



SOLUTION BRIEF

How Immuta Enables Zero Trust Architectures

In 2009, a total of 12.4 million recorded malware infections affected consumer data. Just over a decade later, this number has surpassed 812 million. With many businesses relying on work-from-home models and cloud infrastructures, the risk of security breaches has increased exponentially.

Traditional perimeter-based information security is no longer a viable option in the current decentralized workforce. With employees accessing company information from varied locations outside of the office, cyber criminals have more opportunities to attack and compromise networks containing sensitive data.

TRUST NO ONE

The Need for Zero Trust

One increasingly popular response to this risk is a Zero Trust architecture. The Biden Administration's [Executive Order on Improving the Nation's Cybersecurity](#) mandates Zero Trust for both federal agencies and private organizations.

This approach eliminates implicit trust associated with traditional systems, and instead follows the "never trust, always verify" principle. Zero Trust builds its security measures on the assumption of breach inevitability. Starting with minimal access and consistently re-verifying users helps establish trust both holistically and across applications and functions.

THE PROBLEM

Zero Trust architectures can conflict with the need for self-service data analytics.

If users need to constantly verify their identities at every turn, analyzing data can become tedious. In turn, this slows the time to access and insights that organizations desire. The key question becomes:

How do we efficiently empower users for self-service analytics, while ensuring effective data security in a Zero Trust model?

WHY IMMUTA

Immuta is the universal cloud data access control platform, providing one platform to automate access control for any data, on any cloud service, across all compute infrastructure.

Users can create plain English policies that span cloud platforms, allowing for uniform application of rules and regulations.

By acting as an integrated layer of automated policy enforcement, Immuta applies security measures without slowing down data consumers. This functionality lets organizations meet Zero Trust security standards and successfully protect against internal and external threats without compromising their employees' accessibility.

How Immuta Helps

Organizations need to control access to sensitive data so they can increase security, compliance, and cloud data platform ROI. Immuta is the leader in automated data access, enabling data teams to increase permitted use cases by 4X, make data access 100X simpler to manage, and allow access to sensitive data in minutes, not months. Immuta's comprehensive cloud data access control is built for DataOps environments:



UNIVERSAL DATA CLOUD COMPATIBILITY

Immuta's native integrations with every major cloud data platform and service ensure data engineers have uniform data protection across preferred cloud analytics and data storage platforms.



SENSITIVE DATA DISCOVERY & CLASSIFICATION

Immuta automatically scans cloud data sources, detects sensitive data, and generates standard tagging across multiple compute platforms, reducing risk and improving data utility.



ADVANCED DATA MASKING & ANONYMIZATION

Immuta's advanced privacy-enhancing technologies (PETs) accelerate data access and data science projects by dynamically masking and anonymizing sensitive data, and are supported by Immuta's expert team of legal engineers.



SCALABLE, ATTRIBUTE-BASED ACCESS CONTROL

Immuta's policy builder empowers data engineers to govern cloud data use with automated policies – scaling user adoption, eliminating approval bottlenecks, and providing trust with security and governance teams.



DYNAMIC POLICY ENFORCEMENT & AUDITING

Immuta enforces data access control policies automatically, on every query, and captures rich audit logs so data teams can ensure data is used securely and compliantly according to rules and regulations.

Immuta's breakthrough innovation makes it the leader in automated data access, providing universal cloud data access control to meet the requirements for all data teams.

To see how Immuta can help your data team, request a demo.

REQUEST A DEMO

The screenshot shows the 'Global Policy Builder' interface. It includes a search bar at the top with the text 'Search Immuta'. Below the search bar is a sidebar with various icons. The main content area is titled 'Global Policy Builder' and contains three sections for configuring a policy:

- What's the name of this policy?** with a dropdown menu showing 'CCPA Re-identification Rule'.
- How should this protect the data?** with a dropdown menu showing 'Mask', 'columns tagged', and 'Discovered > PII'. Below this, there are more dropdowns: 'using hashing', 'for everyone except', and 'when user possesses attribute in Roles Data Scientist'.
- Where should this policy be applied?** with a dropdown menu showing 'On all data sources'.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Create Policy'.

