IMMUTA
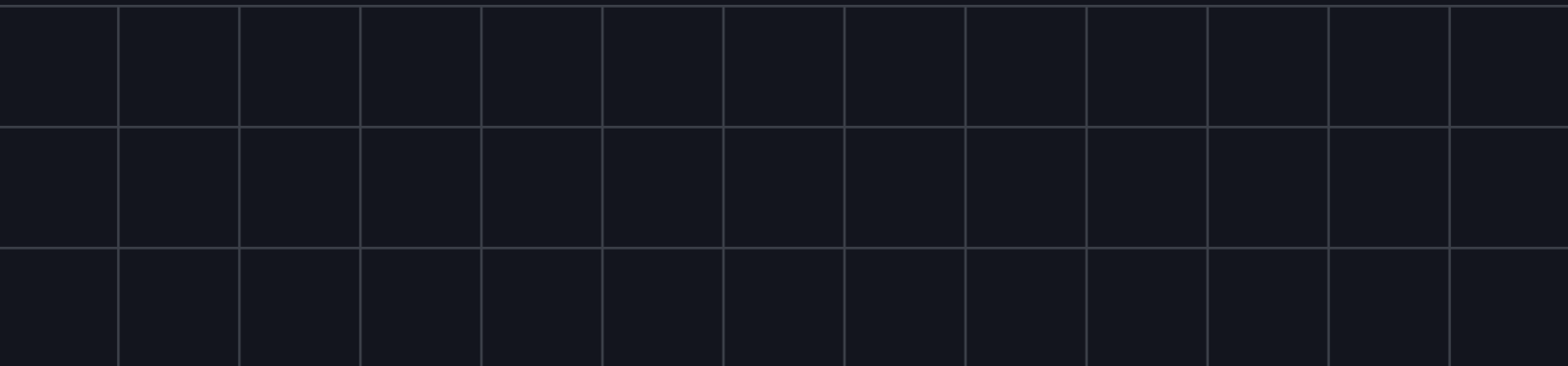
National law enforcement agency toughens fight against crime with Immuta

About the National Law Enforcement Agency

A European government's law enforcement agency has continually looked for ways to improve the country's fight against serious and organized crime.

The agency has a broad area of responsibility, including drug trafficking, human trafficking, cybercrime, economic crime, and firearms trafficking. Its 7,000 employees work closely with other government agencies, international law enforcement agencies, and private companies to combat these threats. Like many large enterprise organizations, this agency recognizes the importance of data in achieving its mission.

Architecture

IMMUTA

amazon REDSHIFT

aws | **S3**

okta

jupyter

Industry

Law Enforcement

Key Takeaways

- Inability to secure growing amounts of sensitive data impeded timely access to it

- Fine-grained access control and easy auditability meet compliance requirements

- Faster data delivery provides more actionable intelligence to better fight crime

Challenge

The law enforcement agency was concerned that data access was not well managed or governed as it migrated its data from on-prem systems to the cloud. Data stored in S3 buckets and Redshift were difficult to manage at a granular level with native controls, slowing down access. Data sets were either completely masked or entirely exposed. In fact, the agency suspended data delivery to the operational side of the organization until reliable data security could be put in place.

The agency sought new ways to create scalable, flexible, and secure data platforms that would enable its business teams to more quickly and reliably analyze sensitive data subject to appropriate governance, control, and auditing. By nature, intelligence data can quickly become stale; faster access to this data would improve the agency's efficacy in fighting crime. To support this strategy, the agency enlisted the services of technical consultancy Contino to identify, evaluate, and select the most fitting technology solution to meet the agency's data security and access requirements.

Solution

The Immuta Data Security Platform was selected as the best solution for a few key reasons: real-time policy orchestration, fine-grained access control, and operational efficiencies from faster data access.

First, Immuta is capable of consistently managing data across multiple environments, both in the cloud and on-prem. It natively supports AWS Redshift, Amazon's massively parallel columnar-based cloud data warehouse solution that is part of Contino's wider architecture for the law enforcement agency's AWS Data Platform. For on-premise data, Immuta supports integrations with AWS Athena and Trino, allowing the agency to access slower moving data sets held in the S3 data lake.

Secondly, Immuta enables secure, scalable data access with automated controls that are dynamically applied at query time. It allows access for end users through attribute-based access control (ABAC), which grants access to specific tables, rows, and columns based on user, object, environment, and purpose-based conditions. With sophisticated data masking and privacy enhancing technologies (PETs), Immuta dynamically enables authorized users to see the existence of a column but not necessarily the data contained therein.

Since Immuta is architected to natively integrate with the leading cloud vendors, Contino was able to quickly deploy the solution into the agency's AWS production environment. Data is ingested into the ecosystem from a variety of data sources: intelligence-acquired data, public data, and data from other government agencies. This is processed from S3 into Redshift through several routes, while data access control is managed by a non-technical team of data governors using Immuta policies, tags, and attributes.

Finally, with Immuta's advanced data privacy controls, the agency can accelerate internal and external data sharing–all while meeting data access auditing and reporting requirements. Faster delivery of new data sources provides more actionable intelligence to operational teams working to ensure the safety of the country's residents.

Outcome

With Immuta's scalable data security in place, the law enforcement agency has unlocked the velocity and value of the mountains of intelligence data it collects. Faster data access and analysis enables the agency to more successfully fight and prevent crime.
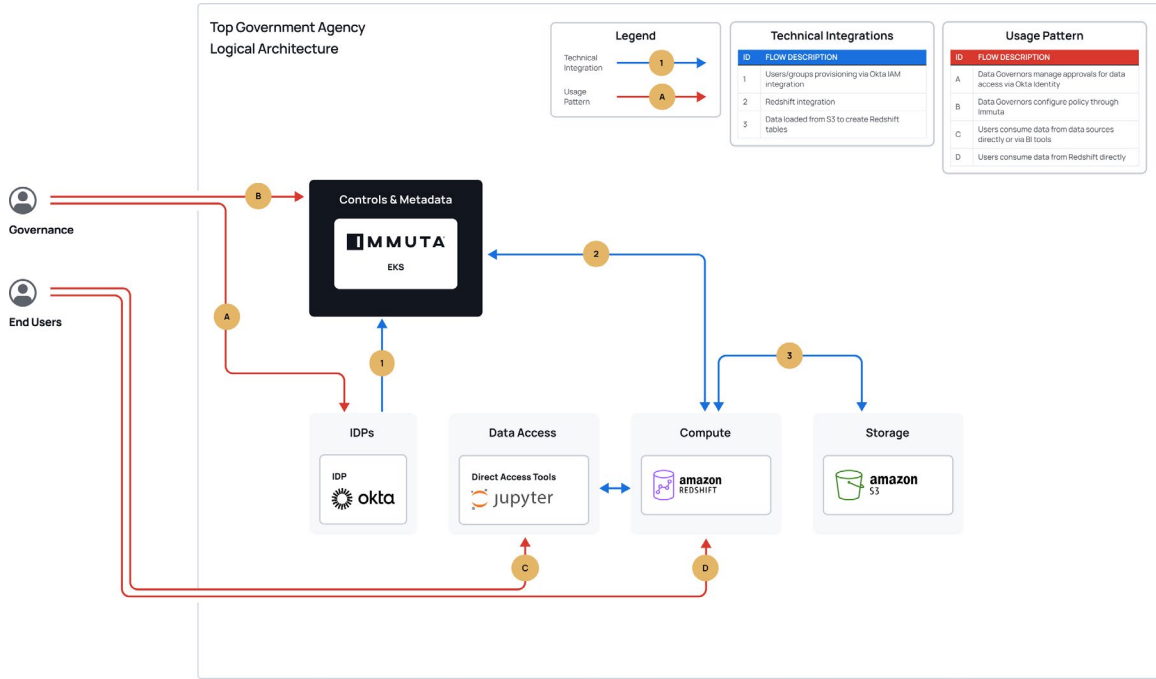
Compared to a traditional role-based access control (RBAC) approach, ABAC removes the burden from directory administrators and empowers data owners and data governance staff to own and manage access to their data. This greatly reduces the time taken to grant access to 50 data sources containing hundreds of tables. These operational efficiencies enabled the agency to reduce its number of data access management FTEs from 12 down to four.

"Given our need to share data with users and partners, Immuta was clearly the right choice both technically and from a business-user perspective," an agency spokesperson said. "It meets our technical requirements with no query performance degradation; is intuitive and easy to use for Data Governance Officers; and provides the level of insight and auditing to meet our governance and compliance needs."

The agency also has the ability to temporarily suspend all data access controls in the most dire circumstances. In cases of extreme urgency, users across the organization can be granted unrestricted data access to tackle imminent threats. However, Immuta still records rich audit logs of all activity for review once emergency situations are resolved.

All in all, the Immuta Data Security Platform allowed the agency to create a secure, flexible, and scalable data environment that allows its business teams to quickly and reliably analyze sensitive data. This has led to faster, more accurate decision-making in a well-governed, controlled, and audited manner. In addition, having the ability to query data in a fully structured and transformed format means that data scientists have to do far less data wrangling and can concentrate on higher-value activities in their mission to make the country a safer place for all.

Architecture

Top Government Agency
Logical Architecture

Legend

Technical Integration	→①→
Usage Pattern	→Ⓐ→

Technical Integrations

ID	FLOW DESCRIPTION
1	Users/groups provisioning via Okta IAM integration
2	Redshift integration
3	Data loaded from S3 to create Redshift tables

Usage Pattern

ID	FLOW DESCRIPTION
A	Data Governors manage approvals for data access via Okta Identity
B	Data Governors configure policy through Immuta
C	Users consume data from data sources directly or via BI tools
D	Users consume data from Redshift directly

Governance

End Users

Controls & Metadata

IMMUTA
EKS

IDPs
IDP
okta

Data Access
Direct Access Tools
Jupyter

Compute
amazon REDSHIFT

Storage
amazon S3

About Immuta

Immuta enables organizations to unlock value from their cloud data by protecting it and providing secure access. The Immuta Data Security Platform provides sensitive data discovery, security and access control, data activity monitoring, and has deep integrations with the leading cloud data platforms. Immuta is now trusted by Fortune 500 companies and government agencies around the world to secure their data. Founded in 2015, Immuta is headquartered in Boston, MA.

■IMMUTA