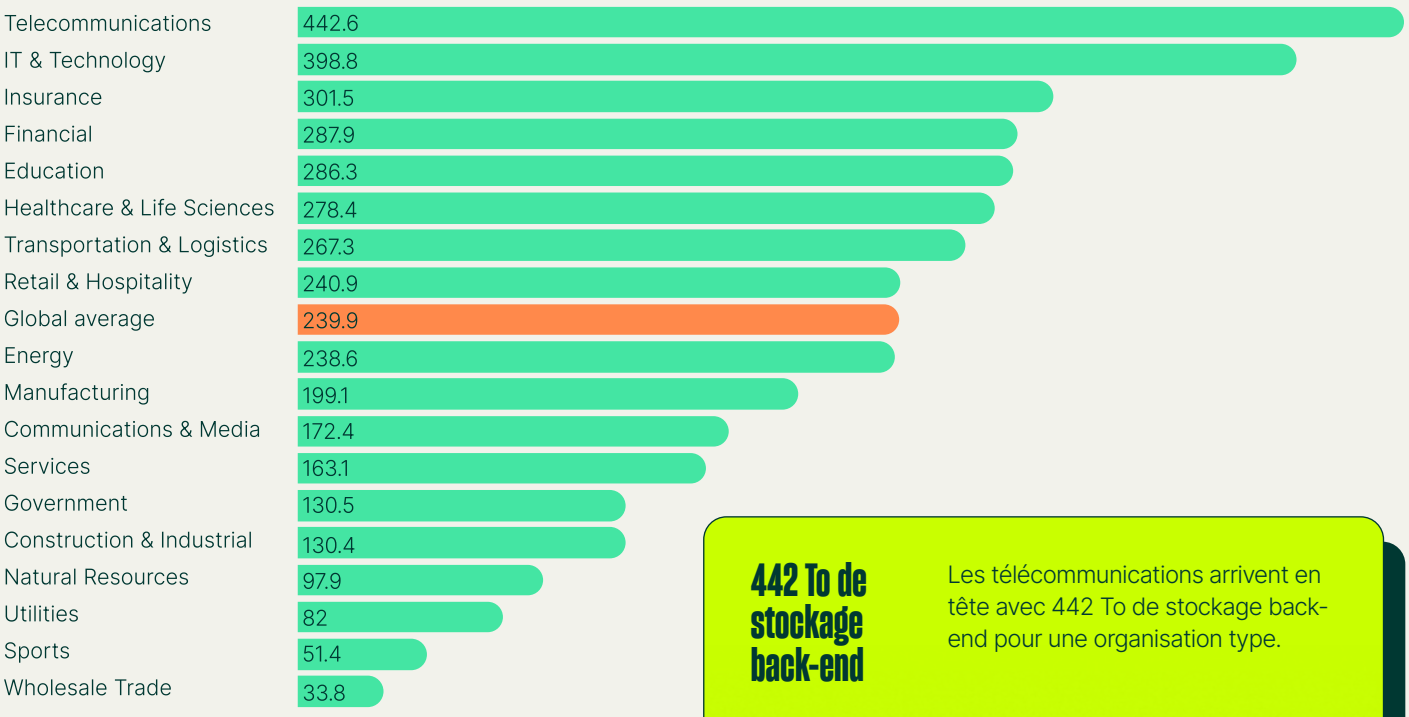
(Sens figuré) Se dit d'une personne qui parle et gesticule beaucoup sans grands effets. Autres expressions : parler dans la vide, brasser de l'air. Exemple : beaucoup de soi-disant influenceurs ne font que brasser de du vent.[1]



Oublions le vent et revenons à nos moutons, à savoir l'analyse, la vraie. Voici le volume de données typique d'une organisation de taille mondiale :



Comparons maintenant les secteurs et les régions : [1]



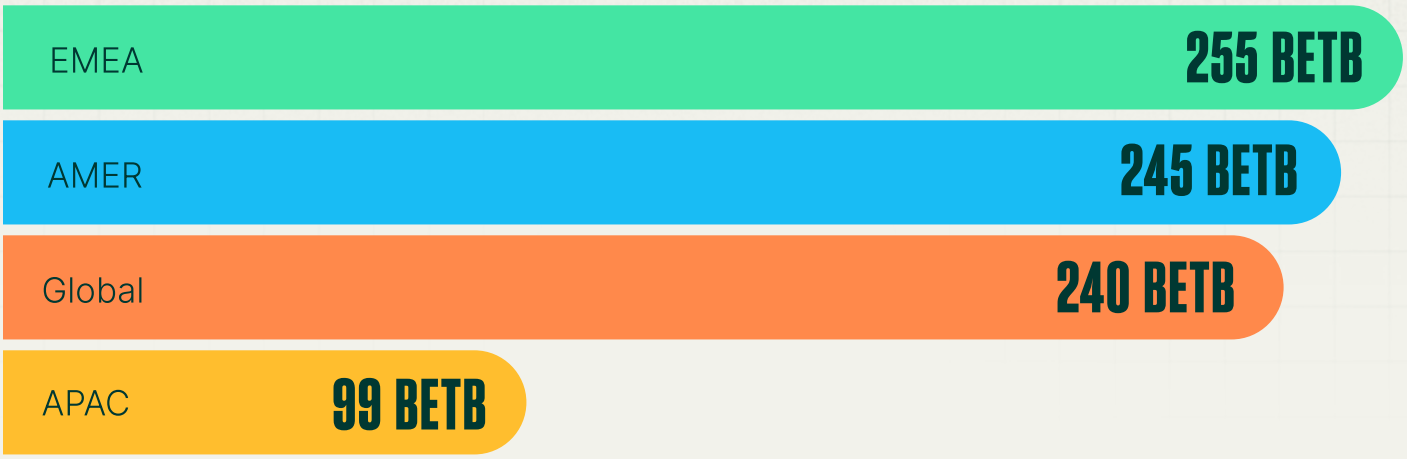
442 To de stockage back-end

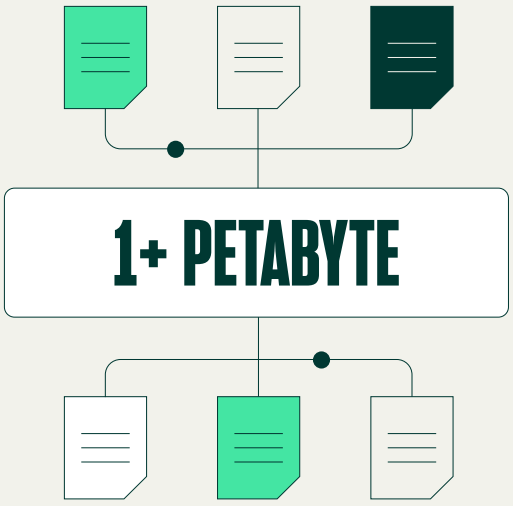
Les télécommunications arrivent en tête avec 442 To de stockage back-end pour une organisation type.

34 To de stockage back-end

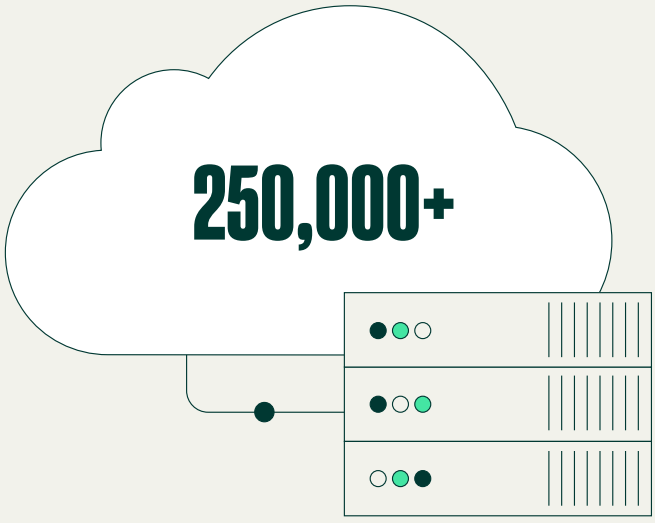
Par comparaison, le commerce de gros brasse le moins de données avec 34 To de stockage back-end, soit environ un treizième du volume d'une télécom type.

Une organisation type de la région APAC possède un volume de données inférieur d'environ 60 % à celui d'une entreprise similaire de la région EMEA ou AMÉRIQUES :





Trois organisations protégées par Rubrik ont plus d'un pétaoctet de données stockées en back-end.



Plus de 250 000 : c'est le nombre le plus élevé de machines virtuelles protégées par Rubrik dans une seule organisation.

ÉTUDE ANNEXE

Les équipes IT et sécurité réfléchissent depuis un certain temps au problème de la croissance des volumes de données.

2008

Wired Magazine annonce le début de **« l'ère du pétaoctet »**[2]

2010

Marissa Mayer, ancienne vice-présidente de Google, note trois évolutions importantes relatives aux données Internet : **les données temps réel, la puissance de traitement sans précédent et les nouveaux types de données**. Elle affirme que le volume de données générées par les utilisateurs a été multiplié par 15, soit un rythme de croissance supérieur à la loi de Moore.[3]

2011

L'industrie de la data publie des rapports indiquant que les nouvelles avancées en matière de **CRM permettront d'obtenir davantage de données** sur les organisations, que la prolifération d'**appareils IoT génèrera une augmentation exponentielle des volumes de données**, et que les évolutions technologiques des bases de données élargiront les cas d'usage de la data.[4]

2013

Les discussions portent sur **un « tournant » de la data,** résultant du passage de l'analogique au numérique et de l'augmentation du volume de données générées par les capteurs.[5]

2014

Les analystes affirment que les réseaux sociaux, les applications mobiles et la publicité sur le web entraîneront une **« explosion du Big Data ».**[6]

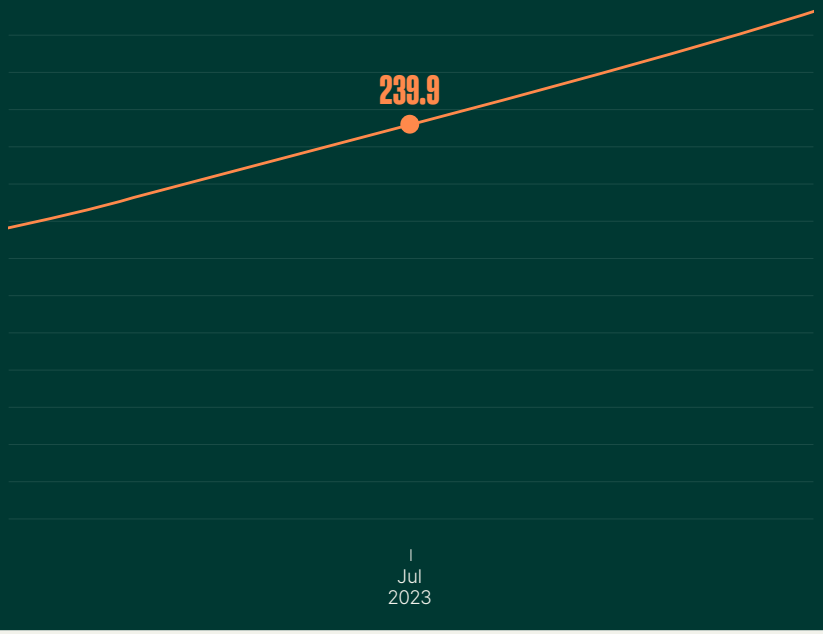
2016

IBM estime que les données de mauvaise qualité coûtent 3 100 milliards de dollars par an aux entreprises américaines.[7]

Comment en sommes-nous arrivés là ?

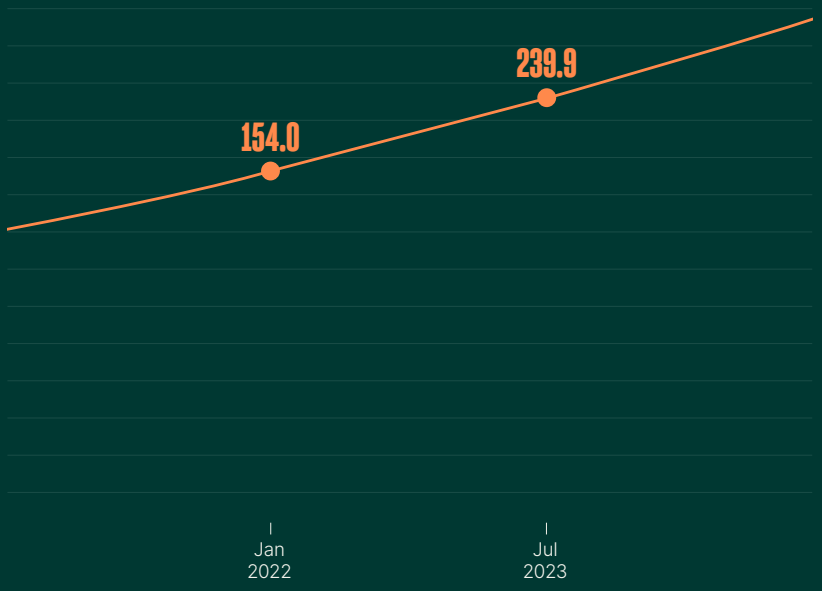
L'augmentation de la data nous inquiète depuis toujours. Et pourtant, nous n'avons encore rien vu. Comment en sommes-nous arrivés là ?

Moyenne totale en To de stockage back-end



Rubrik Zero Labs a analysé les modèles de croissance de janvier 2022 à juillet 2023.[RT]

Moyenne totale en To de stockage back-end



Au cours des 18 derniers mois, les données d'une organisation mondiale type ont augmenté comme suit :

TOTAL : +42 %

ON-PREMISES
+20 %

CLOUD
+73 %

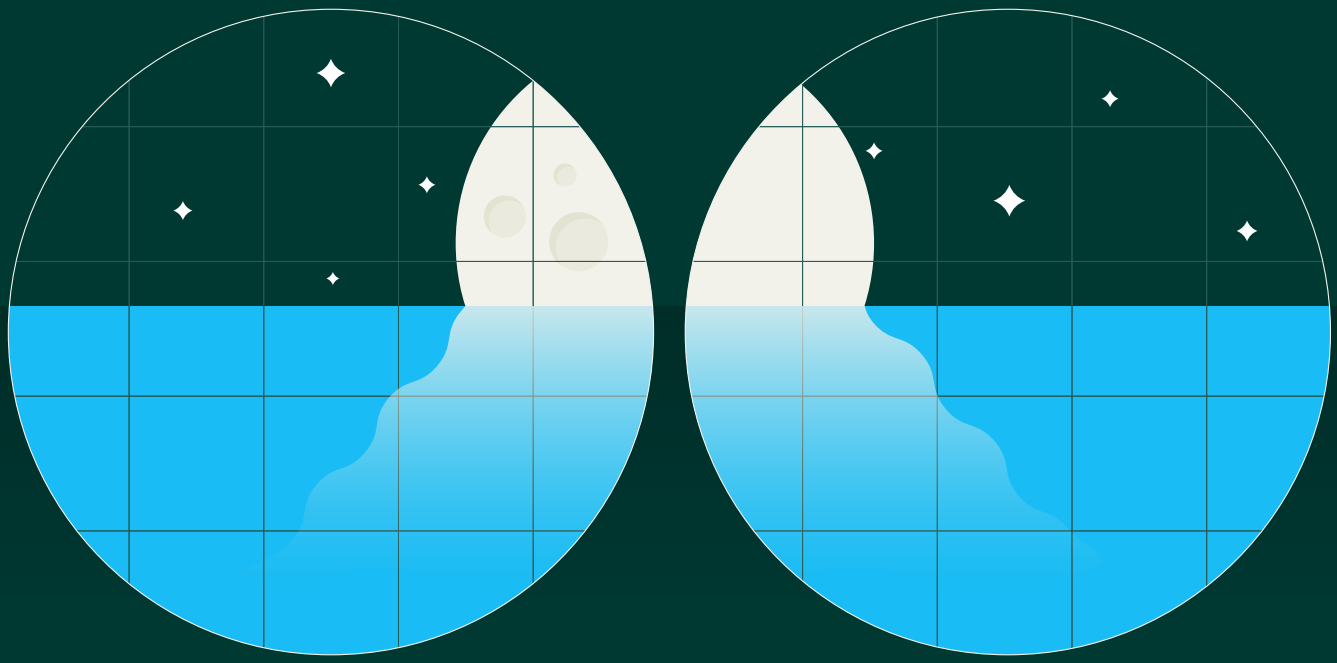
SAAS
+145 %

1 https://www.caranddriver.com/features/a14989657/pontiac-aztek-the-story-of-a-vehicle-best-forgotten-feature/
2 The End of Theory: The Data Deluge Makes the Scientific Method Obsolete
3 The Coming Data Explosion - The New York Times
4 https://www.smartdatacollective.com/where-did-data-explosion-come/
5 https://news.microsoft.com/2013/02/11/the-big-bang-how-the-big-data-explosion-is-changing-the-world/
6 https://www.informit.com/articles/article.aspx?p=2238298&seqNum=3
7 https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year

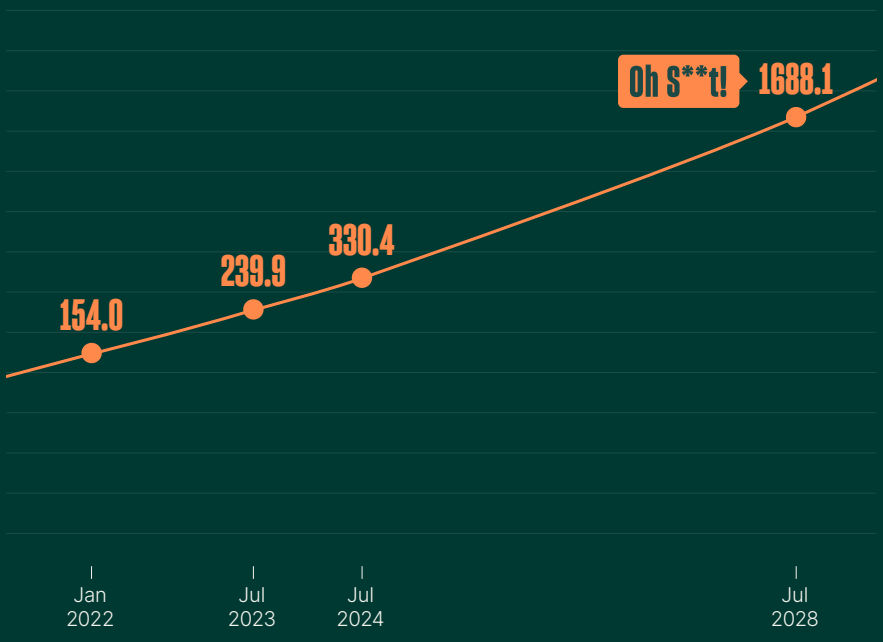
PRÉDICTIONS

SCRUTER L'HORIZON

La passé, c'est le passé. Maintenant, regardons droit devant nous. Rubrik Zero Labs s'est appuyé sur les tendances de croissance pour estimer les volumes de données auxquels les entreprises seront confrontées à l'avenir.



Le volume total de données à sécuriser augmentera de près de 100 To de stockage back-end au cours de l'année prochaine et sera multiplié par 7 d'ici cinq ans.[R]



VRAIMENT ? NOUS AUSSI, NOUS N'EN SOMMES PAS REVENUS !

Les grands changements ont rarement lieu du jour au lendemain. Lorsque les banques américaines ont commencé à faire faillite mi-2007, la première créance hypothécaire titrisée datait déjà de plus de 35 ans. Quant aux prêts hypothécaires à taux variable, ils connaissaient un succès croissant depuis les années 1980.[1][2]

Personne ne sait vraiment quels seront les volumes de données dans cinq ans. Les prévisions de croissance ont d'ailleurs souvent été dépassées, y compris celles de Rubrik Zero Labs, pour être tout à fait honnêtes. Notre étude précédente, basée uniquement sur des données de 2022, prévoyait un taux de croissance de 25 %. Mais en extrapolant un peu sur la base du taux de croissance actuel, c'est là qu'on entre vraiment dans le dur.

1 https://www.investopedia.com/terms/m/mbs.asp
2 https://predatorylending.duke.edu/business-analysis/evolution-of-mortgage-lending/subprime-lending/

ÉVOLUTION DES DONNÉES SENSIBLES

N'EMPORTEZ QUE L'ESSENTIEL

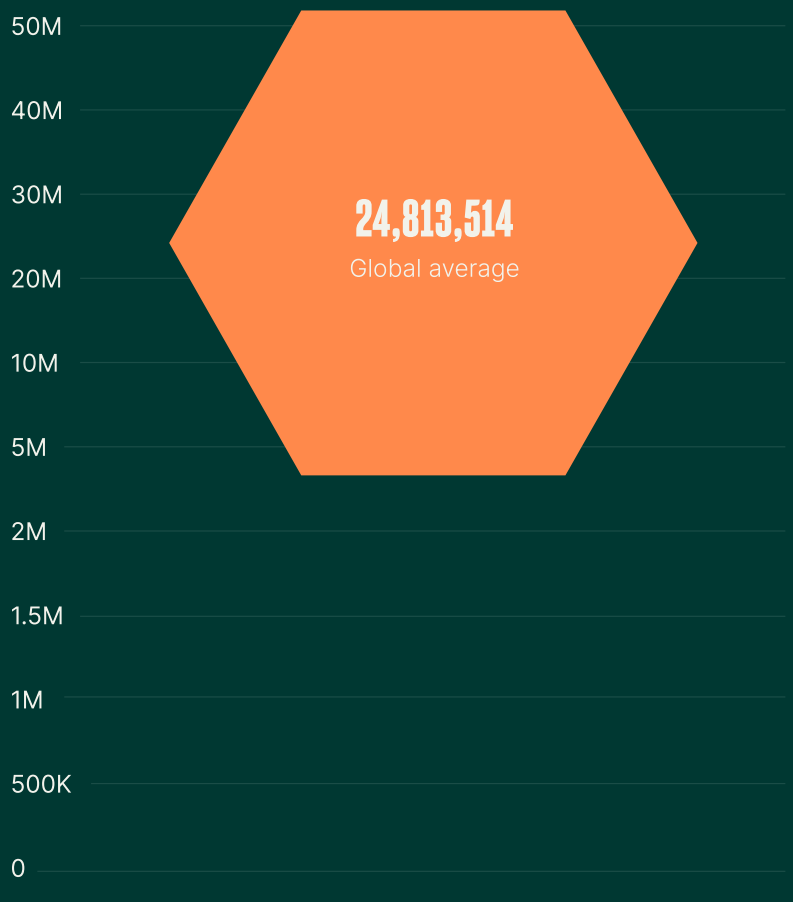
Quand on s'embarque dans une aventure, on prend toujours son essentiel de voyage avec soi. Mais l'essentiel l'est-il toujours vraiment ?

Nous protégeons la quasi-totalité de nos données, mais certaines sont plus importantes que d'autres. Par exemple, personne ne se soucie vraiment de savoir si un dossier de bureau rempli d'anciens blogs a été compromis. En revanche, on s'inquiétera beaucoup plus pour les identifiants utilisateurs, les dossiers médicaux et les business plans d'une entreprise.

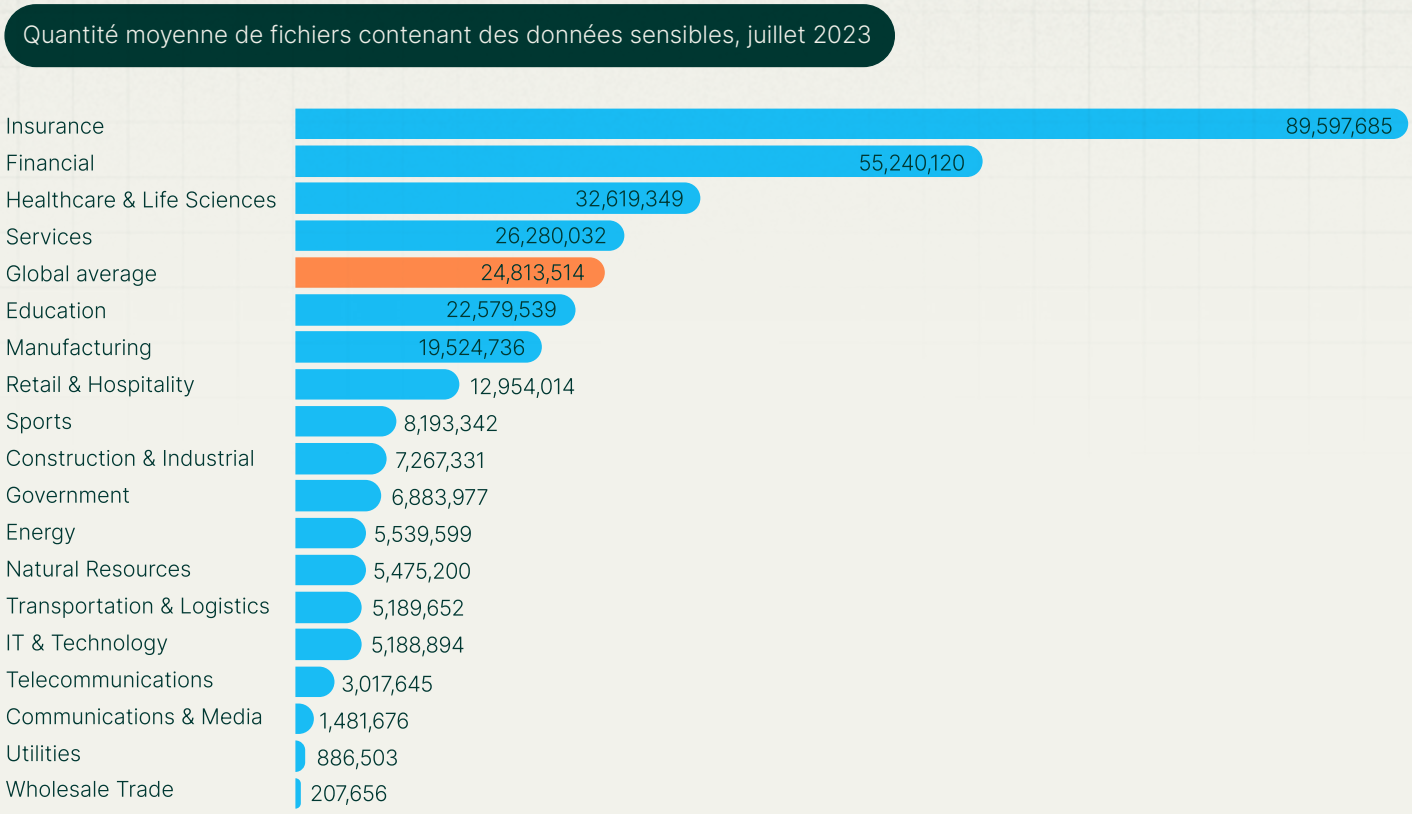
Dans ce rapport, les données sensibles sont identifiées comme telles par les solutions technologiques Rubrik, d'après les paramètres dérivés de diverses normes ou réglementations sectorielles (HIPAA, RGPD, CPAA, etc.).[1234] En outre, chaque organisation peut utiliser la technologie Rubrik pour identifier des données sensibles selon ses propres facteurs (code source, obligations légales, etc.). Ces données sont également incluses dans ces chiffres.®

Voici la moyenne globale pour une organisation type :

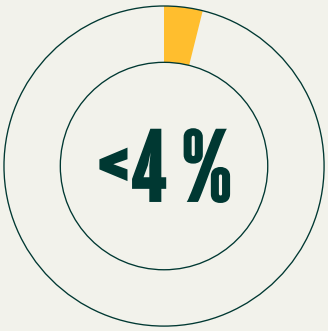
Quantité moyenne de fichiers contenant des données sensibles, juillet 2023



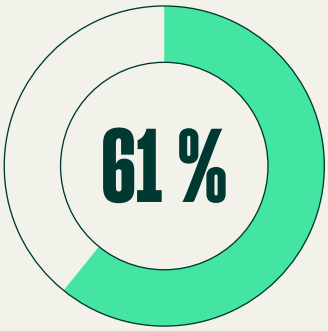
En prenant du recul, on constate des variations significatives. Voici les chiffres par secteur.[RT]



Dans l'une des organisations sécurisées par Rubrik, les données les plus sensibles représentent plus de 1,3 milliard d'enregistrements.



Moins de 4 % des organisations externes disposent d'un emplacement de stockage dédié aux données sensibles. [MR]

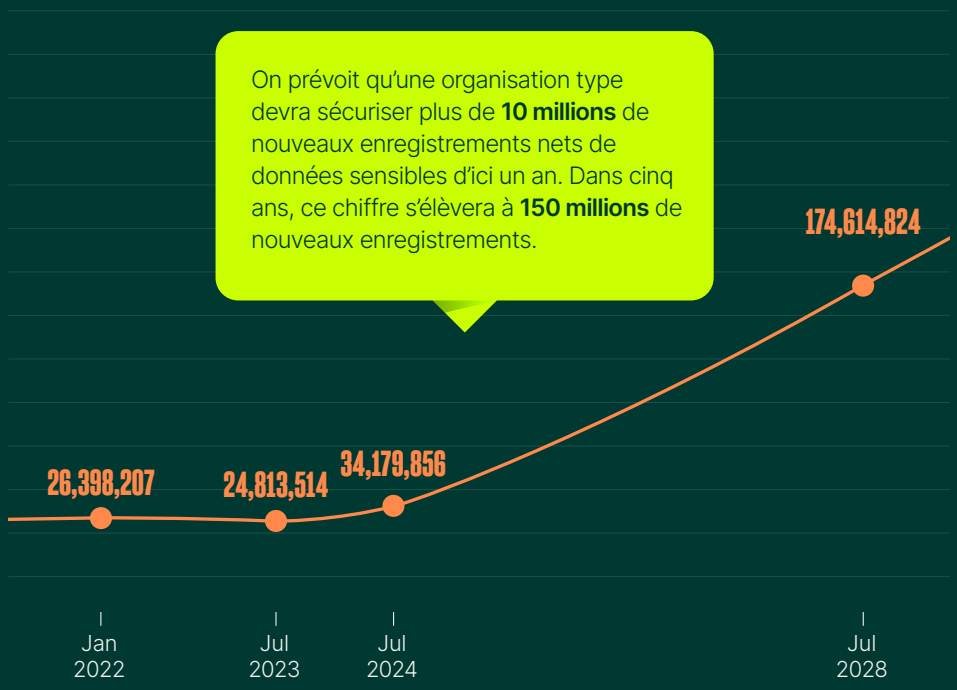


61 % des organisations externes stockent leurs données sensibles en de multiples endroits, dans des environnements cloud, on-premises et SaaS. [MR]

Voici maintenant les projections de croissance du volume de données sensibles : [RT]

Quantité moyenne de fichiers contenant des données sensibles

On prévoit qu'une organisation type devra sécuriser plus de **10 millions** de nouveaux enregistrements nets de données sensibles d'ici un an. Dans cinq ans, ce chiffre s'élèvera à **150 millions** de nouveaux enregistrements.

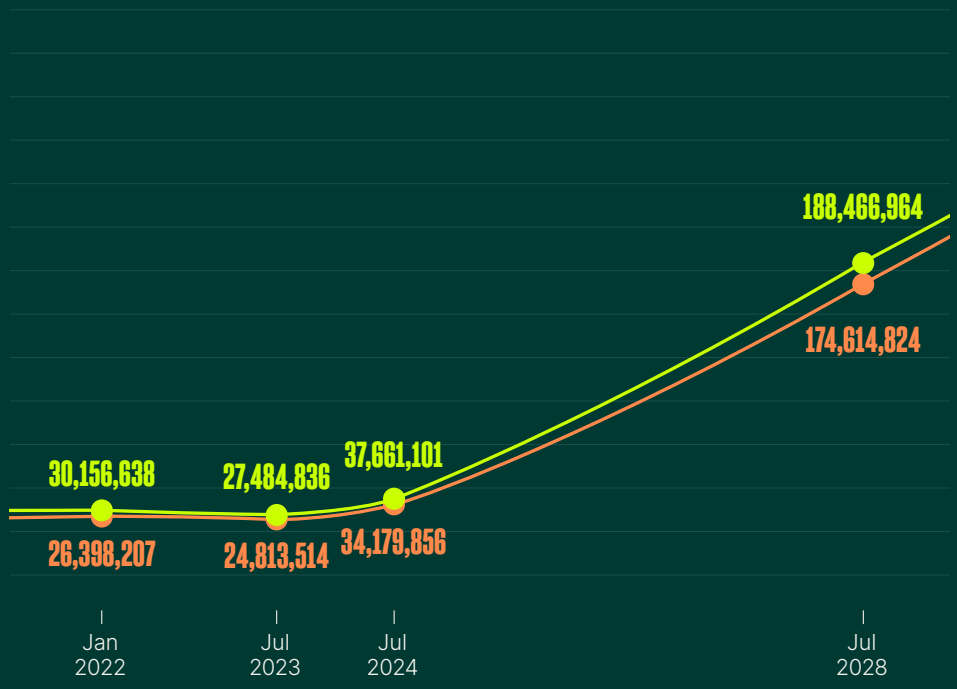


Moyenne globale

RÉPARTITION RÉGIONALE

AMÉRIQUES

Quantité moyenne de fichiers contenant des données sensibles

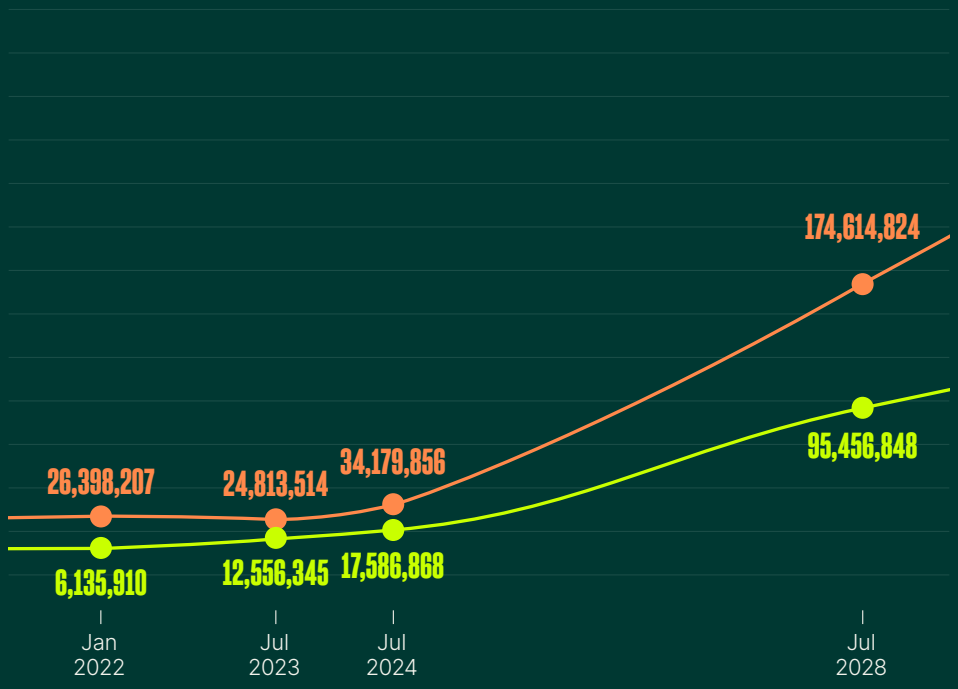


AMÉRIQUES
Moyenne globale

RÉPARTITION RÉGIONALE

EMEA

Quantité moyenne de fichiers contenant des données sensibles

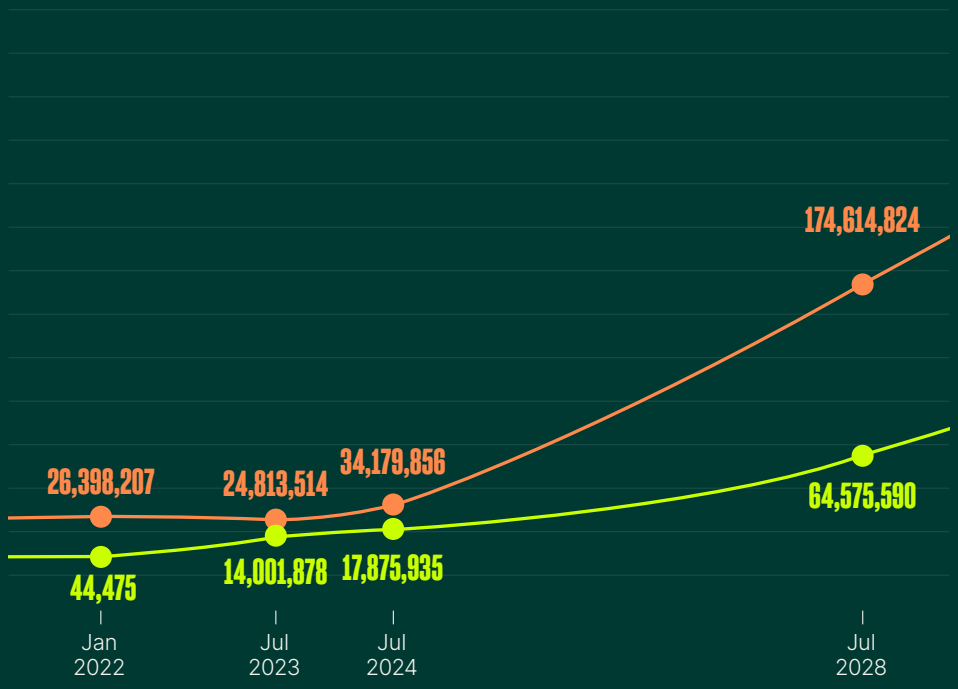


EMEA
Moyenne globale

RÉPARTITION RÉGIONALE

APAC

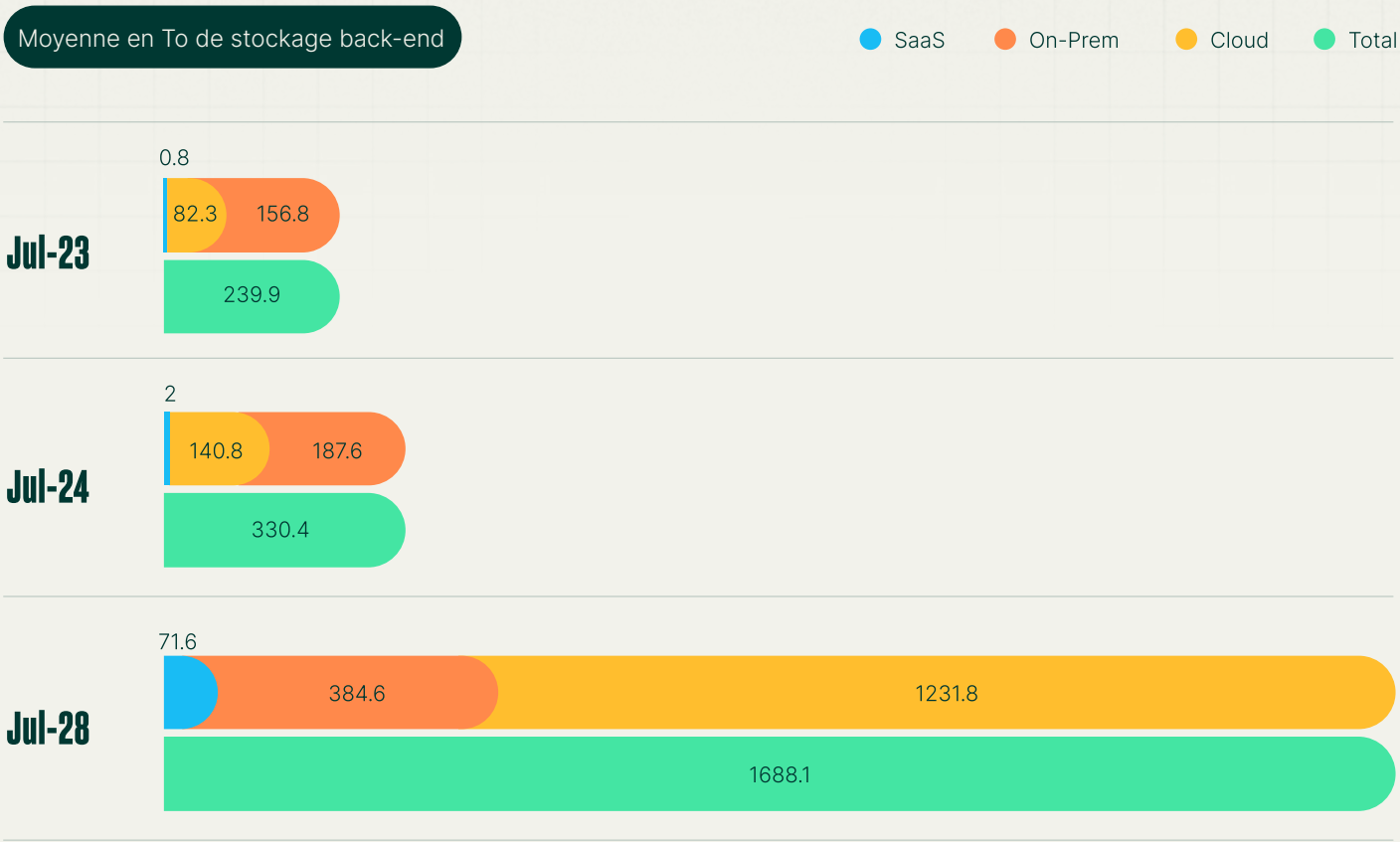
Quantité moyenne de fichiers contenant des données sensibles



APAC
Moyenne globale

Mutations des environnements hybrides

Connaître les volumes à gérer, c'est bien. Savoir où les données sont stockées, c'est mieux.[RT]



Une tendance importante se dessine pour les cinq prochaines années, à savoir le caractère dynamique des environnements hybrides constitués de stockage on-premises, cloud et SaaS. Tout indique qu'ils resteront le modèle dominant, mais dans des proportions radicalement différentes. Sans surprise, le cloud est appelé à détrôner le stockage sur site pour devenir de loin l'environnement de stockage privilégié. Le SaaS pourrait connaître le taux de croissance le plus élevé au cours des cinq prochaines années en atteignant les chiffres actuels du cloud.

1 https://gdpr-info.eu/art-4-gdpr/
2 https://www.cdc.gov/phlp/publications/topic/hipaa.html
3 https://www.dol.gov/general/ppii
4 https://oag.ca.gov/privacy/ccpa#:~:text=The%20right%20to%20limit%20the,personal%20information%20collected%20about%20them.

ÉVALUATION DE LA SÉCURITÉ DES DONNÉES

GARE AUX DANGERS

Nous savons maintenant que les volumes de données explosent. Nous savons aussi que les lieux de stockage de demain seront bien différents de ceux d'aujourd'hui. Qu'en est-il de leur sécurisation ? Utilisons le système de score de sécurité des données pour en savoir plus sur la situation réelle.

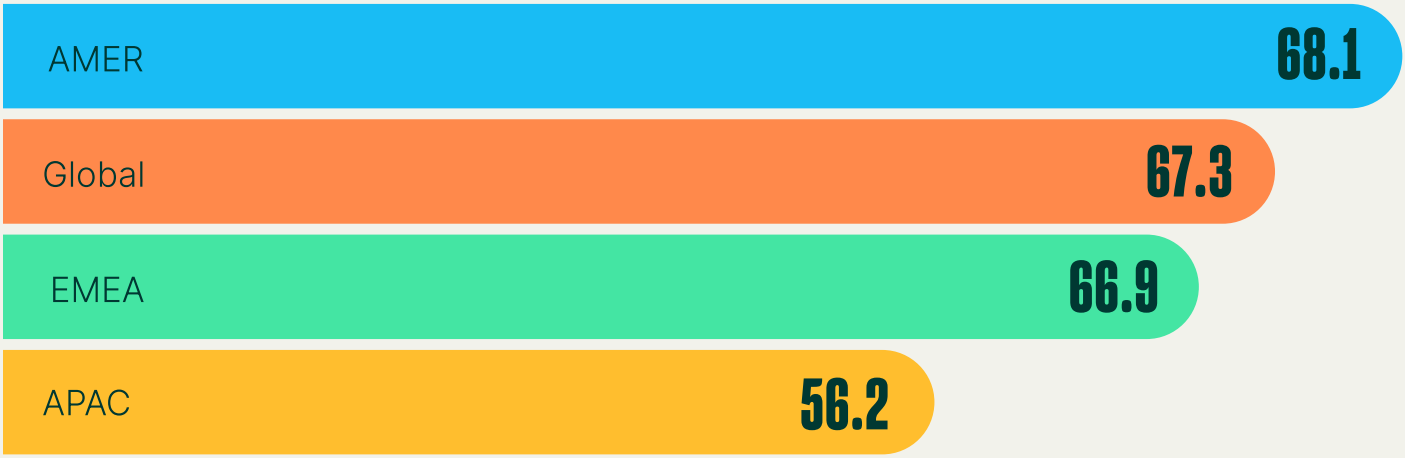
LES ANCIENNES CARTES MARINES METTAIENT LITTÉRALEMENT EN GARDE CONTRE LES « MONSTRES » POUR SIGNALER LES EAUX INEXPLORÉES OU LES ZONES DANGEREUSES.

À propos du score de sécurité des données

Le score de sécurité des données est calculé toutes les 24 heures selon les catégories suivantes :

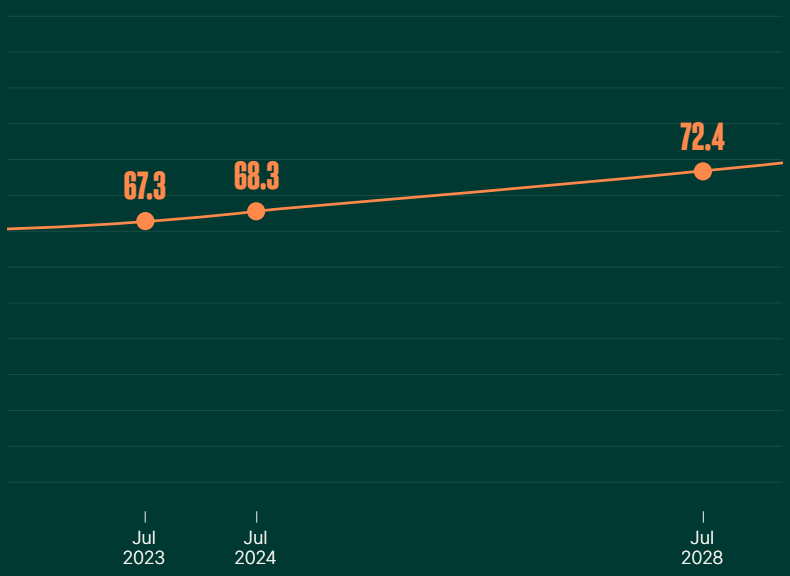
1. **Sécurité de la plateforme :** mesure l'efficacité de la sécurité de l'infrastructure de stockage des données, sur la base de divers facteurs comprenant les contrôles utilisateur, l'authentification des administrateurs, les journaux d'audit, etc.
2. **Protection et restauration des données :** analyse le degré de sécurité des données de sauvegarde, évalue si une copie saine de la dernière sauvegarde est disponible et examine d'autres facteurs associés.
3. **Audit ransomware :** détermine la qualité et la fréquence de la surveillance des menaces de ransomware, et évalue la capacité de récupération des données après un chiffrement.
4. **Découverte des données sensibles :** mesure le degré de protection des données sensibles, les contrôles d'accès à ces données et leur priorisation dans les protocoles de restauration.
5. **Les scores sont évalués de la manière suivante :**
   - 0-50 : insatisfaisant
   - 51-75 : besoin d'amélioration
   - 76-90 : satisfaisant
   - 91 et plus : excellent

Le score de sécurité des données d'une organisation type de taille mondiale est de 67.[RT]



L'analyse de ces tendances et vecteurs nous permet d'établir une projection des scores à un et cinq ans. [RT]

Moyenne des scores de sécurité des données



8 %

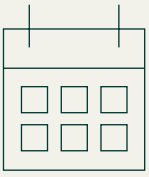
Les scores de sécurité des données ne devraient augmenter que de 1 % l'année prochaine et de 8 % dans les cinq ans à venir. [RT]

16 %

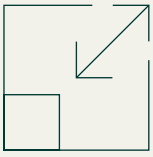
Ces prévisions marquent un net ralentissement par rapport à l'augmentation globale de 16 % en 2022. [RT]

10 sur 18

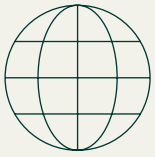
Dans cinq ans, seulement 10 des 18 secteurs et une seule région géographique se classeraient dans la catégorie « satisfaisant » ou « excellent ». [RT]



Au cours des cinq prochaines années, les scores de sécurité des données pourraient rapidement différencier les riches et les pauvres. [RT]

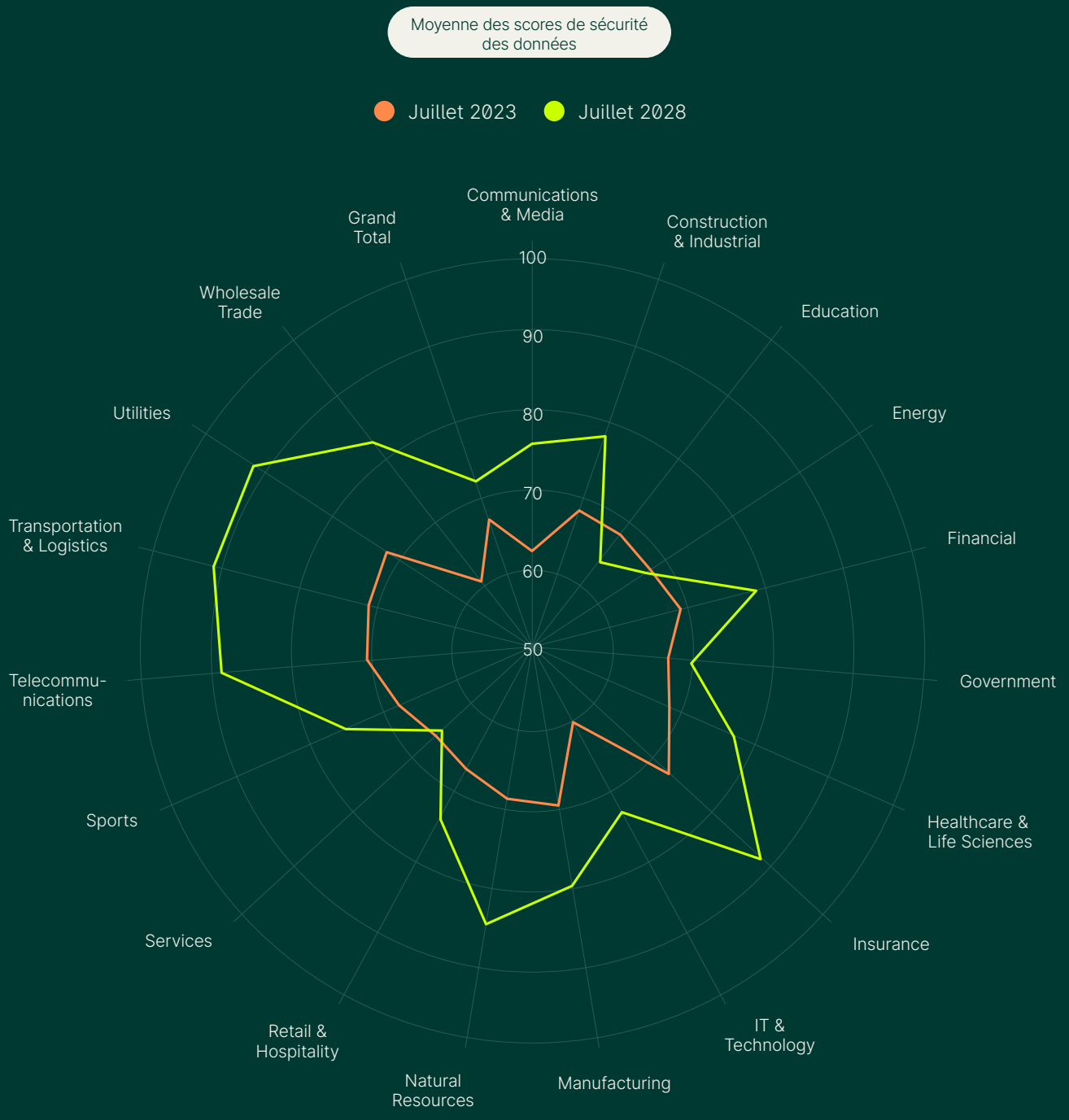


Sur la même période, deux secteurs devraient atteindre un score de 90 (Fournisseurs d'énergie et Transports/logistique), tandis que trois autres secteurs pourraient voir leur score se dégrader (Enseignement, Producteurs d'énergie, et Services). [RT]



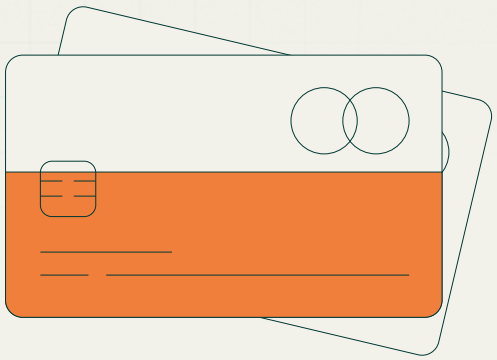
Alors que les Amériques et la région EMEA conserveront probablement des scores similaires, proches de la moyenne mondiale, les projections pour l'APAC pourraient dépeindre un tableau très différent dans la plupart des grandes catégories. [RT]

Nous avons observé plusieurs tendances en matière de sécurité des données. Les voici réunies sur un même diagramme pour les envisager sous une perspective un peu différente.[RT]



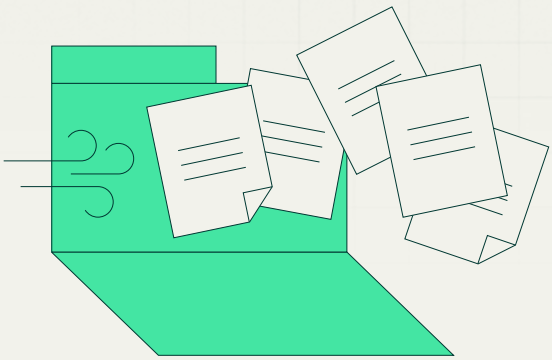
La dure réalité des pertes de données

Jusqu'à présent, nous avons dressé un état des lieux de la data, tantôt sous l'angle de l'intuition, tantôt sous l'angle de l'analyse. Qu'en est-il des menaces qui pèsent sur ces mêmes données ? Retour à l'intuition pour voir ce qu'en disent les responsables IT et sécurité.



53 %

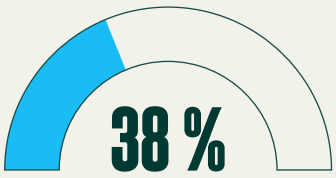
53 % des organisations externes ont subi une perte conséquente d'informations sensibles au cours de l'année dernière [99]



16 %

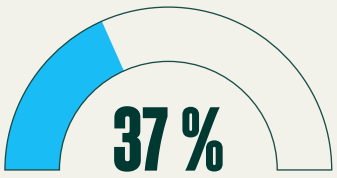
Environ 1 organisation externe sur 6 (16 %) a subi plusieurs pertes conséquentes de données sensibles en 2022 [99]

Types de données compromises dans les organisations externes l'année dernière : [99]



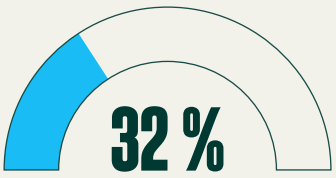
38 %

Données à caractère personnel



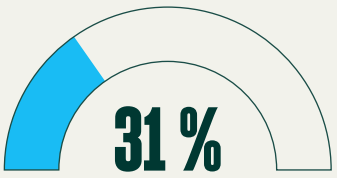
37 %

Données financières de l'entreprise



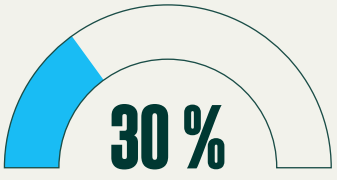
32 %

Données/clés d'authentification



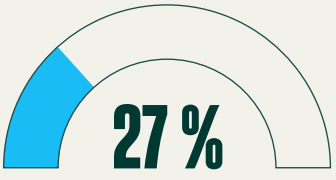
31 %

Propriété intellectuelle



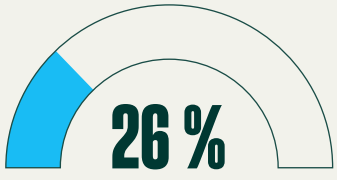
30 %

Données de cartes de paiement



27 %

Numéros de compte



26 %

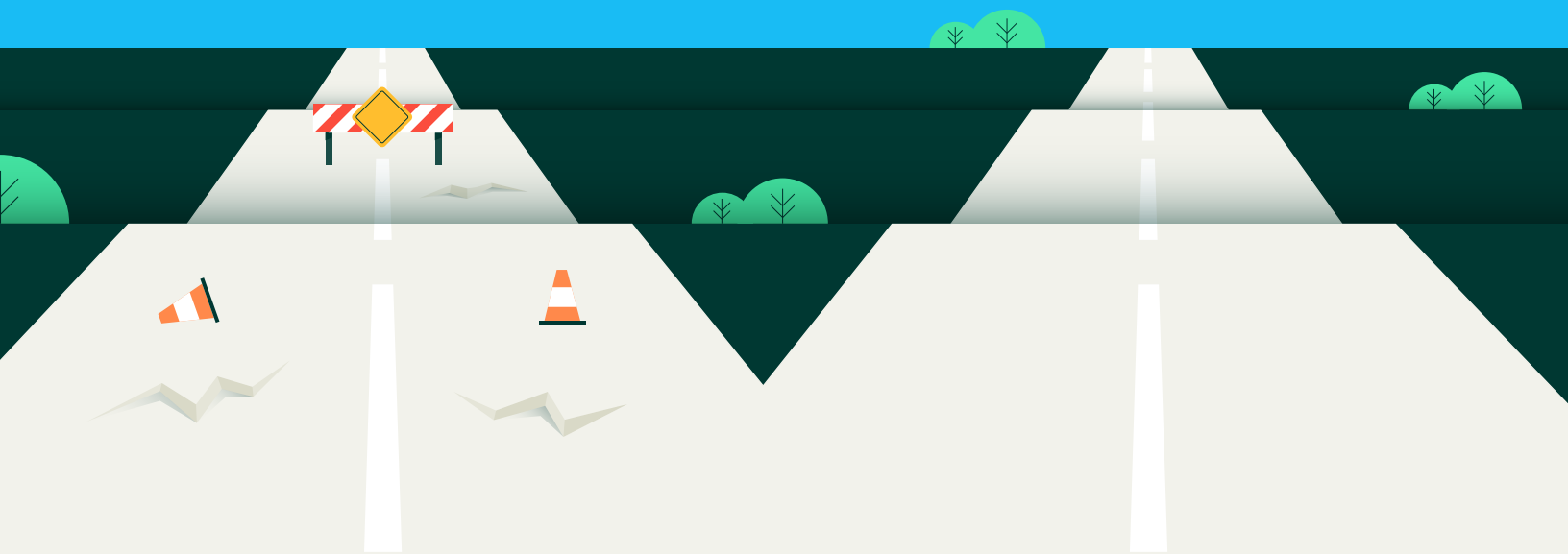
Informations de santé protégées

RECOMMANDATIONS

HORS DES SENTIERS BATTUS

Nul ne sait vraiment ce que l'avenir nous réserve. Ce que nous savons en revanche, c'est que nous disposons de tous les éléments pour renforcer la sécurité des données à l'avenir.

Examinons quelques méthodes de base qui ont prouvé leur efficacité dans ce domaine. Elles peuvent paraître simples. C'est parce qu'elles le sont. Mais les résultats sont là. **Les chiffres parlent d'eux-mêmes.**



98 %

La grande majorité des organisations externes (98 %) se disent actuellement confrontées à des problèmes importants en matière de visibilité des données. [98]

54 %

des organisations externes ont placé les questions de données et de leur sécurité sous la responsabilité d'un de leurs dirigeants. [99]

Rien n'est jamais écrit. Notre avenir n'est que le produit des choix que nous faisons aujourd'hui. Voyons quelques exemples.

Rubrik Zero Labs
Trois recommandations majeures

1.

RECOMMANDATION

Maintenez une bonne visibilité pour auditer régulièrement vos données sensibles.

Lorsqu'une organisation décide de réduire le volume total de ses données de 20 % par rapport à l'année précédente, elle réduit systématiquement sa surface de risque. Elle peut par exemple supprimer les données sensibles non consultées dans les 12 derniers mois, rechercher et supprimer les doublons, ou encore supprimer les données dans les partages utilisateur pour les employés/clients/partenaires qui ont quitté l'entreprise au cours de l'année écoulée.
Cela s'applique également aux données dupliquées dans différents datastores d'une même entreprise.

2.

RECOMMANDATION

Soyez attentif à la croissance des données.

Le volume total, le choix de l'environnement et le nombre total d'environnements sont autant de leviers potentiels. Vous pouvez, par exemple, limiter la croissance des données dans le cloud à 50 % du volume total de l'environnement, supprimer les données selon des politiques clairement définies, limiter le nombre total d'emplacements de stockage à moins de quatre pour toute l'organisation, ou stocker les données sensibles dans une seule enclave.

3.

RECOMMANDATION

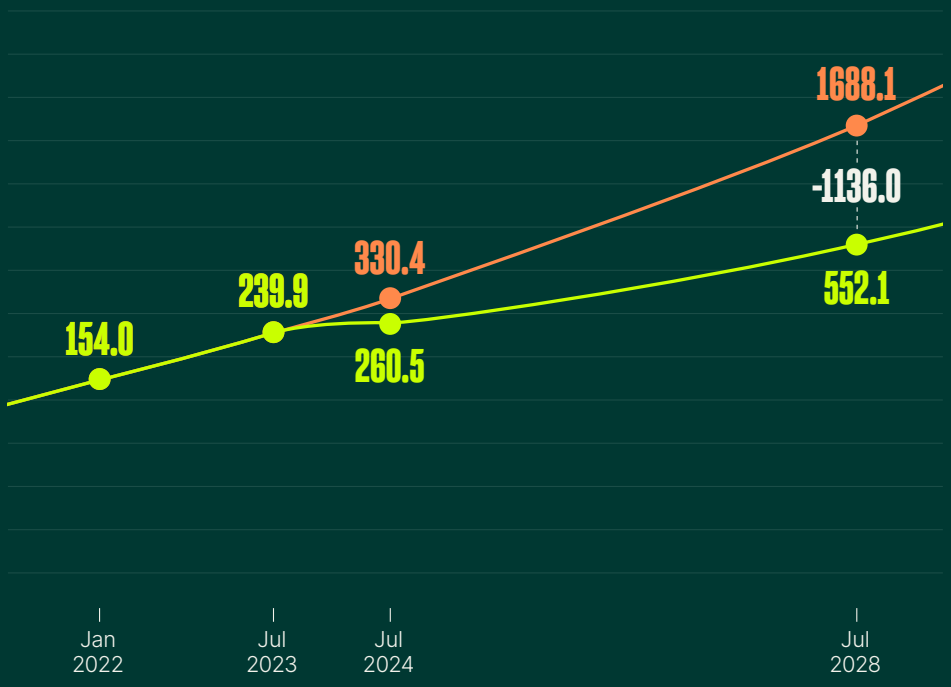
Faites de la sécurité des données un domaine d'action spécifique pour votre Comex.

Nommer un référent pour ces questions, définir des politiques et appliquer les bonnes pratiques sont autant d'éléments qui auront un impact positif et mettront l'accent sur le partage de responsabilité.

Mise en application des recommandations

Moyenne totale en To de stockage back-end [RT]

Voyons ce qui se passerait si ces changements étaient mis en œuvre aujourd'hui.



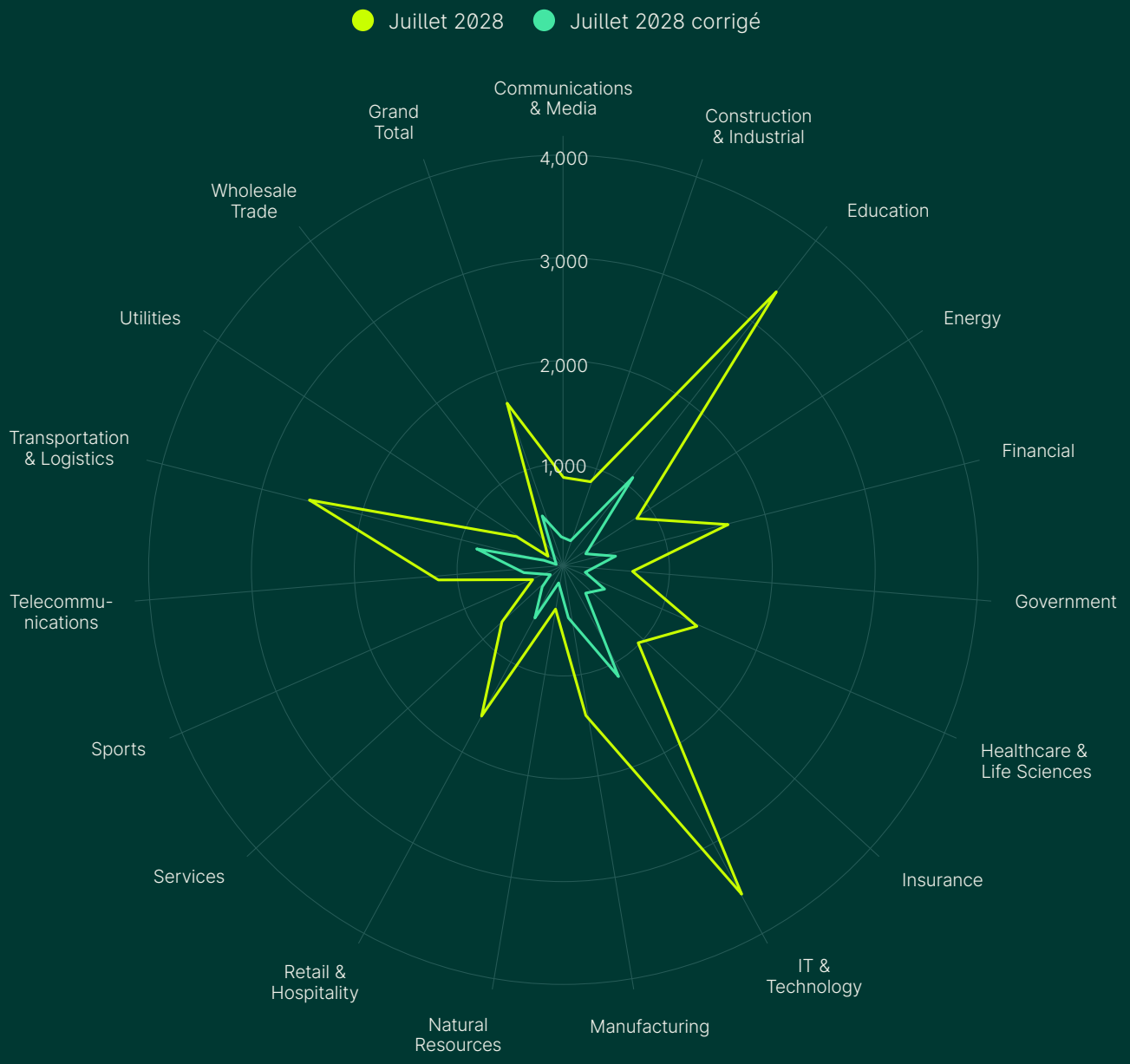
Changement constaté dans cinq ans après application des recommandations : [RT]

RÉDUCTION DE +1 100 TO

de stockage back-end pour une organisation type

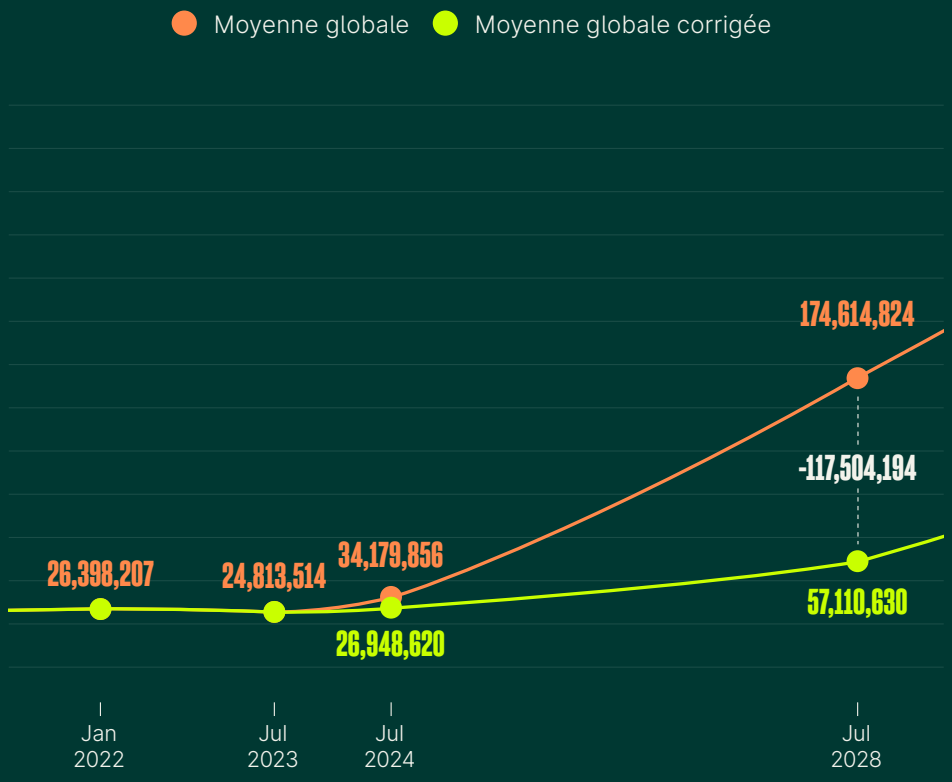
Moyenne totale en To de stockage back-end

Ces recommandations contribuent déjà à des changements tangibles. Maintenant, comparons-les tous en même temps pour dresser un panorama complet :



Mise en application des recommandations

Quantité moyenne de fichiers contenant des données sensibles [RT]

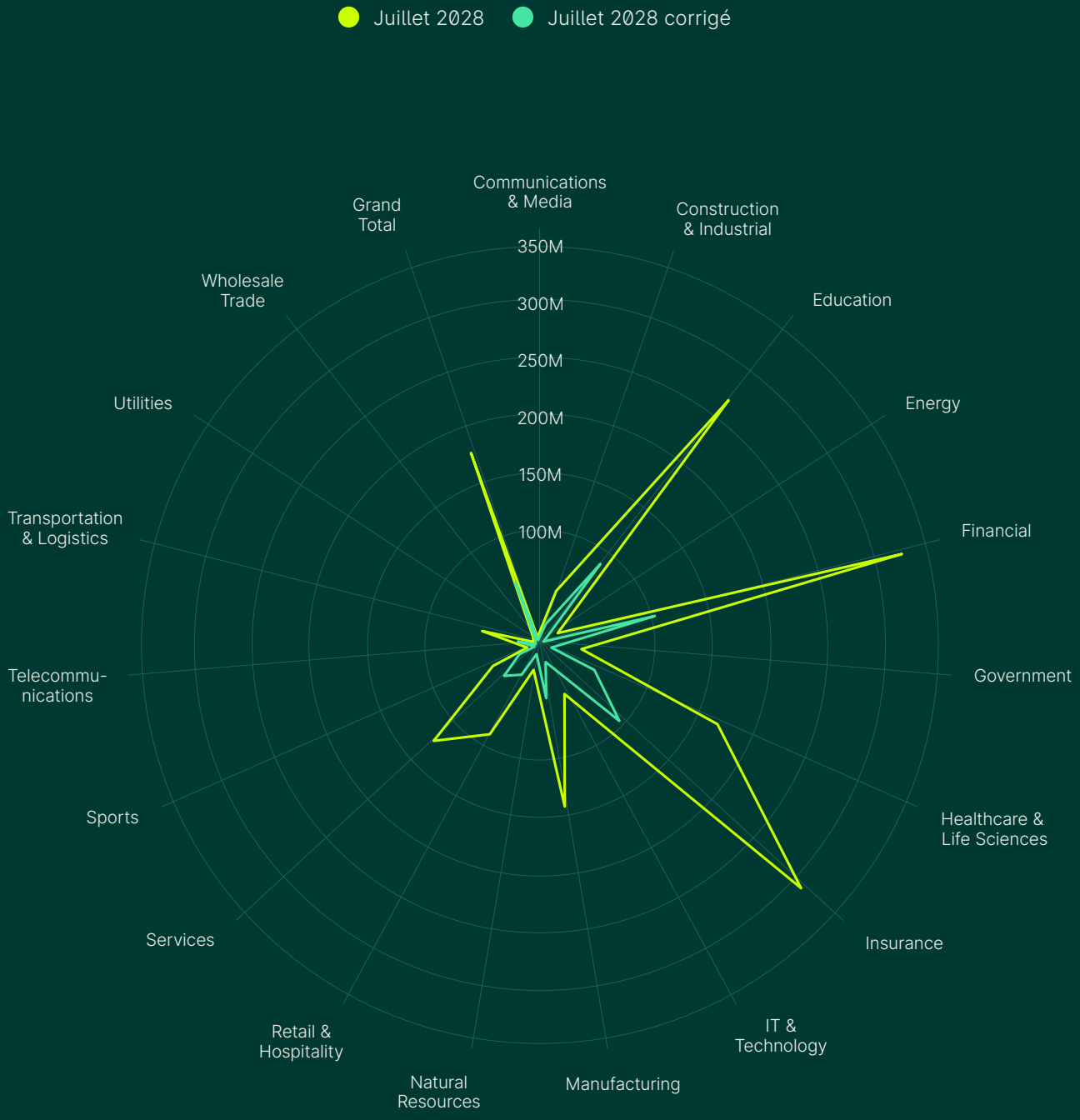


Changement constaté dans cinq ans après application des recommandations : [RT]

RÉDUCTION DE PLUS DE 117 MILLIONS

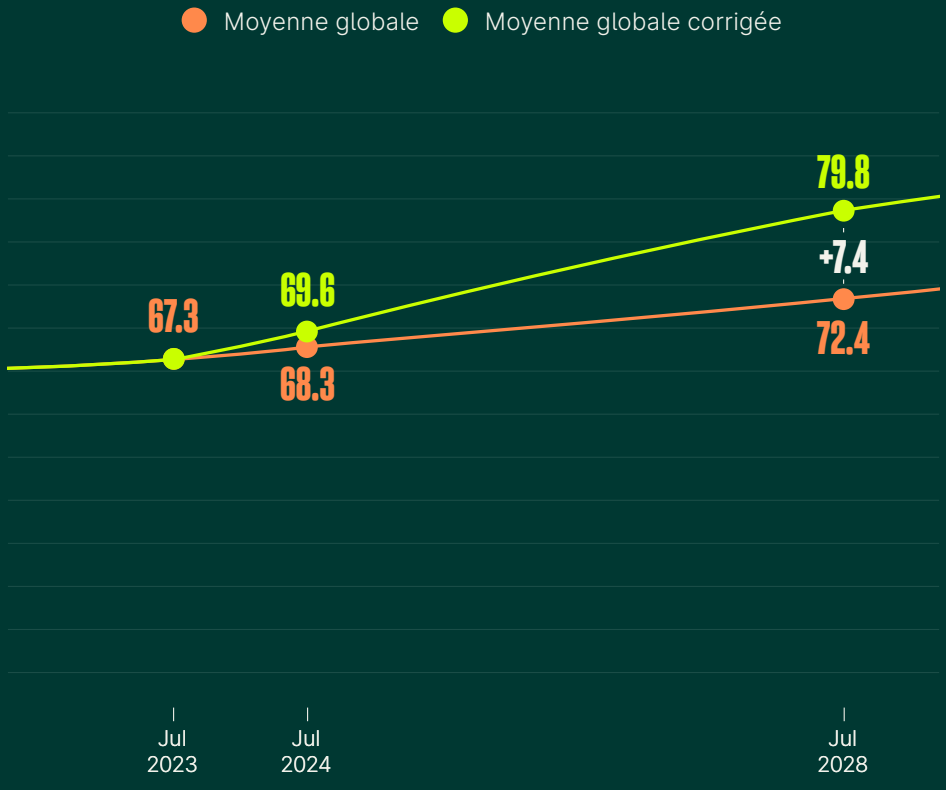
d'enregistrements de données sensibles dans un environnement type

Quantité moyenne de fichiers contenant des données sensibles [RT]



Mise en application des recommandations

Moyenne des scores de sécurité des données [RT]

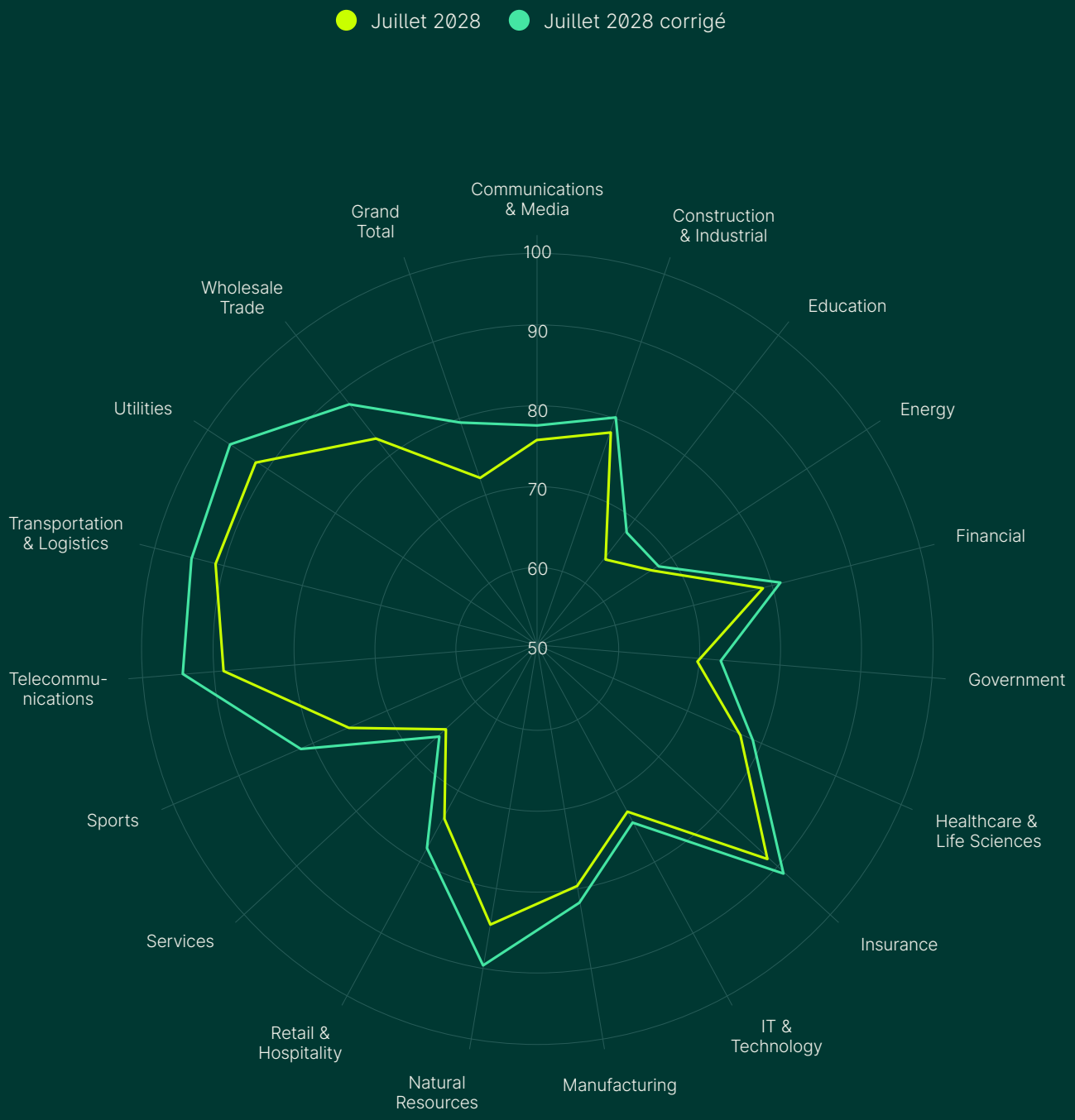


Changement constaté dans cinq ans après application des recommandations : [RT]

AMÉLIORATION DE 10 %

du score de sécurité des données (soit deux fois plus que prévu)

Moyenne des scores de sécurité des données ®

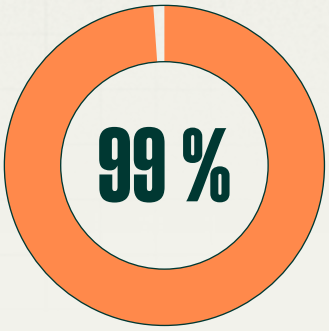


SUMMARY

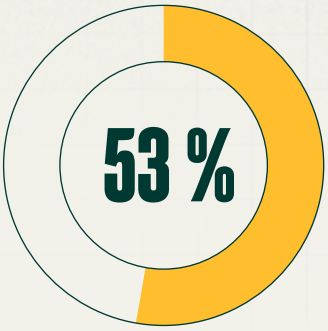
JOURNEY'S END (FOR NOW)

Nous avons commencé ce voyage dans le monde de la data en déclarant que l'être humain est optimiste par nature. Optimistes, nous les sommes aussi et nous espérons que cet état des lieux sans concession vous aidera à vous faire un avis objectif sur vos données.

Y a-t-il du mal à être optimiste ?
Oui et non.



Nombre d'organisations ayant subi une attaque l'année dernière



Nombre d'organisations ayant subi une perte conséquente d'informations sensibles au cours de l'année dernière

Lorsqu'on sait que 99 % des organisations ont subi une attaque l'année dernière et que plus de la moitié ont admis avoir essuyé une perte conséquente d'informations sensibles au cours des 12 derniers mois, force est de constater que les chiffres sont clairement en notre défaveur. Pourtant, il faut une bonne dose d'optimisme aux professionnels de l'informatique ou de la sécurité pour se lancer dans la bataille. Cet optimisme est une bonne chose, car il mobilise les forces pour relever les défis qui nous attendent.

Cependant, comme nous l'avons vu, un trop-plein d'optimisme peut avoir des conséquences désastreuses.

Si vous ne deviez retenir qu'une chose, souvenez-vous de ceci :

- **Restez optimiste.**
- **Analysez la situation.**
- **Repérez des signaux faibles.**
- **Prenez des décisions éclairées.**

Remerciements

Rubrik souhaite conclure ce rapport en exprimant sa sincère gratitude aux personnes qui ont permis à ce travail de voir le jour. Wakefield Research a fourni des données afin de rendre cette étude aussi objective que possible. Shaped By (www.shaped-by.com), une fois de plus, a trouvé un moyen de donner vie aux idées. Enfin, de nombreux collaborateurs de Rubrik ont travaillé dur pour apporter leurs compétences, du contexte et des conseils. Il est impossible de les remercier tous, mais nous tenons à exprimer notre reconnaissance à Amanda « Danger » O'Callaghan, Linda Nguyen, Lynda Hall, Ajay Kumar Gaddam, Ryann Goss, Derek Morefield, Josh Burns, Gunakar Goswami, Prasath Mani, Ethan Hagen, Kevin Nguyen, Caleb Tolin, Kelly Cooper et Olivia Howard.

Rubrik Zero Labs