

DER STAND DER DATENSICHERHEIT

DIE REISE ZUR

ABSICHERUNG



EINER UNGEWISSEN

ZUKUNFT



Rubrik Zero Labs

INHALT

- BRECHEN SIE AUF **04**
- ÜBER DIE DATEN **06**
- RISIKEN VERSTEHEN **08**
- AKTUELLE DATENLAGE **12**
- DATENPROGNOSEN **17**
- VERÄNDERUNGEN BEI SENSIBLEN DATEN **19**
- DATENSICHERHEITSBEWERTUNG **25**
- EMPFEHLUNGEN **30**
- ZUSAMMENFASSUNG **38**

Datenquellen

 **TELEMETRIEDATEN VON RUBRIK**

 **WAKEFIELD RESEARCH**



Dies ist eine Geschichte über Daten.

Darüber, wie viele Daten es derzeit gibt,
wie viele es geben wird
und wie sich diese Mengen auf unsere
Fähigkeit auswirken werden,
unsere Daten zu schützen.

Es ist außerdem eine Geschichte über

Optimismus.



Darüber, wie er uns schadet
und wie er uns helfen kann,
in einer ungewissen Zukunft
den Kurs zu halten.

ÜBER DIE DATEN

ORIENTIERUNG AUF DER LANDKARTE

Rubrik Zero Labs hat sich das Ziel gesetzt, herstellerunabhängige Erkenntnisse zur Reduzierung von Datensicherheitsrisiken zu liefern. Zu diesem Zweck haben wir Erkenntnisse aus zwei unabhängigen Quellen einbezogen.

Telemetriedaten von Rubrik[®]

Wir haben Telemetriedaten von Rubrik genutzt, um so nah wie möglich an den Gegebenheiten der IT-Infrastruktur eines typischen Unternehmens und an den Bedrohungen zu bleiben, denen es ausgesetzt ist. Dieser Ansatz hat uns auch dabei geholfen, aus Datensätzen verwertbare Zukunftsmodelle zu erstellen. Im Sinne der Transparenz erfahren Sie hier noch, woraus sich dieser Datensatz zusammensetzt und welchen Einfluss er auf unsere Perspektive hat. Die Telemetriedaten von Rubrik umfassen:

5000+

Kunden

22

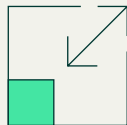
Branchen

35+ EB GESICHERT,

mit 24+ Milliarden sensiblen Datensätzen

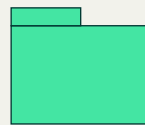


67 Länder in 3 Regionen



Gesamtvolumen
der gesicherten Daten:

35+ Exabyte an logischem Speicher
817 Backend-Petabyte (BEPB)
an physischem Speicher



24+ Milliarden sensible
Datensätze



Die Daten decken
den Zeitraum von Januar
2022 bis Juli 2023 ab

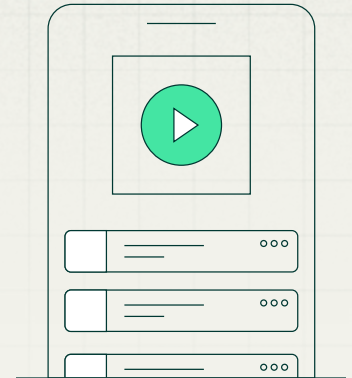
An alle Nerds:

Wenn sie das Wort „Daten“ hören, denken die meisten Menschen an logischen Speicher, auch „Frontend-Speicher“ genannt. Diejenigen von uns, die in der Branche arbeiten, legen den Fokus auf den Backend-Speicher.

Rubrik wendet eine Reihe verschiedener Techniken auf die Gesamtheit der Daten eines Unternehmens an – einschließlich Deduplizierung und Komprimierung –, um die Menge an Frontend-Daten im Backend-Speicher zu reduzieren. Während dieser Reise werden wir Backend-Storage verwenden.

Verschaffen Sie sich ein Gefühl für die Größenordnung: Wie viele Daten sind 35 EB?

Was wäre eine Reise ohne eine geniale Playlist? Ein typischer Song in hoher Tonqualität hat etwa 4,8 MB. Unsere Playlist #2023DataJourneyJamz mit 35 EB kann in diesem Fall 7,3 Billionen Songs mit einer Dauer von 48 Millionen Jahren enthalten¹²³. Und dabei müsste sich kein einziger Song wiederholen.



Wakefield Research ^{WR}

Perspektiven von mehr als 1600 IT- und Sicherheitsverantwortlichen auf der ganzen Welt

10

Länder

49%

CIOs oder CISOs

Wir haben bei Wakefield Research eine Umfrage in Auftrag gegeben, um unsere Rubrik-Telemetriedaten zu ergänzen und einen umfassenderen Blick auf die Datensicherheitslandschaft zu liefern. Wir haben uns auch bewusst dafür entschieden, IT- und Sicherheitsverantwortliche einzubeziehen, um den Unterschied zwischen der Sichtweise der Unternehmensführung und dem zu untersuchen, was wir vor Ort erleben.

1600+

IT- und Sicherheitsverantwortliche

49%

CIOs und CISOs

16%

VPs

38%

leitende Direktoren oder Vorstandsmitglieder



Drei Regionen

(Vereinigte Staaten, EMEA und APAC)



10 Länder

(Vereinigte Staaten, Vereinigtes Königreich, Frankreich, Deutschland, Italien, Niederlande, Japan, Australien, Singapur,



Indien)

Die Untersuchung deckt den Zeitraum vom

1 <https://math.ucr.edu/home/baez/timeline.html#:~:text=50%20million%20years%20ago%20D%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>

RISIKEN VERSTEHEN

SCHNELLE ENTSCHEIDUNGEN IM TREIBSAND

Bevor wir uns auf die Datenreise begeben, hier ein paar Infos dazu, wie wir Entscheidungen treffen. Ein paar Tipps vom Profi, wenn man so will, für die Entscheidungen, die Sie in Zukunft treffen werden.



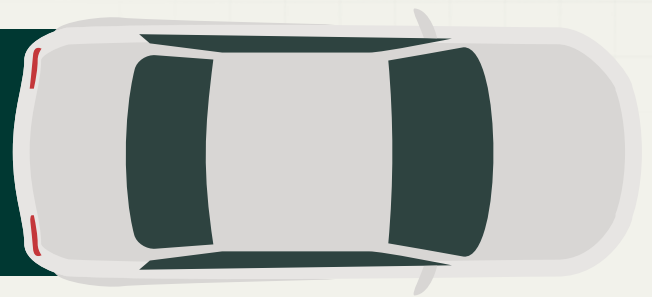
Wir Menschen sind von Natur aus optimistisch.

Das müssen wir auch sein. Wenn wir wirklich die gesamte Not in der Welt bewältigen müssten, würden viele von uns morgens gar nicht mehr aufstehen. Wir brauchen Optimismus, um zu überleben.

Aber genau dieser Optimismus kann uns auch den Blick auf wichtige Tatsachen verstellen.

Irgendwo in unserem Unterbewusstsein wissen wir jedes Mal, wenn wir in ein Auto steigen, dass wir ein Risiko eingehen. Tatsächlich gehen Versicherungsunternehmen davon aus, dass der Durchschnitts-Autofahrer hin und wieder an einem Unfall beteiligt sein wird, nämlich ...

einmal alle 18 Jahre.



Trotzdem gehen die meisten von uns davon aus, dass uns das nicht passieren wird.

Wir schreiben Nachrichten, wählen Telefonnummern, unterhalten uns, lesen, tragen Lippenstift auf ... alles, während wir Auto fahren.

Wir wissen, dass etwas Schlimmes passieren könnte. Aber wir rechnen damit, dass es uns heute nicht passiert.

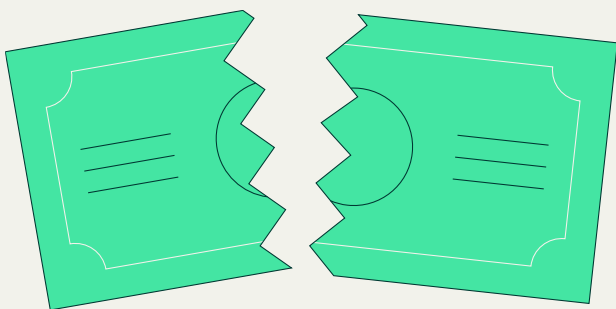
2007

Unser Optimismus betrifft auch die Art und Weise, wie wir Dinge in größeren Gruppen wahrnehmen. Im Jahr 2007 waren die Anzeichen einer bevorstehenden globalen Wirtschaftskrise schon erkennbar. Und manche erkannten sie auch.

Michael Burry, Gründer des Hedgefonds Scion Capital, beschreibt in einem Kommentar für die New York Times mit dem Titel „I Saw the Crisis Coming. Why Didn't the Fed?“ (Ich habe die Krise kommen sehen. Warum tat die Federal Reserve das nicht auch?), wie er die Warnzeichen für den Zusammenbruch des Immobilienmarktes ab dem Jahr 2003 mitverfolgt hat. ¹

Die meisten führenden Experten haben diese wichtigen Signale entweder nicht gesehen oder ignoriert.

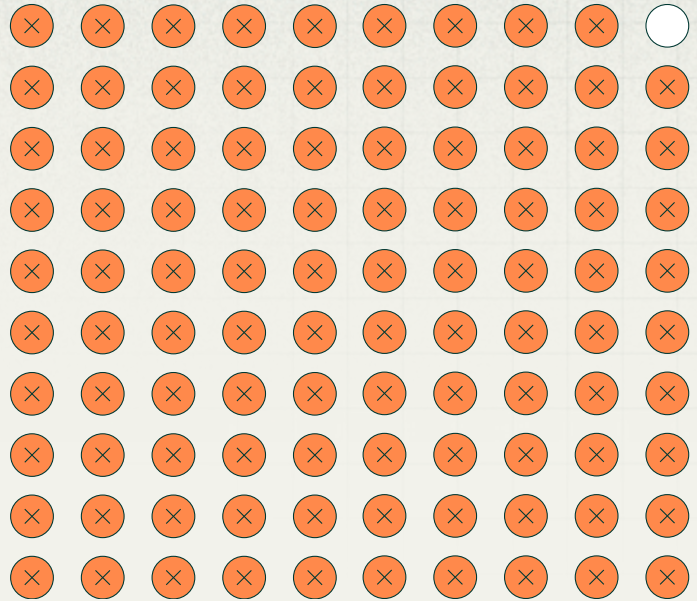
Ironischerweise gehen Unternehmen an das Thema Cyber-Sicherheit, das stark mit Angst, Unsicherheit und Zweifeln verknüpft ist, oft mit mehr Optimismus heran, als man meinen möchte.



99 %

Der Rubrik Zero Labs-Bericht von diesem Frühjahr² ergab, dass 99 Prozent der IT- und Sicherheitsverantwortlichen im Jahr 2022 über mindestens einen Angriff informiert wurden, wobei durchschnittlich 52 Vorfälle bearbeitet wurden. Dieselben Führungskräfte leiten Teams, haben oft nicht genügend Mitarbeiter und sind nicht hinreichend darauf vorbereitet, diese Angriffe zu bewältigen und Daten wiederherzustellen.

Unternehmen wissen, dass sie angegriffen werden könnten. Doch sie reden sich optimistisch ein: „aber nicht wir, nicht heute“.



Das Bauchgefühl



Jedes Mal, wenn wir in ein Auto steigen, eine Hypothek unterzeichnen oder eine der anderen 35.000 großen und kleinen Entscheidungen³ treffen, die wir schätzungsweise jeden Tag treffen, gehen wir ein kalkuliertes Risiko ein.

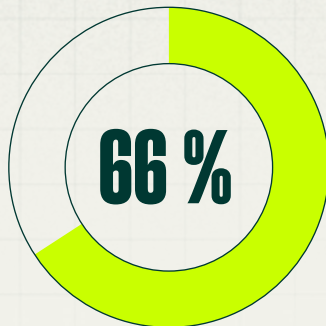
Wie die Forschung zeigt, geschieht diese Risikobewertung auf eine von zwei Arten: **intuitiv oder analytisch.**

Ökonomen und Psychologen debattieren über den Nutzen und die Genauigkeit jeder Art von Denken, aber im Allgemeinen eignet sich Intuition besonders für schnelle Entscheidungen mit geringem Aufwand⁴ und analytisches Denken hilft uns bei komplizierteren Entscheidungen⁵, allerdings langsamer und mit mehr Aufwand.

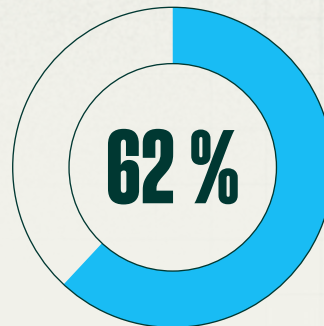
Beide Arten des Denkens sind fehleranfällig, aber das intuitive Denken gilt als weniger genau. Die Genauigkeit bei bestimmten Arten des intuitiven Denkens kann jedoch durch Erfahrung verbessert werden. Deshalb können geschulte Einsatzkräfte die Gefahr „spüren“, noch bevor sie eintritt.

Wir wissen bereits, dass Unternehmen in Bezug auf Cyber-Sicherheit optimistisch sind – zumindest was ihr eigenes Handeln angeht.

Wir wollen uns ein paar intuitive Einschätzungen anschauen:

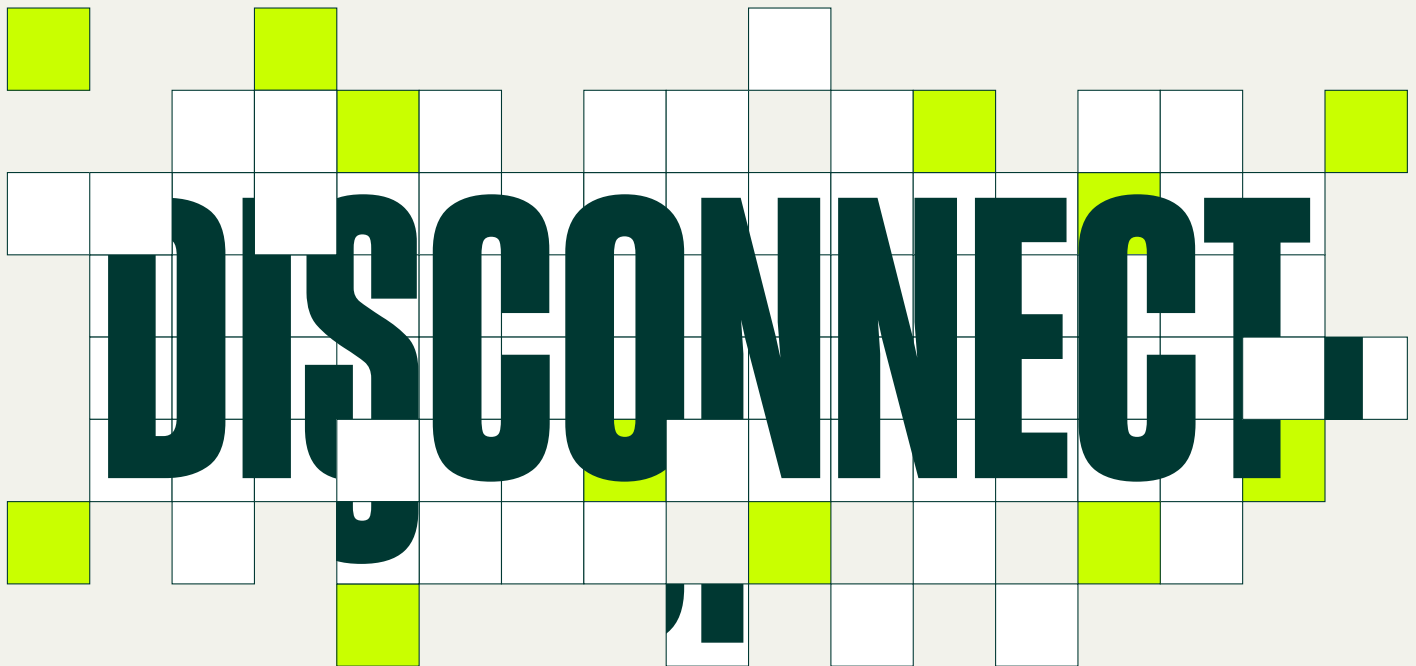


glauben, dass ihr Datenvolumen bereits über die Menge hinausgewachsen ist, die sie sichern und deren Risiko sie bewältigen können. ¹



der externen Organisationen glauben, dass Mitarbeiter unter Verletzung geltender Datenschutzrichtlinien auf Daten zugreifen. ²

Es besteht eindeutig eine Diskrepanz zwischen dem Verhalten von Unternehmen und dem, was ihre Experten von ihrem Datensicherheitskonzept halten.



Gibt es diese Diskrepanz auch im Hinblick auf die nackten Tatsachen? Sind diese Experten eine Art Frühwarnsystem oder handelt es sich um eine aus Intuition erwachsene Panik? *Wir wollen es herausfinden!*

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 CQjw2qKmbHcFARIsAFy8buJQvUD0qwkNaCjbZ1gPhagxEBoYo6z8q6Vxlf0_thil3lfcDPUDozcaAknUEALw_wcB

AKTUELLE DATENLAGE

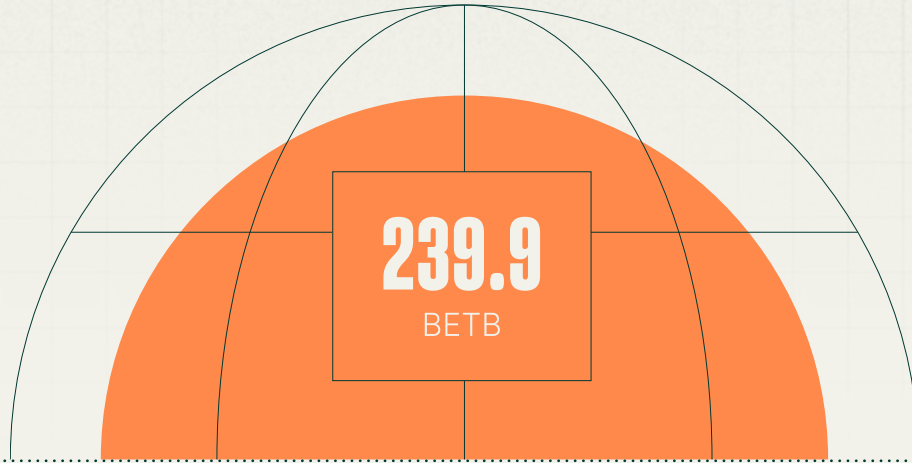
AKTUELLE WEGWEISER

Wechseln wir von der Intuition zur Analyse.
Knallharte Fakten und konkrete Ergebnisse.
Ohne Analysen wären wir nichts als Heiße-Luft-Verkäufer.

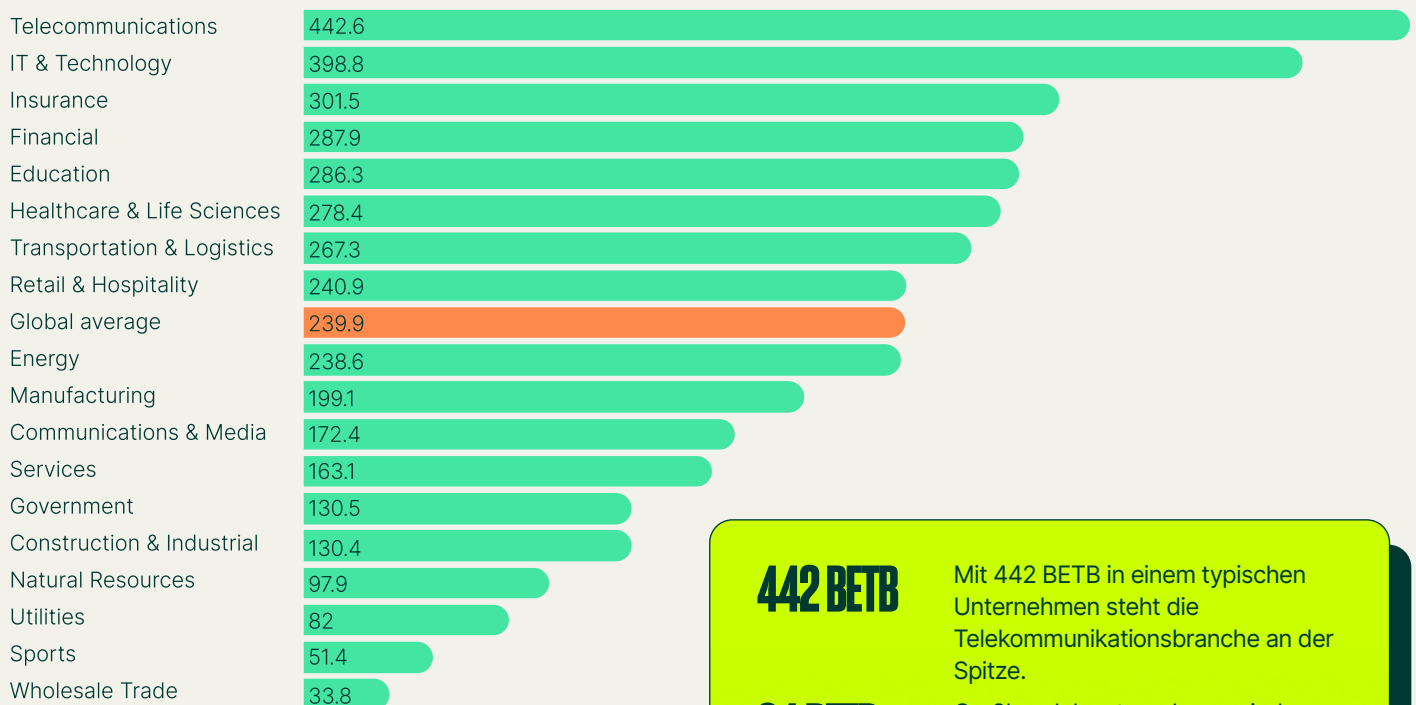
Heiße-Luft-Verkäufer: Substantiv.

Jemand, der alle Entscheidungen auf der Grundlage des eigenen Bauchgefühls oder der eigenen Wahrnehmung dessen trifft, was gerade beliebt/ trendy ist. Man könnte auch „Daten-Influencer“ sagen. Der Begriff ist auch auf alle anwendbar, die an der Gestaltung des Pontiac Aztek beteiligt waren. Beispielsatz: Der Pontiac Aztek wurde zu 100 % von Heiße-Luft-Verkäufern entwickelt.!

Gut, das wäre also geklärt. Beschäftigen wir uns jetzt mit der analytischen Herangehensweise.
Das typische Datenvolumen für ein globales Unternehmen sieht wie folgt aus:



Vergleichen wir jetzt einmal alle Branchen und Regionen miteinander: [®]



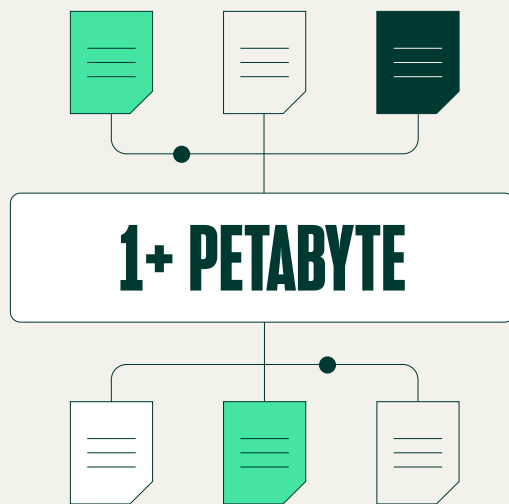
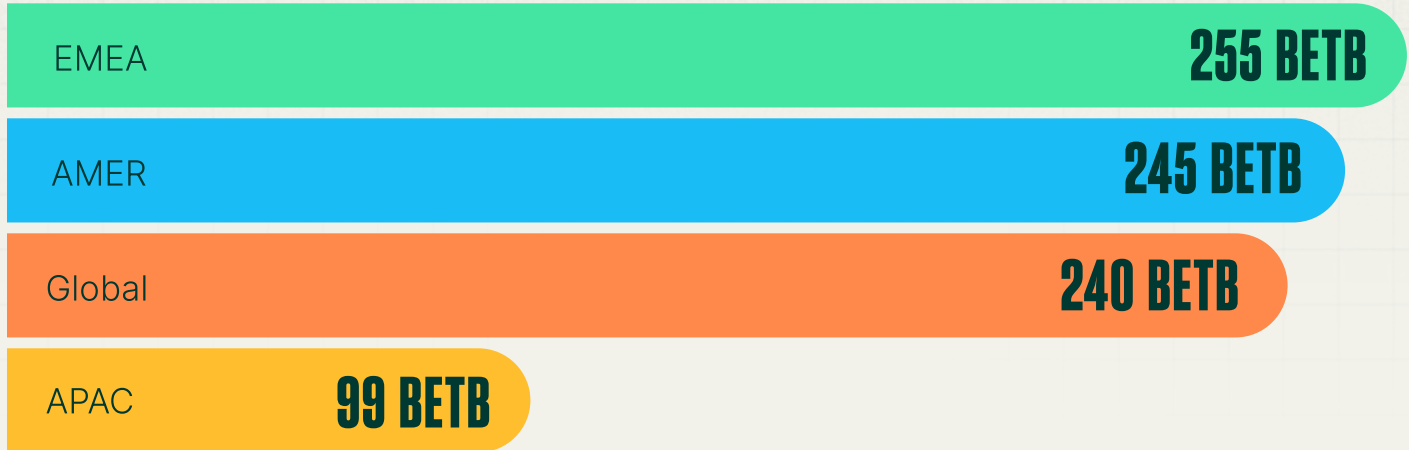
442 BETB

Mit 442 BETB in einem typischen Unternehmen steht die Telekommunikationsbranche an der Spitze.

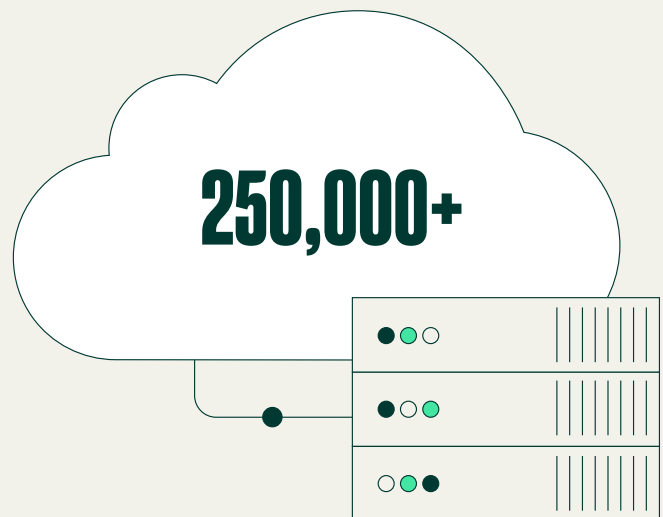
34 BETB

Großhandelsunternehmen sind dagegen mit durchschnittlich 34 BETB am kleinsten – etwa ein Dreizehntel der Größe eines typischen Telekommunikationsunternehmens.

Ein typisches APAC-Unternehmen hat etwa 60 % weniger Datenvolumen als ein vergleichbares Unternehmen in EMEA oder in NORD- oder SÜDAMERIKA:



Drei von Rubrik geschützte Organisationen verfügen über mehr als ein Petabyte an Backend-Datenspeicher.



Die höchste Anzahl von Rubrik-geschützten virtuellen Maschinen in einem einzelnen Unternehmen liegt aktuell bei über 250.000 VMs.

EXKURS!

IT- und Sicherheitsteams machen sich schon seit einiger Zeit Gedanken über die wachsende Datenflut.

2008

Die Zeitschrift „Wired“ ruft den Anfang des „**Petabyte-Zeitalters**“ aus.²

2010

Marissa Mayer, ehemals Vice President bei Google, stellt drei große Veränderungen bei Internetdaten fest: **Echtzeitdaten, eine noch nie dagewesene Verarbeitungsleistung und neue Arten von Daten**. Sie behauptet, dass allein die benutzergenerierten Daten um das 15-fache wachsen, also schneller, als es das Mooresche Gesetz

2011

Berichte aus der Branche zeigen, dass neue **CRM-Vorstöße mehr Daten** über Unternehmen generieren werden, dass eine wachsende Anzahl an „**Internet der Dinge**“-Geräten die **Datenmenge exponentiell ansteigen lassen wird** und dass anstehende Datenbankverbesserungen die Anwendungsmöglichkeiten von Daten erweitern werden.⁴

2013

Bei Diskussionen dreht sich alles um **einen „Daten-Kipppunkt“**, der sich aus dem Übergang von analogen zu digitalisierten Daten und der Zunahme von „Sensor“-Daten ergibt.⁵

2014

Analysten sind der Ansicht, dass Social Media, mobile Daten und Onlinewerbung eine „**Big Data Explosion**“ auslösen werden.⁶

2016

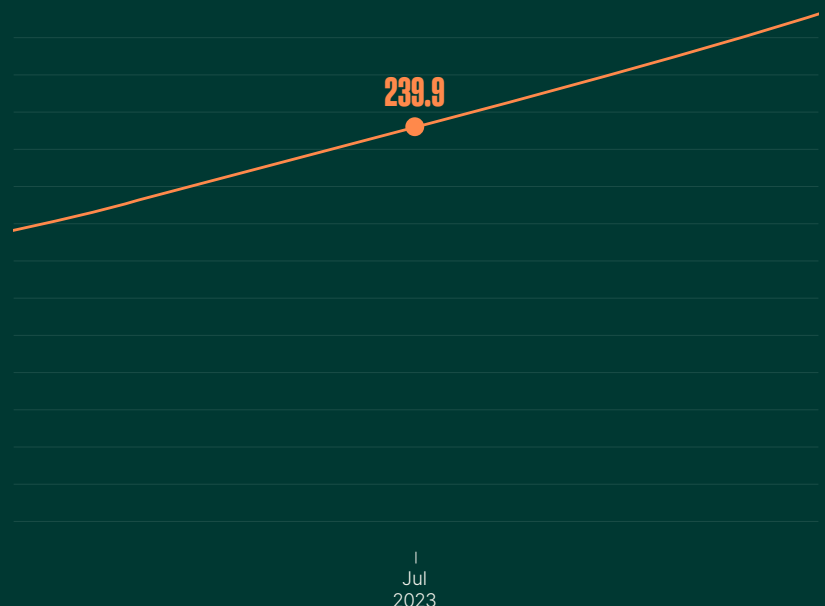
IBM schätzt, dass qualitativ minderwertige Daten US-Unternehmen 3,1 Billionen US-Dollar jährlich kosten.⁷

Wie wir an diesen Punkt gelangt sind

Seit es Daten gibt, machen wir uns Gedanken darüber. Aber wir stehen erst am Anfang. Sehen wir uns einmal an, wie wir an diesen Punkt gekommen sind.®

Durchschnitt
Gesamt-BETB

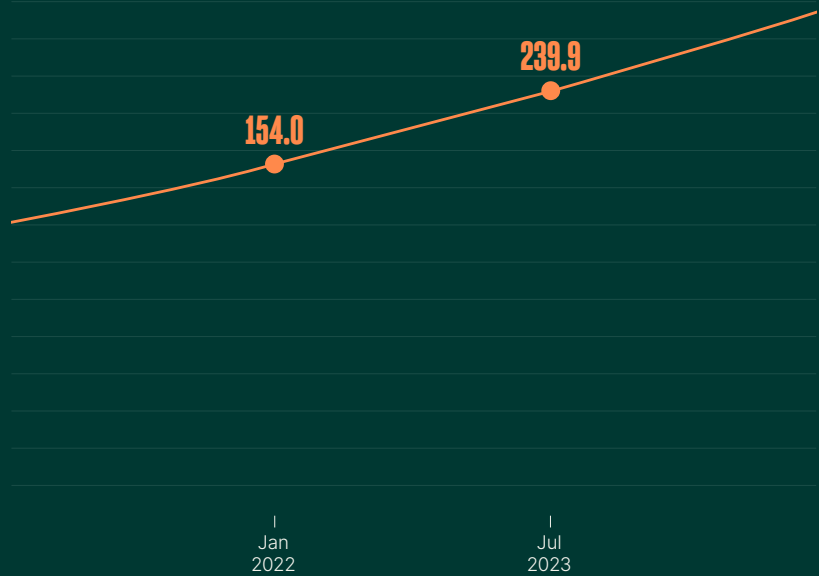
● Global average





Rubrik Zero Labs hat Wachstumsmuster von Januar 2022 bis Juli 2023 analysiert.®

Durchschnitt Gesamt-BETB



● Global average

Die Daten eines typischen globalen Unternehmens sind in den letzten 18 Monaten im folgenden Tempo gewachsen:

GESAMT: 42 %

LOKAL

20%

CLOUD

73%

SAAS

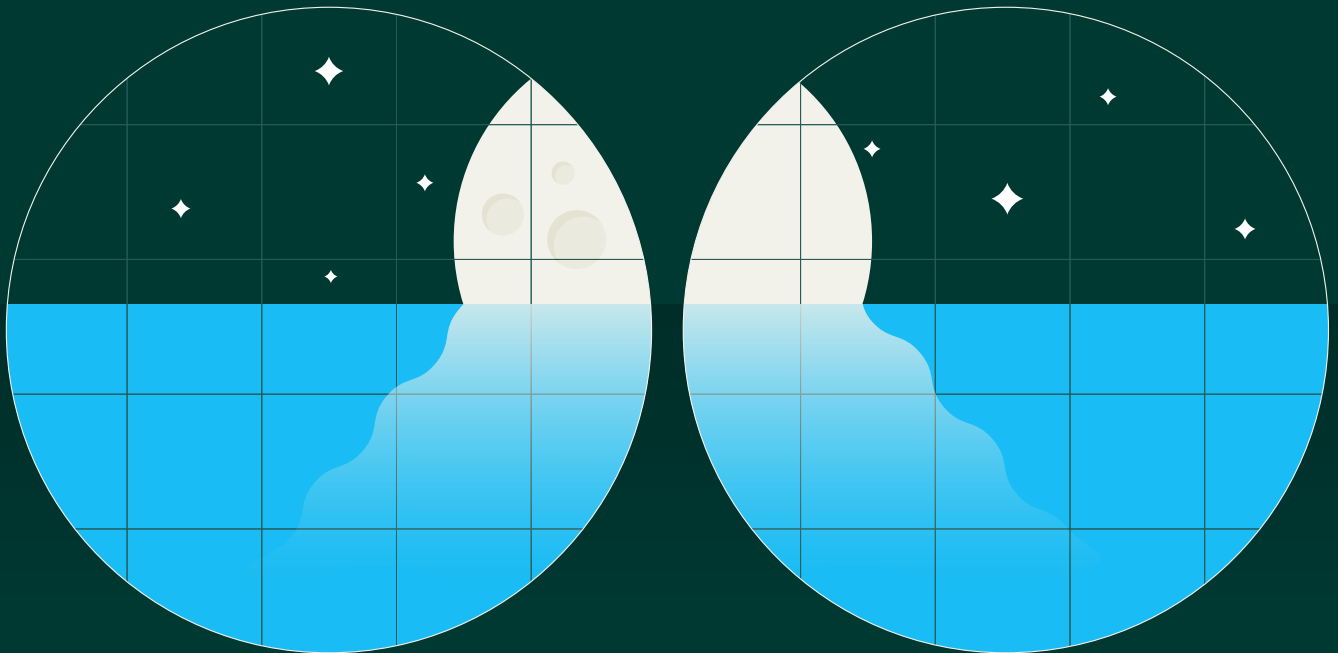
145%

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>

DATENPROGNOSEN

BLICK AUF DEN HORIZONT

Wir wollen nach vorne schauen statt zurück. Rubrik Zero Labs hat die Trends des Datenwachstums angewandt und extrapoliert, um herauszufinden, was wahrscheinlich in Zukunft auf Unternehmen zukommt.

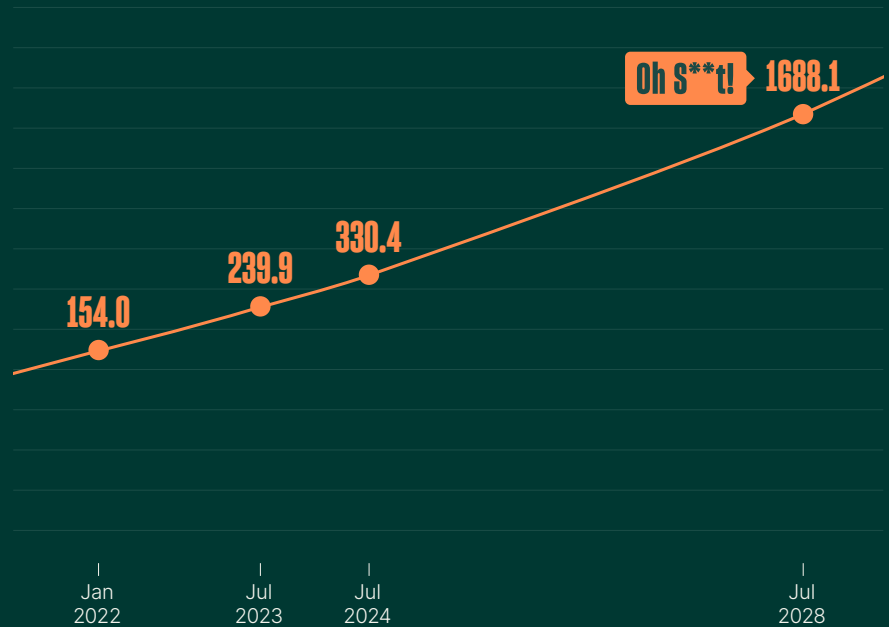




Das Gesamtvolumen der Daten, die ein typisches Unternehmen sichern muss, wird im nächsten Jahr um fast 100 BETB und in den nächsten fünf Jahren um das Siebenfache wachsen.[®]

Durchschnitt Gesamt-BETB

● Global average



UNGLAUBLICH, ODER? WIR KENNEN DAS GEFÜHL! GENAU DAS WAR AUCH UNSERE REAKTION!

Große Veränderungen geschehen selten über Nacht. Als die US-Banken und Hypothekenbanken Mitte 2007 zusammenzuberechnen begannen, war das erste hypothekarisch gesicherte Wertpapier bereits mehr als 35 Jahre alt und Hypotheken mit variablen Zinssätzen waren seit den 1980er Jahren immer beliebter geworden.^{1,2}



Niemand weiß wirklich, wie viele Daten wir in den nächsten fünf Jahren haben werden. Prognosen zum Datenwachstum wurden bisher regelmäßig übertroffen. Fairerweise müssen wir dazu sagen: Dasselbe trifft auch auf Rubrik Zero Labs zu. Unsere früheren Untersuchungen, die sich ausschließlich auf Daten aus dem Jahr 2022 stützten, ergaben eine Datenwachstumsrate von 25 %. Aber wenn wir auf Basis der heutigen Wachstumsrate andere Bereiche extrapolieren ... Wir kommen der Sache näher.

1 <https://www.investopedia.com/terms/m/mbs.asp>

2 <https://predatorylending.duke.edu/business-analysis/evolution-of-mortgage-lending/subprime-lending/>

VERÄNDERUNGEN BEI SENSIBLEN DATEN

PACKEN SIE NUR DAS WICHTIGSTE FÜR DIE REISE

Sie können absehen, wie viel Gepäck
Sie auf dieser Reise tragen werden,
aber muss es wirklich so viel wiegen?

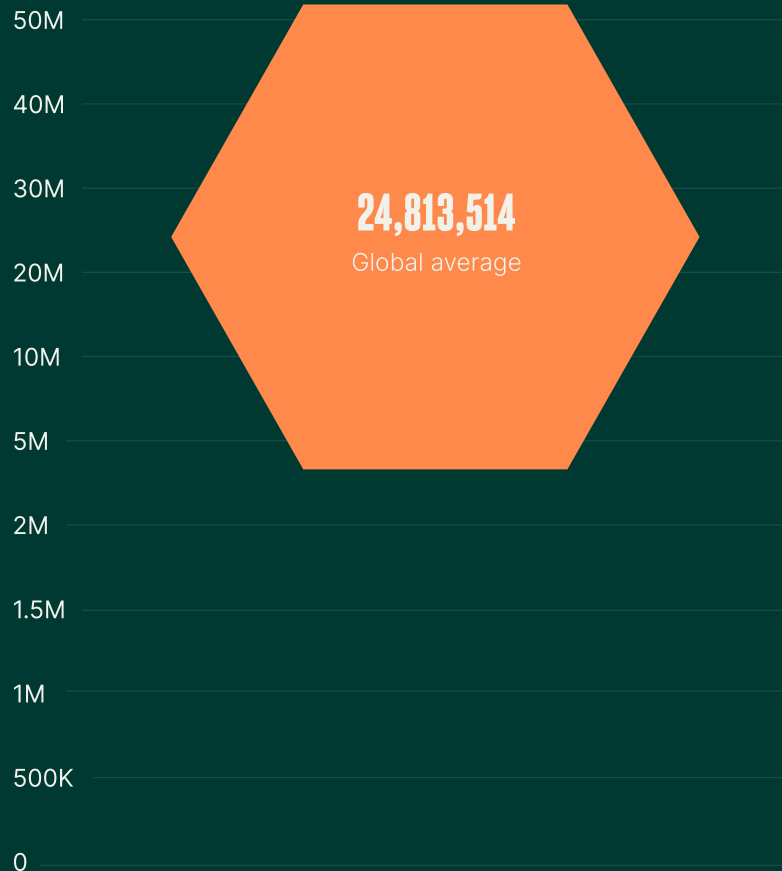


Uns liegt an fast allen unseren Daten etwas, aber manche sind wichtiger als andere. So kümmert es beispielsweise niemanden, wenn ein Desktop-Ordner voller alter Blogs gefährdet ist. Aber Informationen wie Ausweisnummern, Gesundheitsdaten und Geschäftspläne – die liegen uns schon etwas mehr am Herzen.

„Sensible Daten“ sind in diesem Bericht als Datenelemente definiert, die von Rubrik-Technologielösungen anhand von Parametern, die von verschiedenen Industriestandards oder Vorschriften abgeleitet wurden, als sensibel gekennzeichnet werden – beispielsweise PII, HIPAA, DSGVO und CPAA.¹²³⁴ Darüber hinaus kann eine Organisation Daten mithilfe von Rubrik-Technologie auf Basis eines beliebigen Faktors ihrer Wahl als sensibel kennzeichnen (Quellcode, rechtliche Sperrfrist usw.). Diese Daten sind ebenfalls in diesen Zahlen inbegriffen.

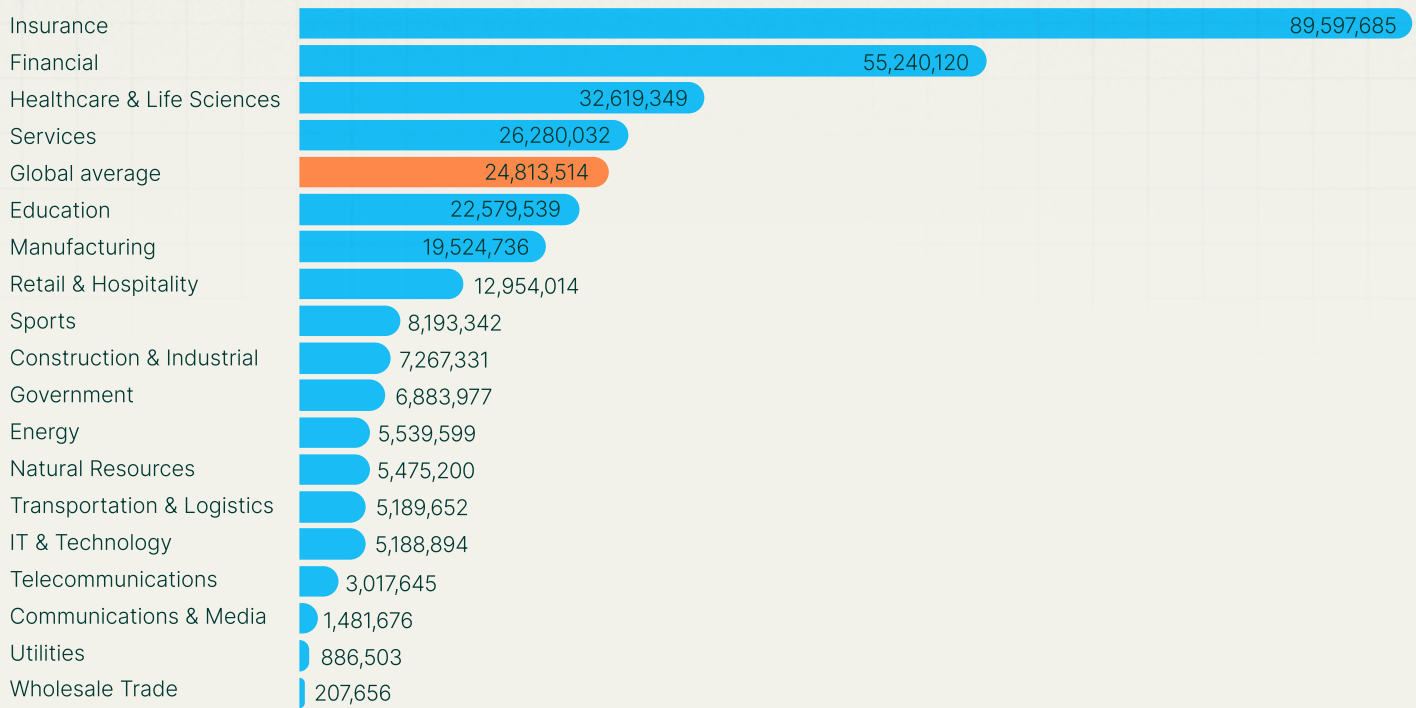
So sieht der globale Durchschnitt für eine typische Organisation aus:

Juli 2023, Dateien mit sensiblen Daten (durchschnittlich)

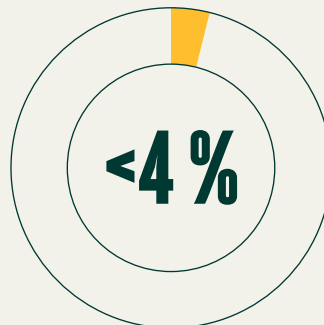


Aus der Ferne betrachtet, sehen wir erhebliche Unterschiede. So sieht es für alle Branchen aus.™

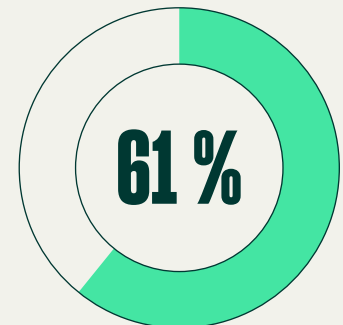
Juli 2023, Dateien mit sensiblen Daten (durchschnittlich)



Die größte Menge sensibler Daten in einem einzigen durch Rubrik gesicherten Unternehmen liegt bei über 1,3 Milliarden sensibler Datensätze.



Weniger als 4 % der externen Organisationen verfügen über einen gesonderten Speicherort für sensible Daten.™



61 % der externen Unternehmen speichern sensible Daten an mehreren Orten in der Cloud, lokal und in SaaS-Umgebungen.™

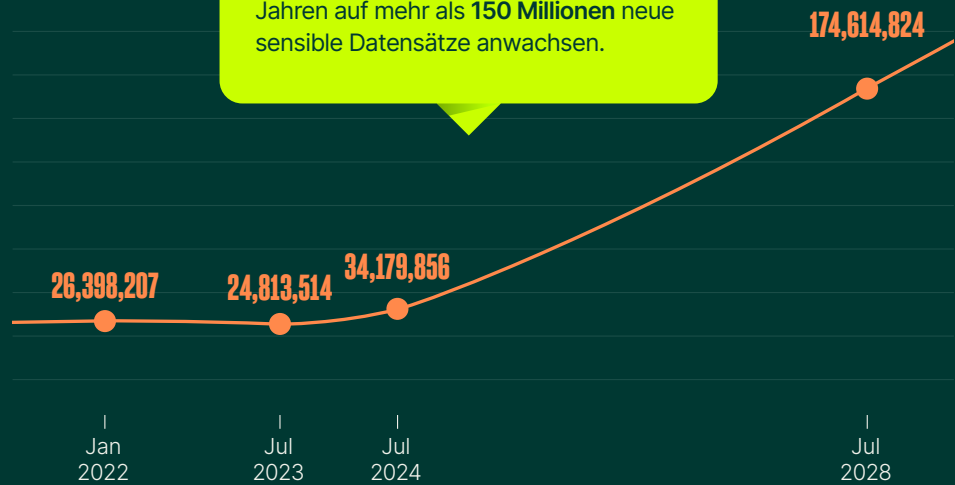


Nun wollen wir uns das prognostizierte Wachstum sensibler Daten ansehen, die Sie in Zukunft werden verwalten müssen:^(*)

Dateien mit sensiblen Daten (durchschnittlich)

Ein typisches Unternehmen wird in einem Jahr voraussichtlich netto **mehr als 10 Millionen** neue sensible Datensätze zu sichern haben. Diese Zahl wird in fünf Jahren auf mehr als **150 Millionen** neue sensible Datensätze anwachsen.

● Globaler Durchschnitt

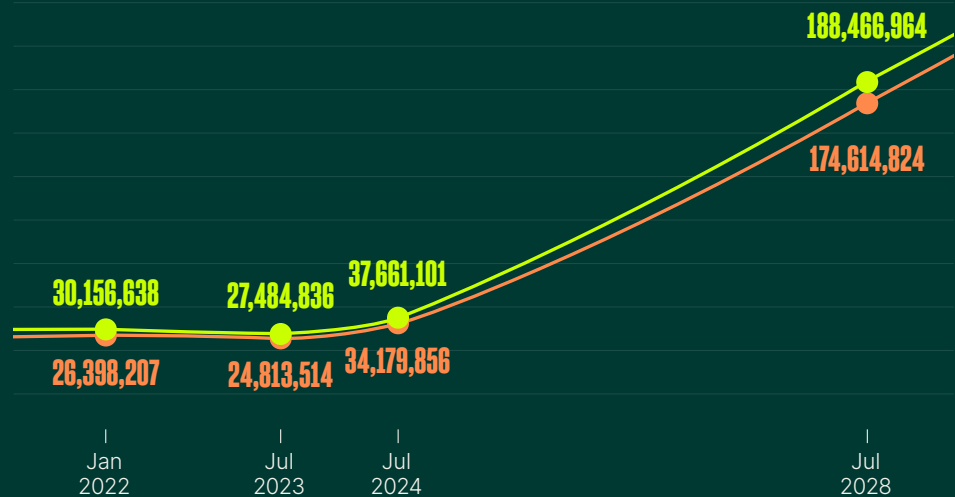


AUFSCHLÜSSELUNG NACH REGION

AMER

Dateien mit sensiblen Daten (durchschnittlich)

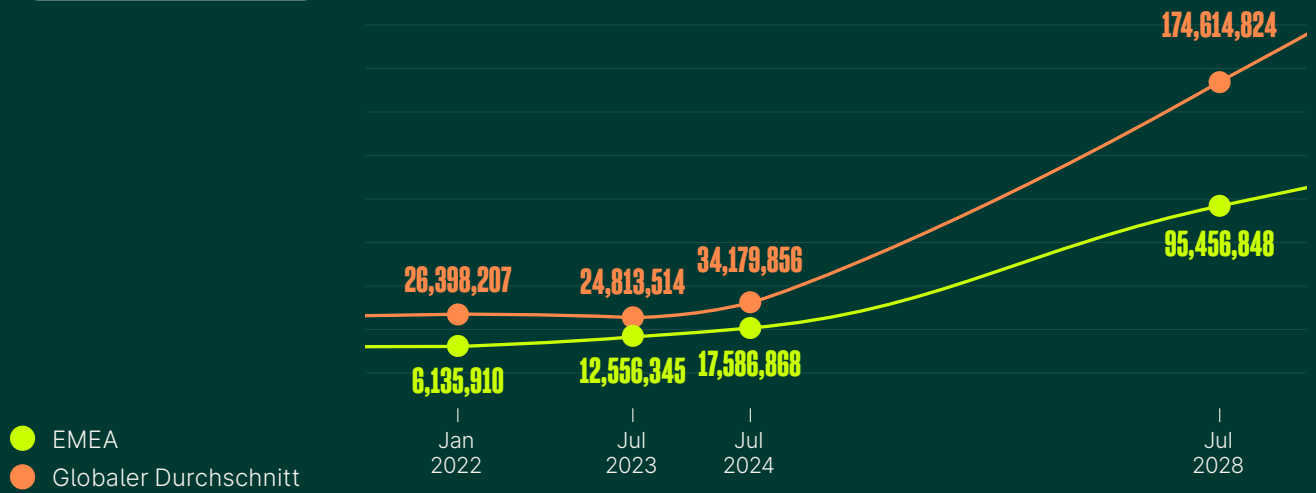
● AMER
● Globaler Durchschnitt



AUFSCHLÜSSELUNG NACH REGION

EMEA

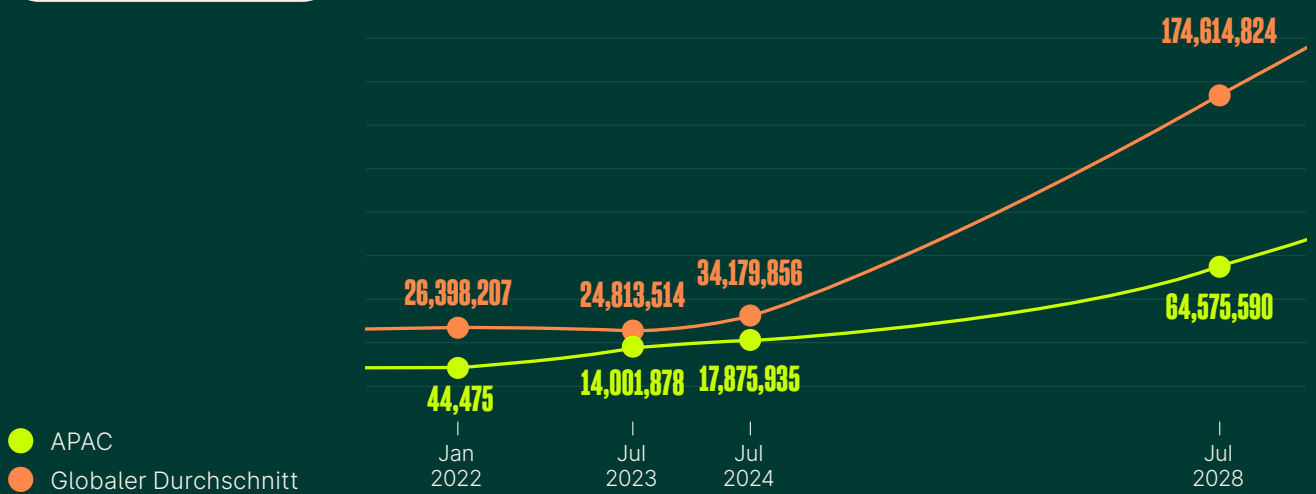
Dateien mit sensiblen Daten (durchschnittlich)



AUFSCHLÜSSELUNG NACH REGION

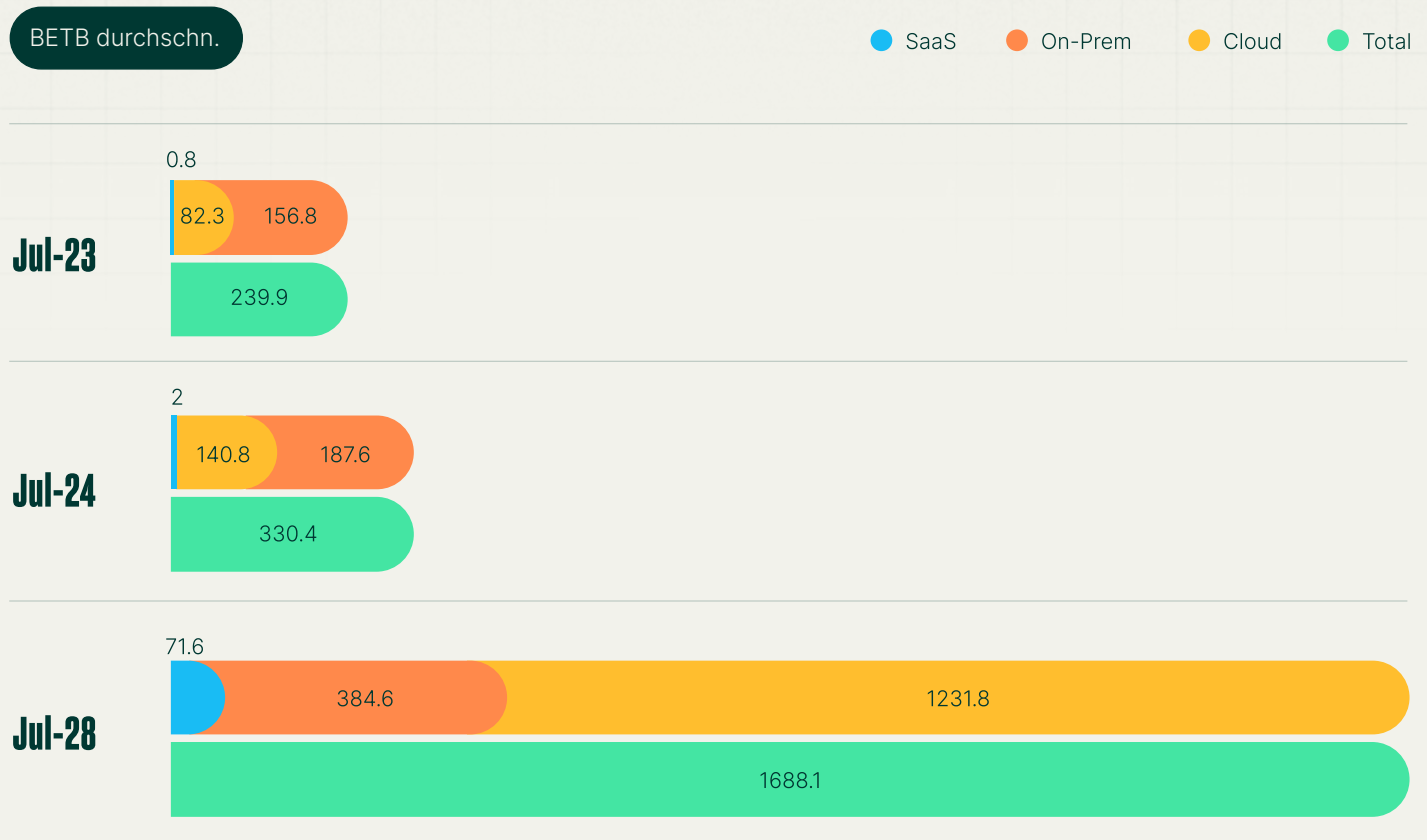
APAC

Dateien mit sensiblen Daten (durchschnittlich)



Veränderung in Hybridumgebungen

Es geht nicht nur darum, wie viele Daten Sie haben. Es geht auch darum, wo diese Daten gespeichert sind.¹⁾



Ein wichtiger Trend für die nächsten fünf Jahre ist die Dynamik hybrider Umgebungen (eine Mischung aus lokalen, Cloud- und SaaS-Anwendungen). Alles deutet darauf hin, dass „Hybrid“ der dominierende Umgebungstyp bleiben wird, aber die Verhältnisse werden sich dramatisch verschieben. Die Cloud wird lokalen Speicher als bevorzugtes Speichermedium weit hinter sich lassen. SaaS wird in den nächsten fünf Jahren die höchste Wachstumsrate aufweisen und für Unternehmen die Rolle der Cloud übernehmen.

1 <https://dsgvo-gesetz.de/art-4-dsgvo/>
 2 <https://www.cdc.gov/php/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.>

DATENSICHERHEITSBEWERTUNG

HIC SUNT DRACONES

Es sind also eine Menge Daten zu sichern, und sie werden zunehmend an anderen Orten gespeichert als bisher. Wie sieht es heute mit der Sicherheit unserer Daten aus? Nutzen wir mal Datensicherheitsbewertungen, um eine datengestützte Grundlage zu erhalten.



DER SATZ ‚HIC SUNT DRACONES‘ WAR FRÜHER AUF LANDKARTEN EIN HINWEIS AUF UNERFORSCHTE GEWÄSSER ODER MUTMASSLICH GEFÄHRLICHE GEGENDEN.

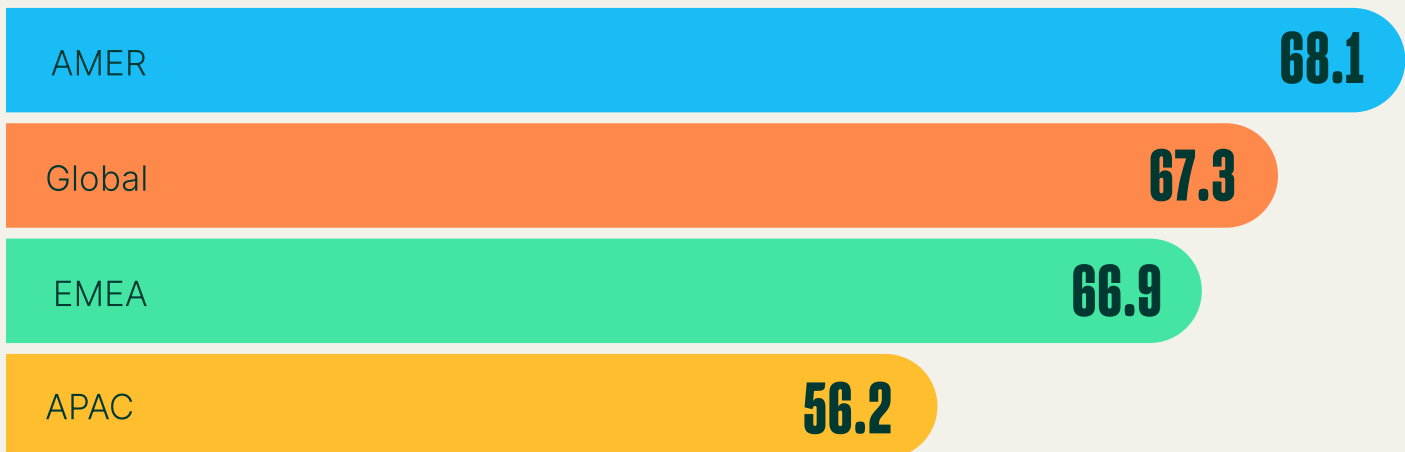


Infos zu Datensicherheitsbewertungen

Diese Bewertungen werden alle 24 Stunden basierend auf den folgenden Kategorien berechnet:

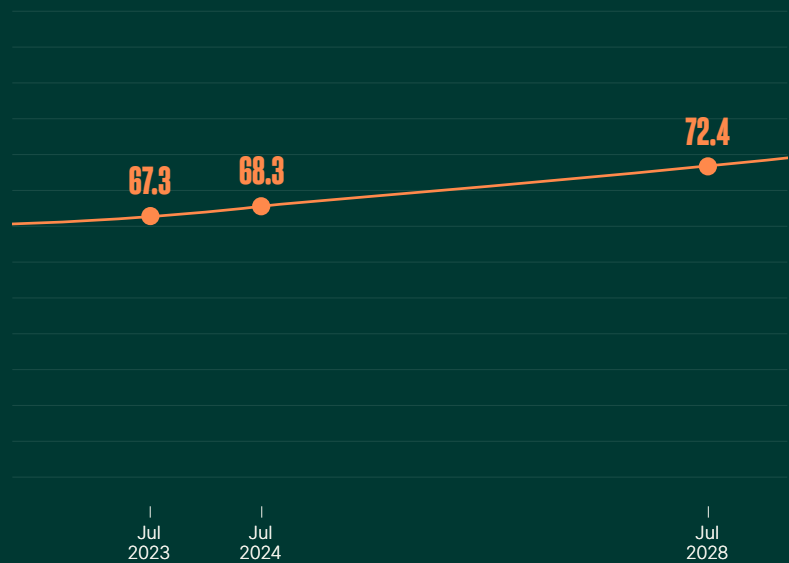
1. **Plattformsicherheit:** Misst die Wirksamkeit der Sicherheitsmaßnahmen für die Infrastruktur, in der Daten gespeichert sind, und umfasst Aspekte wie Benutzerkontrollen, Administrator-Authentifizierung und Prüfprotokolle.
2. **Datenschutz und Wiederherstellung:** Analysiert, wie gut die Backup-Daten gesichert sind, ob eine saubere Kopie des letzten Backups verfügbar ist, und andere damit zusammenhängende Faktoren.
3. **Ransomware-Untersuchung:** Bestimmt die Qualität und Häufigkeit der Überwachung auf Ransomware-Bedrohungen und auch, ob Daten nach einem Verschlüsselungsereignis wiederhergestellt werden können.
4. **Erkennung sensibler Daten:** Misst, wie gut sensible Daten geschützt werden, bewertet die Zugriffskontrollen für diese Daten und bestimmt, ob sensible Daten für die Wiederherstellung priorisiert werden.
5. **Punkte werden wie folgt vergeben:**
 - 0-50: Mangelhaft
 - 51-75: Verbesserungsbedürftig
 - 76-90: Befriedigend
 - 91+: Ausgezeichnet

Das typische globale Unternehmen hat eine Datensicherheitsbewertung von 67.®



So wird es basierend auf der Analyse dieser Trends und Vektoren in Zukunft aussehen. ^(M)

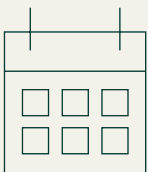
Datensicherheitsbewertung, Durchschnitt



● Globaler Durchschnitt

8%

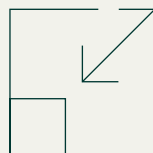
Datensicherheitsbewertungen sollen im nächsten Jahr nur um voraussichtlich 1 % und innerhalb von fünf Jahren um 8 % steigen. ^(M)



In den nächsten fünf Jahren werden die Ergebnisse im Bereich der Datensicherheit zwischen Unternehmen mit guter und solchen mit schlechter Datensicherheit weit auseinanderklaffen. ^(M)

16%

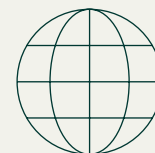
Diese Prognosen zeigen eine deutliche Richtungsänderung gegenüber einem Gesamtanstieg von 16 % im Jahr 2022. ^(M)



Zwei Branchen werden auf das 90. Perzentil steigen (Versorgungsunternehmen und Transport/Logistik), während drei andere Branchen ihren Durchschnitt im gleichen Zeitraum verschlechtern werden (Bildung, Energie und Dienstleistungen). ^(M)

10 von 18

Nur 10 von 18 Branchen und eine einzige geografische Region werden in fünf Jahren Punktezahlen im Bereich „Befriedigend“ oder „Ausgezeichnet“ erreichen. ^(M)

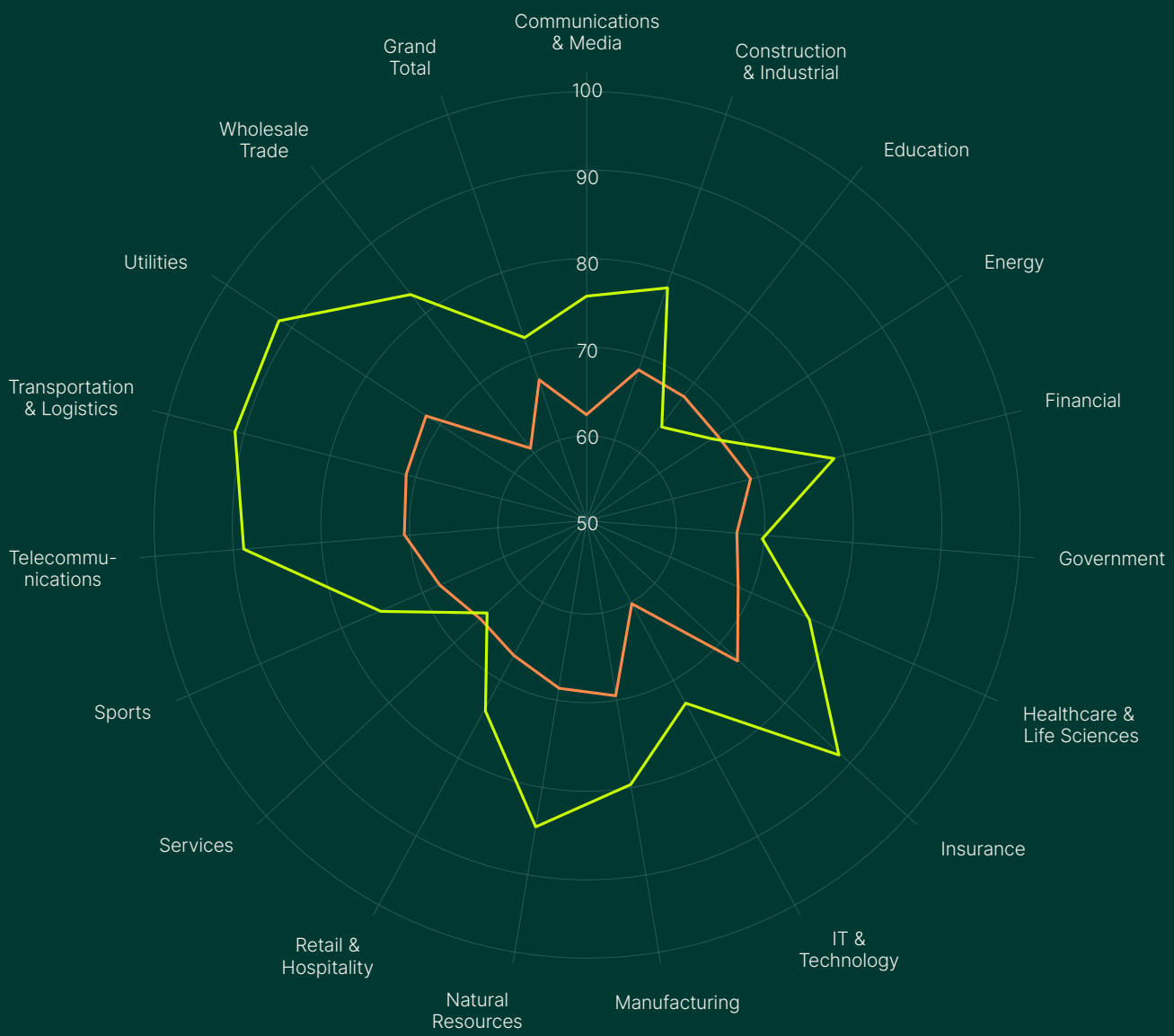


Während Nord- und Südamerika sowie die EMEA-Region weiterhin nahe beieinander und ähnlich nahe am globalen Durchschnitt liegen werden, sieht es in der APAC-Region in den meisten wichtigen Kategorien deutlich anders aus. ^(M)

Wir haben im Laufe der Zeit mehrere Datensicherheitstrends untersucht. So sehen sie im direkten Vergleich aus.™

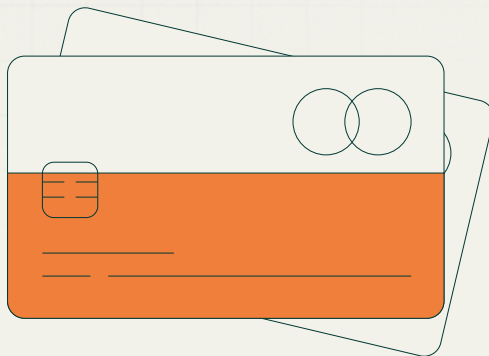
Datensicherheitsbewertung, Durchschnitt

● Juli 2023 ● Juli 2028



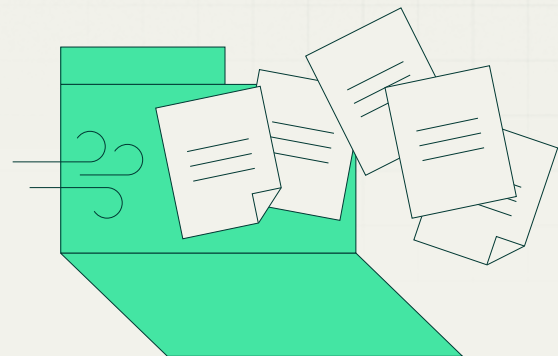
Fakten zu Datenverlusten

Bisher haben wir basierend auf Intuition und Analysen die Daten als Ganzes betrachtet. Wie sieht es mit Bedrohungen für diese Daten aus? Wechseln wir wieder zurück zur Intuition und lassen wir Ihre Kollegen zu Wort kommen.



53 %

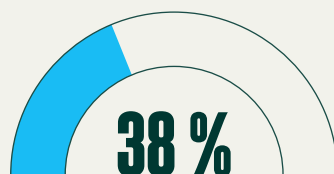
53 % der externen Organisationen hatten im vergangenen Jahr einen erheblichen Verlust sensibler Informationen zu verzeichnen. [™]



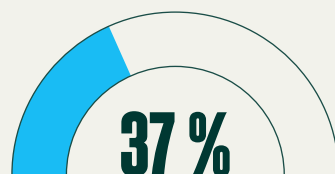
16 %

Ungefähr jede sechste externe Organisation (16 %) musste 2022 mehrere erhebliche Verluste sensibler Daten hinnehmen. [™]

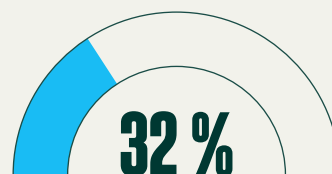
Datentypen, die im letzten Jahr in externen Organisationen kompromittiert wurden: [™]



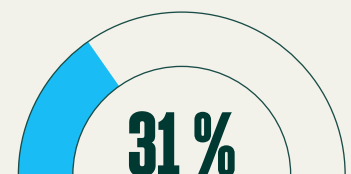
Personenbezogene Daten



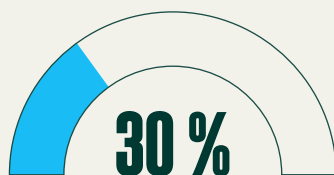
Daten zu Unternehmensfinanzen



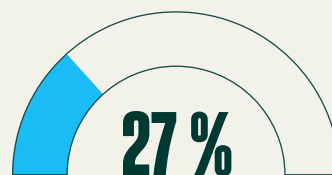
Authentifizierungsnachweise/-schlüssel



Geistiges Eigentum



Zahlungskartendaten



Kontonummern



Geschützte Gesundheitsinformationen

EMPFEHLUNGEN

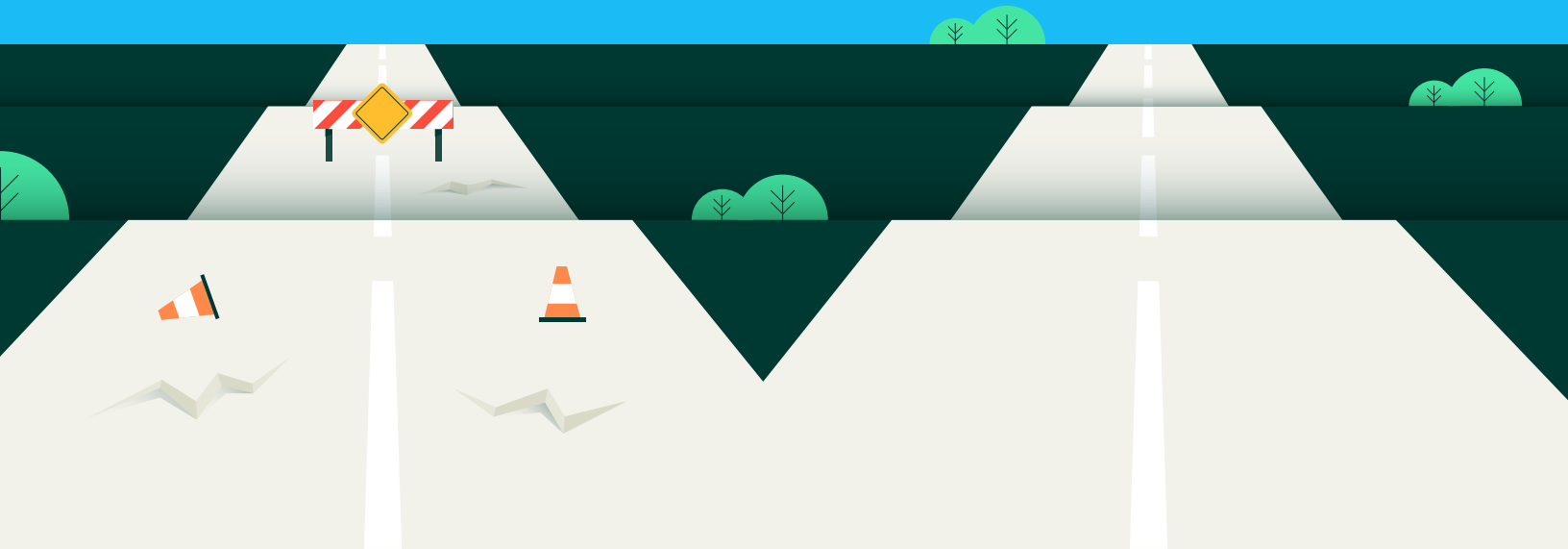
NEUE WEGE

Wir sind vielleicht nicht besonders gut darin, unsere Zukunft vorauszusagen. Aber jetzt haben wir einen Wegweiser, der uns helfen kann, eine neue Richtung einzuschlagen.

Wir wollen einige grundlegende, bewährte Methoden zur Verbesserung der Datensicherheit untersuchen. Diese klingen möglicherweise sehr einfach.

Das sind sie auch. Und sie funktionieren auch noch sehr gut.

Sie brauchen uns nicht beim Wort zu nehmen – wir beweisen es Ihnen.



98 %

Die überwiegende Mehrheit der Unternehmen (98 %) ist der Ansicht, dass sie derzeit erhebliche Probleme mit der Datentransparenz haben. ©

54 %

der Unternehmen haben einer einzigen Führungskraft die Verantwortung für Daten und deren Sicherheit übertragen. ©

Diese Zukunft ist nicht in Stein gemeißelt. Unsere Entscheidungen heute haben Auswirkungen auf unsere Zukunft. Sehen wir uns ein paar Beispiele an.

Rubrik Zero Labs

Drei wichtige Empfehlungen

1.

EMPFEHLUNG

Nutzen Sie Datentransparenz, um sensible Daten regelmäßig proaktiv zu überprüfen.

Wenn ein Unternehmen die Gesamtdaten des Vorjahres um 20 % reduziert, funktionieren mehrere Maßnahmen zur Risikominderung sofort besser. Zur Datenreduzierung könnten sensible Daten entfernt werden, auf die im letzten Jahr kein Benutzer zugegriffen hat, doppelte Datenkopien aufgespürt und gelöscht werden oder Daten in Benutzerfreigaben für Mitarbeiter/Kunden/Partner, die im letzten Jahr ausgeschieden sind, entfernt werden. Dies gilt auch für doppelte Daten in verschiedenen Datenspeichern in einem Unternehmen.

2.

EMPFEHLUNG

Gehen Sie das Thema Datenwachstum bewusst an.

Die Gesamtgröße, die Wahl der Umgebung und die Gesamtzahl der Umgebungen sind allesamt potenzielle Stellschrauben. Zu Beispielen entsprechender Maßnahmen zählen das Begrenzen des Cloud-Wachstums auf maximal 50 % der gesamten Umgebung, das Löschen von Daten auf Basis festgelegter Richtlinien, das Begrenzen der Gesamtzahl der Speicherorte auf weniger als vier in der gesamten Unternehmensumgebung oder das Speichern sensibler Daten in nur einer Enklave.

3.

EMPFEHLUNG

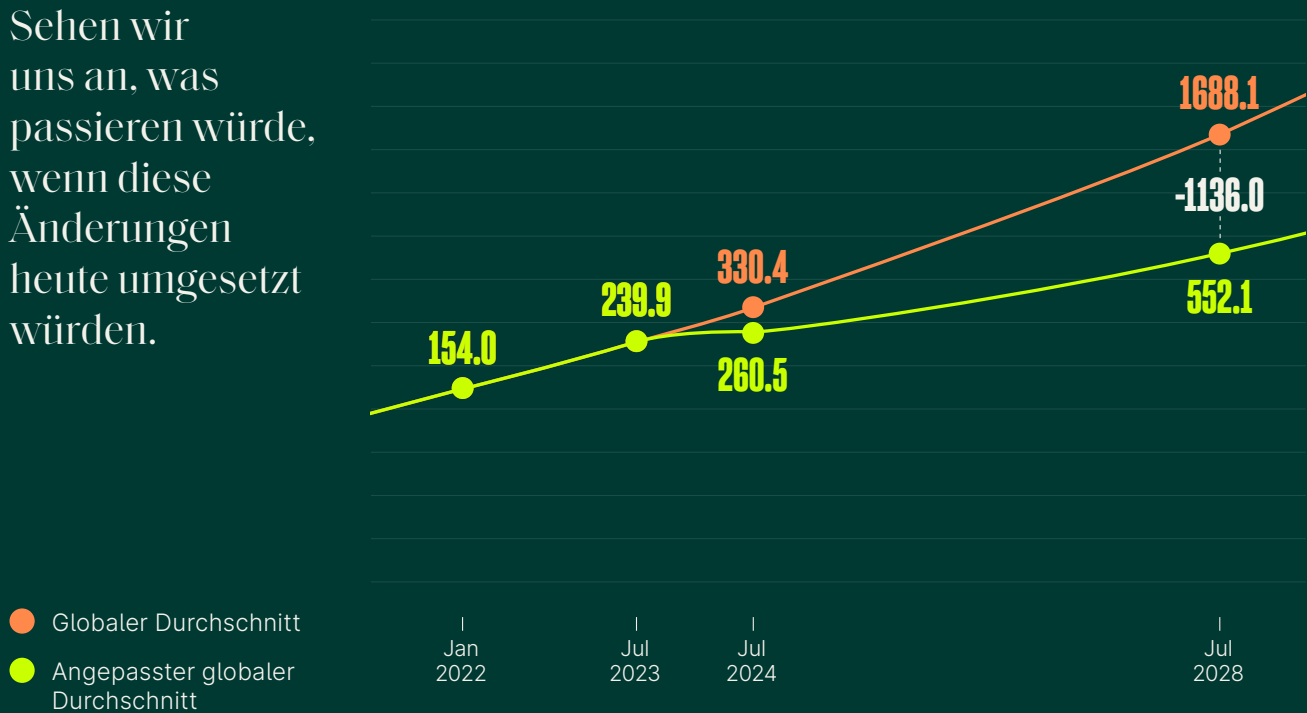
Machen Sie die Datensicherheit zu einem besonderen Schwerpunkt auf Führungsebene.

Ein benannter Verantwortlicher, zu erwartende Richtlinien und die Anwendung bzw. Durchsetzung von Best Practices in der Organisation werden allesamt zu tiefgreifenden positiven Auswirkungen und einem tieferen Verständnis der gemeinsamen Verantwortung führen.

Angewandte Empfehlungen

Durchschnitt Gesamt-BETB[®]

Sehen wir uns an, was passieren würde, wenn diese Änderungen heute umgesetzt würden.



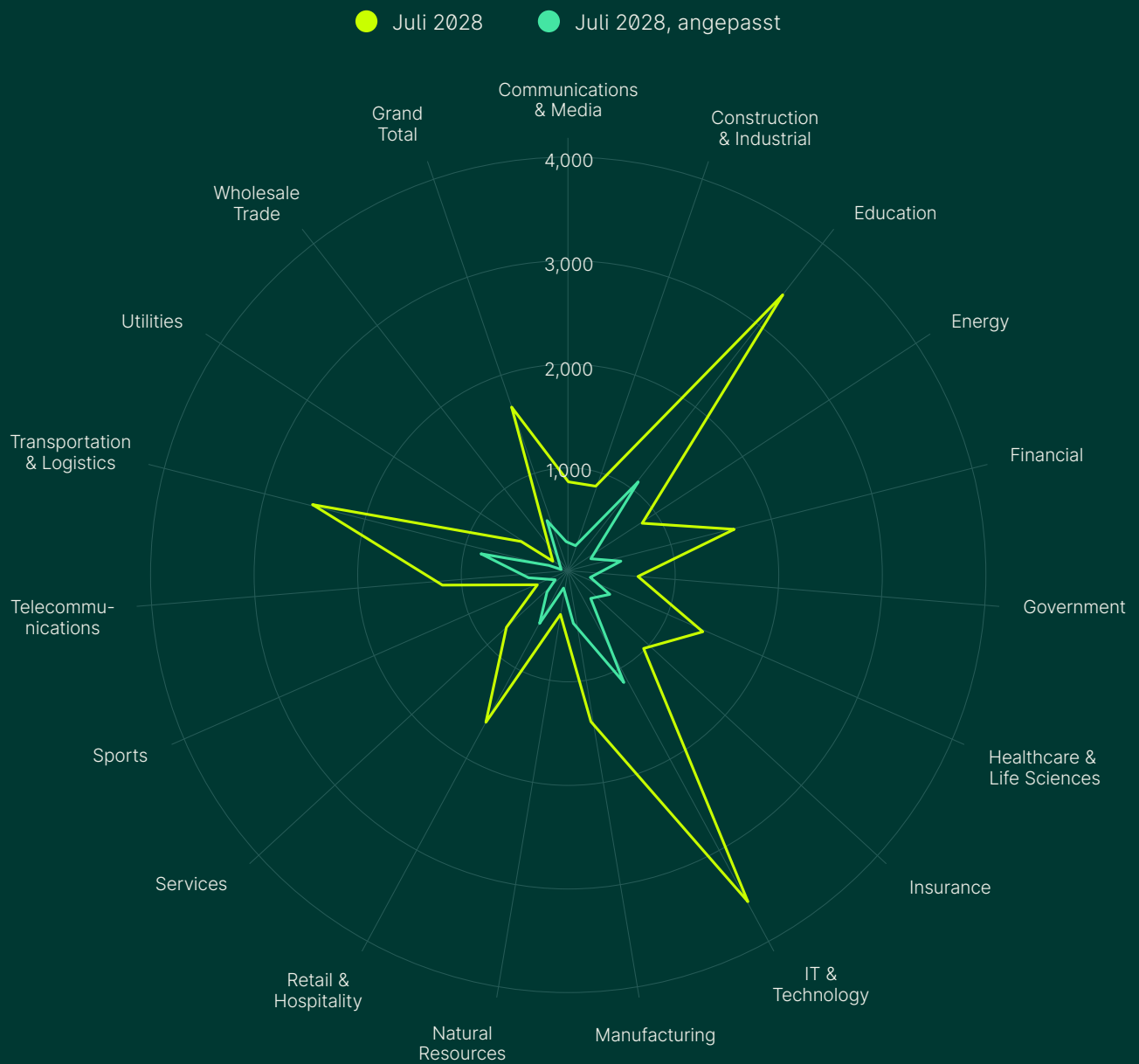
Die Anwendung dieser Empfehlungen würde in fünf Jahren folgende Unterschiede bewirken: [®]

1100+ BETB WENIGER

benötigter Datenspeicherplatz für ein typisches Unternehmen

Durchschnitt Gesamt-BETB[®]

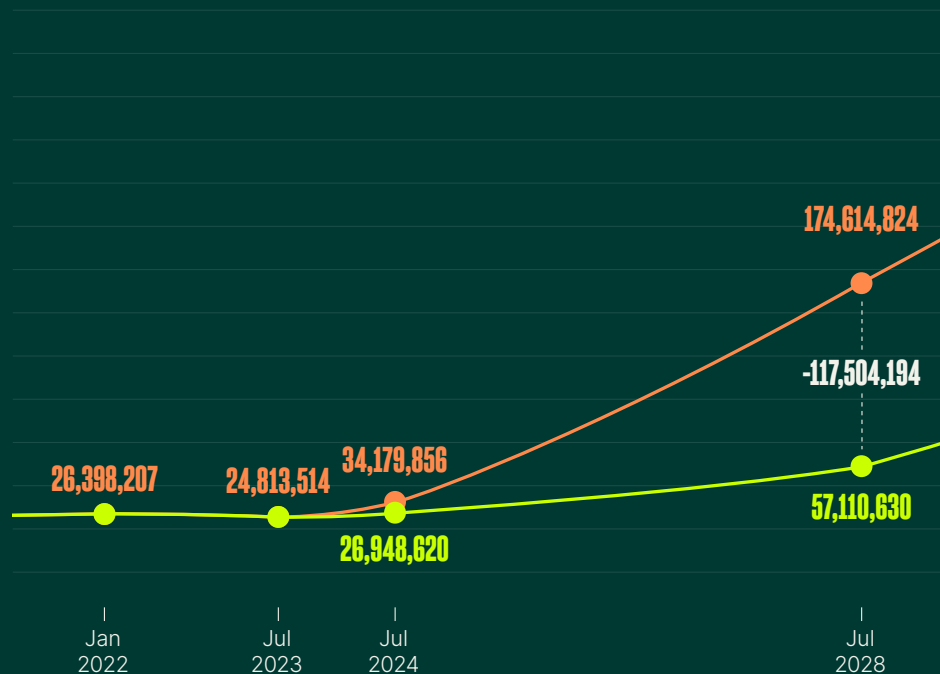
Auf der Grundlage dieser Empfehlungen können wir bereits nachweisbare Veränderungen feststellen. Lassen Sie uns alle davon gleichzeitig miteinander vergleichen, um einen Gesamtüberblick zu erhalten:



Angewandte Empfehlungen

Dateien mit sensiblen Daten (durchschnittlich) [®]

● Globaler Durchschnitt ● Angepasster globaler Durchschnitt



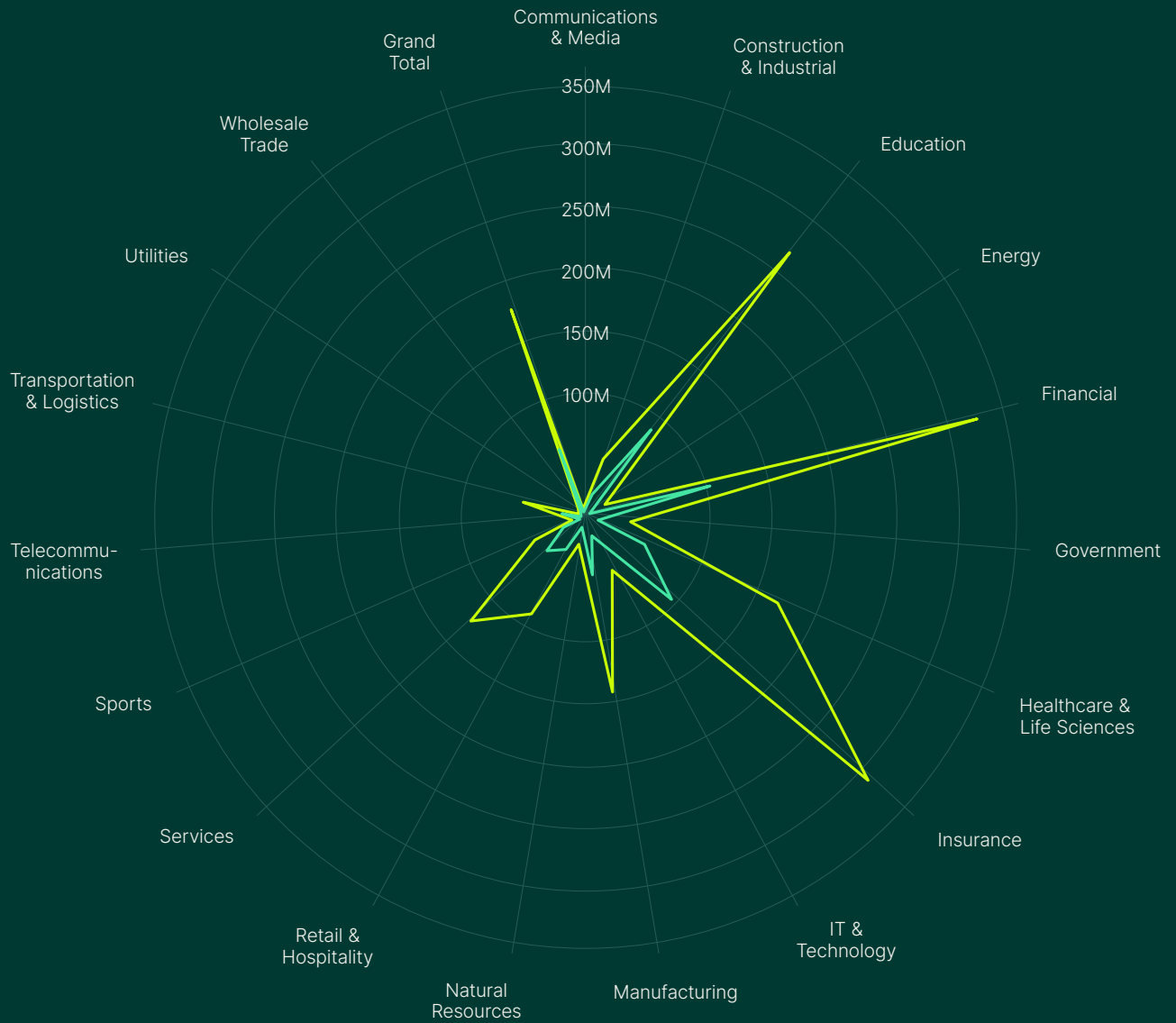
Die Anwendung dieser Empfehlungen würde in fünf Jahren folgende Unterschiede bewirken: [®]

EINE REDUZIERUNG UM MEHR ALS 117 MILLIONEN

sensibler Datensätze in einer typischen Umgebung

Dateien mit sensiblen Daten (durchschnittlich) [®]

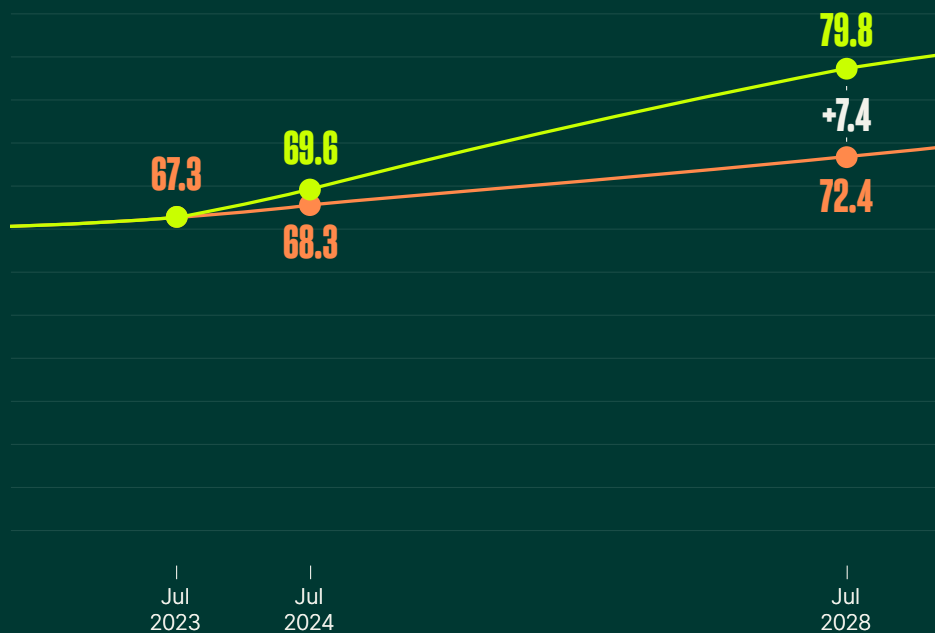
● Juli 2028 ● Juli 2028, angepasst



Angewandte Empfehlungen

Datensicherheitsbewertung, Durchschnitt[®]

● Globaler Durchschnitt ● Angepasster globaler Durchschnitt



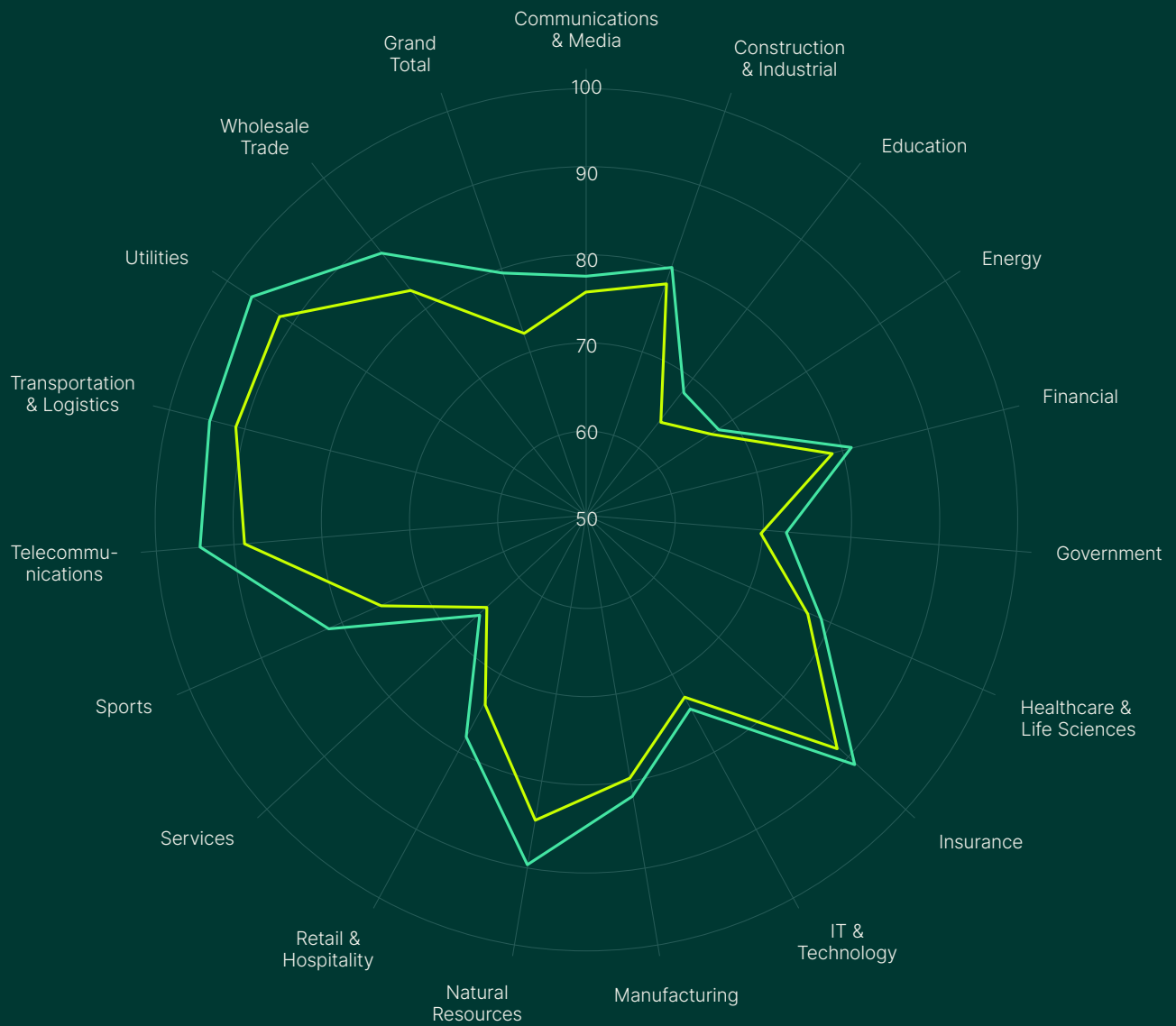
Die Anwendung dieser Empfehlungen würde in fünf Jahren folgende Unterschiede bewirken:[®]

VERBESSERUNG

der Datensicherheitsbewertung um 10 % – mehr als das Doppelte des prognostizierten Wachstums

Datensicherheitsbewertung, Durchschnitt[®]

● Juli 2028 ● Juli 2028, angepasst





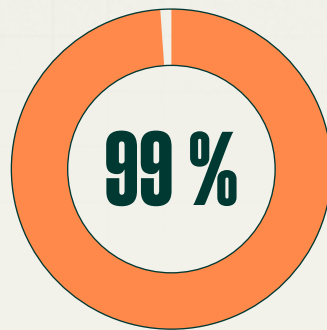
SUMMARY

**DAS ENDE
DER REISE**
(ERSTMAL)

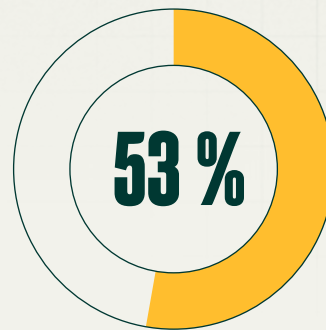
Am Anfang dieser Reise sagten wir, dass Menschen von Natur aus optimistisch sind. Nach dieser gemeinsamen Reise sind wir optimistisch, dass Sie ein besseres Verständnis Ihrer Daten und davon haben, ob Sie sie bisher durch eine rosarote Brille betrachtet haben.

Aber ist Optimismus denn so etwas Schlechtes?

Ja und nein.



Anzahl der Organisationen, die im vergangenen Jahr Opfer eines Angriffs wurden



Zahl der Organisationen, die im vergangenen Jahr einen erheblichen Verlust sensibler Informationen zu verzeichnen hatten

Wenn 99 Prozent der Unternehmen im letzten Jahr einen Angriff erlebt haben und mehr als die Hälfte zugeben, dass sie in den letzten 12 Monaten sensible Daten verloren haben, sprechen die Zahlen eindeutig gegen Sie. Kein klar denkender IT- oder Sicherheitsexperte würde sich ohne ein gewisses Maß an Optimismus in diesen Kampf begeben. Es ist gut, dass wir optimistisch sind, denn wir brauchen alle Mann an Deck, um die vor uns liegenden Herausforderungen anzugehen.

Aber wie wir gesehen haben, kann übertriebener Optimismus schlimme Folgen haben.

Hoffentlich nehmen Sie Folgendes aus diesem Bericht mit:



Bleiben Sie optimistisch.



Analysieren Sie die Lage.



Beachten Sie die Zeichen.



Treffen Sie fundierte Entscheidungen.

Danksagungen

Rubrik möchte sich am Ende dieser Reise aufrichtig bei denjenigen bedanken, die an dieser Arbeit beteiligt waren. Wakefield Research hat Daten bereitgestellt, damit diese Untersuchung so objektiv wie möglich sein konnte. Shaped By (www.shaped-by.com) hat wieder einmal kreative Wege gefunden, Konzepte lebendig darzustellen. Und schließlich haben viele Menschen bei Rubrik hart gearbeitet, um Know-how, Kontext und Tipps bereitzustellen. Wir können uns unmöglich bei jedem einzeln bedanken, besonders danken möchten wir aber Amanda „Danger“ O’Callaghan, Linda Nguyen, Lynda Hall, Ajay Kumar Gaddam, Ryan Goss, Derek Morefield, Josh Burns, Gunakar Goswami, Prasath Mani, Ethan Hagen, Kevin Nguyen, Caleb Tolin, Kelly Cooper und Olivia Howard.



Rubrik Zero Labs