

Why The Future Of Data Use Is Automated

In today's data ecosystem, automation is the only way to achieve efficient, scalable workflows. Not only does automated data access control remove the burden of manual processes, but it ensures policy enforcement is repeatable, consistent, and auditable.

Data is the lifeblood of modern governments. The insights it provides to public sector agencies can enable everything from more accurate budget forecasting to identification of public health threats. Yet, agencies continue to underutilize their data due to hesitations about modernizing from legacy systems to cloud data platforms. The change management and perceived risk of relocating data to the cloud prevents many teams from adopting technologies that could get more data into the hands of more users.

Agencies are starting to realize the limitations of legacy systems — and those that haven't yet soon will. As more data is generated, collected, and stored for analysis by more users, these siloed systems



Nancy Patel

Vice President of Public Sector
Immuta

are unable to scale, limit sharing, and prevent fusion of data to produce new insights. In an environment where real-time access to quality data is mission critical, manually managing access requests puts a burden on data stewards' time, while significantly delaying speed to access for

data consumers. Consequently, agencies are less able to respond to time-sensitive data needs that, in some cases, could mean life or death.

Compounding the problem, the ongoing proliferation of data laws like the CCPA and GDPR, require data teams to ensure that access policies are compliant, data is secure, and access can be audited at any time. It may seem like table stakes, but with a rapidly expanding amount of data, users, and regulations, this becomes unmanageable — particularly with legacy systems. This inhibits data access for internal users and blocks efficient interdepartmental data sharing, which is essential for a functioning government.

It's time for a new approach: automation.

Unlocking More Data Through Automation

Reservations to automating data access controls are understandable. Many stakeholders feel that automation means relinquishing the control that comes with manual human inspection. The fact is, automated processes can (and should) still be verified by humans, but they eliminate human error and remove time delays. After all, mistakes are bound to happen when manually combing through high volumes of access requests and resolving them as quickly as possible.

In today's data ecosystem, automation is the only way to achieve efficient, scalable workflows. Not

only does automated data access control remove the burden of manual processes, but it ensures policy enforcement is repeatable, consistent, and auditable. A decade ago, this approach might not have been necessary.

However, with exponentially more data, threats, and often, budget constraints, automation is no longer a nice-to-have — it's essential. Removing the guesswork and manual processing from access management is the key to unlocking more data without additional overhead or risk.

Scaling Secure Data Access with Dynamic Controls

Automation is the first step in improving data access management, but equally important is how that automation is put to use. Legacy approaches like role-based access control (RBAC) are simply not built for the future of data use, and will only hold agencies back from reaching data-driven objectives.

For this reason, data teams across the public and private sectors are turning to more granular [attribute-based access control](#) (ABAC). This dynamic, scalable framework has been recommended by [NIST](#) as the preferred method for managing who can access what data, when, and for what purpose.

Unlike RBAC, [ABAC](#) makes context-aware access decisions at query runtime based on user, data object, environment, and action-specific attributes. Since access is not tied to predetermined user roles, ABAC delivers fine-grained access control with minimal maintenance, so data teams are able to efficiently get more data to the users who are authorized to see it. Compared to RBAC, ABAC has been shown to [reduce policy burden](#) by 75x.

Agencies that invest in automated data access platforms will be in the best position to succeed with data now and in the future.

Plain Language Policy Authoring

Data access control platforms like Immuta centralize policy management into a single control plane that is abstracted from data platforms, enabling consistent policy enforcement across all technologies in the data stack. This applies to tools built for analysts with skills across the spectrum, from point-and-click dashboards in Business Intelligence Tools to advanced notebooking environments, to build state-of-the-art machine learning models.

Immuta's plain language [policy authoring](#) allows public sector data teams to create easily understandable policies in compliance with any federal or agency-specific regulation, which in turn streamlines approval workflows with legal and compliance stakeholders. Finally, continuous monitoring and on-demand auditing simplify the process of proving compliance and proactively responding to any data anomalies. Protecting data dynamically at the data layer streamlines accreditation efforts and ultimately leads to fielding mission critical analytics, dashboards, and insights more rapidly.

The ability to maximize data privacy and utility is a core focus for public sector data teams, and with the right tools it's not difficult to achieve. Agencies that invest in automated data access platforms will be in the best position to succeed with data now and in the future. ■