

INDUSTRY / DEFENSE &amp; SECURITY TECHNOLOGY

# Give critical operations a dependable software foundation.

BELTO can engineer protected data flows, secure communications and test environments for security-adjacent organizations. We define trust boundaries and responsibility early so the system can be reviewed, operated and handed over.

## WHAT WE CAN BUILD FOR YOU

### 01 Connect distributed systems securely

Design encrypted communication paths and segmented infrastructure for the agreed actors and operating conditions.

#### VALUE TO YOUR TEAM

Reduce unnecessary exposure and give operators a clearer response to connectivity failures.

### 02 Track the origin of mission data

Build storage and transfer workflows with provenance, access boundaries and observable handling of exceptions.

#### VALUE TO YOUR TEAM

Help teams understand where data came from and which systems or people can act on it.

### 03 Test failures before field deployment

Build synthetic scenarios and examine component provenance across the software and hardware supply chain.

#### VALUE TO YOUR TEAM

Expose weak assumptions and integration failures while the team can still change the design.

## WHY BRING BELTO INTO THE WORK?

One engagement can connect Security & assurance, Systems engineering, Private infrastructure, Data governance. We define the interfaces, build the agreed path and verify its behavior with the people who will operate it.

### HOW WE MAKE THE VALUE VISIBLE

Recovery behavior / Provenance completeness / Unresolved control exceptions

Export-controlled scope is reviewed before work. No clearance or export-authorization claim is made.

## ILLUSTRATIVE APPLICATIONS / SCOPED TO YOUR SYSTEMS

# Let's scope the first useful step.

Bring the system boundary, authorized scope and the operating scenarios that need to be demonstrated.

Talk to BELTO

---

DEFENSE & SECURITY TECHNOLOGY / FROM SCOPE TO DELIVERY

# Choose the capability your operation needs.

A starting scope can cover one specialist area or connect several into a complete workflow. The service map below shows the published coverage and the operating value each area is intended to support.

## Mission data infrastructure

Engineer protected operational-data storage and movement with provenance. Make data movement and provenance reviewable.

## Secure communications

Design encrypted communication paths with resilience and a constrained signature. Preserve necessary connectivity with explicit trust and recovery boundaries.

## Simulation & modeling

Use synthetic environments to investigate system failures before field deployment. Find weak assumptions before committing to field deployment.

## Supply chain security

Track component and software provenance to expose substitution or tampering. Expose provenance gaps and unauthorized changes in components.

---

### WHAT YOUR TEAM RECEIVES

An agreed system boundary and interface map; working software or infrastructure for the contracted scope; tests tied to acceptance criteria; and operating documentation with named owners. The exact package is agreed before delivery.

### A PRACTICAL FIRST ENGAGEMENT

Start with one of the examples on the previous page. We review representative inputs and exceptions, establish the current baseline, then deliver a bounded path your team can inspect. Expand only after the first increment supports a useful decision.

Export-controlled scope is reviewed before work. No clearance or export-authorization claim is made.

---

### ILLUSTRATIVE APPLICATIONS / SCOPED TO YOUR SYSTEMS

## Let's scope the first useful step.

Bring the system boundary, authorized scope and the operating scenarios that need to be demonstrated.

Talk to BELTO