

Production readiness, with evidence.

A concise buyer brief for evaluating deployment, identity, data boundaries, connector permissions, auditability, recovery, security testing, and production acceptance.

Signal
Evidence
Authority
Action
Outcome

The production boundary, in four answers.

What runs today

The working demonstration connects audience command views, AI governance, Agent Gate, evidence review, decision policy, delivery lineage, outcome verification, and executive reporting.

What must be configured

Enterprise identity, durable tenant data, connector workers, authorization enforcement, production audit storage, telemetry, backup, recovery, and organization-specific policy.

What a pilot must produce

An approved architecture, tested access boundaries, a connector permission manifest, audit and recovery evidence, security-test results, and an explicit outcome decision.

What must be true before production

Each foundational control is documented, tested, owned, and accepted. The pilot ends with an explicit go, extend, or stop decision.

Evidence standard

Product views use demonstration records. A production claim is accepted only when the control has a named owner, a documented configuration, a completed test, retained evidence, and an explicit approval. Catalyst does not treat configuration intent as operating proof.

Context enters. Authority decides. Proof leaves.

Catalyst coordinates systems of record. It does not replace identity, security, ticketing, billing, evidence, or reporting platforms. Tenant context is established before records are read. An approved decision precedes every action-capable handoff.

SOURCE SYSTEMS	CATALYST TENANT BOUNDARY	CONTROLLED DESTINATIONS
Identity and ownership Entra, Okta, CyberArk	Normalized record Tenant, environment, owner, source, freshness	Authorized delivery Jira, ServiceNow, workflow
Signals and evidence SIEM, CNAPP, GRC, data	Decision policy Risk, data class, cost, quorum, expiry	Agent enforcement Hook, proxy, gateway, sidecar
Spend and economics Azure, AWS, billing exports	Authority and audit Named approval, conditions, challenge, receipt	Executive proof Verification, reports, exports

Connector control rules

Read-only by default	Begin with the minimum read scope needed for the approved scenario.
Action requires authority	Write-capable adapters require a named decision, approved conditions, and an environment-specific permission manifest.
Secrets stay bounded	Isolate secrets by tenant and environment, rotate them under a named owner, and keep them out of the browser.
Every handoff leaves a receipt	Retain source identifiers, policy version, decision, conditions, external record, result, and verification.

Ten decisions and the evidence required to exit.

#	CONTROL	REQUIRED EXIT EVIDENCE
01	Deployment model	Approved topology, network boundary, region, environments, private connectivity, and named service owners.
02	Tenant isolation	Negative cross-tenant tests and authorization tests proving records and actions remain isolated.
03	Identity and SSO	SSO, MFA, group mapping, joiner and leaver handling, privileged review, and emergency access.
04	Data residency	Signed data map covering storage, processing, subprocessors, retention, transfer, and verified deletion.
05	Encryption and keys	Transit and at-rest controls, custody, rotation test, revocation, and key-ownership decision.
06	Connector permissions	Reviewed manifest, read-only defaults, protected secrets, and separate authority for action connectors.
07	Audit retention	Searchable export, synchronized timestamps, access logging, retention, and immutability test.
08	Backup and recovery	Recovery objectives, successful restore test, dependency map, runbook, and escalation owner.
09	Security testing	Threat model, code and dependency testing, secret checks, access tests, and resolved critical findings.
10	Pilot exit criteria	Signed success measures, rollback path, export and deletion test, and go, extend, or stop decision.

A pilot is complete only when every in-scope control has a named owner, retained evidence, an accepted exception or completed test, and an explicit outcome decision.

Production enforcement must fail safely and leave proof.

The working demonstration shows deterministic policy evaluation, held requests, linked decisions, lease simulation, and readable reasons. Production readiness requires a deployed enforcement point and evidence for each control below.

CONTROL	REQUIRED BEHAVIOR	PILOT EVIDENCE
Bind identity	Verify the agent and workload identity against tenant and environment before policy evaluation.	Signed assertion and negative impersonation test.
Fail closed	Release no action-capable route when identity, policy, evidence, or availability is insufficient.	Timeout, outage, stale evidence, and missing-authority tests.
Revoke and expire	End a lease on expiry, revocation, owner change, scope change, or defined risk condition.	Measured propagation time and blocked replay test.
Return a receipt	Return decision ID, effective conditions, operation, result, external record, and timestamp.	Receipt reconciled to the external system and audit record.

Decision at pilot exit

GO	EXTEND	STOP
Controls pass, operating ownership is accepted, rollback is tested, and the measured outcome supports production use.	The scenario remains valuable, but named gaps require a time-boxed extension with new acceptance evidence.	The control boundary, operating burden, evidence quality, or measured result does not support production use.

Next step

Use one real security decision to define the architecture, permission manifest, acceptance tests, and measurable outcome before any production connection is authorized.