Saviynt

Solution Guide

Saviynt Identity Security Sovereign Cloud

Extend jurisdictional control to the identity layer with Saviynt's tiered, AI-ready sovereign cloud for governments, critical infrastructure, and regulated enterprises.

Most digital sovereignty strategies focus on data and infrastructure. They leave out identity. If the system that governs who can access your data is compromised or subject to foreign legal reach, keeping the data within your borders doesn't fully protect you.

Saviynt's Identity Security Sovereign Cloud applies the same jurisdictional controls to user profiles, credentials, and access logs that other sovereign solutions apply to data and infrastructure. It's offered across three tiers, Data Residency, Sovereign Cloud, and Air-Gapped Cloud, so organizations can match their investment to their actual level of risk instead of adopting a single fixed model.

- **Identity sovereignty, the fourth pillar most strategies overlook**
- **Three tiers, from Data Residency to Air-Gapped, matched to risk**
- **Local ownership and staffing, governed entirely under your jurisdiction**
- **Full platform parity across human, non-human, and AI identities**
- **Reduced exposure to foreign legal demands and service disruption**

Own Your Digital Sovereignty at Every Layer

Identity Is the Missing Layer in Most Sovereignty Strategies
Digital sovereignty is usually described in terms of three pillars. Data sovereignty means data stays within national borders. Technical sovereignty means the technology stack is independent of external control. Operational sovereignty means the people running the service can be trusted.

There's a fourth pillar that gets less attention: **identity sovereignty**, which governs whether trusted people and systems under local jurisdiction control access to all of the above. National ID numbers, security clearances, biometrics, and access histories are some of the most sensitive data an organization holds, and they map exactly who can reach what. A sovereign cloud that doesn't secure this layer leaves its most operationally important piece exposed.

A Tiered Model Matched to Risk
Different types of organizations require different sovereignty solutions. For example, a national defense ministry and a social services agency face different threat models and regulatory obligations. Saviynt offers three tiers so organizations can choose the level that fits their actual exposure.

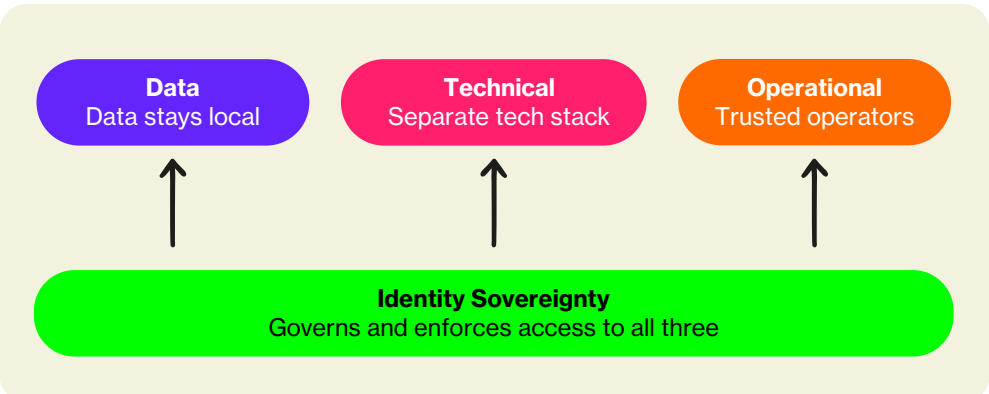
- Data Residency, the foundational tier, keeps all data, including identity governance data, within a chosen region under requirements like IRAP, GDPR, and the EU-US Data Privacy Framework. Local support is available in the EU, UK, and US.
- Sovereign Cloud is locally owned, locally staffed, and locally governed. Saviynt's FedRAMP-authorized environment, live since 2019, is an example, with capabilities extending toward US DoD IL5 requirements.

- Air-Gapped Cloud is the highest tier, built for critical national infrastructure and defense organizations. It's disconnected from the public internet and inaccessible even to Saviynt, operated by cleared local employees from a secure facility.

A Track Record, Not a Roadmap

Saviynt's Sovereign Cloud has full feature parity with its commercial identity platform, covering human, non-human, and AI identities. Saviynt has been offering sovereign cloud solutions since 2019.

Saviynt Sovereign Cloud	Organizational Benefit
Identity Sovereignty (the fourth pillar)	Covers the layer that data, technical, and operational sovereignty models leave out
Tiered model (Data Residency, Sovereign Cloud, Air-Gapped)	Lets organizations match spend to their actual risk level
Feature parity with commercial platform	Full IGA, PAM, and AAG, including human, non-human, and AI identities
Local ownership, staffing, and jurisdiction	Reduces exposure to foreign legal demands, interference, and service interruption



- **A tiered sovereign cloud model built around identity, not just data**
- **Data residency in production today across IRAP, GDPR, and EU-US DPF regions**
- **A sovereign cloud tier that's locally owned and staffed, live since 2019**
- **An air-gapped tier for critical infrastructure and defense, cut off from the public**

Next Steps

Reach out to your Saviynt representative to discuss which sovereign cloud tier fits your organization's risk profile and jurisdictional requirements.

About Saviynt

Saviynt is the identity security platform built to secure the modern enterprise. With Zuma, its complete AI security platform, Saviynt helps organizations build, run, and scale AI with confidence. The world's leading brands trust Saviynt to reduce risk, improve visibility, and support compliance while enabling business agility. For more information, please visit **www.saviynt.com.**

Saviynt

Headquarters
1301 E El Segundo Blvd, Suite D
El Segundo, CA 90245
USA

310.641.1664
info@saviynt.com
www.saviynt.com