TRUSTLOGIX

Unified Global Data Governance: A Telecom Success Story

See how TrustLogix unified global access governance to accelerate secure data sharing, strengthen compliance, and enable AI-driven innovation.

Industry:
Telecommunications

Geography:
Global

Challenges:

- Role-based access controls couldn't scale with the unified data architecture and business requirements
- Enforcement of privacy compliance on international data transfers
- Weak enforcement at the source left sensitive data exposed to security risk

Results:

- Unified access governance across 100+ data products, reducing policy silos
- Strengthened security and compliance with centralized, risk-based controls
- 30% productivity boost and 50% faster data product rollout through improved collaboration

Product Deployed:
TrustLogix Data Security Platform

Customer Profile

As one of the world's largest telecom providers, this global leader was investing in a harmonized enterprise data architecture to efficiently manage and securely handle sensitive data—from financial records and contracts to telemetry and customer experience metrics—across diverse applications and processes. The goal was to support complex analysis, enable telecom AI, and drive operational efficiency through data-driven decision-making at scale. By collecting data once and making it available across authorized applications, the company aimed to eliminate silos, reduce redundancy, and accelerate time-to-insight across the enterprise.

At the same time, a surge of targeted attacks on global telecom infrastructure exposed critical vulnerabilities in the industry. These persistent, coordinated threats sought long-term access to sensitive customer data, network configurations, and proprietary business intelligence. The incidents highlighted the need to secure data at its source—especially as sensitive information spanned cloud-native platforms like Snowflake and Databricks.

When Manual Governance Couldn't Keep Up

A growing challenge threatened to stall progress on both fronts. With hundreds of data products across its business and operational systems, manual data access enforcement was breaking down. Compliance teams were constantly firefighting, audits moved slowly, and security gaps were increasingly difficult to track. Without a global access governance framework to complement their unified data pipeline, the organization risked undermining the very efficiency and intelligence it set out to achieve. This lack of control left the company vulnerable—not just to internal inefficiencies, but to external threats exploiting the same weaknesses.

Internal audits revealed that without a standardized access control framework, business units implemented inconsistent controls based on subjective interpretations rather than objective requirements. Various scenarios were identified, including:

Network Data:

Customer data regulated by contractual terms often faced access bottlenecks. When approval requests raised uncertainty, the default response was denial, causing significant project delays.

Hardware Supply Chain Management Data:

Non-human identities (Application IDs, Functional IDs, Bot IDs) accessing supply chain analytics created security vulnerabilities. Audits uncovered blind spots where these automated identities can inadvertently expose sensitive data to embargoed users.

Corporate Internal Data:

Business-sensitive contracts and customer information lacked fine-grained access controls based on Market Area and Terms & Conditions flags, that can potentially cause compliance violations.

At the same time, overly rigid controls were hindering productivity, frustrating data teams, and straining alignment between security and business needs. The company needed a scalable, policy-aware access governance framework—one capable of protecting critical data without slowing down the organization.

The Shift to Scalable Data Security

To solve these challenges, the company deployed the TrustLogix Data Security Platform, built to unify and automate governance across hybrid environments. Immediate improvements included:

Granular Access Control across Business and Operational Data

TrustLogix replaced broad permissions with policy-based access controls (PBAC), ensuring employees and non-human identities (NHI) could only access data tied to their eligibility based on Contractual obligations, residency restrictions and project assignments. This eliminated cross-account visibility and fully segregated customer data —reinforcing trust and reducing the risk of data leakage.

Zero Trust Security for Data

Using Policy-Based Access Control (PBAC), the company enforced strict separation of duties within all the systems to enforce fine grained policies that separate human users and non-human identities. Teams could share Network data by enforcing policies that leveraged Organization information, Role of the identity and purpose for which data was being requested. Upholding customer privacy and ensuring Contractual obligations.

Geographic and Regulatory Compliance

Geography-based access controls ensured compliance with data residency laws and trade restrictions. EU data remained in-region, and embargoed-country employees were prevented from accessing U.S. systems—eliminating regulatory violations and legal exposure.

Secure Data Sharing and Cross-Border Governance

TrustLogix provided real-time oversight of Snowflake External Functions, allowing the company to monitor and control outbound data-sharing requests. This prevented unintentional cross-border data exposure and ensured secure, compliant data integration.

TrustLogix Data Security Platform: built to unify and automate governance across hybrid environments

Operationalizing Trust: Security That Accelerates the Business

The most significant outcome of implementing TrustLogix was the shift to a unified, global model for access governance—exactly what the company had been missing as it scaled its harmonized data ingestion architecture. Previously, access decisions were managed in silos, enforced manually, and riddled with inconsistencies. With TrustLogix, the company established centralized policy automation across its hybrid infrastructure, ensuring consistent, scalable enforcement for more than 100 data products spanning business and operational systems.

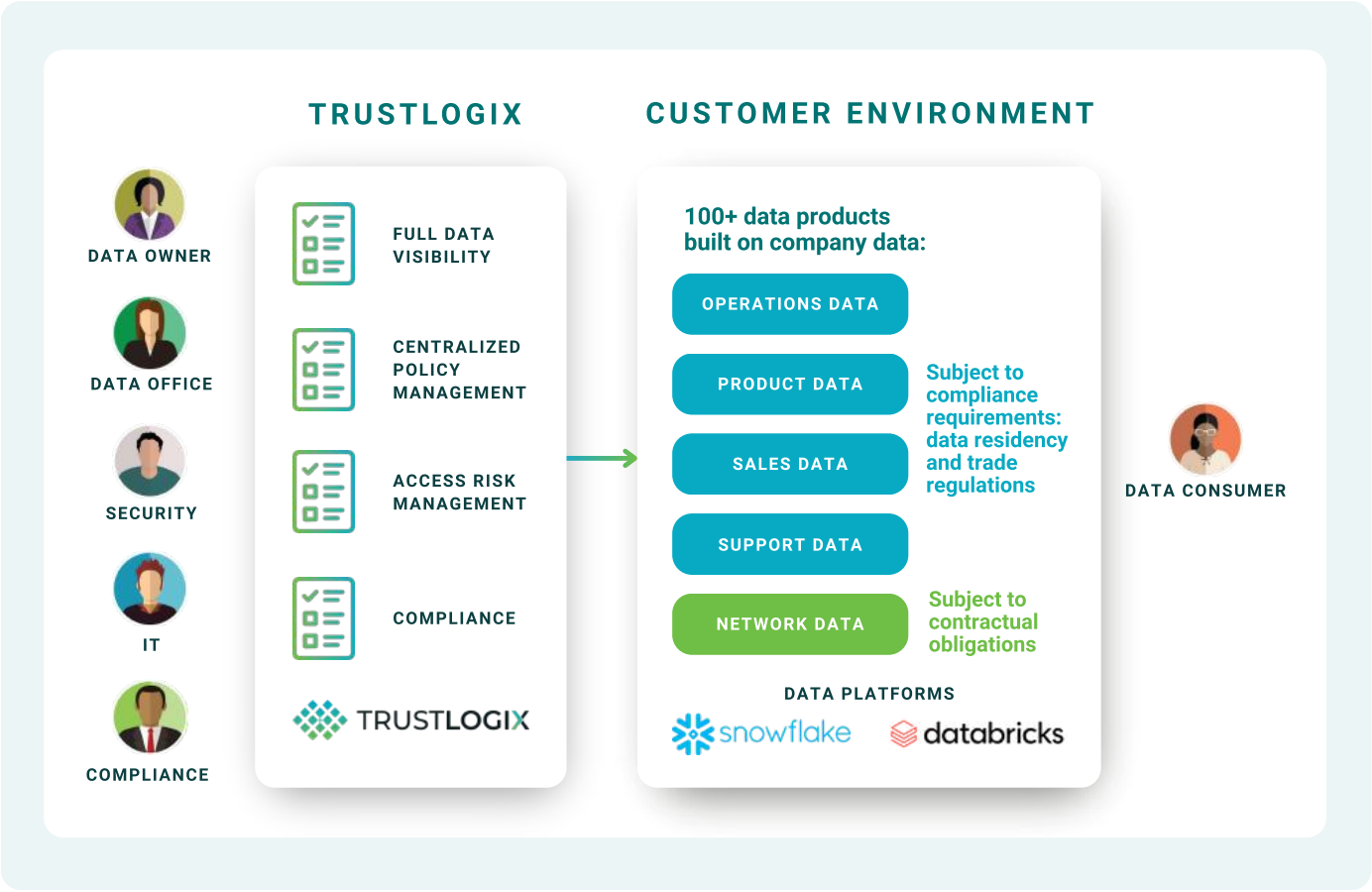

Figure: Teams across the organization have consistent visibility into data, allowing them to centrally manage and enforce access policies, data security, and compliance while efficiently granting appropriate access to data consumers.

This unified governance framework directly addressed the core challenges outlined at the start of the initiative: enabling secure, efficient data sharing; reducing access-related risk exposure; and accelerating the operational agility required for AI-driven decision-making. Policies defined by the data office could now be implemented automatically by IT, eliminating bottlenecks while maintaining full accountability. The business no longer had to choose between speed and control.

With policy standardization in place, the company gained real-time visibility into data activity across platforms like Snowflake and Databricks. This brought compliance, security, and data teams into alignment—enabling them to flag and resolve risky access quickly, while allowing authorized requests to move forward without delay. The result was a measurable increase in execution speed: projects like launching new cross-platform data products were completed in half the time, contributing to a 30% improvement in team productivity.

At the same time, the company dramatically improved its security posture. End-to-end access visibility enabled continuous risk assessment, helping the organization detect policy drift and maintain compliance with data residency and privacy regulations. AI-driven insights strengthened control even further by identifying patterns of excessive access and emerging gaps before they became exposures.

What had once been a barrier became a business accelerator. TrustLogix helped the organization operationalize Zero Trust principles—securing data at its source with context-aware, least-privilege access across cloud and on-prem environments. For a global telecom provider, this shift meant more than reducing risk. It meant transforming compliance from a constraint into a competitive advantage—and turning data governance into a foundation for innovation, resilience, and trust.

Policies defined by the data office could now be implemented automatically by IT, **eliminating bottlenecks while maintaining full accountability**. The business no longer had to choose between speed and control.

TrustLogix
800 W. El Camino Real, Suite 180
Mountain View, CA 94040

hello@trustlogix.io
www.trustlogix.io