controlplane

AI, Data & Automation Security

Ensuring Confidence, Compliance and Security in AI Adoption.

ControlPlane's experts tackle the adversarial risk and compliance uncertainty of AI/ML systems - something that is becoming more vital as 74% of IT Security professionals report significant impact from AI-powered threats.

We transform fragile, ad-hoc assurance into a deterministic, policy-driven capability built on hardened, auditable architectures that ensures compliance and confidence.

The Top Challenges Our Clients Face

1. **Hidden Security Risks:**
   Models risk silent failure from data poisoning, adversarial attacks, and open-source dependencies, bypassing traditional security testing.
2. **Trust & Incident Response:**
   Models lack verifiability and demonstrable assurance of lineage, reproducibility, and integrity, compromising incident response times and customer trust.
3. **Operational Inefficiency:**
   Lack of internal skills and mature AI security patterns, manual reviews create operational friction, diverting resources and slowing innovation.
4. **Navigating Compliance Uncertainty:**
   Complex new AI regulations mean most architectures are ill-equipped, risking non-compliance, fines, and operational bans.

Shift From Reactive Practices to Security- And Compliance-By-Design

Some of the lasting value we deliver:

- **A deterministic, auditable model lifecycle**, which significantly de-risks deployment from ingestion to production.
- **Hardened, secure AI/ML pipeline blueprints** enable teams to eliminate reliance on ad-hoc, fragile security approaches.
- **Confidence in compliance**, as controls are actively aligned with global obligations, such as the EU AI Act and NIST AI RMF.
- **Incident response capabilities** are enhanced by embedding cryptographic provenance and attestation (SBOM-for-AI) for every model artefact.

Working With ControlPlane

AI isn't going anywhere, so why not approach adoption with proactive security and governance? We run bespoke projects, and alongside this, we also offer training and fixed fee services:

- Security Health Check:
  Tactical AI security assessment evaluates MLOps posture across the SDLC, delivering actionable risk recommendations.
- Threat Modelling:
  Interactive workshop or mini-project, we evaluate AI/MLOps security end-to-end, delivering a prioritized view to harden pipelines and reduce real-world risk.
- Maturity Assessments:
  Company-wide assessment that benchmarks MLOps maturity, guiding investment and enabling secure, compliant delivery.
- Tabletop Exercise:
  This exercise assesses and improves your AI security incident readiness, building cross-team response fluency.
- Security Training:
  One or five day, hands-on training equips teams at all levels to understand and mitigate AI/ML-specific risks.

About Us

ControlPlane is a highly specialised Enterprise DevSecOps and AI Security consultancy founded to design, build, and secure Cloud Native solutions for organisations where trust is non-negotiable.

Our mission is to accelerate innovation where trust, compliance, and security are non-negotiable. As such, we have worked with multiple Fortune 100 and FTSE 100 companies, developing long-term collaborative relationships.

We are active in the community and industry events, as we Co-Chair the Linux Foundation's Technical Advisory Group on Security (CNCF TAG Security). We contribute to the Open Source Security Foundation (OpenSSF) and Fintech Open Source Foundation (FINOS) community working groups. We were also chosen by Google to audit and author the CIS Benchmarks for GKE.