

Aembit's Approach to Closing the AI Identity Gap

THE PROBLEM

Every agent your teams deploy today is running under someone else's identity – a shared API key, a human's full session, or nothing distinct at all. That's not a gap that closes itself: 97% of security leaders expect a material agent-driven incident in the next year, and most can't yet tell you, after the fact, whether it was a person or an agent that took action.

97%

of enterprise security leaders expect a material AI agent-driven security incident within the next twelve months.

Enterprise security survey, 2026

6%

of security budgets are allocated to address it.

Same population

AEMBIT'S APPROACH

01 Identity Control Plane for Agents

Aembit is the identity control plane that sits between every agent or workload and everything it needs to reach – deciding, at the moment of each request, whether its identity is valid, what access level it gets, and which credential the destination system requires.

02 Run-Time Policy, Evaluated Per Request

That decision draws on blended identity (user + agent) plus real-time posture signals from the device or environment, evaluated together for fine-grained authorization rather than the agent inheriting access wholesale.

03 Credential Exchange

Aembit exchanges that decision for whatever credential the destination system actually accepts – the agent or workload never needs to store a secret. Aembit enforces the same model across cloud, SaaS, and on-premises environments and works with existing workforce IAM systems and gateways without displacing them.

BENEFITS

Attributable

Every event carries both the human and the agent that acted.

Revocable

Cut one agent's access with a one-click policy.

Least-Privileged

Short-lived credentials scoped per task, not inherited from a user.

PROOF

A \$300 billion investment firm rolled this out across their enterprise Claude deployment in two weeks, with under six hours of security team time – replacing stored long-lived secrets and full-identity impersonation with scoped, attributable access, on top of the Okta instance they already had.

\$300B

investment firm,
heavily regulated.

2 weeks

from start to production
deployment.

<6 hours

of security team
time required.

Manage Access, Not Secrets.

Secure Claude across your workforce without loosening your security standards.

[Download the Complete Whitepaper](#)

[aembit.io](#)