Case Study
Secure AI Data Sharing in IL5 Environments
IronBank-Hardened APISIX API Gateway Enables Compliant, High-Performance Analytics and AI

Data Center Services (DCS)
March 2026

Case Study
Secure AI Data Sharing in IL4/5 Environments
IronBank-Hardened APISIX API Gateway Enables Compliant, High-Performance Analytics and AI

Data Center Services (DCS)
March 2026

Executive Summary

A secure, scalable way to expose APIs for AI-driven analytics and machine learning models while maintaining full NIST RMF compliance in an Impact Level 4/5 (IL4/5) environment.

Data Center Services (DCS) designed and implemented an **IronBank-hardened Apache APISIX API Gateway** based on Red Hat UBI9 minimal. The solution provids centralized traffic management, zero-trust security controls, and AI-specific protections, accelerating data sharing without compromising accreditation boundaries.

Results:

- Achieved RMF-compliant API exposure in under 90 days
- Sub-millisecond latency for AI inference routing
- Strong protection against prompt injection and data exfiltration
- Reduced attack surface through Iron Bank hardening
- Enabled secure bridging between classified and unclassified analytics platforms

The Challenge

Modern DoD missions increasingly rely on AI and advanced analytics to process vast amounts of mission data. However, traditional approaches created significant hurdles:

- Direct exposure of backend services violated zero-trust principles and RMF controls
- High risk of prompt injection, token leakage, and sensitive data exfiltration in LLM interactions
- Complex multi-LLM routing and rate limiting across disparate AI providers
- Lengthy accreditation timelines due to custom hardening requirements
- Need to operate securely within DISA SCCAand IL4/5 Azure environments

Mission owners need a single, auditable control point that could handle both traditional APIs and emerging AI workloads while inheriting DoD-approved security controls.

The DCS Solution

DCS leveraged its deep expertise in DISA Secure Cloud Computing Architecture (SCCA), Cloud Access Points (CAP), and NIST RMF to deliver a purpose-built solution:

- **IronBank-Hardened APISIX Container** — Built on Red Hat UBI9 minimal for minimal attack surface and full alignment with DoD Container Hardening Guide.
- **AI Gateway Capabilities** — Intelligent routing across multiple LLM backends, token-based rate limiting, prompt guard / response filtering, and content moderation.
- **Zero-Trust Security** — mTLS, OAuth2/OIDC integration, JWT validation, IP whitelisting, and fine-grained access controls.
- **Observability & Compliance** — Native Prometheus/Grafana integration plus detailed logging to support continuous monitoring and eMASS artifacts.
- **Integration with Existing Environment** — Seamless deployment within the customer's IL4/5 accreditation boundary, building on prior DCS work with VDMS and CMRS.

Configuration was delivered through the **APISIX Hardened Support Bundle** (GSA Schedule 47QTCA21D00B9), providing expert DevSecOps engineering and Principal Cyber Security Architect hours for RMF documentation.

Implementation Highlights

- Rapid prototyping validated architectural decisions in a sandbox environment (leveraging DCS experience with rapid prototyping).
- Hot-reload dynamic configuration enabled zero-downtime updates.
- AI-specific plugins protected against prompt injection while allowing secure data sharing for analytics platforms.
- Full inheritance of Iron Bank security controls streamlined the RMF assessment process.

Results & Benefits

- **Speed**: Full integration and initial ATO artifacts completed in under 90 days — significantly faster than traditional gateway hardening efforts.
- **Performance**: Consistent sub-millisecond latency even under heavy AI inference loads.
- **Security Posture**: Dramatically reduced vulnerabilities through minimal base image and Iron Bank compliance; strong defenses against common AI gateway threats.
- **Mission Impact**: Enables secure, real-time data sharing between operational systems and AI analytics platforms, directly supporting data-centric DoD objectives.
- **Cost Efficiency**: Fixed-price support bundle avoided expensive custom development while providing priority expert access.

This deployment builds on DCS's proven track record, including the first IL4 production CAP submission in the IL4 Azure environment, multiple live CAP migrations (1.0 → 3.0) with zero downtime, and the successful 2025 cArmy Azure production and development migrations for AFMIS.

Why DCS?

Led by Robert Hermanns (MS, former Northrop Grumman Senior Cybersecurity Architect and author of the DCLD 101 DoD Cloud Access Point course), DCS combines hands-on RMF expertise with modern hardened container capabilities — directly competing with and surpassing commercial offerings in DoD compliance depth.

Next Steps

Ready to secure your AI and analytics data flows?
Add the **IronBank-Hardened APISIX** and **APISIX Hardened Support Bundle** to your GSA order today.

Contact DCS
6000 Technology Blvd, Sandston, VA 23150
gsa-sales@d8acenter.com | (804) 336-6814
www.d8acenter.com | GSA Schedule 47QTCA21D00B9

Data Center Services (DCS) — Delivering Mission Enhancing Capability at the Speed of Relavance