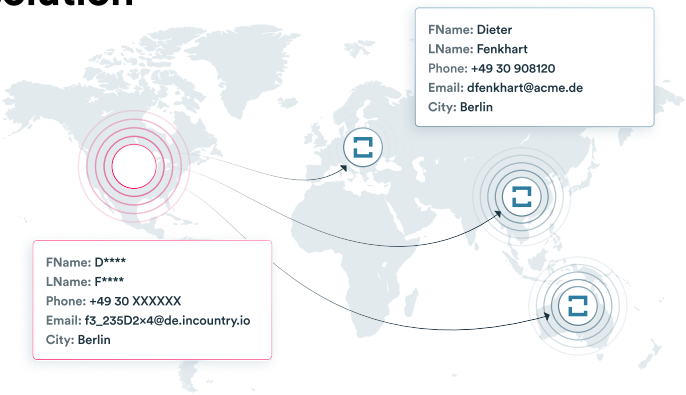
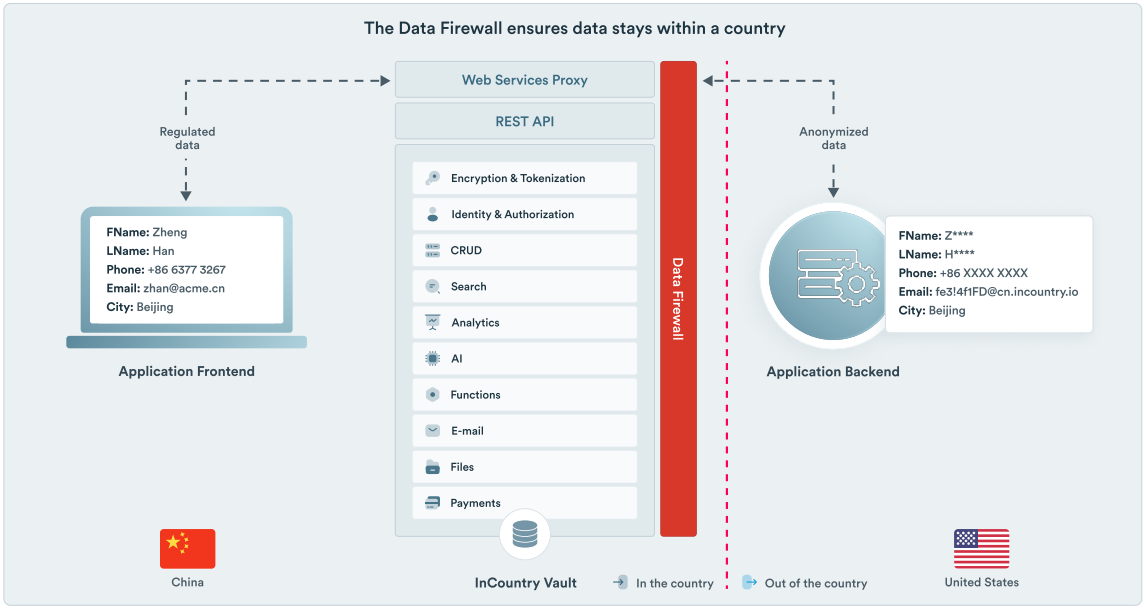
The enterprise ready data residency solution

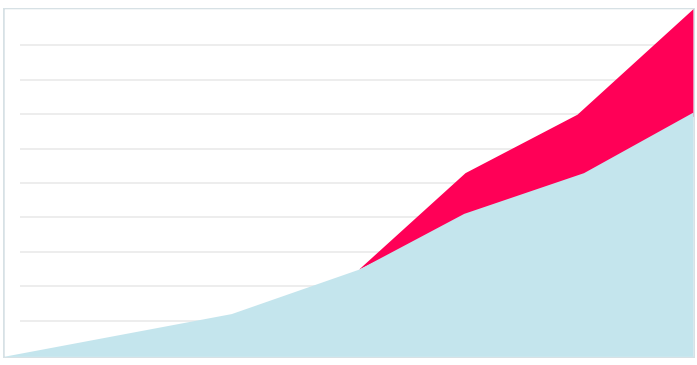
- → Run a global app with data isolated in each country
- → Easily add anonymized cross-border data transfers
- → Two points of presence in each country with active-active failover
- → SaaS, single-tenant on any cloud, AWS Outposts, and sovereign cloud options
- → Guaranteed messaging across unpredictable networks



Scale globally with local compliance

- → Data loss prevention across borders with data firewall that uses IP addresses and VPN detection to ensure data stays within a country
- → Detect PII leakage with AI that detects names and other identifying data from the origin country language
- → Detailed support for regulatory approval in complex jurisdictions
- → Downloadable audit logs track every event



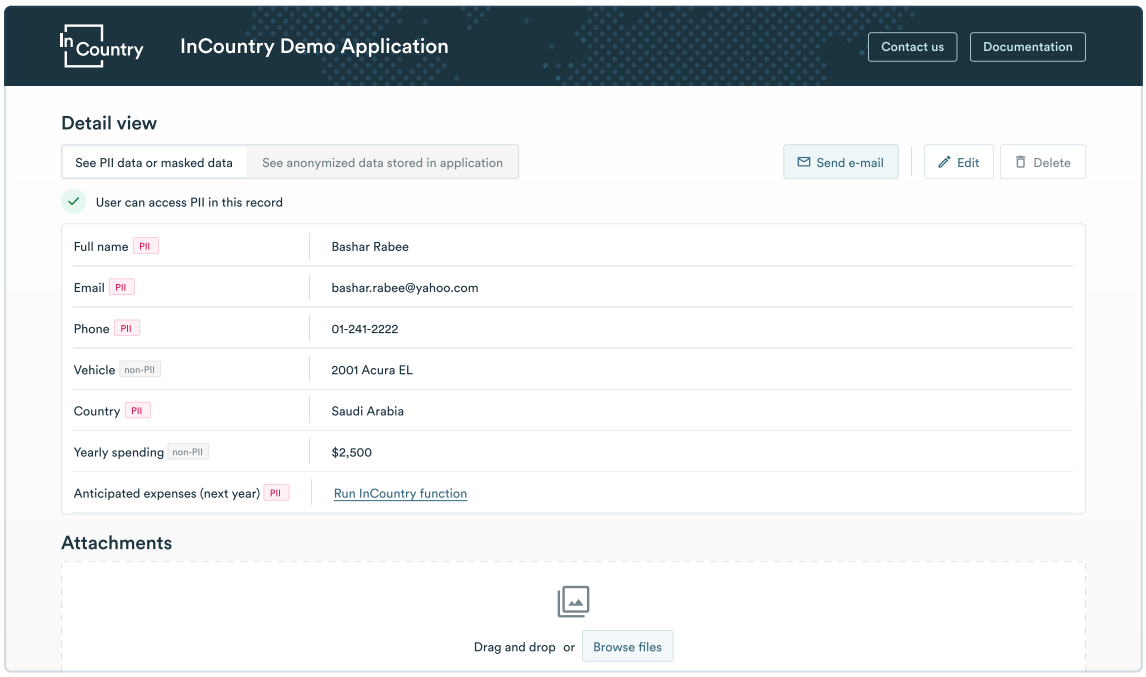


New countries Existing countries

Expand into high growth markets without worrying about data infrastructure

Focus on core customer and product experiences rather than building out new infrastructure and compliance globally. InCountry's Data Residency-as-a-Service helps multinational companies enter new markets and maintain compliance in existing markets.

Add InCountry data residency to your app and compliantly deploy to users globally



Benefits

IT: Simpler to use a global system instead of duplicating functionality across multiple systems.

Business: Global view of customers, tickets, and other business functions.

Compliance/Legal: Compliant and auditable in multiple jurisdictions and scales with changing regulations.

End-users: Continue to use a global SaaS system with full local visibility in each country.

CIO: Digitally transform to global SaaS systems while maintaining local data residency.

Extensive security and compliance

While InCountry manages the application's regulated data for a particular country, the source application continues to provide user authentication and authorizes all actions and data access. The InCountry data firewall's data loss prevention ensures that regulated data remains within a country and only permitted data crosses borders.

The source application and identity provider specify what countries a user can access and authorizes access to data with Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC). Using the existing application authorization model is critical as it can be very difficult to replicate and maintain cloned access policies, especially for applications with fine-grained access controls.

InCountry's detailed compliance mappings has enabled customers to gain regulatory approval in complex jurisdictions ranging from the Chinese Ministry of Public Security to the Saudi Arabian Monetary Agency.