BALANCING DATA PRIVACY WITH DATA SCIENCE PRODUCTIVITY

Survey of Fortune 500 Companies on Cloud, Compliance and Data Security

SURVEY RESPONDENTS

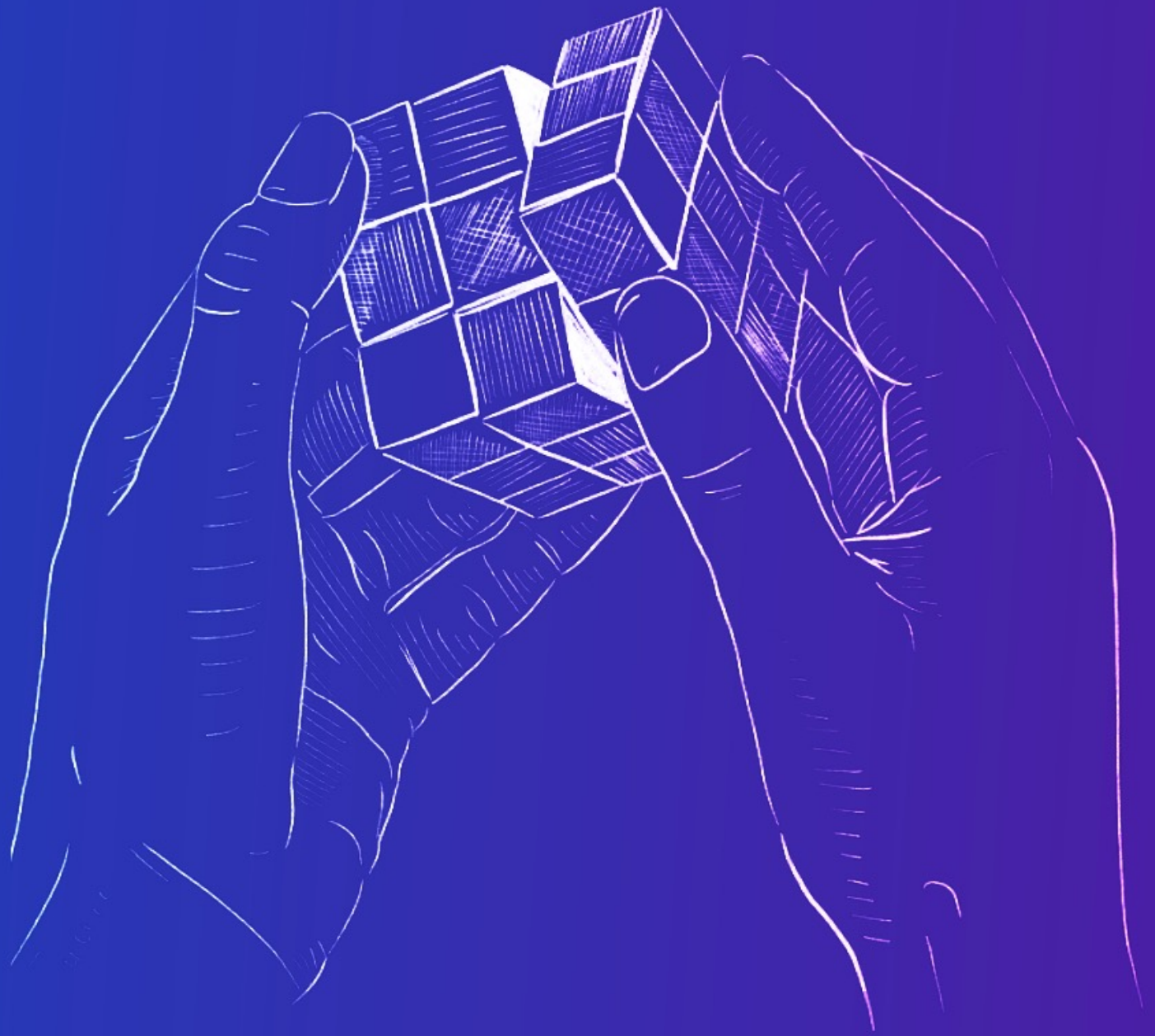
Telephone interviews with executives from Fortune 500 companies in Q1 2021 on cloud, data security and access control

100
INTERVIEWS

PRIVACERA

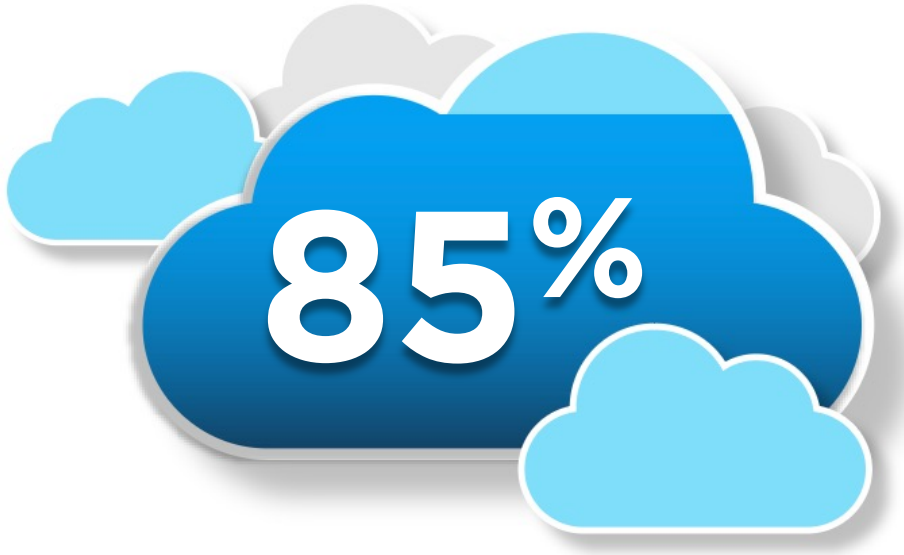
SECTION ONE

The Impact of Digital Transformation on Data Science and Data Privacy



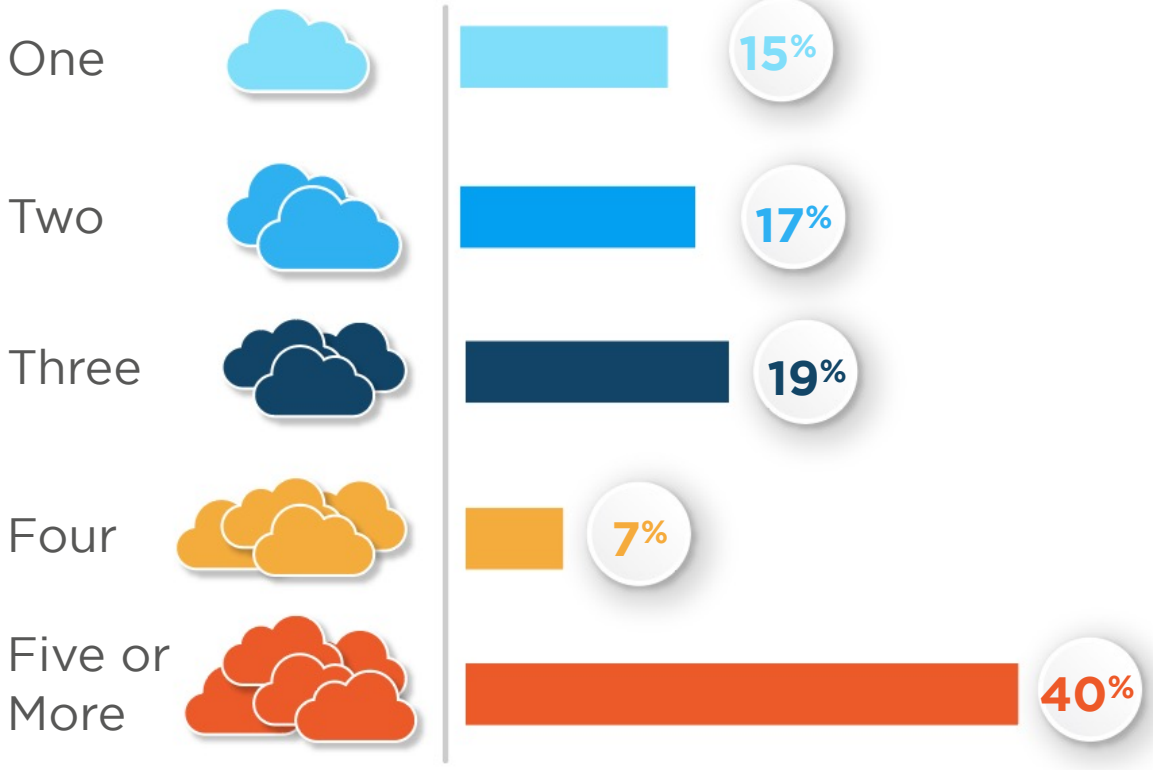
PRIVACERA

DIGITAL TRANSFORMATION IS DRIVING MULTI-CLOUD MIGRATION



of respondents have **2 or more cloud providers** for data storage & analytics

NUMBER OF CLOUD PROVIDERS



PRIVACERA

INCREASING PRIVACY REGULATIONS

GDPR/CCPA and Other Privacy Regulations Make Cloud Migration More Difficult

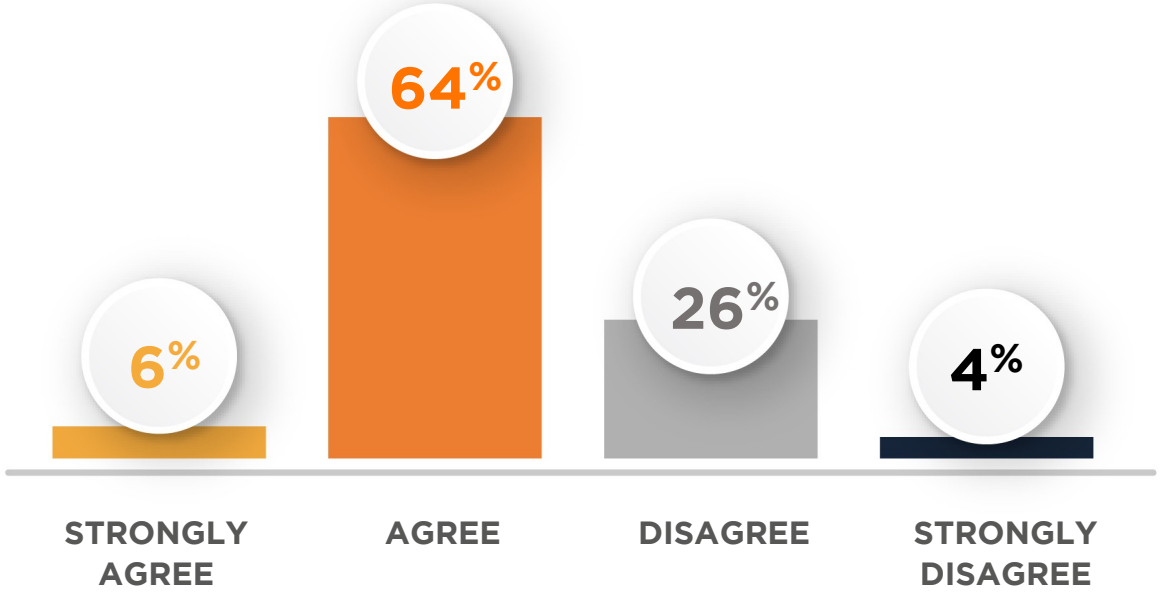
GDPR

HIPAA

CCPA

LGPD

Increasing privacy regulations must be considered when migrating to the cloud



70% said cloud migration & analytics has been made more complex due to compliance with privacy regulations

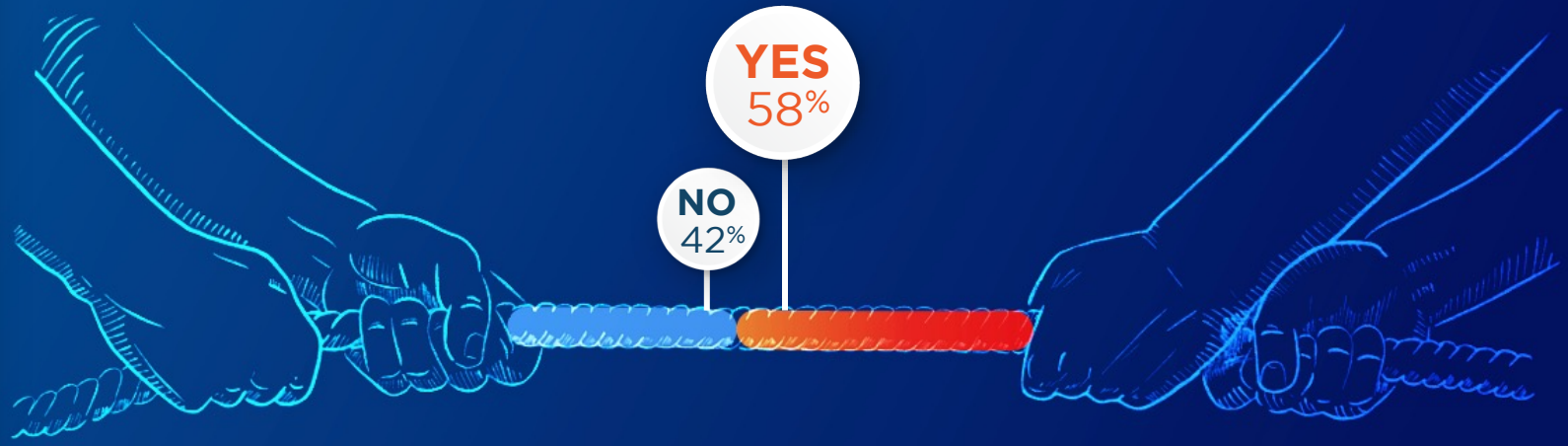
PRIVACERA

ANALYTICS TEAM PRODUCTIVITY CONFLICTS WITH PRIVACY

58%

of the Fortune 500 respondents report conflict between data scientists and data security & compliance teams due to access restrictions.

Does your business experience conflict between data science teams requesting data access and the need for data security and privacy?



DATA SCIENCE & ANALYTICS

PRIVACY AND SECURITY

PRIVACERA

SECTION TWO

What's at Stake?

PRIVACERA

MANAGING DATA PRIVACY AND SECURITY IS A CORPORATE IMPERATIVE

CONSEQUENCES

3,932 publicly disclosed data breaches in 2020

37 BILLION compromised data records

$3.62 MILLION average cost of one data breach

Source: Risk-Based Security; 2020 Year End Data Breach QuickView Report

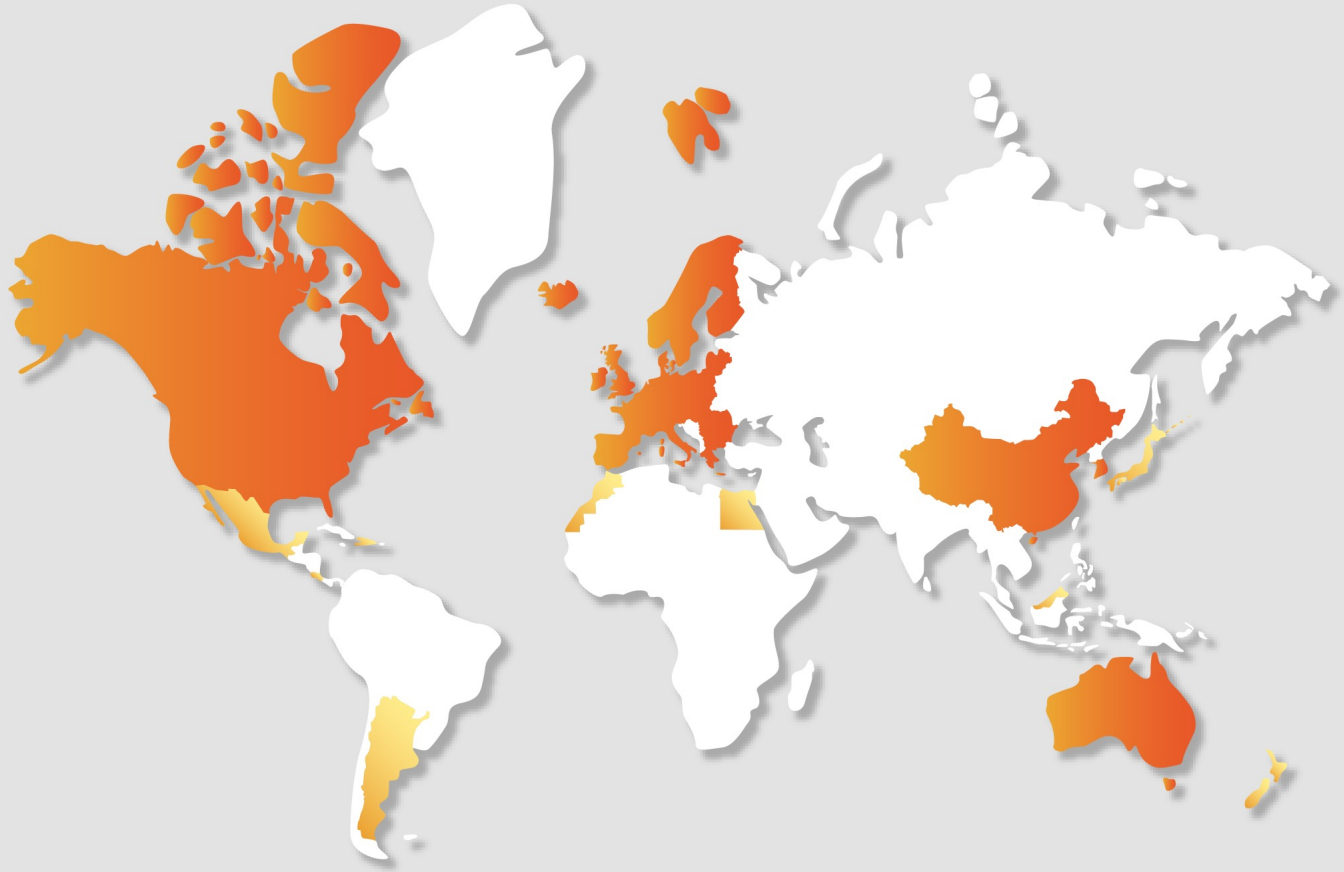
PRIVACERA

ADHERING TO WORLDWIDE PRIVACY REGULATIONS IS DIFFICULT

Privacy regulations are being increasingly adopted worldwide:

- US HIPAA (2016)
- EU GDPR (2018)
- CA CCPA (2020)
- Brazil LGPD (2020)

WORLD DATA REGULATION & ENFORCEMENT HEATMAP



Source: https://www.dlapiperdataprotection.com/

PRIVACERA

WHAT'S NEEDED TO COMPLY?

Regulations require:

Manage 'personal data'
Information relating to an identified or identifiable natural person ('data subject')

Pseudonymisation
Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

Right to Erasure/
Right To Be Forgotten
The ability to erase personal data

Audits of location and usage of personal data

Sources:
Full GDPR details here; Full CCPA details here; Full LGPD details here;
More details on worldwide privacy regulations: DLA piper

PRIVACERA

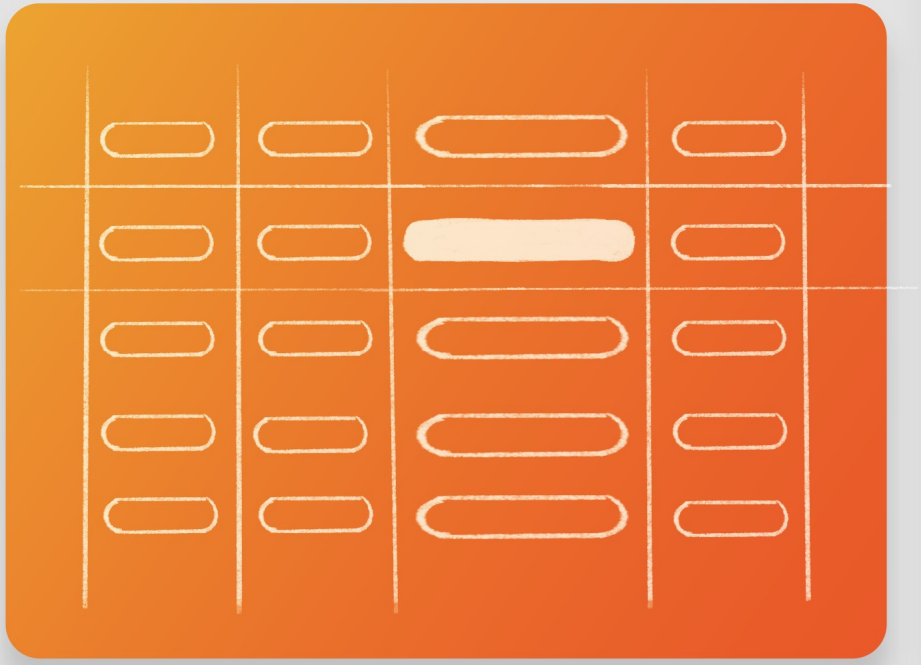
SECTION THREE

How are Companies Coping?

PRIVACERA

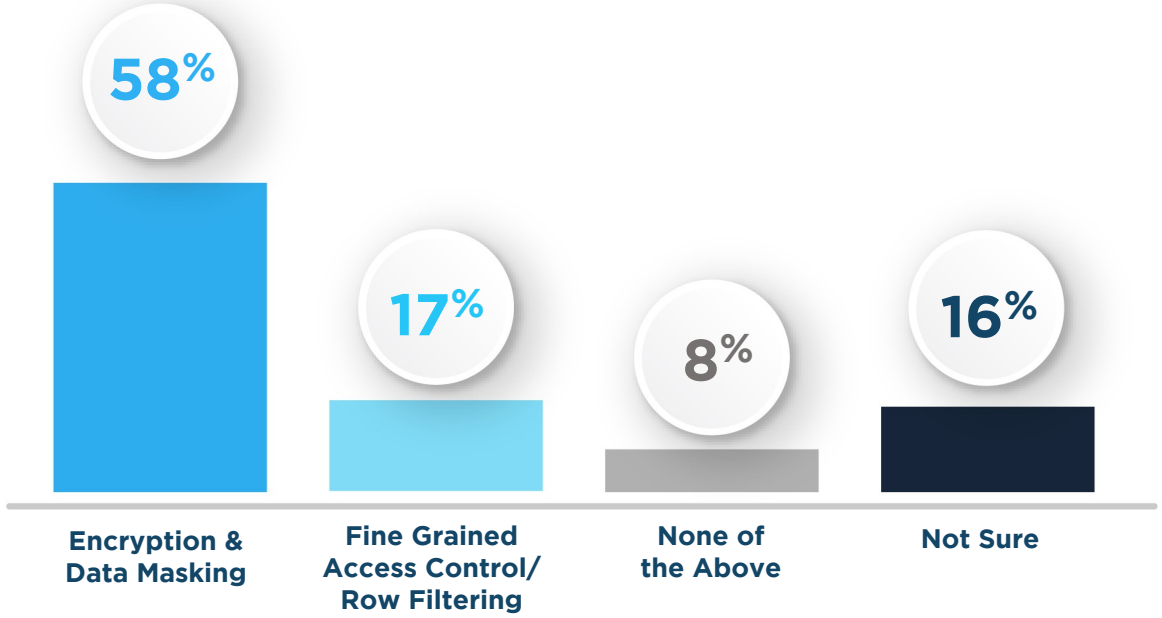
HOW DO YOU SECURE YOUR DATA?

ONLY 17% have fine-grained access control/row-filtering for data security without impeding data science & analytics



Do you rely on IAM (Identity and access management methods such as single sign-on) **to limit access to cloud data services?**

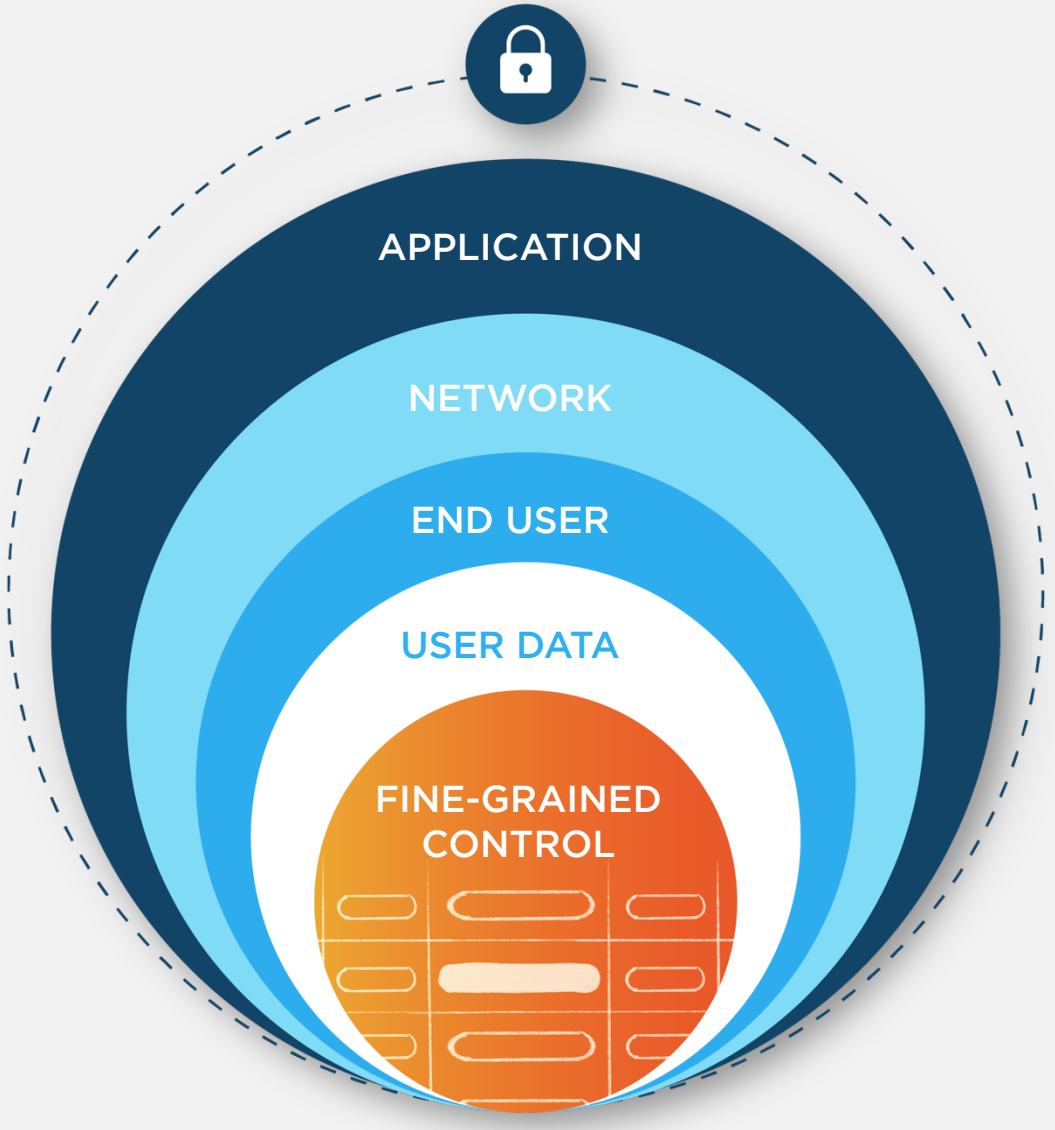
Are you using any of the following technologies to secure critical data?



PRIVACERA

The Layered Approach to Data Security

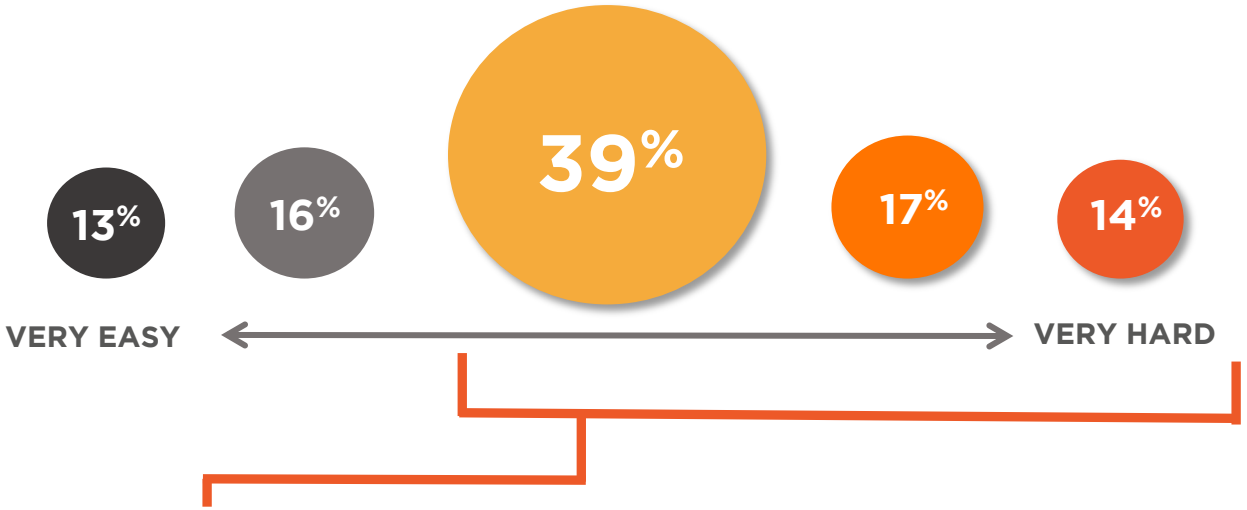
IAM only controls access to the outside of the system and fails to secure the data inside, leaving your system vulnerable to data breaches and leaks.



HOW DIFFICULT IS IT TO SECURE SENSITIVE DATA?

WE ASKED:

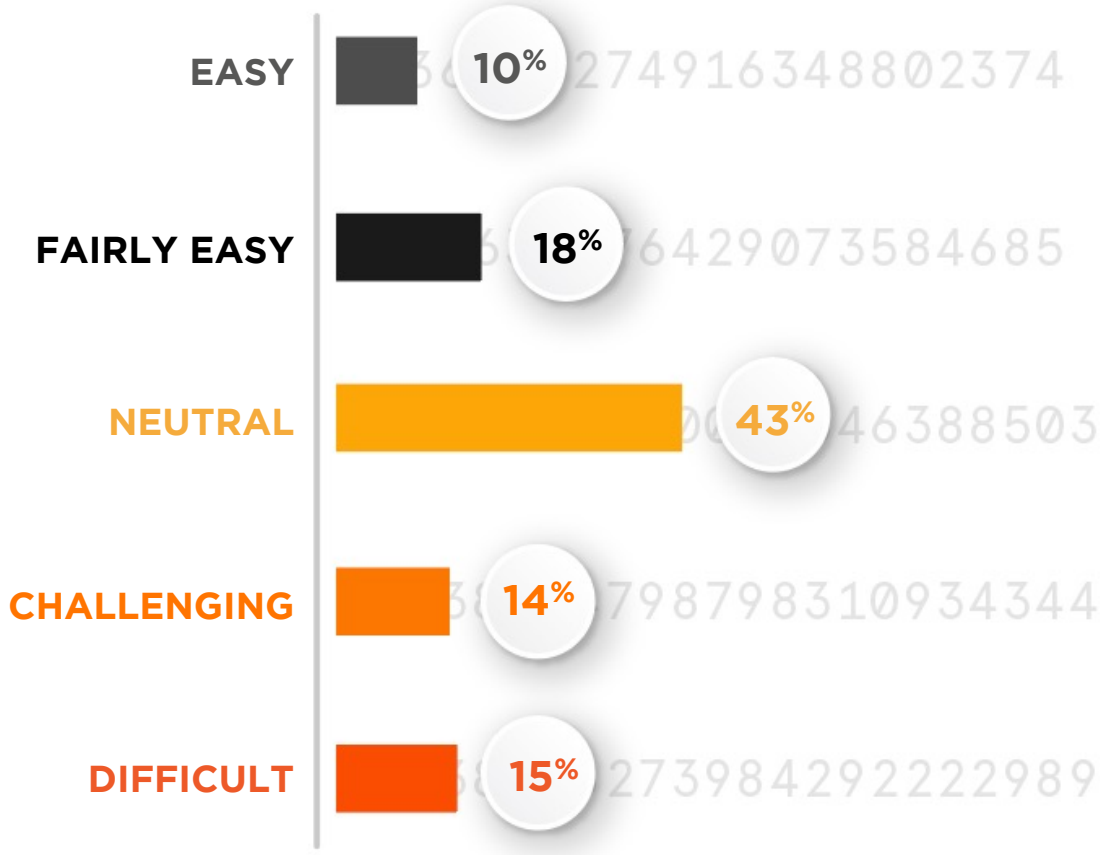
Once you have identified and classified all sensitive data across cloud-based repositories, **how difficult is it to manage access to sensitive data in compliance with external or internal governance policies?**



70% of respondents could benefit from an easier option to ensure privacy and security of sensitive data

PRIVACERA

HOW DIFFICULT IS IT TO ANONYMIZE PERSONALLY IDENTIFIABLE INFORMATION ?

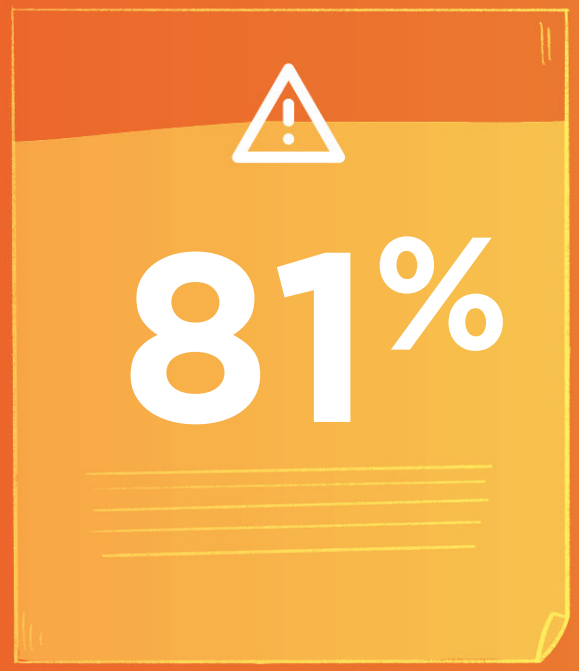


WE ASKED:

How difficult is it to ensure the anonymization of personally identifiable information (PII) to comply with privacy laws like GDPR (EU), CCPA (USA), and LGPD (Brazil)?

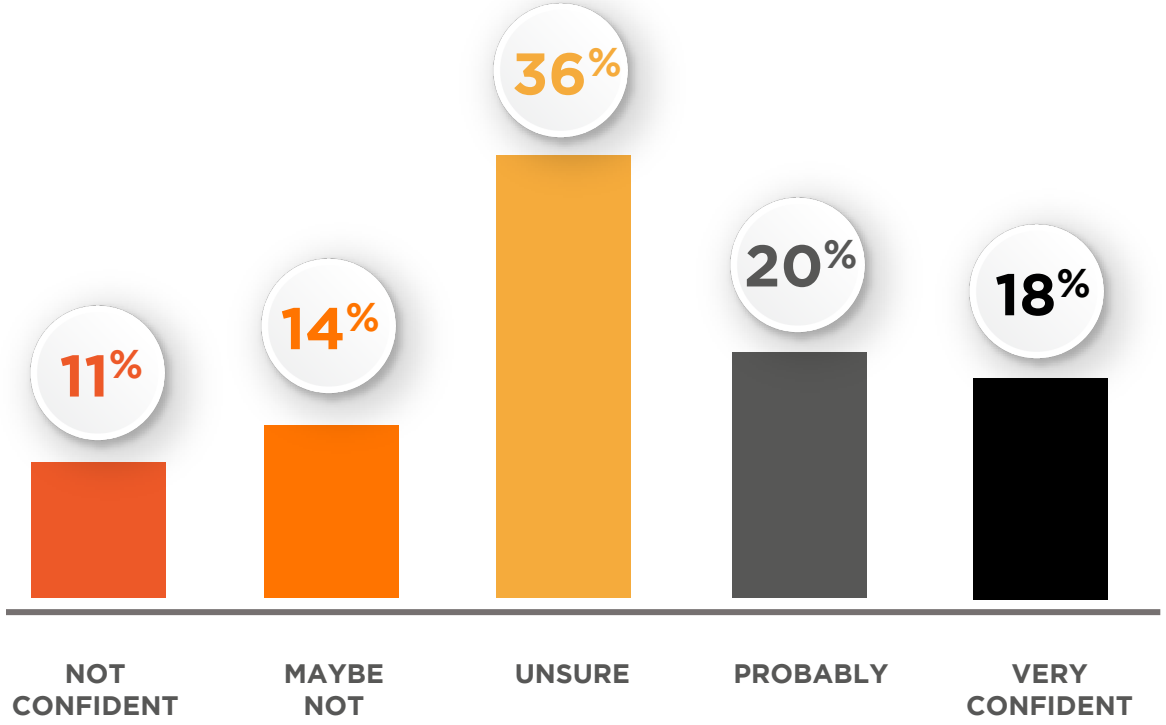
PRIVACERA

DO YOU TRULY HAVE CONTROL OF YOUR DATA?



of respondents are not sure that a request from a past customer to delete all information could be executed across all data repositories.

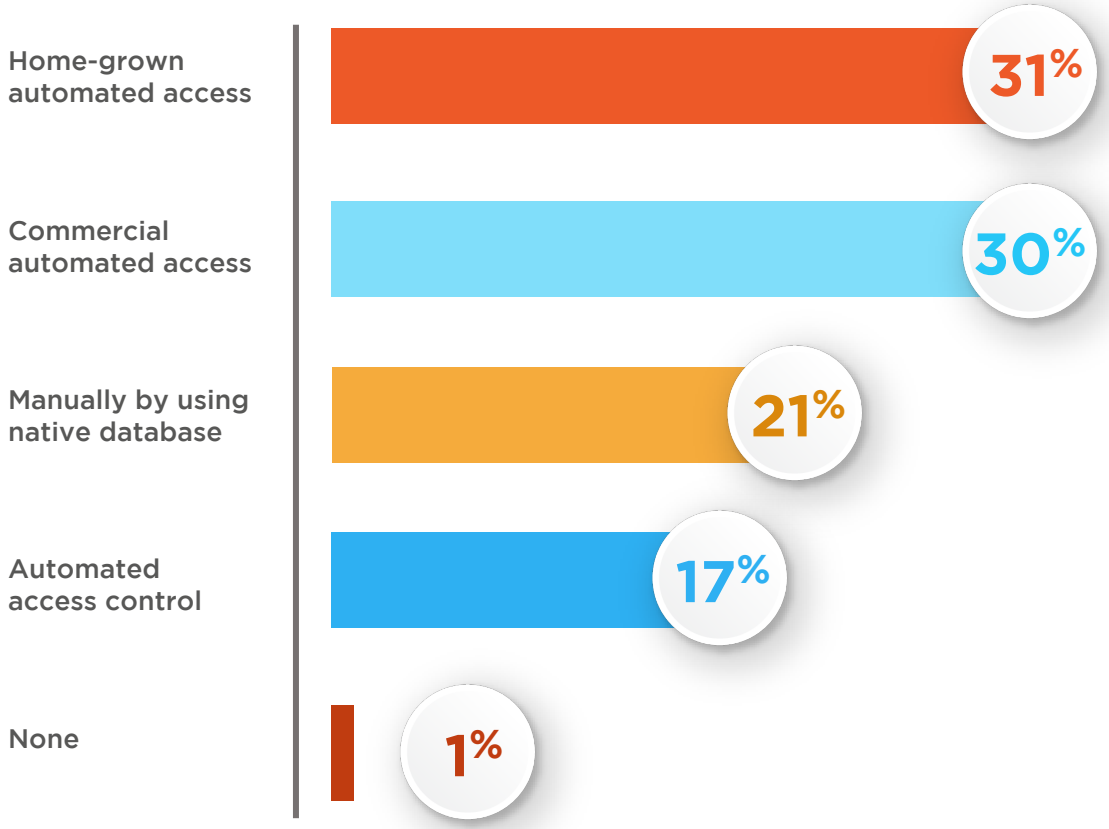
HOW CONFIDENT ARE YOU THAT A REQUEST FROM A PAST CUSTOMER TO DELETE ALL INFORMATION COULD BE EXECUTED ACROSS ALL DATA REPOSITORIES?



PRIVACERA

DATA ACCESS CONTROL IS A COMMON CHOICE FOR MANAGING DATA GOVERNANCE AND COMPLIANCE

HOW DO YOU CURRENTLY MANAGE DATA COMPLIANCE AND GOVERNANCE?



But what's in place today may not be the ideal solution for tomorrow...

- How easily are homegrown access control solutions updated?
- Does the automated access control scale to petabytes of data?
- Does the solution scale to multiple cloud providers?
- How does access control secure zero-trust environments?
- Alternative approaches and tools, or no data governance.

PRIVACERA

AUTOMATION SOLUTIONS FOR DATA GOVERNANCE AND ACCESS CONTROL WILL BE NEEDED WITHIN 1-3 YEARS

70% Over the next 1-3 years

20% Not in the immediate future

10% In 2021

WE ASKED:

Do you believe that migration to a hybrid multi-cloud environment will force companies to invest more money into automated tools to ensure data governance and access control?

WHAT'S YOUR INVESTMENT PLAN?

Digital transformation initiatives are driving growth in enterprise analytics with a five-year CAGR of 12.5%

Source: IDC: Worldwide Big Data and Analytics Software Forecast, 2019–2023

Data is moving to the cloud. Worldwide market for cloud systems and management software has a forecasted five-year CAGR of 24.1%

Source: IDC: Worldwide Cloud System and Service Management Software Forecast Update, 2020–2024: Enterprise Investments Rebound,

PRIVACERA

SECTION FOUR

Tips for Managing Data Privacy Across Cloud Providers

PRIVACERA

AUTOMATION SOLUTIONS FOR DATA GOVERNANCE AND ACCESS CONTROL WILL BE NEEDED WITHIN 1-3 YEARS

TYPICAL APPROACH TO DATA PRIVACY AND SECURITY ACROSS CLOUD SERVICES

For privacy and security, most enterprises **restrict the amount of data** accessible for analytics

1

Each cloud provider has its own built-in governance capabilities in a **siloed, repository-specific approach**

2

IT teams are **inundated with requests for access** to disparate data sets across different on-prem and cloud datastores

3

Sensitive data isn't being analyzed, costing enterprises valuable insights

4

PRIVACERA

WHAT'S NEEDED TO MEET PRIVACY AND COMPLIANCE ACROSS MULTIPLE CLOUD PROVIDERS?

Are you hitting a home run in data governance?

SINGLE: Complete visibility into all enterprise data wherever it lives

DOUBLE: Users can access only the data they are authorized to access via fine-grained data access policies

TRIPLE: Make more data available for analytics by only masking "sensitive" elements, eliminating wholesale redactions

HOME RUN: Hitting all the bases with a centralized platform that is easy to deploy and manage

PRIVACERA

ARE YOU READY TO EMPOWER ANALYTICS WITHOUT COMPROMISING DATA SECURITY?

PRIVACERA

Data Access Governance

- Automates sensitive data discovery, and tagging across multiple cloud services
- Reduces errors and wasted time with unified, fine-grained access control
- Anonymizes and encrypts sensitive data
- Creates automated workflows based on predefined policies
- Balances data privacy and data sharing across your enterprise

PRIVACERA

Data democratization without compromising compliance

Take a deeper dive and see Privacera in action

general@privacera.com

510.413.7300

privacera.com