

INDUSTRY BRIEF · FOR CIO · CISO · CTO · HEAD OF DATA · CCIO

GOVERNMENT AI. **AIR-GAPPED.** SOVEREIGN.

Public-sector AI cannot depend on a retrieval vendor reachable over the commercial internet. XERJ is a single Rust binary that runs inside a sealed rack, a SCIF, or a national-cloud enclave — with every retrieval primitive an AI workload needs and zero telemetry egress when air-gap mode is on.

AIR-GAP-READY · SOVEREIGN DEPLOYMENT · SIGNED OFFLINE UPDATES

02 · WHY THIS MATTERS NOW

AI MANDATES MEET THE ATO REALITY.

Every national government has published an AI strategy. Every agency has been told to adopt one. Every CIO has discovered the same constraint: the AI retrieval stack most commercial vendors ship cannot pass an ATO (Authority-to-Operate) review because it depends on infrastructure outside the perimeter.

DATA SOVEREIGNTY	Citizen data, classified material, and intelligence must not leave the national perimeter. A hosted vector DB in a commercial region fails before the conversation starts.
AIR-GAP REQUIREMENT	Classified networks, SCIFs, and defence enclaves have no internet. Installing, updating, and operating the retrieval layer must work offline with signed artifacts.
LONG ATO CYCLES	A new piece of infrastructure takes quarters to accredit. The less the retrieval stack is — binaries, network dependencies, third-party SaaS — the faster the ATO.
FEDRAMP / IL5 / CJIS	Controls frameworks vary by mission. The retrieval layer must produce audit artifacts in the shape regulators already accept. Custom logging pipelines delay everything.

03 · SOVEREIGN AI DATA STACK

ONE BINARY. AIR-GAP MODE. SIGNED UPDATES.

13 MB static binary. Runs on Linux, on a sealed rack, in a SCIF. Offline install + signed release manifest. When XERJ_AIRGAP=1 is set, zero telemetry egress — no phone-home, no update check, no license ping.

FOOTPRINT

13 MB**STATIC BINARY**
OFFLINE-DEPLOYABLE

Ship on media. Verify signed manifest. Run on any Linux box. No JVM, no JRE, no dependency graph.

AIR-GAP

1 ENV VAR**NO TELEMETRY**
NO PHONE HOME

XERJ_AIRGAP=1 disables all egress. Offline-update channel · signed bundle · installable into a SCIF.

SOVEREIGNTY

100 %**ON YOUR
HARDWARE**

No commercial cloud dependency. National-cloud, on-prem, or classified enclave. Data never leaves the perimeter.

ACCREDITATION

SBOM**SIGNED BUILDS**
SBOM + SLSA

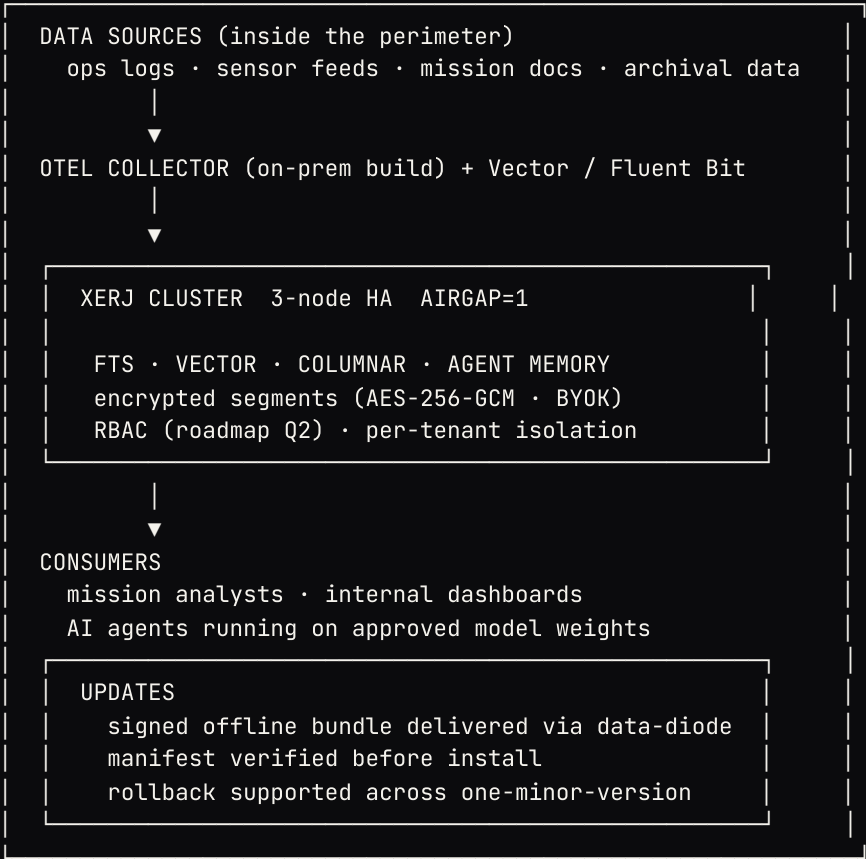
Every release ships an SBOM. SLSA-compliant provenance (roadmap Q3). Cross-walkable to FedRAMP Moderate + IL5 controls.

04 · AIR-GAPPED BLUEPRINT

SEALED RACK. ONE BINARY.

A three-node XERJ cluster inside a classified enclave. No outbound connectivity. Offline-update channel through a data-diode. Same binary, same configuration surface as a commercial deployment.

CLASSIFIED ENCLAVE no-internet · signed-media only · physical access control



no outbound · no telemetry · no license ping · no update probe

SIZING · 3-NODE HA · OFFLINE OPERATION · ONE-MINOR-VERSION ROLLBACK

05 · WHERE XERJ APPLIES

MISSION.
OPERATIONS.
SERVICES.

The AI workloads every public-sector CIO has on the 24-month roadmap. Each maps to one XERJ deployment pattern.

WORKLOAD	PATTERN	STORE
CITIZEN SERVICES	Retrieval-augmented case workers across benefits, tax, licensing. Sovereign RAG over agency knowledge bases. Per-agency RBAC.	HYBRID
DEFENCE INTEL	Semantic search over classified reports, OSINT, sensor feeds. Air-gap-mandatory. Agent memory for investigation sessions.	VECTOR
CYBER SOC	Federal / state SOC over log fleet. MTTD in milliseconds. SIEM battery 74× faster than legacy on 1 M events.	LOGS
LEGISLATIVE ANALYSIS	Bill text, precedent case law, policy documents · hybrid BM25 + vector search for research staff and committees.	HYBRID
AUDIT & IG	Inspector-general workflows · retrieval across contract records, financial transactions, correspondence. Legal-hold markers.	FTS
EMERGENCY RESPONSE	Real-time ingest of sensor + situational data + responder comms. Unified retrieval for command-and-control agents.	HYBRID
BIOMEDICAL RESEARCH	Grant portfolios, publication corpus, clinical-trial registries. RAG for research-officer productivity. Per-agency quotas.	VECTOR

ALL SEVEN · ON ONE XERJ PLATFORM · AIR-GAP-CAPABLE

06 · ATO-READY CONTROLS

BUILDING BLOCKS FOR ATO.

Self-hosted means most accreditation scope is inherited from agency controls. XERJ supplies the engineered-in controls the ATO body expects to see in the submission.

STANDARDS & CERTIFICATIONS

STANDARD	RELEVANCE	STATUS
FedRAMP MODERATE	Commercial SaaS offering; self-hosted inherits agency baseline	ROAD 2027
FedRAMP HIGH	Higher-impact workloads · planning phase	ROAD 2027+
DoD IL5	BYOK + FIPS-validated crypto + air-gap · engineering scope ready · accreditation roadmap	ROAD 2027
CJIS	Tenant isolation + audit trail + encryption at rest + access control	INHERITED (SELF-HOSTED)
NIST 800-53 REV5	Controls cross-walk available · security control implementation summary (SCIS) template	GA
NIST AI RMF	Per-query explain-plan + audit trail aligns with "measure" + "manage" functions	GA
ISO 27001	ISMS scope · commercial track	ROAD Q4 2026
CMMC Lvl 2	DFARS 252.204-7012 · self-hosted inherits organizational controls	INHERITED
SUPPLY CHAIN	Every release ships an SBOM. SLSA-compliant provenance (roadmap Q3). Reproducible builds. Signed Git tags + signed artifact manifests.	
CRYPTO	AES-256-GCM at rest · TLS 1.3 in transit · FIPS 140-2 validation (roadmap 2027). BYOK via KMS / HSM · Thales Luna · CloudHSM · AWS KMS.	

07 · GOVERNMENT STACK · INTEGRATED

YOUR STACK. APPROVED.

The tools agencies already run — ES-backed SIEMs, PIV / CAC authentication, Red Hat / Oracle Linux · air-gapped KMS — work out of the box.

CATEGORY	TOOLS	STATUS
OS / RUNTIME	RHEL · Oracle Linux · Ubuntu LTS · SUSE · amd64 + aarch64 · offline RPM / DEB bundle	GA
IDENTITY	PIV / CAC · smart-card via OIDC bridge · SAML 2.0 · Active Directory · Okta · agency IdP	ROAD Q2
CLOUD	AWS GovCloud · Azure Gov · GCP Assured Workloads · Oracle Gov Cloud · VMware on-prem	GA
KMS / HSM	Thales Luna · AWS CloudHSM · Azure Dedicated HSM · HashiCorp Vault (FIPS) · BYOK	ROAD Q2
SIEM	Wazuh · Elastic Security · commercial SIEMs via ES wire · Sigma rule conversion	GA
COLLECTORS	Otel Collector (on-prem) · Vector · Fluent Bit · Filebeat · syslog TCP/UDP listeners (roadmap)	GA
AGENT FRAMEWORKS	LangChain · LlamaIndex · Haystack · DSPy · local model weights · air-gapped RAG pipelines	GA
BACKUP / DR	Object storage (S3-compatible) · on-prem S3 appliances · incremental, encrypted, restorable per segment	GA
STIG / HARDENING	Config templates aligned with STIG controls · CIS benchmark · hardened container images (planned)	ROAD Q3

08 · OPERATIONAL MEASURED

NUMBERS. REPRODUCIBLE.

The performance profile an agency cares about is the one that fits inside a constrained deployment envelope. XERJ numbers on a single node against a 4-node ES baseline.

METRIC	XERJ	LEGACY (ES 8.13)
BINARY FOOTPRINT	13 MB	~620 MB JAR + JRE — 56×
COLD START	50 ms	~15 s JVM warm-up — 300×
IDLE MEMORY	400 MB	8.5 GB (4-node) — 21×
SIEM AGG P95 · 1 M EVENTS	0.4 ms	29.8 ms — 74×
DISK · 1 M EVENTS	85 MB	240 MB — 2.8×
NETWORK DEPENDENCIES	0 external	varies
OFFLINE-INSTALL TIME	< 5 min	hours (JRE · deps · config)
AUDIT ARTIFACT PER QUERY	explain-plan built in	application-level plumbing
MISSION IMPACT	Smaller deploy footprint fits inside ATO boundaries that reject JVM-based stacks. Offline-operation capability means accreditation bodies approve the same binary deployed in commercial and classified enclaves.	
SOURCES	SIEM_BATTLE_2026-04-14 · CLUSTER_BATTLE_2026-04-14 · CAPPED_RAM_BATTLE_2026-04-13 — all reproducible with scripts that ship with the binary.	

09 · FROM POC TO ATO

LAB.
UAT.
PRODUCTION.

Public-sector deployments start in an unclassified lab, graduate to a low-side UAT, and finally cross into the production enclave once the ATO evidence is complete.

01	UNCLASSIFIED LAB WEEKS 1-4	Install on an unclass lab network · reproduce SIEM_BATTLE + RAG_BENCH on open data · architecture review with agency CISO · draft ATO package outline.
02	UAT · LOW-SIDE MONTHS 2-4	Deploy in low-side staging · integrate with agency IdP · conduct vulnerability + penetration testing · finalize ATO package · interim authority considerations.
03	ATO AUTHORIZATION MONTH 5	Submit accreditation package · respond to ARs · obtain ATO. NIST 800-53 crosswalk and SBOM accelerate review.
04	PRODUCTION ENCLAVE MONTHS 6-9	Deploy to production perimeter · air-gap mode on · offline-update channel commissioned · first mission workload migrated · runbooks handed to ops team.
05	MULTI-MISSION QUARTER 4	Additional mission workloads migrate onto the same data plane · tenant-isolated indices · shared RBAC and audit trail · consolidated ops surface.

OFFLINE-OPERATION · SIGNED UPDATES · REVERSIBLE AT EVERY PHASE

10 · NEXT STEPS

PROVE IT. IN YOUR LAB.

An unclassified lab pilot. Offline-install bundle. Reproduction scripts for the SIEM and RAG battle reports on open data. Architecture review with your CISO / accreditation body.

PUBLIC SECTOR CONTACT

HELLO@XERJ.AI

XERJ.AI · XERJ.COM · XERJ.DEV

LAB KIT

Offline-install bundle · signed manifest · SBOM · NIST 800-53 crosswalk · SIEM_BATTLE + RAG_BENCH reproduction scripts.

COMPANION
BRIEFS

xerj-tech-brief.pdf (architect) · xerj-usecase-security.pdf (cyber SOC) · xerj-usecase-rag.pdf (research RAG)