

SÉCURITÉ DES DONNÉES : ÉTAT DES LIEUX

Mesurer le
RISQUE DATA



Rubrik Zero Labs



SOMMAIRE

INTRODUCTION **03**

DONNÉES ET MÉTHODOLOGIE **04**

Vos données dans

LE VISEUR DES HACKERS **14**

Le risque

INHÉRENT AUX DONNÉES **19**

Les répercussions

D'UNE ATTAQUE **28**

Restaurer

ET RÉCUPÉRER **37**

Se préparer à la

PROCHAINE OFFENSIVE **41**

REMERCIEMENTS **48**

Ceci est une histoire de



LA DATA

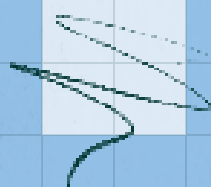
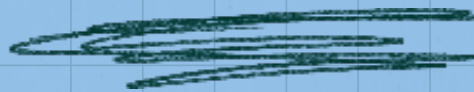
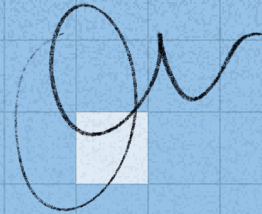
Du type de données que vous gérez, de leur évolution
et des menaces qui les accompagnent.

C'est aussi une histoire de risque. Un risque protéiforme
et permanent que vous devez mesurer et anticiper.

Mais avant de commencer, *quelques précisions s'imposent.*



DONNÉES ET MÉTHODOLOGIE





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 à partir de quatre sources différentes.

TÉLÉMÉTRIE DE RUBRIK = ◆

Les données télémétriques de Rubrik nous ont permis de mieux comprendre la réalité de l'environnement data d'une organisation type, mais aussi des risques auxquels elle est exposée.

WAKEFIELD RESEARCH = ▲

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

PARTENAIRES RUBRIK = ●

Recherches et conseils fournis par deux organisations partenaires de Rubrik.

AUTRES CONTRIBUTEURS = ■

Études menées par des acteurs reconnus dans le monde de la cybersécurité.

TÉLÉMÉTRIE DE RUBRIK ◆

Au Rubrik Zero Labs, nous croyons aux vertus de la transparence. Dès lors qu'une organisation nous confie ses données, il est de notre devoir de lui dire ce que nous en avons appris. Voici donc l'ensemble des sources qui constituent le jeu de données ayant servi de base à notre analyse et à l'élaboration de notre perspective.

N.B. : pour la première fois dans cette étude, nous utilisons des données issues de Laminar, une plateforme leader de gestion de la posture de sécurité des données rachetée par Rubrik en 2023.

LES DONNÉES TÉLÉMÉTRIQUES DE RUBRIK, C'EST :

6 000+ clients

68 pays

42 EO sécurisés, soit plus de 38,4 milliards d'enregistrements de données sensibles



Volume total de données sécurisées :

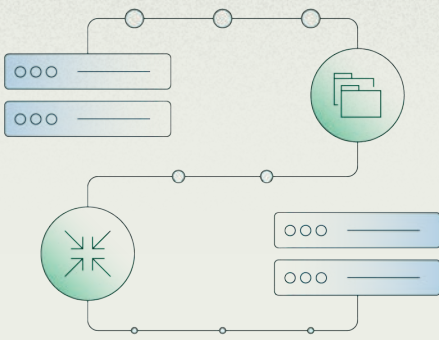
- Plus de 42 exaoctets (Eo) de stockage logique
- 963 pétaoctets (Po) de stockage back-end physique



Plus de 38,4 milliards d'enregistrements de données sensibles



Données couvrant la période du 1er janvier 2023 au 31 décembre 2023



Front-end vs back-end

Petit aparté pour les geeks de la data : 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 appuyons sur les données de stockage en back-end dans la suite de ce rapport.

Que représentent 42 Eo de données ?

Prenez votre dossier médical, et tout ce qu'il contient (formulaire, radios, résultats d'IRM, observation des médecins, etc.). En général, ce genre de dossier pèse grosso modo 80 Mo.

Prenez maintenant les 42 Eo de données sécurisées par Rubrik. Pour atteindre ce chiffre, il faudrait pas moins de cinq dossiers médicaux complets pour chacune des 117 milliards de personnes qui ont foulé notre belle Terre depuis l'aube de l'humanité. Ça en fait, des données !

WAKEFIELD RESEARCH [▲]

Nous avons demandé à Wakefield Research de mener une étude auprès de responsables IT et sécurité. Les statistiques ainsi obtenues complètent la télémétrie Rubrik par des points de vue et observations issues du terrain. Par souci d'objectivité, aucun client Rubrik n'est représenté dans ce jeu de données.

1 600+ responsables IT et sécurité

10 pays

50%+ de DSI ou RSSI

1 625

décideurs travaillant dans des entreprises d'au moins 500 salariés, dans 10 pays (France, Royaume-Uni, Allemagne, Italie, Pays-Bas, États-Unis, Australie, Inde, Japon, Singapour) de trois régions (EMEA, Amériques et APAC)

50 %

de DSI ou de RSSI

50 %

de décideurs IT

50 %

de directeurs ou VP

50 %

de décideurs sécurité



PARTENAIRES RUBRIK

Nous nous sommes appuyé sur les jeux de données et conseils de deux partenaires Rubrik participant à nos efforts d'amélioration de la résilience des données.



Microsoft nous a transmis les données issues de son Rapport de défense numérique 2023¹, notamment les taux d'exfiltration de données et ses recommandations en matière de résilience.



Aon nous a apporté de précieuses données issues de son rapport sur la cyber-résilience 2023², en particulier sur la réalité des sauvegardes de données et les activités post-intrusion.

AUTRES CONTRIBUTEURS

Pour dresser un tableau aussi objectif que possible, nous enrichissons la télémétrie Rubrik de données provenant de plusieurs entreprises et d'une université qui bénéficient d'une perspective unique sur certains domaines.



Mandiant nous a communiqué la durée de présence des attaquants mesurée lors de ses missions IR/MDR en 2023³.



L'équipe Unit 42 de Palo Alto Networks nous a communiqué le montant des rançons réclamées par les cybercriminels et versées par leurs victimes au cours de leurs missions IR/MDR en 2023.



Proofpoint a mis à notre disposition des données sur les attaques ciblant le cloud, telles que rapportées dans Threat Report – Le facteur humain 2023⁴.



Recorded Future nous a livré toutes les tendances ransomware observées en 2023⁵.



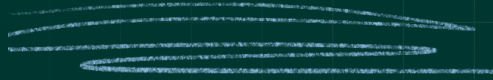
La School of Public Health de l'université du Minnesota Twin Cities nous a fait part de l'impact des ransomwares sur les établissements publics de santé, mesuré dans le cadre de son étude « Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients⁶ », en cours d'examen par ses pairs.

1 <https://www.microsoft.com/fr-fr/security/security-insider/microsoft-digital-defense-report-2023>
2 <https://www.aon.com/2023-cyber-resilience-report/> (en anglais)
3 <https://www.mandiant.fr/m-trends>

4 <https://www.proofpoint.com/fr/resources/threat-reports/human-factor>
5 <https://therecord.media/ransomware-tracker-the-latest-figures> (en anglais)
6 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292



PARLONS RISQUE



Parlons clair. Gros plan sur les trois principes directeurs de cette étude du risque.

PRIMO

Une simple addition suffit pour calculer le risque :

La probabilité que vos données soient impactées par une entité externe



Le risque inhérent à vos données à un instant



L'impact associé à ce risque

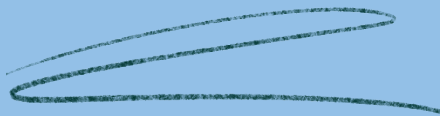


Vos décisions face à cet impact



Le risque total

PAS BESOIN D'AVOIR FAIT MATH SUP !





SECUNDO

Zoom sur la data

En tant qu'expert de la sécurité des données, la data reste notre domaine de prédilection. Nous laisserons donc de côté les aspects infrastructurels ou architecturaux pour nous focaliser uniquement sur les risques qui pèsent sur vos données.

Une étude ciblée

Soyons honnêtes. Vous n'avez pas de temps à perdre avec des rapports à rallonge qui décortiquent chaque aspect de la sécurité des données. C'est pourquoi notre étude se limite à quelques thèmes phares :



Cloud

L'émergence du cloud public remonte déjà à plusieurs dizaines d'années. Et pourtant, la sécurité des données cloud reste une pratique assez mal maîtrisée. Truffés d'angles morts et donc plus difficiles à défendre, ces environnements dématérialisés sont maintenant plus souvent attaqués (et compromis !) que leurs pendants on-prem.



Ransomware

Il n'y a pas si longtemps de cela, les experts prédisaient un déclin du ransomware. Résultat : il ne s'est jamais aussi bien porté, comme en témoignent les dégâts provoqués dans des structures de tous horizons.

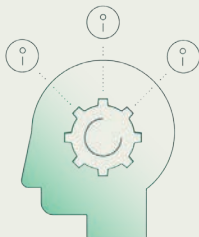


Santé

À quelques exceptions près, les acteurs de la santé génèrent et stockent plus de données sensibles que dans tout autre secteur. Ils sont d'ailleurs soumis à des réglementations beaucoup plus strictes, notamment en matière de transparence. Et qui dit plus de transparence, dit plus de données à étudier !

TERTIO

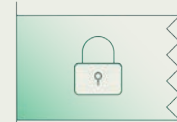
À qui s'adresse cette étude ?



Tous les décideurs n'ont pas besoin des mêmes informations. En général, le risque est une décision qui se prend dans les plus hautes sphères de la hiérarchie.



Notre objectif ? Nourrir les discussions des Comex autour des enjeux IT, métiers et de cybersécurité.



En offrant à tous ces décideurs une grille de lecture commune, ils pourront coordonner leur action face aux risques.



NOTRE ATTITUDE FACE AU RISQUE



L'humain n'aime pas l'incertitude.
Face à la probabilité qu'un événement se produise,
nous adoptons un point de vue assez binaire :

« OUI, ÇA VA SE
PRODUIRE,
C'EST CERTAIN. »

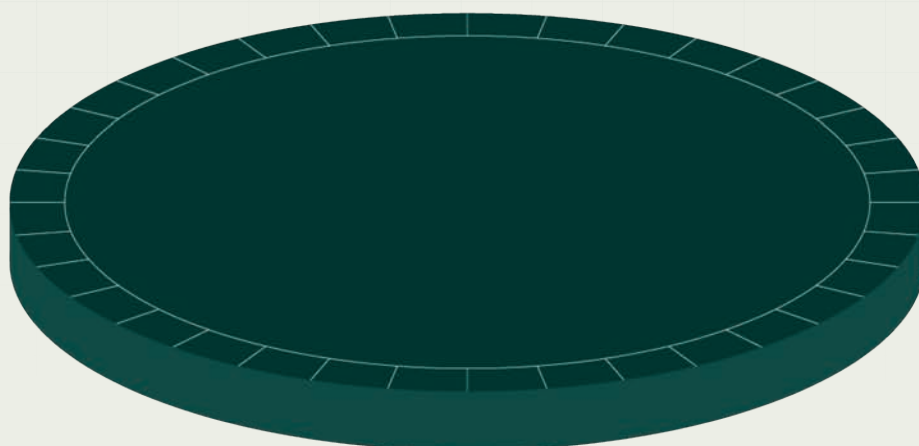
EN RÉALITÉ,
LES CHOSES SONT UN
PEU PLUS NUANCÉES

« NON, ÇA
N'ARRIVERA
JAMAIS. »



Si la météo affiche une probabilité de précipitation
de 52 % dans votre agglomération,
elle ne vous dit pas de façon catégorique
« Oui, il va pleuvoir » ou « Non, il ne pleuvra pas. »

**CE QU'ELLE VEUT DIRE,
C'EST QUE LES PROBABILITÉS
D'UNE AVERSE SE JOUENT À
PILE OU FACE**





Et puis il y a tous ces petits détails, ceux qui nous intéressent vraiment : quelle quantité de pluie ? Petite bruine ou grosse averse ? Dois-je prendre mon parapluie ? Ou vais-je plutôt faire une journée de télétravail ?

*Ces décisions, c'est vous
et vous seul qui les prenez.*

Ce serait tellement plus facile si l'on pouvait décider une bonne fois pour toutes.

**Mais les choses ne sont pas si simples
que cela.**



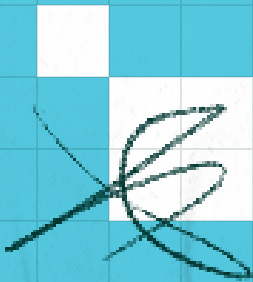
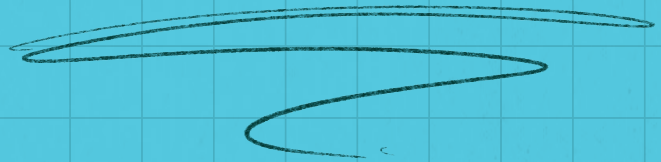
La façon dont vous vivez cet épisode pluvieux aujourd'hui influera sur votre perception du bulletin météo de demain. Et vous en aurez également tiré quelques leçons qui vous permettront de rester au sec au prochain déluge.

Bref, cette combinaison de facteurs modifie à chaque fois la façon dont vous percevez le risque, que ce soit la probabilité d'une ondée... ou d'une cyberattaque.

**Commençons par les menaces
venues de l'extérieur.**



Vos données dans le
VISEUR DES HACKERS





La première question à vous poser :

Les attaquants convoitent-ils *mes données* ?

Votre frigo intelligent veut-il votre peau ?

Les ransomwares s'en prennent maintenant à ESXi

IA : nouvelle arme absolue des attaquants

CES NEWS VOUS CONCERNENT-ELLES VRAIMENT ?

Une autre attaque à la « SolarWinds » ?

La compromission du siècle : des millions de données parties en fumée

Ou est-ce que vous vous faites du souci pour rien ?

Strawberry Tempest : nouveau nom, mêmes méthodes

Personne ne peut vous dire avec certitude si vous serez, oui ou non, victime d'une cyberattaque. En revanche, ce que nous pouvons vous dire, c'est ce que des organisations comme la vôtre ont vécu au cours de l'année passée.

La quasi-totalité de vos pairs ont essuyé une cyberattaque toutes les deux semaines environ.

Petit récapitulatif de l'année écoulée pour les responsables IT et sécurité : ▲

94 % des responsables IT et sécurité ont indiqué avoir subi une cyberattaque majeure l'an passé.

30 événements malveillants en moyenne ont été portés à l'attention des dirigeants en 2023.

93 % des organisations ont rempli une déclaration officielle de perte de données auprès des autorités compétentes.



Les cyberattaques ont un taux de probabilité bien supérieur aux vols physiques ou aux incendies.



Pour mettre en perspective le risque de cyberattaque, la compagnie d'assurance Aviva¹ a comparé sur une même période le nombre d'incidents cyber et celui de sinistres plus conventionnels. Voici ce qu'elle a observé :

67 % Dans les organisations, le risque de cyberattaque est 67 % plus élevé que le risque d'un vol physique.

5x Les organisations ont cinq fois plus de risque d'être victime d'une cyberattaque que d'un incendie.

20 % des organisations ne savent pas comment réagir en cas de cyberattaque.

¹ <https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/>

Les attaquants sont passés maîtres dans l'art de l'exploitation des *environnements hybrides*.

Face à ce risque bien réel, mieux vaut connaître la nature de la menace et où elle risque de frapper. Parmi les 94 % d'organisations victimes d'une cyberattaque, bon nombre ont été ciblées via de multiples types d'environnements : ▲

67 % **66 %** **51 %**

SaaS

Cloud

On-prem

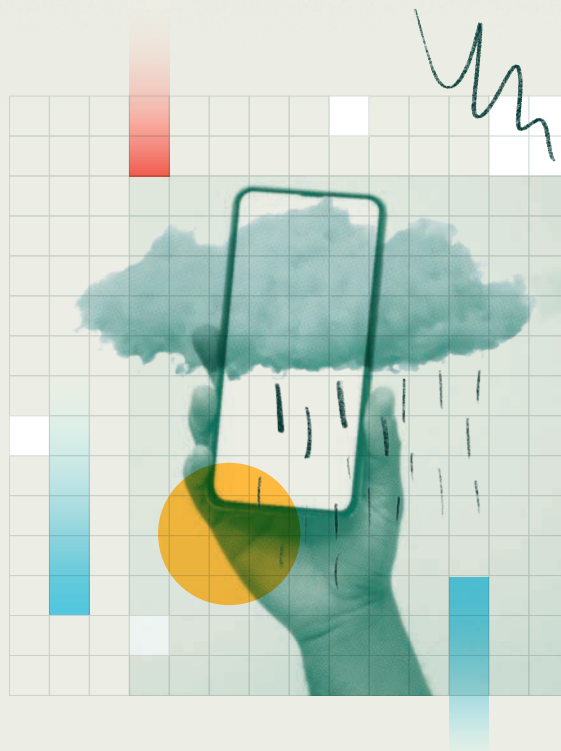
Voici les deux types d'attaques les plus courants dans ces environnements : ▲

38 %

de ces structures ont subi au moins une compromission de données.

33 %

de ces structures ont été victimes d'au moins une attaque par ransomware.



La quasi-totalité des tenants cloud ont été visés, et les deux tiers ont été compromis en 2023.

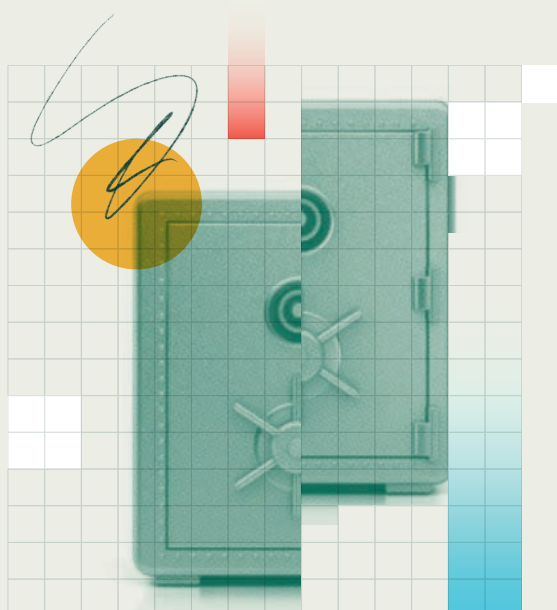
Nous ne sommes pas les seuls à l'avoir observé. Dans son rapport¹, Proofpoint indique que : ■

94 %

des tenants cloud ont été ciblés tous les mois au cours de l'année passée.

62 %

des tenants cloud ciblés ont été compromis.





Les attaquants *ont accès à vos données* pendant des jours entiers avant d'être repérés.

Mandiant définit la durée de présence d'un attaquant¹ comme le nombre de jours passés dans l'environnement de sa victime avant d'être détecté.

10 JOURS 5 JOURS

La durée de présence médiane, tous événements confondus, était de 10 jours l'année passée.

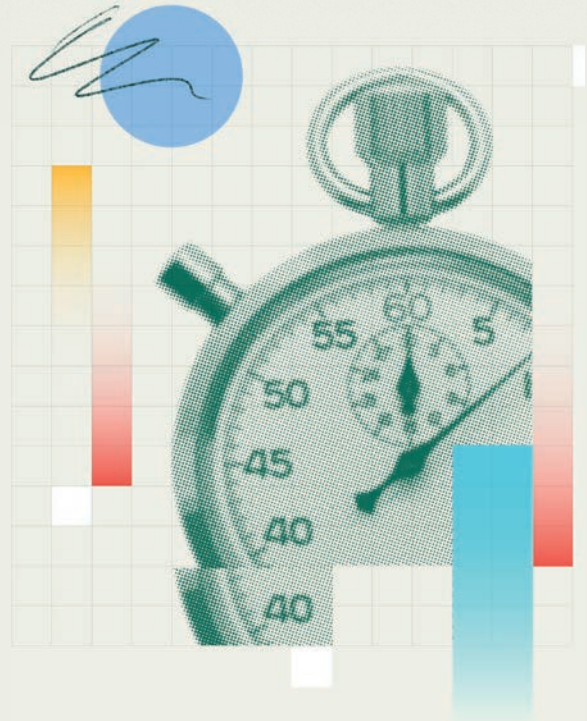
La durée de présence médiane lors d'une attaque par ransomware était de 5 jours.

LE PLUS

Il s'agit des durées de présence les plus courtes jamais observées par Mandiant.

LE MOINS

Elles laissent encore largement le temps aux acteurs malveillants pour atteindre leurs objectifs.



NON, VOUS NE RÊVEZ PAS. LE NOMBRE DE RANSOMWARES EXPLOSE (+70 %).¹

Recorded Future a observé une hausse significative du nombre d'attaques par ransomware rendues publiques au cours de l'année passée :

46 %



358 attaques ciblant le secteur de la santé (+46 % en 12 mois)

70 %



4 399 attaques tous secteurs confondus (+70 % en 12 mois)

Penchons-nous maintenant sur le risque inhérent à vos données.

¹ <https://www.mandiant.fr/m-trends>

Le risque
INHÉRENT AUX DONNÉES

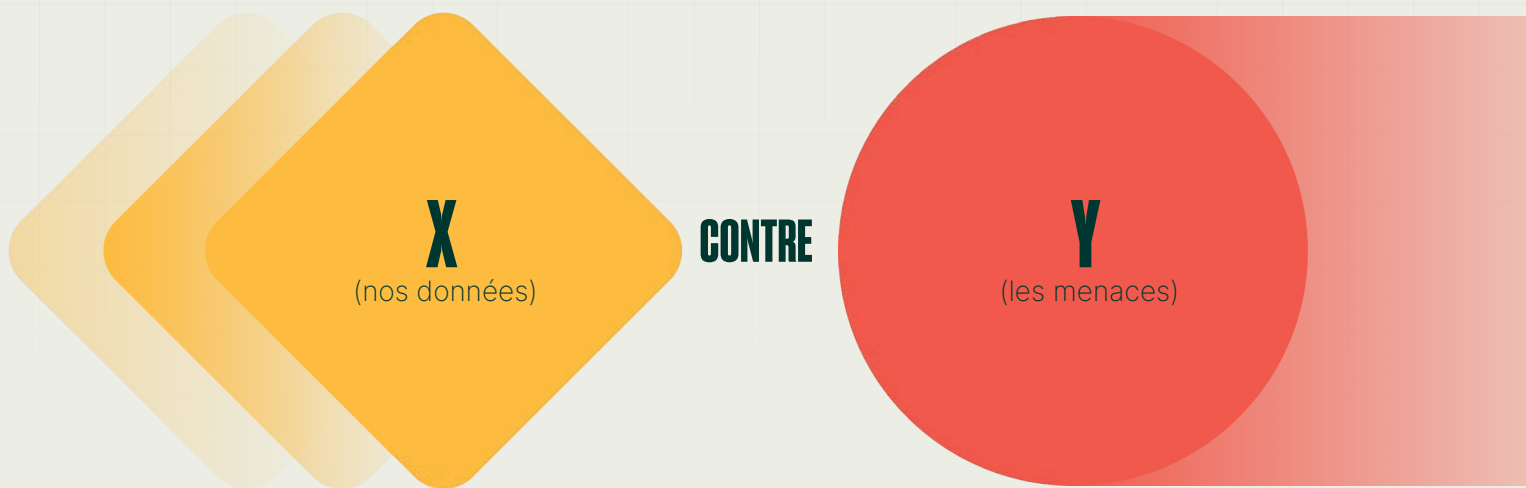


Vous connaissez maintenant la probabilité d'une attaque (et, en toute franchise, les statistiques ne jouent pas en votre faveur). Vous devez donc tout faire pour minimiser le risque en réduisant :

LE RISQUE QU'UNE ATTAQUE ATTEIGNE SON BUT

LES REVENUES D'UNE ATTAQUE

Ce que nous cherchons à faire est finalement très simple (du moins en apparence). Nous voulons protéger



Mais pour cela, nous devons considérer les deux inconnues de l'équation. Voyons ce que les opérationnels attendent de leurs équipes de sécurité.



LA DATA

grandit à un rythme qui dépasse les capacités de vos systèmes de défense à s'adapter.

Dans la santé, les équipes de sécurité doivent protéger des données plus nombreuses et plus sensibles que dans les autres secteurs. Les volumes augmentent aussi plus vite que dans la moyenne. ♦

Les acteurs de la santé sécurisent 22 % de données en plus que la moyenne mondiale.

334 BETB

Santé

273 BETB

Moyenne globale

Le B.A.-BA des BETB

FRONT-END vs BACK-END

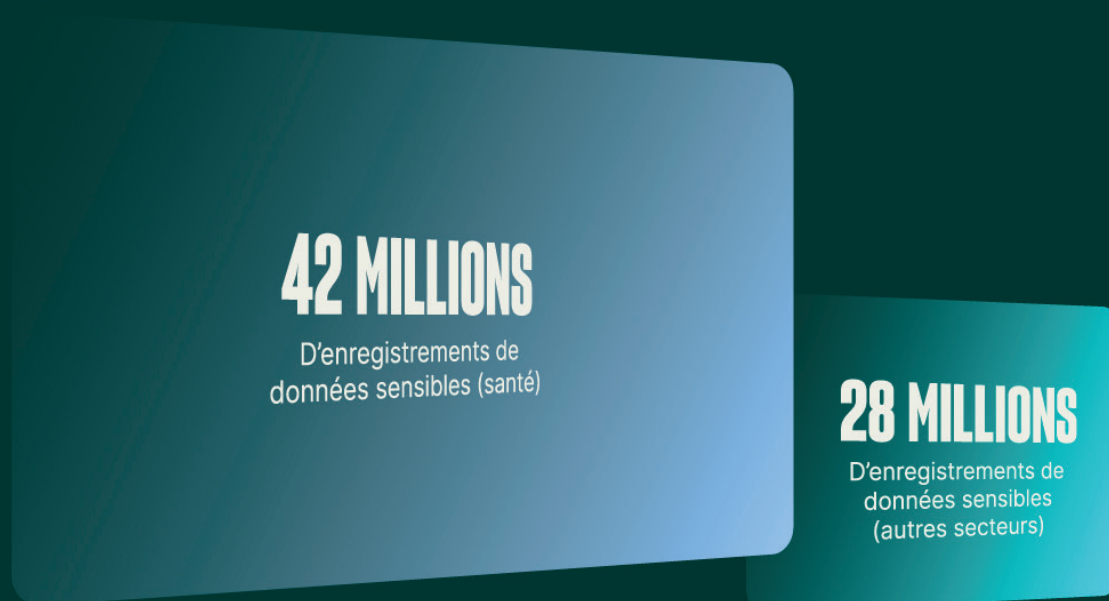
Petit rappel : quand le commun des mortels entend le mot « données », il pense au stockage logique, autrement dit au stockage front-end. Nous qui évoluons dans le monde de la data, nous préférons nous concentrer sur le stockage back-end. Rubrik prend l'intégralité des données d'une organisation et applique différentes techniques (notamment la déduplication et la compression) pour réduire le volume de données stockées en back-end. C'est pourquoi nous nous appuyerons sur les données de stockage en back-end dans la suite de ce rapport.



Les acteurs de la santé ont vu le volume de données qu'ils traitent augmenter de 27 % l'année passée (contre 23 % pour les autres organisations).



Les acteurs de la santé traitent 50 % de données sensibles en plus que la moyenne des autres secteurs.





Le nombre d'enregistrements de données sensibles dans le secteur a augmenté de plus de 63 % en 2023, soit cinq fois plus que la moyenne mondiale tous secteurs confondus (13 %).

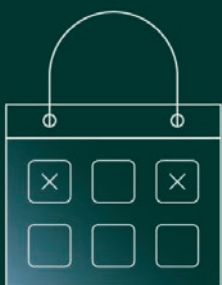


UN NOMBRE RECORD DE PROBLÈMES À GÉRER EN 2023

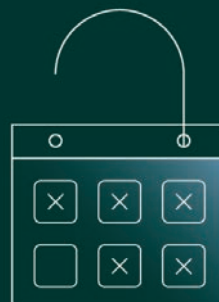
Le nombre de vulnérabilités détectées n'est pas forcément la mesure la plus fiable pour calculer le risque d'exposition, mais elle a le mérite de nous donner une idée précise de l'ampleur des risques liés aux solutions externes.

L'année 2022 avait atteint un plus haut historique en termes de vulnérabilités signalées.

Record battu en 2023. Le nombre de vulnérabilités a augmenté de 16 % par rapport à l'année précédente.



25 083
vulnérabilités détectées



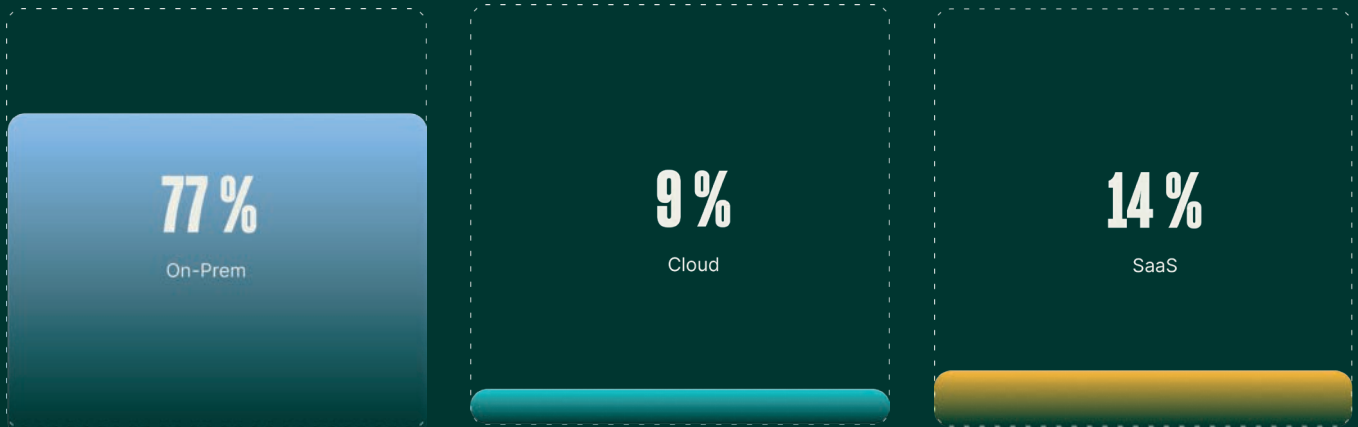
29 065
vulnérabilités détectées



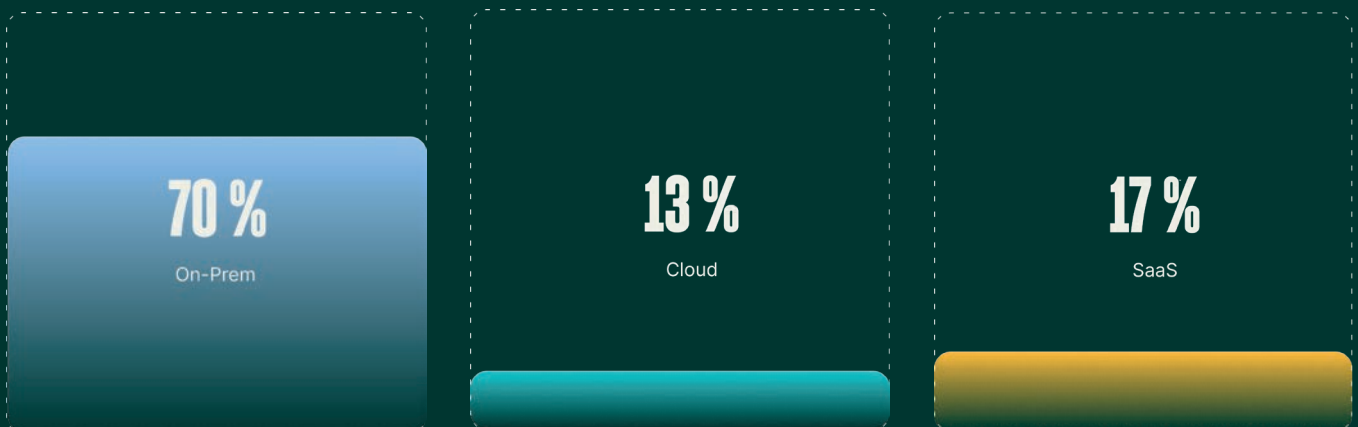
LES ORGANISATIONS DÉPENDENT TOUJOURS PLUS DU CLOUD ET DU SAAS ♦

À l'ère du tout-numérique, la migration vers le cloud devient un impératif. Résultat, les environnements hybrides penchent de plus en plus vers le cloud et le SaaS, tandis que les architectures on-prem perdent du terrain.

2022



2023





LE CLOUD EST TRUFFÉ D'ANGLES MORTS

Sécurité des données cloud

ANGLE MORT N° 1

70 % des données d'une instance cloud type sont stockées sous la forme d'objets ♦

Or, le stockage d'objets a un inconvénient : lorsqu'elles sont entreposées sous cette forme, les données deviennent généralement illisibles pour les équipements de sécurité. Elles sont donc plus difficiles à protéger.

Sécurité des données cloud

ANGLE MORT N° 2

88 % des données stockées sous forme d'objets sont soit des fichiers textes, soit des données semi-structurées (CVS, JSON ou XML) ♦

Imaginons que vos outils et vos processus vous permettent de voir à l'intérieur des objets stockés. Vous vous heurtez alors à un nouveau problème. Ce type d'objet est composé majoritairement de données non structurées (fichiers textes) ou semi-structurées. Mais toutes ne sont pas lisibles par machine ou couvertes par les mêmes technologies et services de sécurité.

Sécurité des données cloud

ANGLE MORT N° 3

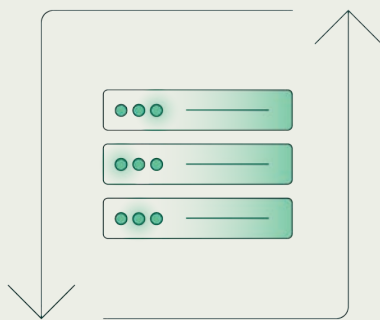
Plus de 25 % des données stockées sous forme d'objets sont soumises à des réglementations (données de santé ou à caractère personnel) ♦

Le problème est simple : les capacités opérationnelles des organisations sont de plus en plus dépendantes du cloud, mais les données réglementées qui y sont stockées sont moins visibles et moins bien protégées que dans les environnements on-prem.



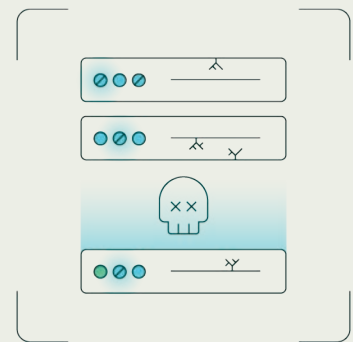
LA PLUPART DES SOLUTIONS DE SAUVEGARDE NE SONT PAS À LA HAUTEUR

Utilisées depuis des décennies dans la quasi-totalité des structures, les technologies de sauvegarde et de restauration sont des outils indispensables pour la reprise après sinistre ou la conformité... tant qu'elles fonctionnent correctement. Mais pour beaucoup d'organisations, c'est loin d'être gagné.



99 %

Dans notre rapport 2022¹, plus de 99 % des organisations indiquaient disposer d'une solution de sauvegarde. ♦



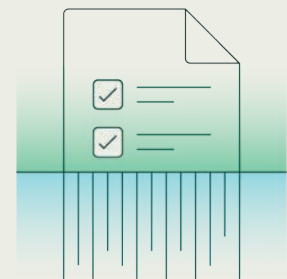
93 %+

Mais plus de 93 % de ces organisations se sont heurtées à de graves problèmes causés par leur solution existante. ♦



70 %

Selon Aon², 70 % des organisations ne stockent pas leurs sauvegardes hors site ou n'utilisent pas un format de sauvegarde immuable. •



40 %

Près de 40 % des organisations observées par Rubrik n'ont défini aucune politique de conformité pour la sauvegarde de leurs données. ♦

1 <https://www.rubrik.com/zero-labs/2023-spring>
2 <https://www.aon.com/2023-cyber-resilience-report/> (en anglais)



SOYEZ SUR VOS GARDES

Les cybercriminels ont repéré la faille et ciblent quasi-systématiquement les sauvegardes

Les attaquants ont cherché presque à chaque fois à désactiver les options de sauvegarde et de restauration des outils de sécurité. **D'après les déclarations des organisations victimes d'une attaque : ▲**

96 %

Les attaquants ont essayé de corrompre les sauvegardes dans 96 % des cas...

74 %

... et y sont parvenus (au moins en partie) dans 74 % des cas.

Les solutions de restauration sont efficaces, mais les cybercriminels gardent un atout dans leur manche

Ils observent comment les outils de sécurité réagissent pour adapter leur mode opératoire. Dans le cas d'un ransomware, par exemple, ils ne se contentent plus de chiffrer les données. Ils les exfiltrent et menacent de les révéler au grand jour. De cette manière, si la victime parvient à faire sauter le verrou qu'ils ont placé sur ses données, les attaquants disposent toujours d'un moyen de pression supplémentaire pour lui faire payer la rançon.

2x

Selon Microsoft, le nombre d'exfiltrations de données potentielles après une compromission initiale a doublé depuis novembre 2022. •

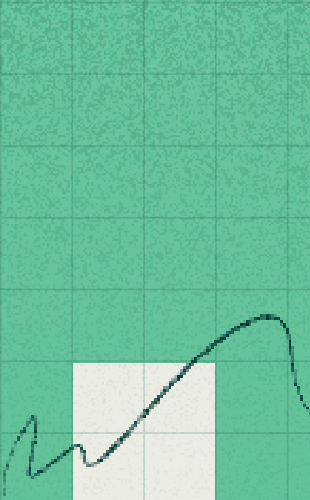
12 %

D'après Aon, une compromission de données est 12 % plus préjudiciable pour une organisation que le ransomware en lui-même. •


93 %

Parmi les organisations victimes d'un ransomware, 93 % ont indiqué avoir payé la rançon, et 58 % avouent avoir cédé par peur de voir leurs données étalées sur la place publique par les attaquants. ▲

Nous connaissons désormais la probabilité d'une attaque. Mais qu'en est-il de son impact ?



Les répercussions **D'UNE ATTAQUE**





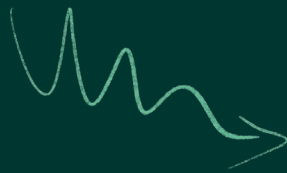
La fin d'une
cyberattaque
ne marque pas
la fin de l'histoire.

Elle n'en est que
le tournant.



Reprenons notre métaphore météo. Ce n'est pas parce qu'il pleut *que votre journée doit s'arrêter pour autant.*

La vie continue ! Ce que vous pouvez faire en revanche, c'est vous adapter à la situation. Comment faire pour rester au sec ? Est-ce que vous sortez le chien sous la pluie ? Et qu'allez-vous faire si vous vous retrouvez complètement trempé ?



Comme pour la pluie, si une cyberattaque vous prend par surprise, vous devrez continuer à avancer. Remédiation, restauration, reporting... il y a beaucoup à faire.

Mieux vous vous préparerez, mieux vous ferez face à l'adversité.

Voici un aperçu des dégâts causés par les cyberattaquants, en particulier par leurs ransomwares, dans le secteur de la santé au cours de l'année écoulée.

LES RÉPERCUSSIONS D'UNE CYBERATTAQUE

Environ 1 Américain sur 3 s'est fait dérober des données médicales à la suite d'une compromission au cours de l'an passé¹.



personnes (en moyenne) ont été impactées lors d'une seule cyberattaque perpétrée contre une structure de santé en 2023.

186 %

Hausse depuis 2022

> 133 M

d'Américains ont vu leurs données compromises à la suite d'une cyberattaque ciblant des structures de santé au cours de l'année passée

1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



Les attaques par ransomware ciblant les acteurs de la santé impactent cinq fois plus de données sensibles que dans les autres secteurs. ♦

Pour évaluer ce risque, Rubrik tient compte à la fois de la quantité de données compromises par les attaquants et de la proportion de données sensibles qui se trouvent dans le lot. Le terme « fichiers impactés » désigne tous les fichiers chiffrés, effacés ou exfiltrés par les cybercriminels.

Impact des opérations de chiffrement ciblant l'environnement de production d'un établissement de santé

Acteurs de la santé

16,8 M

de fichiers impactés à chaque opération de chiffrement menée par un groupe de ransomware.

8,4 M

d'enregistrements de données sensibles se trouvent dans ces fichiers impactés.

20 %

des données sensibles détenues par les établissements de santé sont impactées à chaque opération de chiffrement.

Dans les autres secteurs, les données sensibles sont en moyenne beaucoup moins impactées

13,7 M

de fichiers impactés à chaque opération de chiffrement menée par un groupe de ransomware

1,7 M

d'enregistrements de données sensibles impactés à chaque opération de chiffrement

6 %

des données sensibles détenues par l'organisation



La virtualisation, talon d'Achille de la santé ♦

Comme vous pouvez le constater, les ransomwares frappent très majoritairement dans les architectures virtualisées.

97 %

des données chiffrées, dans le secteur de la santé, l'ont été dans des environnements virtualisés

83 %

des données chiffrées, dans l'ensemble des autres secteurs, l'ont été dans des environnements virtualisés

Pourquoi une telle prépondérance du virtuel ?

1.

Les architectures virtualisées sont généralement moins bien protégées que les équipements traditionnels. Ces failles créent non seulement des angles morts, mais permettent également aux attaquants d'accéder aux données sans se faire repérer.

2.

Une fois que les cybercriminels ont accès au système de contrôle de l'hyperviseur, ils peuvent se déplacer rapidement partout dans l'environnement, au seul moyen des identifiants compromis.



DES SOMMES TRÈS VARIABLES

La rançon versée par les victimes est souvent moins élevée que le montant initialement exigé par les cybercriminels. Au cours de l'année passée, l'équipe Unit 42 de Palo Alto Networks a observé plusieurs tendances dans le paiement des rançons : ■

| | TOUS SECTEURS CONFONDUS | SANTÉ |
|---|-------------------------|------------|
| Somme médiane exigée | 800 000 \$ | 200 000 \$ |
| Rançon médiane versée | 275 000 \$ | 100 000 \$ |
| Somme médiane des cinq plus grosses rançons versées | 25 000 000 \$ | 297 000 \$ |

La restaurabilité des sauvegardes et l'exfiltration de données influent sur la décision des victimes.

[L'Université de Twente](https://databreaches.net/university-of-twente-maps-decision-making-process-for-ransomware-victims/#:~:text=for%20the%20best-,article,-)¹ a étudié les facteurs incitant les victimes à payer une rançon et, dans une étude séparée, les paramètres déterminant le montant de la somme versée. Les résultats parlent d'eux-mêmes :

Les organisations dotées de sauvegardes récupérables sont



¹ <https://databreaches.net/university-of-twente-maps-decision-making-process-for-ransomware-victims/#:~:text=for%20the%20best-,article,->



En revanche, les victimes dont les données ont été exfiltrées sont plus enclines à céder aux exigences des cybercriminels (avec des rançons beaucoup plus élevées).

40 %

ont payé la rançon à la suite d'une exfiltration de données

25 %

ont payé la rançon sans exfiltration de données

5,5x

La somme des rançons versées est 5,5 fois plus élevée lorsque les cybercriminels ont exfiltré des données (au lieu de seulement les chiffrer).

Saturation du stockage : le danger dont personne ne se méfie !

Un malheur n'arrive jamais seul. Peu d'organisations savent que les attaques par ransomware peuvent générer un déluge de données.

Lorsqu'un ransomware chiffre ou modifie 16,8 millions de fichiers d'un établissement de santé, cela signifie qu'il crée dans l'environnement de la victime 16,8 millions de « nouveaux » fichiers (13,7 millions dans les autres secteurs). ♦

Ces fichiers sont ensuite sauvegardés dans l'espace de stockage, où ils prennent une place phénoménale.

16,8 M

de fichiers de santé impactés

16,8 M

de nouveaux fichiers

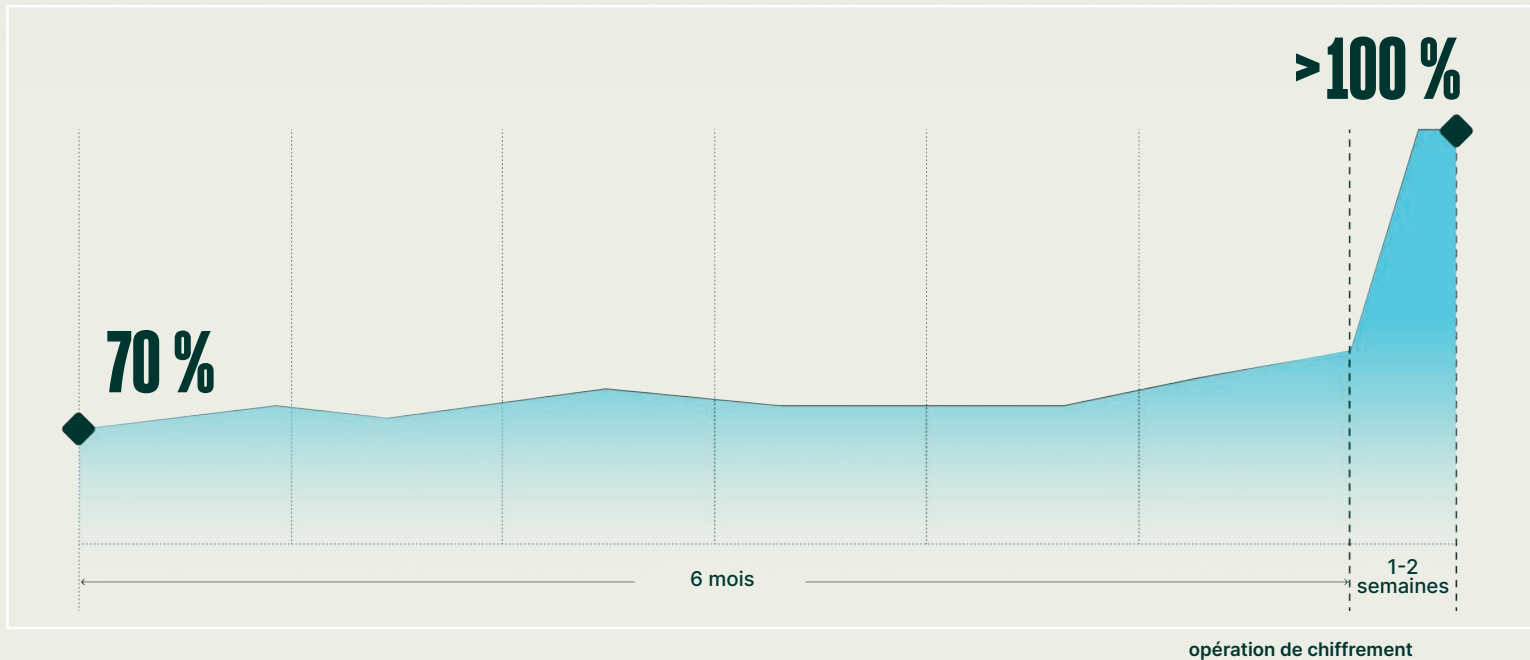
13,7 M

de fichiers impactés en moyenne

13,7 M

de nouveaux fichiers

Si l'espace de stockage de la victime était déjà plein à 70 % avant l'attaque, alors ces nouvelles données peuvent saturer ses capacités de restauration en une ou deux semaines. ♦



Comme si cela ne suffisait pas, les victimes doivent elles-mêmes créer de nouvelles données dans le cadre de la réponse à incident : images forensiques pour les analyses, copies immuables pour les procédures judiciaires, etc. Dans la plupart des cas, les workflows de réponse/de reprise après sinistre requièrent également la duplication des données. Bref, les capacités de stockage sont rapidement saturées.

Selon l'équipe Ransomware Response de Rubrik, qui compte à son actif plus de 200 opérations de restauration sur le terrain, les victimes ont deux options :

1. Augmenter rapidement leur capacité de stockage, ce qui implique une pression supplémentaire sur les budgets et les équipes.
2. Dégrader intentionnellement leurs capacités de restauration pour ralentir la prolifération des données, au risque de freiner la reprise de l'activité.



42 DÉCÈS AUX ÉTATS-UNIS IMPUTABLES AUX RANSOMWARES

Les attaques par ransomware n'impactent pas uniquement les données. Elles peuvent aussi avoir des conséquences désastreuses et parfois dramatiques, en particulier dans le secteur de la santé où la disponibilité de ces données est littéralement une question de vie ou de mort. ■

La School of Public Health de l'université du Minnesota Twin Cities a mesuré les conséquences bien réelles des ransomwares sur les établissements de santé et les soins aux patients entre 2016 et 2021¹.



20 %

Les capacités de soin aux patients ont diminué de 20 % dans la semaine qui a suivi une attaque. ■

Ces attaques représentent une véritable menace pour les données, les organisations et la confidentialité. Mais dans certains cas, elles peuvent aussi mettre des vies en danger.

1 sur 4

Seuls 5 % des hôpitaux américains ont été directement touchés par un ransomware pendant toute la durée de l'étude. Cela peut paraître peu, mais il faut également compter les hôpitaux voisins (20 % supplémentaires) qui ont dû accepter en urgence les patients transférés depuis les établissements paralysés.

0,5 à 1 %

Un seul ransomware a fait perdre en moyenne de 0,5 % à 1 % de leur chiffre d'affaires aux hôpitaux concernés.

2 À 3 semaines

C'est la durée nécessaire à un établissement de santé pour revenir à la normale après une attaque par ransomware.

42 À 67 décès

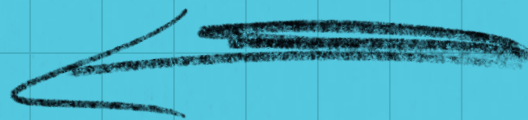
Les répercussions des attaques par ransomware ont directement causé la mort de 42 à 67 patients aux États-Unis².

¹ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

² <https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/>



Restaurer **ET RÉCUPÉRER**



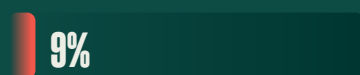
La réponse initiale est terminée. Le ransomware a été neutralisé.
 Votre organisation retrouve un semblant de normalité.
 Mais l'onde de choc continue de se faire ressentir.

IL Y A DU BON ET DU MOINS BON



Les cyberattaques *impactent* aux niveaux collectif et individuel

Selon le rapport Aon, chaque incident cyber majeur entraîne une baisse de : •



de la valeur actionnariale.

Les organisations signalent également des répercussions au niveau organisationnel : ▲



Remaniement de l'équipe de direction



Mauvaise presse et érosion de l'image de marque



Perte de chiffre d'affaires



Perte de clients

Mais les dégâts sont aussi émotionnels : 96 % des responsables IT et sécurité font état d'une dégradation de leur état psychique et émotionnel directement imputable à la cyberattaque qu'ils ont subie : ▲



Hausse de l'anxiété au travail



Perte de confiance envers leurs collègues et leur équipe



Préoccupations pour la sécurité de leur emploi



Insomnies ou troubles du sommeil



Les dirigeants doutent de la capacité de leur organisation à *se relever de la prochaine* attaque.

60 %

des responsables IT et sécurité sont très, voire extrêmement préoccupés par leur capacité à poursuivre leurs activités pendant une cyberattaque. ▲

28 %

des organisations estiment que leur Comex ou leur CA a peu ou pas confiance en la capacité des équipes à restaurer les données et applications critiques après une cyberattaque. ▲

LES PROBLÈMES CAUSÉS PAR LES CYBERATTAQUES SONT POURTANT PRÉVISIBLES

Voici les problèmes qui se produisent le plus souvent lors d'une cyberattaque et les changements auxquels les organisations doivent se préparer une fois la tempête passée :

Le plus grand obstacle auquel les organisations se sont heurtées au cours d'une attaque : ▲

19 %

Problèmes liés aux environnements hybrides

18 %

Manque de coordination des équipes

18 %

Solutions de sauvegarde et de restauration inefficaces

17 %

Manque d'implication de la part des dirigeants

16 %

Problèmes de visibilité

Les changements les plus courants au sortir de la crise : ▲

24 %

Renforcement de la surveillance par les dirigeants

20 %

Remplacement des technologies de cybersécurité

19 %

Refonte des stratégies et procédures de cybersécurité

19 %

Responsabilisation accrue

18 %

Moral en berne chez les équipes IT et de sécurité



Les cyberattaques peuvent aussi avoir des effets positifs.

Les organisations qui tirent les leçons de ces épreuves peuvent sortir renforcées de la crise.

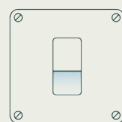
Selon les observations d'Aon, les organisations qui ont su rebondir après une cyberattaque ont enregistré une hausse de **18 % de leur valeur actionnariale** par rapport à leurs concurrents. •

Après une cyberattaque, les organisations interrogées ont : ▲



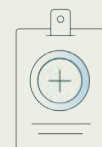
55 %

investi dans de nouvelles technologies ou de nouveaux services



42 %

changé de fournisseurs ou de partenaires




37 %

augmenté leurs effectifs

Le risque zéro n'existe pas. En revanche, vous disposez de nombreux leviers pour réduire votre surface de risque.



Se préparer à la
PROCHAINE OFFENSIVE



Cette histoire n'a pas de
« happy ending »...

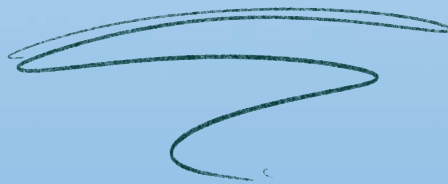


... tout simplement
parce qu'elle
n'a pas de fin.



VOUS AVEZ SURVÉCU À LA TEMPÊTE, MAIS IL Y EN AURA D'AUTRES.

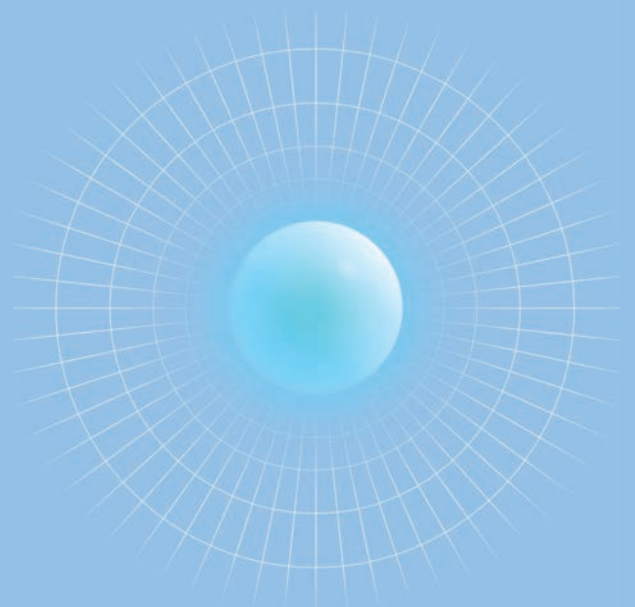
La prochaine sera peut-être même plus redoutable encore, avec de nouveaux risques qui vous prendront peut-être par surprise.



Certains facteurs de risque resteront malheureusement toujours entre les mains de vos adversaires. Chercher à maîtriser ces paramètres reviendrait à vouloir contrôler le temps qu'il fait.

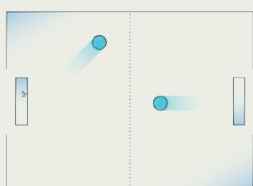
Mais si vous ne pouvez pas influencer sur les aléas que la vie vous réserve, vous pouvez en revanche choisir comment vous y préparer.

Voyons ensemble comment sortir d'une crise par le haut pour mieux affronter la prochaine. Ces recommandations sont le fruit d'une étude approfondie des cyberattaques, de leur impact sur la data et des répercussions attendues.

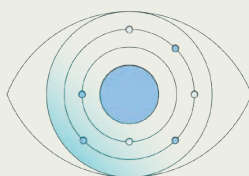


COMMENT RÉDUIRE EFFICACEMENT LE RISQUE DATA ?

Actionnez ces leviers pour réduire le risque sur vos données :



Préparez-vous à affronter vos adversaires sur tous les terrains de l'hybride. Ces architectures ont la cote auprès des organisations, mais les attaquants en connaissent déjà toutes leurs failles.

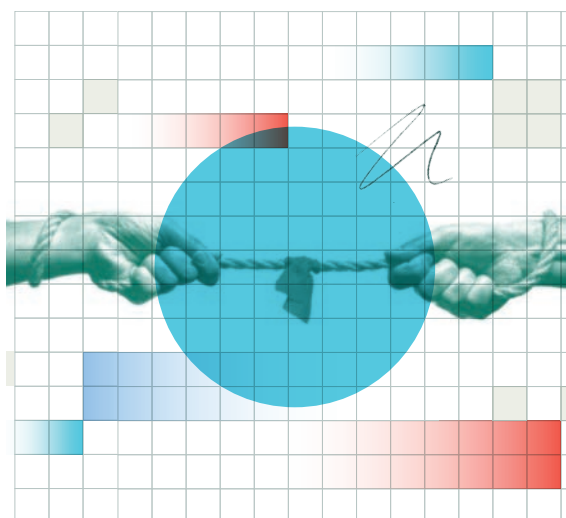


Améliorez *la visibilité sur vos données* :

- Couvrez tous les aspects des environnements hybrides.
- Localisez vos données sensibles et identifiez les réglementations qui s'appliquent à chacune d'entre elles.
- Préparez-vous à rendre davantage de comptes aux dirigeants. Vous devrez leur montrer que vos investissements produisent les résultats escomptés.



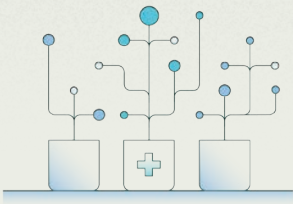
Soyez proactifs : communiquez toutes les mesures post-cyberattaque engagées à vos dirigeants.



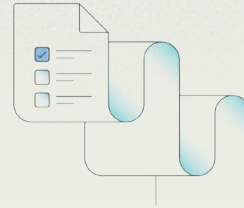
Préparez la reprise de vos activités mais soyez vigilants : *vos adversaires ne vous laisseront pas faire.*

Nos recommandations :

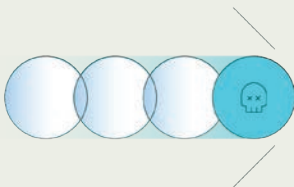
- Assurez-vous que les sauvegardes sont 100 % immuables et disponibles en cas de crise.
- Automatisez au maximum le processus de restauration.
- Testez les stratégies de restauration dans les environnements hybrides.
- Utilisez les services et les technologies de sécurité existants pour contrôler l'immuabilité et l'intégration des technologies de sauvegarde.



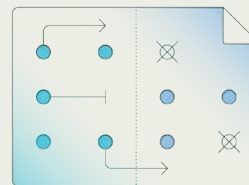
Anticipez la prolifération de vos données (en particulier de vos données sensibles) pour mieux enrayer la spirale. Priorisez la protection de vos données critiques.



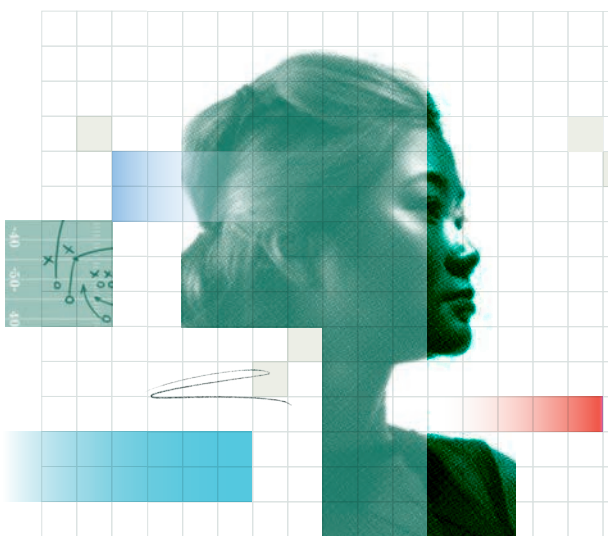
Attendez-vous à devoir répondre aux questions des autorités en pleine tourmente, alors même que votre environnement sera paralysé par des attaquants qui menaceront de divulguer vos données.



Soyez prêt à prendre des décisions difficiles dans le sillage d'une cyberattaque : investissement dans de nouvelles technologies, renforcement des équipes, remplacement des fournisseurs et partenaires, etc. Capitalisez sur ces périodes de changement pour créer un maximum d'impact.



Communiquez régulièrement vos plans et vos objectifs à l'échelle de l'organisation pour remotiver les troupes et réinstaurer un climat de confiance au sein des équipes.



Fédérez toutes vos forces vives avant, pendant et après une cyberattaque.

Nos recommandations :

- Créez des playbooks transverses à toutes les fonctions et menez des exercices de simulation.
- Désignez les équipes dotées de pouvoirs décisionnaires pour différents scénarios.
- Déterminez les meilleurs canaux de transmission de l'information au risk owner désigné.
- Assurez-vous que toutes les équipes ont accès aux mêmes données pour accélérer la prise de décisions et éviter les dissonances.



UNE AUTRE PERSPECTIVE

Comme nous l'avons déjà souligné, le Rubrik Zero Labs aborde toujours le risque dans une démarche data. Pour élargir notre perspective, nous avons choisi de consacrer une page de notre rapport aux recommandations de résilience extraites du Rapport de défense numérique 2023 de Microsoft¹. L'angle d'analyse y est totalement différent du nôtre, ce qui vous donne deux fois plus de perspective pour réduire efficacement le risque.

99 %

Selon Microsoft, la seule application de ces principes d'hygiène cyber protégera vos données contre 99 % des attaques.●

Ses principales recommandations : ●

- Activer l'authentification multifacteur (MFA)
- Appliquer les principes du Zero Trust, en particulier pour les assets protégeant les données et fonctions critiques
- Utiliser des outils de détection étendue et anti-malware pour couvrir les principaux aspects de vos environnements hybrides
- Appliquer les correctifs pour les systèmes et applications clés dès leur publication
- Identifier et localiser les données critiques pour déployer les mesures de défense appropriées

Microsoft va même plus loin en proposant cinq mesures fondamentales pour éradiquer la capacité de nuisance des ransomwares : ●

1

Moyens d'authentification sophistiqués avec identifiants résistant au phishing

2

Principe du moindre privilège appliqué à toute la stack technologique

3

Environnements protégés contre les menaces et les risques

4

Gestion de la posture de sécurité pour la conformité et l'intégrité des appareils, des services et des assets

5

Automatisation des sauvegardes dans le cloud et de la synchronisation des fichiers pour les données utilisateurs et métiers critiques



Au tout début de ce rapport, nous avons résumé notre objectif en une équation élémentaire : protéger X contre Y.

Mais dans le domaine du risque comme en mathématiques, rien n'est jamais aussi simple.

**L'ÉCOSYSTÈME
INFINIMENT COMPLEXE
QU'EST VOTRE SURFACE
DE DONNÉES**

**ENTRE EN
COLLISION
AVEC**

**UNE SURFACE DE
MENACES TOUT AUSSI
COMPLEXE ET EN
PERPÉTUELLE MUTATION.**

RISQUE

Sachant que l'équation du risque data compte des millions de variables, il est impossible d'en cerner les contours ou de l'éliminer complètement. Vous n'empêcherez pas la pluie de tomber. Mais en actionnant les bons leviers, en anticipant les issues prévisibles et en agissant de façon cadrée et méthodique, vous pourrez mettre votre organisation à l'abri de l'orage.

Vous avez maintenant toutes les clés pour réduire les risques et vous préparer aux prochaines menaces. À vous de jouer !

REMERCIEMENTS

Rubrik remercie chaleureusement toutes les équipes qui ont contribué à cette étude par leur expertise et leur travail acharné.

- Nos partenaires chez Microsoft et Aon, pour leurs conseils et leurs précieuses données.
- Les organisations qui ont mis à notre disposition leurs analyses et toute la documentation nécessaire pour faciliter la catégorisation de ces éclairages :
 - Proofpoint
 - Recorded Future (Allan Liska, aka « Ransomware Sommelier »)
 - Mandiant (Kirstie Failey, aka « Swiftie »)
 - Palo Alto Networks Unit 42 (Ingrid Parker)
- La School of Public Health de l'université du Minnesota Twin Cities (Hannah Neprash, Claire McGlave et Sayeh Nikpay) pour nous avoir confié leurs résultats et expliqué en détail leurs recherches, mais aussi pour leur collaboration avec le Rubrik Zero Labs en vue de coordonner leur étude et notre analyse du secteur.

Tous nos rapports Rubrik Zero Labs sont nés d'un vrai travail d'équipe. Wakefield Research nous a fourni une mine de données pour rendre cette étude aussi objective que possible. Shaped By a fait des miracles pour donner corps à ces données. Enfin, nous remercions les nombreux Rubrikains qui ont travaillé d'arrache-pied pour apporter du contexte et une orientation à cette étude, en particulier : Amanda O'Callaghan (aka « Danger »), Linda Nguyen (aka « Taskmaster »), Lynda Hall (aka « Go Niners »), Ben Long, Peter Chang (aka « I'm the Law »), Ajay Kumar Gaddam, Ryan Goss, Derek Morefield, Josh Burns, Gunakar Goswami, Prasath Mani, Ethan Hagan, Kevin Nguyen, Caleb Tolin (aka « Social King »), Kelly Cooper, Hannah Battillo, Sindhu Nagendra, Caitlin O'Malley (aka « Plz stop letting Steve talk to reporters ») et Fareed Fityan.

