Watchlight AI

SAMPLE DELIVERABLE · ARCHITECTURE BLUEPRINT

Authorization & Runtime Control Architecture

Reference blueprint for agent identity, scoped authority, delegation chains, and runtime policy enforcement.

PREPARED FOR	Acme Logistics
SECTOR	Global Logistics & Supply Chain (Illustrative)
ENGAGEMENT	Authorization and Runtime Control Architecture Workshop
SCOPE	Enterprise AI agent platform (22 agents across 8 workflows)
DELIVERED	March 2026

01 Executive Summary

Target architecture for authorization and runtime control infrastructure governing Acme Logistics's 22 AI agents across route optimization, customs brokerage, and exception handling workflows.

ARCHITECTURE THESIS

Acme Logistics's existing IAM infrastructure (enterprise IdP, PAM, SCIM provisioning) provides strong human and service identity. AI agents introduce a new control requirement: runtime authorization based on declared intent, delegation chain, and current task context. The proposed architecture adds a compositional Agent Runtime Governance layer that consumes existing identity signals and applies runtime-specific policy evaluation.

Architecture Highlights

IDENTITY MODEL **SPIFFE/SPIRE + Enterprise OIDC**	POLICY LANGUAGE **Cedar (with AuthZEN API)**
ENFORCEMENT PATTERN **Proxy + SDK hybrid**	CREDENTIAL BACKEND **Enterprise PAM + Vault broker**
DELEGATION MODEL **Signed chains, scope narrowing**	AUDIT TARGET **SIEM + lineage graph**

Key Design Decisions

1. Hybrid enforcement: proxy for legacy, SDK for new agents

DECISION

New agents integrate via an SDK that calls the policy engine directly. Legacy agents route traffic through a transparent enforcement proxy. This allows incremental migration without rewriting existing agent code.

2. Cedar for policy authoring, AuthZEN for evaluation API

DECISION

Cedar provides the expressive policy language with strong tooling. AuthZEN standardizes the PDP API, enabling future policy engine substitution. Policies are stored in Git with CODEOWNERS for change control.

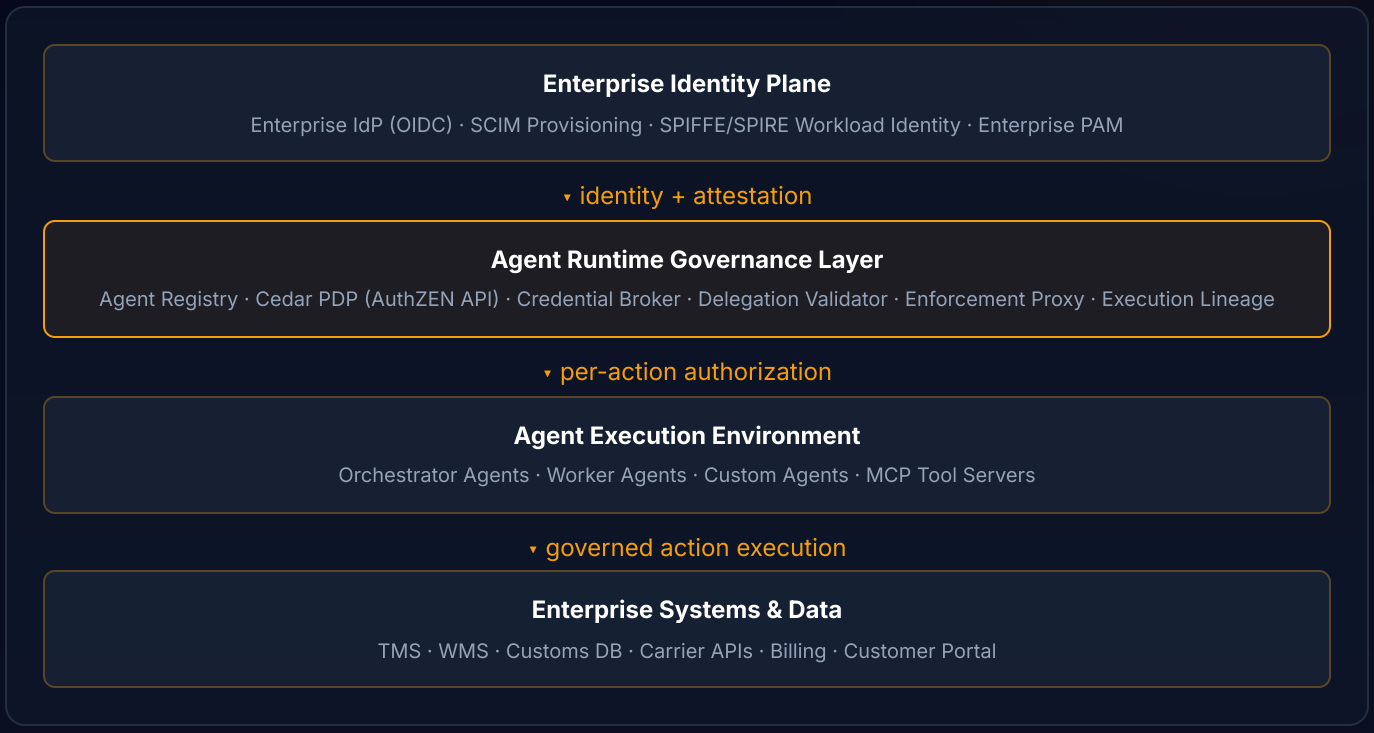
3. Capability tokens instead of raw credential passthrough

DECISION

Agents request short-lived, purpose-bound capability tokens from the credential broker. Tokens are single-use, time-bounded (5 minutes), scope-locked to declared intent, and audit-enriched. Raw credentials never reach agent memory.

02 Target Architecture

Layered target architecture for Acme Logistics. The Agent Runtime Governance layer sits between existing identity infrastructure and the agent execution environment.



Control Plane Components

COMPONENT	PURPOSE	TECH
Agent Registry	Stores agent identity, ownership, trust state, and capability declarations	PostgreSQL + SCIM API
Policy Decision Point	Evaluates Cedar policies on every agent action with full context	Cedar + AuthZEN
Credential Broker	Issues short-lived capability tokens bound to intent and delegation chain	Vault + PAM backend
Delegation Validator	Verifies cryptographic delegation chains and enforces scope narrowing	Custom service (Rust)
Enforcement Proxy	Transparent policy enforcement for legacy agents via reverse proxy	Envoy + ext_authz
Execution Lineage	Captures event stream and materializes the execution graph	NATS JetStream + Postgres

03 Identity and Policy Model

Agent identity is provisioned through SCIM and attested via SPIFFE. Policies are authored in Cedar and evaluated on every action with declared intent and delegation context.

Agent Identity Model

```
// Example agent registration (SCIM-compatible)
{
  "agent_id": "spiffe://acme.example/agents/route-optimizer-01",
  "display_name": "Route Optimizer 01",
  "owner": "logistics-platform@acme.example",
  "trust_state": "trusted",
  "framework": "langgraph",
  "allowed_intents": ["optimize_route", "check_carrier_availability"],
  "resources": ["tms:read", "carrier_api:invoke"],
  "attestation": "svid:x509:...",
  "lease_ttl_seconds": 3600
}
```

Example Cedar Policy

```
// Allow route optimization agents to read TMS data
// only when intent matches and within business hours
permit(
  principal in AgentGroup::"RouteOptimizers",
  action == Action::"ReadShipment",
  resource in Resource::"TMS::Shipments"
) when {
  principal.intent == "optimize_route" &&
  principal.delegation_depth <= 3 &&
  principal.authority_expires > context.now
};

// Deny any write to customs declarations from agents
// whose delegation chain does not include customs role
forbid(
  principal,
  action == Action::"WriteCustoms",
  resource
) unless {
  principal.delegation_chain.contains(Role::"CustomsBroker")
};
```

Delegation Chain Validation

When Orchestrator A delegates to Worker B, the delegation token is signed by A, contains a narrower scope than A's own authority, has a shorter TTL, and records the delegation link in the chain. The Delegation Validator checks all four properties before B's action is permitted. Scope widening is rejected at the PDP level.

04 Implementation Roadmap

Phased implementation plan for the target architecture. Each phase delivers independent value and reduces risk incrementally. Total elapsed time: 4–5 months.

PHASE 1 · MONTH 1

Registry & Identity

- Deploy agent registry
- Onboard all 22 agents
- SPIFFE attestation rollout
- SCIM integration with Ping
- Trust state management

PHASE 2 · MONTH 2

Policy Engine

- Deploy Cedar PDP
- Author policies for top 4 workflows
- AuthZEN API exposure
- GitOps policy workflow
- Shadow mode evaluation

PHASE 3 · MONTH 3

Enforcement

- SDK for new agents
- Envoy proxy for legacy
- Credential broker deployment
- Cut over 8 agents
- Fail-closed enforcement

PHASE 4 · MONTHS 4–5

Delegation & Lineage

- Delegation validator service
- Scope narrowing enforcement
- Execution lineage graph
- SIEM OTel bridge
- Full production cut over

Resource Requirements

SECURITY ENGINEERING	2 FTE for 5 months
PLATFORM ENGINEERING	1.5 FTE for 5 months
IDENTITY / IAM TEAM	0.5 FTE for 2 months
INFRASTRUCTURE	3 additional Kubernetes nodes
LICENSE / SAAS	Minimal (open source stack)
TRAINING	2 days Cedar policy authoring

Success Criteria

- 100% of production agents registered with verified identity by end of Phase 1
- Zero agents holding long-lived credentials by end of Phase 3
- Every agent action evaluated by policy engine by end of Phase 3
- Complete execution lineage for any production agent by end of Phase 4
- Mean time to reconstruct an agent action chain: under 5 minutes
- Policy authoring time per new workflow: under 4 hours