adaptcx

DECISION GUIDE

Sovereign Deployment vs. SaaS

A decision guide for public-sector AI - how to choose the deployment model that belongs in your environment.

A practical framework for security, legal, cloud and procurement teams evaluating regulated AI. AdaptCX builds on an earlier, smaller version. The expanded platform has not yet been deployed in full at a customer site.

GUIDE MAP

Contents

What's actually being decided Your legal and procurement teams want a cleaner data processing agreement default is Sovereign Deployment

SECTION

What's actually being decided

Every AI procurement conversation in the public sector hits this fork: vendor-hosted SaaS, or Sovereign Deployment - where the vendor's software runs inside your cloud organization. The question sounds operational. It is actually architectural - and the wrong choice cascades through your security boundary, contract structure, and three-year operating cost. This guide separates the decision into the dimensions that matter: data sensitivity, regulatory posture, cloud team bandwidth, contract structure, and consumption economics. We give you a framework that produces a reasoned default for any given workload, and we name the cases where the default is wrong. Note on terminology: the broader market calls the in-tenant model "Sovereign Deployment" (Sovereign Deployment). We use Sovereign Deployment throughout this guide because it captures the value the model actually delivers - data sovereignty for the buyer - rather than the mechanics of how it's deployed. The two terms are interchangeable; we'll note where the distinction matters When SaaS is correct SaaS is the default in commercial enterprise software for good reasons - vendor operates the platform, ships features continuously, owns scaling. For some public-sector AI workloads, the same logic applies. SaaS works when - The data is non-sensitive - public information chatbots,

SECTION

What's actually being decided (continued)

anonymous citizen feedback, marketing-site assistants - Your organization is in pre-production exploration with synthetic data and no production traffic yet - The vendor independently holds the certifications you need (FedRAMP Moderate or High, StateRAMP, HITRUST) at your impact level - and you're willing to inherit their continuous monitoring posture and personnel screening - Your projected consumption is light enough that the vendor's per-user fee is cheaper than running the infrastructure yourself When Sovereign Deployment is correct Sovereign Deployment means the vendor's software runs inside your cloud organization, under your IAM, with your encryption keys. You provide the cloud estate; they provide the software and ongoing engineering. Sovereign Deployment works when - Your data has sensitivity (PHI, PII, CJI, FTI, sealed records, regulatory metadata) - You already operate a compliant cloud environment - and want to keep using it - You expect production traffic at meaningful scale (above $8K/month in equivalent cloud spend)

SECTION

Your legal and procurement teams want a cleaner data processing agreement

- - You want the option of inheriting your existing security boundary rather than expanding it Sovereign Deployment is the default for any workload involving regulated data. It is not the default for proof-of-concepts, pilots, or non-sensitive applications. The five dimensions of the decision Data sensitivity If the data is regulated - covered by HIPAA, FERPA, CJIS, or any state-level analog - the default is Sovereign Deployment. The exception is when the SaaS vendor independently holds certification at your impact level and you've reviewed their boundary diagram. For non-regulated data, SaaS is fine Existing cloud posture If your organization already runs on a compliant cloud environment - your existing GCP, AWS, or Azure tenancy with the right control mappings - Sovereign Deployment inherits that posture by construction. You don't need to authorize the vendor separately. If you don't have a compliant cloud yet, SaaS-with-vendor-certification may get you to value faster, at the cost of being locked into the vendor's authorization for the lifetime of the contract. Cloud team bandwidth Sovereign Deployment requires a quarterly architecture review with the vendor and an internal cloud operator. If your cloud team is at zero capacity, SaaS removes that work - but transfers it to a vendor relationship review instead. Be honest about

SECTION

Your legal and procurement teams want a cleaner data processing agreement (continued)

which kind of work your team handles better. Contract simplicity Sovereign Deployment contracts are typically simpler. The vendor licenses software; you operate it. The data processing agreement is shorter because the vendor isn't a processor in the GDPR sense. SaaS contracts have more terms because the vendor is doing more on your behalf - including being a data processor with all that entails. Consumption economics Conventional wisdom says SaaS is cheaper because the vendor amortizes infrastructure across customers. This is true at small scale and inverts above ~$8K/month in equivalent cloud spend. Once your AI traffic generates meaningful Gemini, AlloyDB, Cloud Storage, and Document AI consumption, the per-customer cloud spend in Sovereign Deployment is comparable to or below the all-in SaaS price - and you capture every committed-use discount you've already negotiated. Decision framework

SECTION

default is Sovereign Deployment

Walk through the five questions in order. If your answer to any is Sovereign Deployment, the - Is the data regulated? PHI, PII, CJI, FTI, sealed records? - Do you have an existing compliant cloud environment you'd prefer to use? - Do you expect production traffic above $8K/month equivalent? - Does your legal team prefer a clean data processing relationship? - Do you have at least 0.25 FTE of cloud-team bandwidth for vendor architecture reviews? If yes to two or more, Sovereign Deployment. If yes to none, SaaS is fine. If yes to one, the answer is workload-specific - separate regulated traffic from non-regulated traffic and route them differently. What we recommend (and why) Sovereign Deployment is the intended architecture for customer-controlled environments. AdaptCX builds on an earlier, smaller version. The expanded platform presented here has not yet been deployed in full at a customer site. Capabilities and illustrative workflows should be evaluated against the scope of a specific implementation. Review identity, encryption, service dependencies and audit ownership before implementation.

NEXT STEP

Continue the conversation

If this guide surfaced questions about your architecture, compliance posture, deployment model or AI operating model, talk with an AdaptCX engineer or solutions architect.

Talk to AdaptCX →