

Securing the Defence Transaction Plane.

Automated compliance. Real-time intellectual property protection. Zero application friction.

The Canadian defence and aerospace sector is facing unprecedented cybersecurity scrutiny. As prime contractors mandate stricter compliance—pushing frameworks like the Canadian Cyber Security Certification (CCCS) and CMMC down to Tier 2 and Tier 3 suppliers—static, manual audits are no longer sufficient to guarantee data security.

To maintain operational readiness and qualify for high-value defense procurement, organizations need continuous, automated verification. You must prove that sensitive engineering data, ITAR/Controlled Goods, and proprietary IP are protected at the execution layer during every single digital transaction.



The permissions and compliance authorization platform **designed for national security environments.**



CONTROLCORE

Control Core operates as an attribute-agnostic control plane engineered for high-stakes defence architectures. Deploying an inline, stateless proxy—the Bouncer—the platform instantly ingests any available signal source, including network telemetry, user or device or agent identity, payload metadata, threat vectors, and real-time data structures.

Completely decoupled from your underlying software stack, it ingests these multi-dimensional signals to execute Smart Permissions across any transport protocol—whether managing standard HTTP APIs, raw TCP loops, gRPC streams, or legacy SQL database traffic—enforcing intelligent decisions at line rate.

CONTINUOUS COMPLIANCE AUDIT

Replace slow, point-in-time paper reviews with a passive, continuous mapping of your actual network traffic, generating instant audit-ready proof for regulators.



ABSOLUTE DATA CONTAINMENT

A 100% local Virtual Private Cloud (VPC) deployment guarantees that your telemetry, transaction metadata, and proprietary engineering designs never touch foreign servers.



ZERO ARCHITECTURAL DISRUPTION

Secure legacy manufacturing databases, tactical mainframes, and modern APIs without software refactoring, extending the operational lifespan of your current infrastructure.



Tactical Execution

Continuous CCCS Compliance Audit

- Passively map vendor and API traffic across the supply chain to instantly verify alignment with Level 2 defense cyber certifications.

Real-Time IP Redaction

- Automatically inspect and mask classified aerospace blueprints, PII, and proprietary specifications before data leaves the secure enclave.

Zero-Trust Legacy Modernization

- Wrap aging manufacturing databases in modern, context-aware authorization controls to prevent internal lateral movement.

Autonomous AI Guardrails

- Restrict engineering AI models and agents to designated operational boundaries, preventing unauthorized data scraping.

Secure Cross-Domain Sharing

- Safely execute joint-operation data exchanges by validating the payload intent and identity of every micro-transaction.

TECHNICAL POSTURE

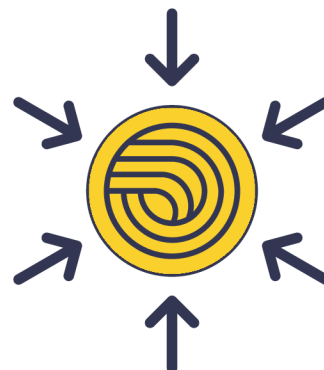
Control Core centralizes these disparate rules into a single, intelligent engine.

The Bouncer: An inline, stateless component that intercepts and normalizes traffic, executing context-aware security decisions in under 5 milliseconds.

Smart Permissions: Define granular, context-aware rule sets in natural language. Our engine translates these instantly into machine-readable, executable policies.

Automated Compliance Audit: Run passively in the background to map API traffic, expose regulatory vulnerabilities, and generate continuous, audit-ready proof or controls.

Inline Data Redaction: Automatically detect and mask sensitive information (PII, PHI, Proprietary IP) before it ever leaves your secure boundary.



STANDARDS WE MAP TO

- CCCS Defence (Canadian Cyber Security Certification Levels 1 & 2)
- NIST SP 800-53 / 800-171 (Federal Information Security Standards)
- CMMC (Cybersecurity Maturity Model Certification)
- Dual-Use Controls (Export/Import and Controlled Goods compliance)

Prove your compliance. Protect your IP.

Run a zero-impact Compliance Audit on your active network traffic today.

Identify and resolve security vulnerabilities before your prime contractors do.

Deploy your audit: controlcore.io **Contact:** info@controlcore.io

