CASE STUDY · MILITARY & DEFENSE · DATA CONTROL & ENTERPRISE DATA BOUNDARY

A defence integrator ran AI against controlled data with the boundary enforced, not promised

Clearance-scoped roles and a fail-closed boundary let controlled programme data reach a model at all — under conditions the programme office could verify.

Scenario	Published	Orcher components
Defence systems integrator · controlled programme environment	2026-09-30	Data Control Gateway, Role Identity Fabric, Immutable Audit Ledger

Summary

A defence systems integrator needed AI assistance on documentation inside a controlled programme environment. Orcher enforced clearance-scoped access and a fail-closed data boundary per directive, with evidence for the programme office produced by execution itself.

0
controlled-data routes to unapproved endpoints

100%
of directives classified before routing

Approved
programme office sign-off for AI assistance
previously prohibited outright

48%
reduction in documentation drafting hours

The situation

- Programme rules prohibited controlled data reaching any endpoint without a verified handling posture.
- A blanket prohibition had been the default, which meant no AI assistance at all on the programme.
- Any approved approach had to produce evidence the programme office could review without a special project.

What Orcher enforced

- Directives are classified before routing, and the gateway fails closed when classification, clearance and endpoint posture do not agree.
- Role bindings are clearance-scoped: an agent can never see data the directing engineer could not see.
- Model selection is constrained to endpoints approved for the specific classification, with the decision recorded.
- The ledger produces per-directive evidence that the programme office reads as its standing control report.

The data

Classification	Approved endpoints	Directives	Refused pre-route	Evidence produced
Unclassified	All approved	14,200	0	Per directive
Controlled — general	2 endpoints	6,850	31	Per directive
Controlled — programme	1 endpoint	2,140	88	Per directive
Restricted	None	0	412 attempts blocked	Per attempt

Routing outcomes by classification over the engagement period.

Outcomes

- AI assistance exists on the programme at all, which was the binary outcome that mattered.
- The programme office reviews a standing report rather than commissioning audits.
- Blocked attempts became a training signal for engineers about what the classification rules actually mean.
- The pattern is being reviewed for a second programme with tighter constraints.

> “The question was never whether the model was useful. It was whether we could prove, afterwards, exactly where the data went.”
>
> — Programme Security Officer, defence systems integrator (composite, modelled scenario)

Read further

- Trust and standards — dippai.com/trust
- The Data Control Gateway — dippai.com/orcher/data-control-gateway
- Full case study — dippai.com/case-studies/defense-integrator-boundary-and-identity

Disclosure. Modelled reference scenario. The organisation is representative of the sector and scale described, not a named customer. Figures are produced by Orcher's own observability and ledger instrumentation for this configuration over the stated period and have not been independently audited. Market figures carry their own source line.