CASE STUDY

Risk Management · Federal

InterSec
Ignite . Inspire . Innovate

Securing Global ERP Systems for the U.S. Department of the Army

As a subcontractor supporting the Army's CIO/G6 office, InterSec embedded secure DevOps practices and cost-optimized disaster recovery to harden globally distributed ERP systems against fast-moving threats within tight budget constraints.

CLIENT	PROFILE	STATUS
U.S. Department of the Army (CIO/G6)	Globally distributed ERP for logistics, finance, and personnel	In progress

Secure DevOps
Security built into the ERP lifecycle

Risk-based
Highest-impact modules hardened first

FinOps
Disaster recovery scaled to cost

Global
Logistics, finance, personnel secured

ENGAGEMENT	SYSTEMS	FOCUS	RESILIENCE
Subcontractor to CIO/G6	Global ERP platforms	Secure DevOps and ERP hardening	Cloud disaster recovery

THE CHALLENGE

The Army needed a strong security posture for its global ERP systems while holding to stringent DoD guidelines and tight budgets. Running multiple large-scale systems introduced real complexity in patch management, identity management, and disaster recovery. Vulnerabilities had to be addressed at their source rather than patched reactively, and advanced disaster recovery was required without runaway cost.

THE APPROACH

InterSec applied a risk-based methodology so the highest-impact systems got attention first, and brought financial-operations discipline to disaster recovery. Three moves defined the work: prioritize by risk and harden the high-impact ERP modules; build security into development through secure DevOps, with code reviews, automated scanning, and continuous feedback; and apply FinOps principles to balance cloud resources, holding cost down while keeping uptime where the mission needed it.

> **Security built into the lifecycle costs far less than security bolted on after something breaks.**

THE SOLUTION IN PRACTICE

InterSec coordinated development practices aligned with defense coding directives, so security entered the software earlier rather than being inspected in at the end. The team hardened ERP configurations, strengthened identity and access controls, and tightened patch cycles to reduce standing exposure. For resilience, InterSec established cloud-based disaster recovery that scaled to the Army's needs, expanding or contracting with demand rather than sitting idle at full cost.

RESULTS & IMPACT

- ✓ ERP layers were secured through DevSecOps practices built into the development lifecycle.
- ✓ Cloud-based disaster recovery improved the return on the Army's resilience spending.
- ✓ Downtime was minimized, directly supporting critical Army operations.
- ✓ A risk-based plan kept a high-security posture within a tight budget.

KEY TAKEAWAYS

Build security in, do not inspect it in.
Secure DevOps catches vulnerabilities at the source, cheaper and safer than patching them in production.

Prioritize by mission impact.
Hardening the highest-impact modules first turns an unbounded problem into a focused plan.

Resilience has a price, and FinOps manages it.
Disaster recovery that scales with demand delivers readiness without paying for idle capacity.

Budget constraints are a design input, not an excuse.
A risk-based plan lets a high-security posture and a tight budget coexist.

CAPABILITIES DEMONSTRATED

Secure DevOps Integration · ERP Hardening · Risk-Based Vulnerability Prioritization · Cloud-Optimized Disaster Recovery · DoD Security and Budget Alignment

Hardening mission-critical systems under federal mandates and real budget limits is a daily balance.
InterSec builds security into the lifecycle of ERP and enterprise platforms. Let's talk about a risk-based plan.

Let's talk →