akto

Securing Agent Identities

AI agents act at machine speed with privileged identities. Akto helps you secure and govern every agent identity.

THE CHALLENGE

Your IAM program is missing agent identities

Traditional identity tools were built for humans and known service accounts. Agents don't follow scripts - they decide, chain actions, and reach for credentials no one is tracking.

Ungoverned, persistent access

Agents run on standing credentials with no verification at the point of use. When one is compromised, the access simply persists.

Overprivileged by default

Employees hand agents broad, static permissions across enterprise assets - far more scope than any single task requires.

No owner, no audit trail

Most agents run with no clear owner, no scoped policy, and no record of what they touched - leaving nothing for forensics or compliance.

THE SOLUTION

Identity governance, built for agents

Akto discovers every agent identity, maps its access, and governs it across the full lifecycle - at machine speed

Discovery

Discovers every identity tied to an AI agent - API keys, bearer tokens, OAuth credentials, etc.

Identity Context

Understand their ownership, permissions, and purpose with complete context.

Lifecycle Management

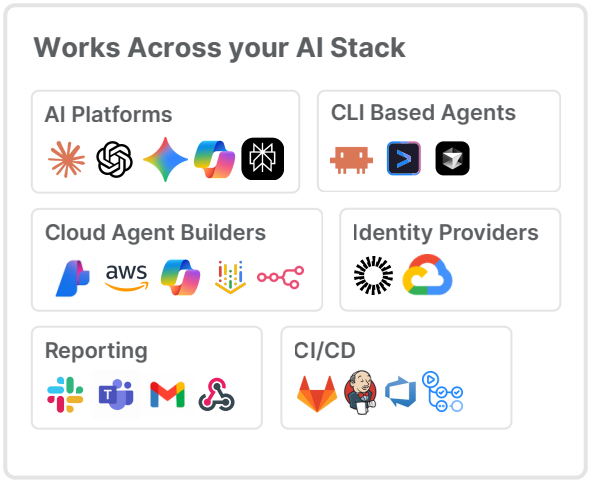
Automate identity lifecycle and enforce policies around identity rotation, expiration and segregation.

Threat Detection

Catch real-time threats, compromised identities, and anomalous behavior across your agent fleet.

Posture Management

Surface excessive privileges, stale machine access, and misconfigurations.



USE CASES

Akto in practice

Traditional identity tools were built for humans and known service accounts. Agents don't follow scripts - they decide, chain actions, and reach for credentials no one is tracking.

A new agent ships

Register it at creation, assign an owner, and scope its access automatically - no orphan identity, no standing key.

Agents call MCP servers

Grant scoped, consented, time-bound access to MCP servers instead of persistent, always-on credentials.

A credential leaks

Detect the compromise, see the blast radius, and revoke or rotate before the access can be abused.

Audit season arrives

Produce a full inventory of every agent identity, what it can reach, and what it has touched - ready for forensics and compliance.

Access has sprawled

Surface overprivileged agents and stale machine access, then right-size every identity down to least privilege.

Existing agents go untracked

Discover every API key, bearer token, and OAuth credential agents use - and the scope each one actually needs.

Gartner Peer Insights. 4.8

AI agents act at machine speed with privileged identities. Akto helps you secure and govern every agent identity.

sales@akto.io | +1 (415) 329-1415

