CROSS-BORDER DATA PROTECTION

EMPOWER GLOBAL BUSINESS WITH BORDERLESS DATA™

PROTEGRITY

CONTENTS

INTRO

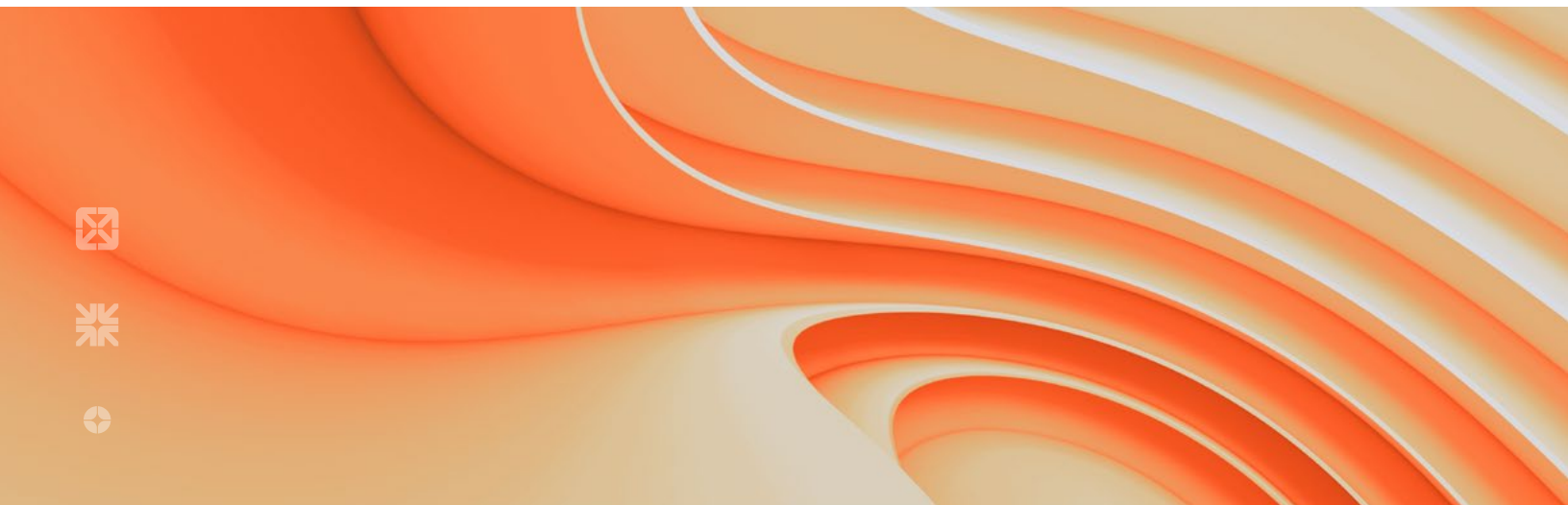
INTRODUCTION

"Data [is] becoming the new raw material of business."

—Craig Mundie, Microsoft

Data is the currency of the digital age. In the decade from 2006–2016, McKinsey notes that "the world is more connected than ever," as cross-border data flows grew by a factor of over 45, with data flows accounting for $2.8 trillion in GDP.[1] Globalization has enabled businesses to access new markets and customers worldwide, expanding their operations and increasing revenues.

To facilitate globalization, centralized processing was the streamlined mechanism organizations used to allow for more efficient and cost-effective data flow using fewer resource requirements.



However, organizations that once thrived in the interconnected world of integrated markets operating on the free flow of people, goods, and data are now challenged by the rapidly growing number of data privacy laws. Recent forces, such as shifts in global data policies, increased consumer awareness of their digital footprints, and geopolitical tensions, further increase the fragmentation of trade systems and technology standards. Moreover, fragmentation has also contributed to digital sovereignty, with more nations and regions looking to control their digital destiny, from data to AI.

Maintaining the status quo is no longer an option. Organizations that solve expanding data localization challenges using simple foundations in technology can achieve much more than data compliance across their entire organization.

"Companies that figure out how to move seamlessly across geographies will enjoy significant rewards — growth and increased market share — by complying with local requirements while at the same time offering a great customer experience and leveraging the power of their global data sets."[2] Proactive organizations can create new business and establish a competitive advantage by enabling business in any country.

This eBook explains the changing data landscape, how companies can turn challenges into opportunities, and how they can position themselves as market leaders with the power of Borderless Data™.

02

THE GROWING COMPLEXITY OF DATA SOVEREIGNTY, DATA LOCALIZATION, AND PRIVACY REQUIREMENTS

137 out of 194 UN countries have data and privacy legislation in place.[3]

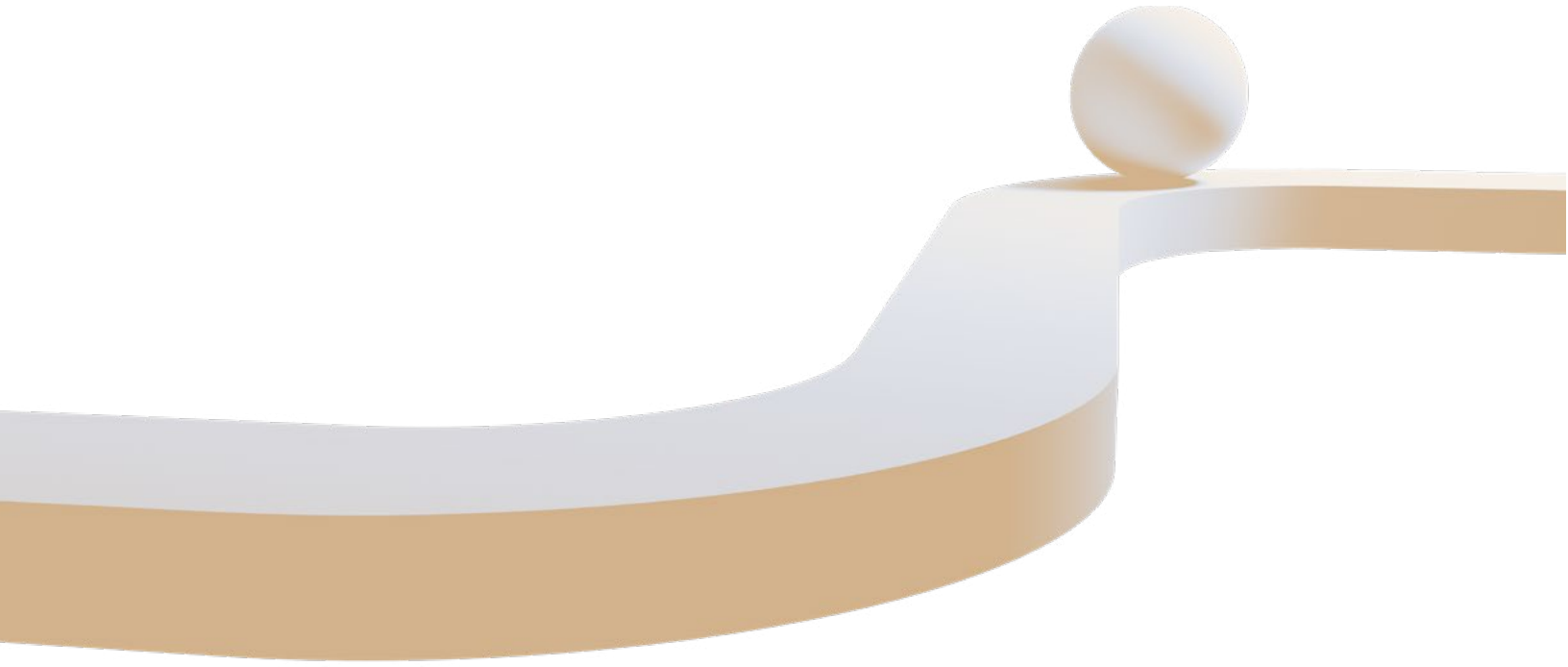
Businesses built to compete on global supply chains, leveraging economies of scale and centralized decision-making processes, are now challenged due to the growing complexity of data sovereignty, data localization, and privacy requirements.

COMPLEX

Data Sovereignty

One of the most significant issues facing multinational businesses today is data sovereignty. Data sovereignty is the idea that data is subject to the laws and regulations of the country in which it is collected. Because data sovereignty laws vary significantly from region to region, it is challenging to move data across changing geographical locations.

For example, the European Union's General Data Protection Regulation (GDPR) is one of the strictest data privacy laws in the world. It requires companies to obtain explicit consent from individuals before collecting, processing, or storing their data. Failure to comply with GDPR can result in litigation and hefty fines, as exhibited in two of the most significant international privacy cases in recent history — Schrems I and Schrems II.



Legal Precedents

The Court of Justice of the European Union (CJEU) case of Maximillian Schrems v Data Protection Commissioner, (commonly referred to as Schrems I), arose from a complaint by Austrian privacy advocate Max Schrems against Facebook and its data transfers from the EU to the United States. The ruling of the CJEU on October 6, 2015, invalidated the Safe Harbor arrangement, which had previously governed data transfers between the EU and the US. As a result, in 2018, the EU issued Facebook (now Meta) over $8.8 billion in fines for their GDPR violation.

Five years later, on July 16, 2020, the CJEU ruled in the landmark "Schrems II" case (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems) that the EU-US Privacy Shield was invalid. The Court also questioned the ability of the European Commission's Standard Contractual Clauses (SCCs) to legitimately authorize transfers of personal data to the US and globally.

As a result, the SCCs are still valid as a data transfer mechanism in principle but require additional, more detailed safeguards to ensure compliance.

CHALLENGES WITH MAINTAINING DATA SOVEREIGNTY COMPLIANCE

RAPIDLY EVOLVING LAWS

Privacy laws across countries and regions are being updated or created so quickly that keeping pace with their requirements is difficult.

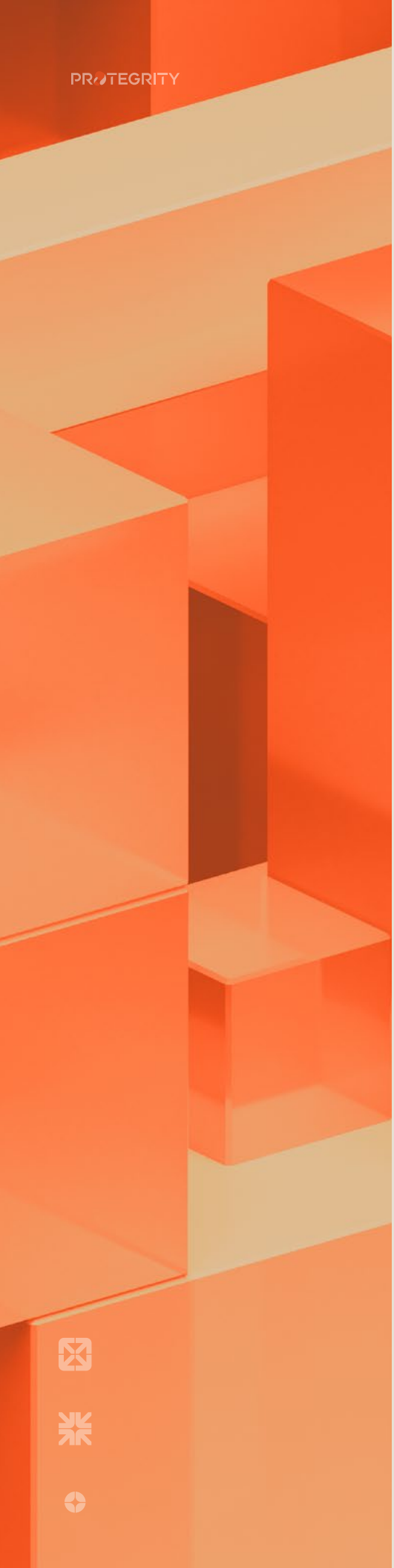
EXPANSION TO NEW REGIONS

Every time your business wants to expand to new territories, regions, or countries, new data sovereignty laws may apply to your data.

CLOUD DEPLOYMENTS

Cloud infrastructure can be located across the globe. Your cloud deployments likely exist in countries with conflicting data sovereignty requirements. You may also be limited in your choice of cloud server as some data sovereignty regulations dictate where data can be processed.

"By year-end 2024, Gartner predicts that 75% of the world's population will have its personal data covered under modern privacy regulations."[4] To remain competitive, businesses and their leaders must adapt to the changing data landscape.



Data Localization

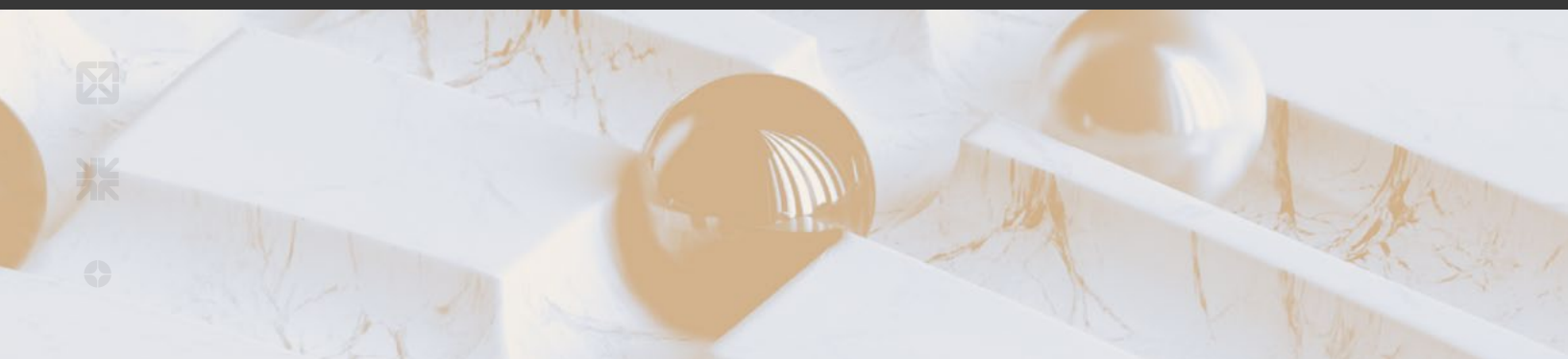
Data localization works contrary to globalization and hinders the open exchange of information. It requires a local approach to data, which limits an organization's ability to provide consistent services worldwide. Under many data localization laws, data must be stored and processed in the region it was collected, and it cannot leave its original jurisdiction. These requirements often lead to duplicate people and technology in individual markets.

Other data localization laws allow for some data movement outside its originating region, but only if organizations moving the data meet strict regulatory requirements. Data localization laws generally also include provisions for data storage and protection criteria for sector-specific and regulated sensitive data.

03

THE BUSINESS IMPACT OF MAINTAINING THE STATUS QUO

Companies that leverage new technologies and processes to comply with regulations and improve their operations will thrive. Those that fail to adapt to the changing data landscape, however, risk falling behind their competitors. **The financial cost of noncompliance is an estimated three times the cost of compliance.[5]**



BEYOND FINANCIAL COSTS, COMPANIES THAT MAINTAIN THE STATUS QUO FACE MANY OTHER ISSUES, INCLUDING:

POOR INDIVIDUALIZED CUSTOMER EXPERIENCES DUE TO PRIVACY CONSTRAINTS

Privacy constraints can severely limit an organization's ability to collect and process customer data, making it difficult to provide personalized customer experiences. This situation can lead to decreased customer satisfaction and loyalty. According to a recent Salesforce survey, 62% of customers expect companies to anticipate their needs, and 52% expect offers to always be personalized.[6]

SIGNIFICANT OR UNKNOWN DATA RISKS THROUGHOUT SUPPLY CHAINS

Cross-border business operations involve multiple stakeholders, business lines that rely on third parties, applications, technologies, and third-party providers. With so many possible kinks, it makes it challenging to identify and mitigate data risks throughout the supply chain. Without adequate risk management, organizations may be exposed to potential data security threats, financial losses, and reputational damage from third-party actions.

DUPLICATION OF TECHNOLOGY, PEOPLE, OR RESOURCES TO MEET SOVEREIGNTY CHALLENGES

Data sovereignty laws require organizations to store and process personal data within the region in which it was collected. Businesses often duplicate internal resources across regions or countries to comply with these regulations, ensuring data doesn't leave its original jurisdiction. This duplication adds unnecessary operational costs.

EXPENSIVE THIRD-PARTY DATA PROCESSORS FOR LOCALIZATION REQUIREMENTS

Many organizations rely on third-party data processors to meet their localization requirements. While compliance risk may diminish, security risks increase because you share data with another party. Third-party data processing increases business costs and introduces an unknown processing duration depending on their turnaround time.

INEFFICIENT AND COMPLEX DATA CONTRACTS AND AGREEMENTS TO MAINTAIN EXISTING BUSINESSES

Maintaining current cross-border business operations can be challenging due to the complexity of data contracts and agreements required to work in different countries and with third-party vendors. Navigating the intricacies of foreign laws and regulations to ensure compliance can be time-consuming and may require outside legal counsel at an additional cost. Inflexible contracts also make it difficult to respond quickly to changing regulations.

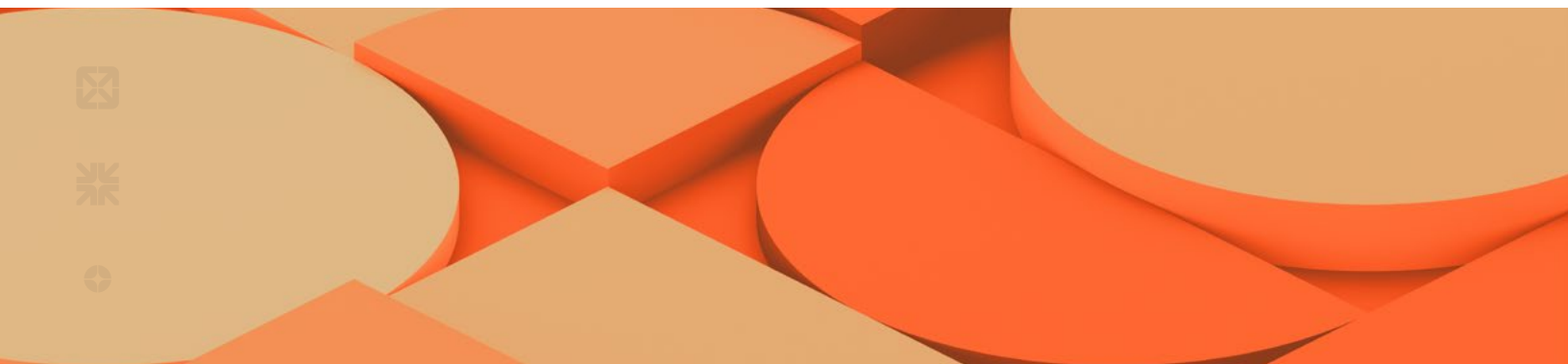
Companies that fail to adapt to the changing data landscape risk falling behind competitors that leverage new technologies and processes that comply with regulations and improve their operations.

04

THE LIMITATIONS OF TECHNOLOGY BUILT FOR THE PAST

"Around the world, new regulations are promoting data localization. To comply, companies must be agile in their investments, but those that get it right could increase their revenues and market share."[7]

LIMITS



Legacy technology is built for a static globalized world without data locality and regulatory considerations. It is not equipped to address today's dynamic privacy concerns and data localization requirements.

ACCESS CONTROL LISTS

Access control lists (ACLs) define user permissions and access rights to resources and files. While they effectively control data access to data that is sitting still, they cannot enable the use of the data outside of where the access is enforced (i.e., in the silo, at rest, etc.).

DYNAMIC DATA MASKING

Dynamic data masking (DDM) is a data protection method that replaces sensitive data with realistic fake values in real time. DDM introduces considerable risk because data at rest remains in clear text. While DDM is useful for protecting low-risk data in situations where simple masking on display is appropriate, it does not meet some of the more stringent requirements set by existing and growing regulatory requirements. Similar to ACL, DDM cannot maintain protection outside the enforcement area.

TRANSPARENT DATABASE ENCRYPTION

Transparent database encryption (TDE) is a database encryption method native to many database management systems (DBMSs). Although it may not impact the functionality of the database, the data is only protected at rest.

To remain competitive and relevant in this new landscape, businesses need to rethink their old data strategies and adopt new technologies that are more agile, decentralized, and customer-centric.

05

SEVEN COMPETITIVE ADVANTAGES OF BORDERLESS DATA™

The challenges of using outdated methods to manage newly emerging data privacy and security requirements are clear, but there are also benefits to be gained from adopting new cross-border data protection.

Today's businesses should look for data protection methods that adhere to localization and privacy requirements while allowing necessary data to be shared across any border.

ADVANTA

Competitive advantages of moving data freely across borders

1. INDIVIDUALIZED POSITIVE CUSTOMER EXPERIENCES

Maintaining current cross-border business operations can be challenging due to the complexity of data contracts and agreements required to work in different countries and with third-party vendors. Navigating the intricacies of foreign laws and regulations to ensure compliance can be time-consuming and may require outside legal counsel at an additional cost. Inflexible contracts also make it difficult to respond quickly to changing regulations.

2. ELIMINATED BUSINESS COSTS

By meeting privacy regulations and enabling Borderless Data™ instead of requiring the duplication of technology, resources, and people across regions to meet data sovereignty requirements, companies can eliminate the costs of that extra infrastructure and the people required to maintain it.

3. CLEARER DATA AGREEMENTS

Previously complex data agreements become much simpler when you have a straightforward way to protect data and comply with privacy regulations, such as data-centric privacy-enhancing technologies (PETs). In addition to data protection, these technologies provide oversight into data transfer agreements. Some existing agreements can even be tossed because you can eliminate third-party processors previously responsible for securing your information.

4. FEWER DATA RISKS AND NEW RISK VIEWS

In a Borderless Data™ environment, there are fewer data risks throughout the supply chain because sensitive data is protected at the field level in real time and never viewable by unauthorized users in the supply chain.

5. REVENUE GROWTH, MARKET EXPANSION, AND NEW MARKET OPPORTUNITIES

With more comprehensive analytics enabled by Borderless Data, companies are more agile and can quickly make more informed decisions regarding customers and products in existing markets. In addition, the ability to share data across new regions opens new markets worldwide. Companies can also securely onboard new vendors and solutions much faster than before.

6. CUSTOMER TRUST AND A REPUTATION FOR PRIVACY AND SECURITY

By complying with privacy and security regulations, organizations can protect customer data, build trust, and enhance their reputation, leading to increased customer loyalty.

7. IN-HOUSE DATA INVESTMENT VALUE

With adequate protection, organizations can again realize the economies of scale and time-to-market benefits of data flowing through in-house processing centers.

Borderless Data™ is the best mechanism to embrace these opportunities, overcome challenges, and become successful future enterprises. It creates significant opportunities for organizations, including revenue growth, reduced costs, and an improved customer experience.

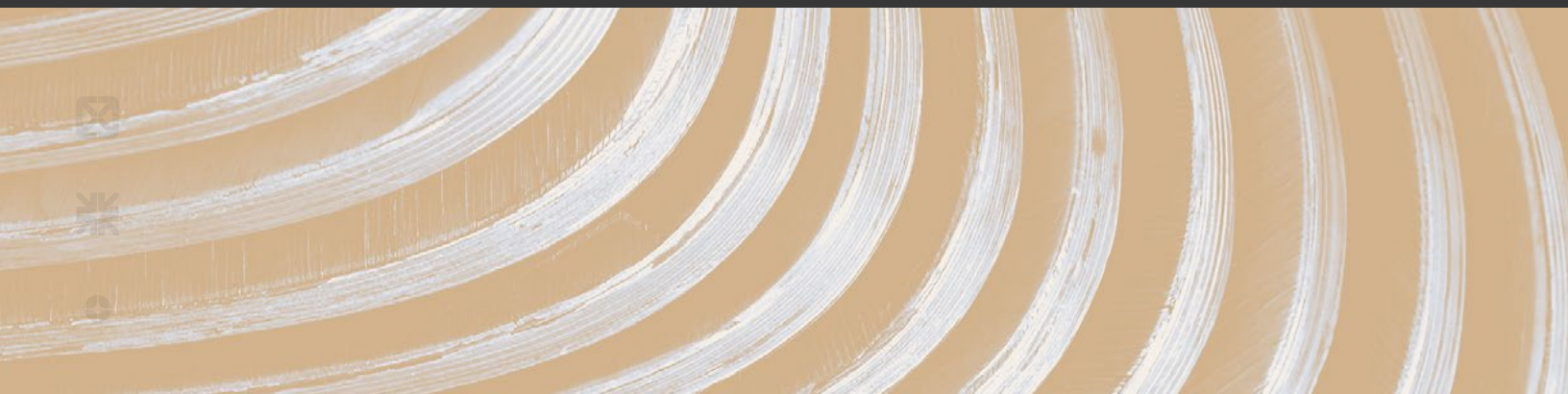
To enable Borderless Data, companies collecting sensitive data subject to privacy regulations de-identify it within its original jurisdiction while maintaining data integrity by preserving the data's type, length, and format. This data protection method meets even the most stringent privacy regulations currently in place, allowing the data to be moved outside its original jurisdiction for further analysis. Users outside the original jurisdiction cannot see the protected fields but can perform actions on the data.

Once the intended business outcome is achieved, the data is sent back to its original jurisdiction and reidentified. Results of the cross-border analysis can be realized within the original jurisdiction, enabled by Borderless Data.

06

EXPLORING A NEW APPROACH: SIMPLE FOUNDATIONS IN TECHNOLOGY

Centralized security control mechanisms are ineffective in a decentralized business environment. The changing world requires a new approach to data security and privacy that uses simple foundations in technology to help you quickly achieve compliance across an entire company and quickly enable new business in any country.



The Four Necessary Tenets of a Borderless Data™ Protection Solution

1. FRICTIONLESS ONBOARDING

- Automate on-ramps
- Leverage existing systems
- Provision as code with DevOps

Fully automated and scalable by design

2. DECENTRALIZED PROTECTION

- Isolate protection locally
- Optimize for performance
- Apply protection as close to the source as possible

Localized support on-premises and in the cloud

3. CENTRALIZED MANAGEMENT

- Standardize policies
- Aggregate auditing reporting
- Integrate with other data governance and security tools

Configure once and protect consistently

4. SELF-SERVICE INTEGRATION

- Inject dynamic business rules at runtime
- Standard API
- Democratize compliance

Seamless integrations for applications and data teams

Benefits of the Protegrity Approach Include:

FLEXIBLE AND ADAPTABLE SUPPLY CHAINS

SELF-SERVICE TO GO AT YOUR OWN PACE

EASE OF ADOPTION

TIME TO VALUE

PROVABLE, ADAPTABLE, AND CONTINUOUS COMPLIANCE

DATA INTELLIGENCE

The ideal Borderless Data™ protection solution is a single, self-service tool that is fully automated and provides an operationalized set of runbooks, accelerators, and auditable configurations out of the box.

It should make it easy to implement new policy changes to match new regulations, be quickly configurable to your unique protection needs, and ensure policy configurations are fully auditable.

07

THE PROTEGRITY DATA PROTECTION PLATFORM

Protegrity centralizes policy, audit, logging, and monitoring to secure sensitive data. Decentralized policy enforcement enables businesses to embed data protection for data in motion, at rest, and in use while allowing organizations to protect specific data types with a full range of protection methods.

PROTECT

Businesses need the ability to fine-tune data protection — at a field level — based on sensitivity and how it will be used. Extending this protection wherever data travels is crucial.

Protegrity Features

CENTRALIZED POLICY MANAGEMENT

FLEXIBLE AND ADAPTABLE SUPPLY CHAINS

LOCALLY-APPLIED DATA PROTECTION

ROLE-BASED ACCESS CONTROL

INDEPENDENT AUDIT LOGS

NATIVE INTEGRATION PER PLATFORM

PERFORMANCE OPTIMIZATION FOR EACH PLATFORM

SEPARATION OF DUTIES FOR SECURITY AND ADMIN

Protegrity's platform natively integrates with your platforms, regardless of the programs used or system locations (on-premises or in the cloud), including mainframes, cloud data warehouses, data types, and more.

08

BUSINESS USE CASES FOR BORDERLESS DATA™

"We have opened many use cases that did not exist or were not possible before Protegrity."

—Global Senior Vice President, Financial Services

The Protegrity Borderless Data Solution enables a variety of use cases across borders, industries, and business areas.

USE CASE

Replace data processors

Enhance the customer experience

EXAMPLE

A global bank wanted real-time fraud and risk analysis. Their processing centers were spread across several geographies, and some of the transaction data was unable to be sent to certain countries for processing to undergo analysis between transaction initiation and transaction completion due to corporate and regulatory requirements on customer data and cross-border restrictions. This was a significant issue for the bank's fraud and risk analysis capabilities.

Historically, the bank would have to work with local data processors, each within the jurisdiction of the customer data. This would fragment the fraud analysis, limit the customer experience, and create significant costs to the bank through additional third-party processor fees.

With Protegrity, the bank could tokenize the sensitive data in the customer's jurisdiction and successfully share customer transaction data across borders, enabling real-time fraud detection and risk analysis on a global scale, improving the customer experience, and significantly reducing costs.

BUSINESS VALUE

- Eliminate third-party data processing fees and reduce time to outcome
- Share data internally across business lines and geopolitical boundaries enhancing overall customer experiences

AREAS OF THE BUSINESS

- Fraud & Analytics

USE CASE

De-risk third-party vendors and data flows

EXAMPLE

An online psychologist service asks customers a series of questions to match them with their best-fit therapist. During this process, they collect personally identifiable information (PII), including date of birth and social security number. The psychologist service sends the collected data to a third-party vendor for analysis to determine which therapist each potential customer should be matched with. Because the service has Protegrity's solution, they can share tokenized data, so there is no risk that the third-party vendor won't follow the service's data privacy requirements and can still process the protected data.

Data protection happens automatically each time the data is sent, in real-time, as the data is being sent.

BUSINESS VALUE

- Extend your business safely and securely into third-party data platforms, products, and services

AREAS OF THE BUSINESS

- Data leaders, application owners, and innovation teams

USE CASE

Replace data processors
Enhance the customer experience

EXAMPLE

A global retailer has stores on several continents, including Europe, Australia, Asia, and North America. When customers make in-person purchases, data on both the customer and the purchase are collected and sent to the retailer's marketing team in North America for analysis with the goal of making additional product recommendations via email. This data collected may include both payment data and other personally identifiable information, such as customer name, age, and gender, through loyalty information. Corporate policy, industry security, and national privacy requirements prevent some of this data from being transferred into North America for processing.

By using Protegrity to protect each customer's payment and personal data, the marketing team is able to analyze customer purchases centrally in north America and make hyper-personalized recommendations to each customer based on their purchase history locally in their jurisdiction, thereby improving the experience and loyalty of that customer.

BUSINESS VALUE:

- Eliminate third-party data processing fees and reduce time to outcome
- Share data internally across business lines and geopolitical boundaries, enhance loyalty program insights, and accelerate data to new AI/ML models

AREAS OF THE BUSINESS:

- Marketing, HR, multinational business lines, and IT
- Data leaders, application owners, production management, and data science teams

09

PROTEGRITY'S EXPERTISE IN CYBERSECURITY

Protegrity has more than 20 years of expertise in the cybersecurity industry, operating in the biggest global markets and serving many Fortune 1000 companies.

OUR CUSTOMERS INCLUDE

8 OF THE 15 LARGEST GLOBAL BANKS WITH OVER 500 MILLION ACCOUNTS ACROSS 160 COUNTRIES

4 OF THE 10 LARGEST NORTH AMERICAN RETAILERS DRIVING OVER $1.1 TRILLION IN REVENUE

4 OF THE 8 LARGEST US HEALTH INSURERS PROTECTING 200+ MILLION PATIENT HEALTH RECORDS

#1 LARGEST GLOBAL CREDIT CARD ISSUER SECURING OVER 200+ MILLION CARD HOLDERS

NATIVE INTEGRATION PER PLATFORM

PERFORMANCE OPTIMIZATION FOR EACH PLATFORM

3 OF THE WORLD'S LARGEST GOVERNMENT AGENCIES COVERING OVER 450 MILLION CITIZENS

Protegrity enables customers to safely de-risk their data moving to third parties, the cloud, and SaaS environments while also realizing new market opportunities.

$50.79M Gross Savings Over Five Years

A multinational bank used Protegrity to protect sensitive customer transaction data as it traveled cross border from the bank to a SaaS CRM provider's marketing cloud to run advanced AI analytics for marketing programs.

$1.2B in Sales

An enterprise retail institution used Protegrity to protect sensitive customer account data when they off-boarded their commercial card management to a self-service SaaS platform. They were able to remove manual processes and reported improved customer satisfaction.

Modern, Mobile-Friendly Platform

A global financial institution used Protegrity to protect sensitive account data moved to their new wealth management SaaS platform, enabling the consolidation and retirement of legacy applications and an improved customer experience.

Revenue

Improved revenue from reduced time to value for applications and services and net-new income streams represents $13.7 million over 3 years.

— **"The Total Economic Impact™ Of Protegrity,"**
a commissioned study conducted by Forrester Consulting on behalf of Protegrity

Time to Value

By deploying Protegrity's platform, a top 5 global bank realized a 126% ROI, with an 8-month solution payback period.

— **"The Total Economic Impact™ Of Protegrity,"**
a commissioned study conducted by Forrester Consulting on behalf of Protegrity

Efficiencies

Application builders spend 55% less time on data security activities with Protegrity as the centralized solution.

— **"The Total Economic Impact™ Of Protegrity,"**
a commissioned study conducted by Forrester Consulting on behalf of Protegrity

We Protect Your Data Wherever You Store It

Here's a sample list of common platforms we support:

DATA WAREHOUSE PROTECTORS

Teradata (up to v16)
Greenplum
Netezza
Presto
Exadata
Athena
Snowflake (AWS and Azure)
Snowflake (Static Policy) (Cloud)
Redshift (AWS) (Cloud)
Redshift (Static Policy) (Cloud)
Yellowbrick (Cloud)
Exasol (Cloud)

BIG DATA PROTECTORS

Cloudera
Hortonworks
MapR
CDP Data Center
CDP AWS (Cloud)
EMR (Amazon) (Cloud)
Dataproc (GCP) (Cloud)
HD Insight (Azure) (Cloud)

[1] McKinsey Global Institute - Digital Globalization: The New Era of Global Flows
[2] McKinsey & Company - Localization of Data Privacy Regulations Creates Competitive Opportunities
[3] United Nations Conference on Trade and Development: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[4] Gartner - Gartner Identifies Top Five Trends in Privacy Through 2024
[5] Ponemon Institute: The True Cost of Compliance: A Benchmark Study of Multinational Organizations[6] Accenture Interactive 2019 Pulse Survey
[6] Salesforce State of the Connected Customer report: https://www.salesforce.com/resources/articles/customer-engagement/
[7] McKinsey & Company - Our Insights: Localization of Data Privacy Regulations Creates Competitive Opportunities

PROTEGRITY

The global standard for ubiquitous data protection.

ABOUT PROTEGRITY

Protegrity protects sensitive data — whatever it is and wherever it resides at any given moment. Our platform frees businesses from the constraints typically associated with accessing and protecting sensitive data, so they can create better customer experiences, make intelligent decisions, and fuel innovation. With Protegrity, organizations prevent non-compliance penalties, retain precision security, glean valuable data insights, simplify data governance, and improve operational efficiencies.

2021 Data Breakthrough Awards
"Data Security Solution of the Year"

2021 Cybersecurity Excellence Awards Gold Winner
for "Product Excellence in Data-Centric Security"

2018 SC Award Winner
for "Best Database Security Solution"

Want to De-Risk Your Data Use?

Contact Us!

info@protegrity.com
www.protegrity.com