ADVISORY WORKSHOP

AI Agent Identity & Access

Give every agent a verifiable identity and least-privilege access.

A hands-on engagement to design and stand up identity and access for your AI agents: a unique verifiable identity for every agent, scoped and time-bound access, and governed delegation, all enforced at runtime under Agent Runtime Governance. Your team leaves with a working reference implementation and a rollout plan.

DURATION	INVESTMENT	AUDIENCE
2–3 days	$22,000–$35,000	Identity architects, IAM teams, security engineers, platform and AI infrastructure leads

WHY THIS MATTERS NOW

Agents are becoming the fastest-growing population of identities in the enterprise, and most hold long-lived credentials with broad, unscoped access. Naming an agent is not the same as governing what it does. Identity must be issued, scoped, delegated, and revoked under runtime governance, not bolted on after deployment.

Focus Areas

- Unique, verifiable agent identity for every autonomous actor (Principle 1)
- Agent identity lifecycle: provisioning, trust state, rotation, and revocation
- Scoped, time-bound authority and zero standing privilege for agents
- Governed delegation: who an agent can act for, and how far authority propagates
- Verifiable credentials and attestation across trust boundaries
- Integration with your existing IAM, identity provider, and secrets infrastructure

Deliverables

- ✓ Agent identity and access architecture mapped to your IAM stack
- ✓ A working reference implementation of agent identity and scoped access
- ✓ Delegation and authority model with runtime enforcement points
- ✓ Operational rollout plan for provisioning, rotation, and revocation at scale

IDEAL FOR

Identity and access management teams extending IAM to cover AI agents, and platform groups standing up agent identity for internal frameworks. Best for organizations that want agent identity issued and governed under Agent Runtime Governance from day one, alongside their existing OIDC, SCIM, SPIFFE, and secrets infrastructure.

1. **Pre-Workshop Discovery**
We review your environment and current controls. A brief intake questionnaire ensures we arrive prepared.

2. **Live Working Sessions**
Hands-on sessions with your security and technical teams. Real architecture, real decisions.

3. **Architecture Review**
We synthesize findings into actionable artifacts: blueprints, gap analyses, and roadmaps.

4. **Final Delivery**
A structured readout with your leadership team. Clear findings and a path forward.

Book a Workshop

We typically respond within 2 business days.

watchlight.ai/workshops/book