Delinea

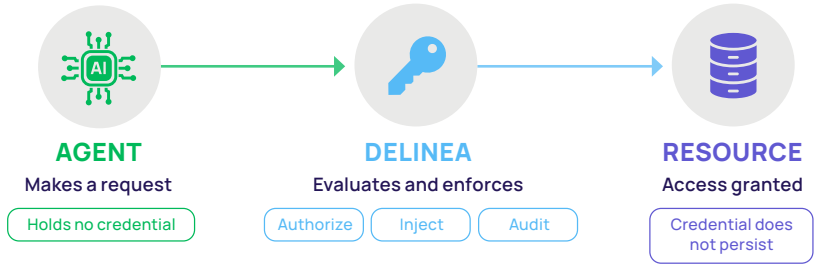
Securing AI Agents

Move at AI speed. Stay in control.

AI agents already carry real privilege inside the enterprise. They query databases, run commands and call tools against production systems, often faster than a security team can track. Most identity programs authenticate a session once, at the door, and trust what happens after that. An agent that opens dozens of connections and takes hundreds of actions in the time it takes a person to log in once breaks that model. Most organizations have no way to see or control what happens once the session begins.

Delinea closes that gap through runtime authorization. Every action an agent takes is authorized before it runs, for the life of the session, tied to a named identity.

How It Works



The agent never holds a credential

Delinea injects the credential at the moment of access, whether that is a vault secret, an IAM role assumption, a certificate or an OAuth token. The credential never enters the agent process or the host. This capability leverages production-proven StrongDM technology, now part of Delinea.

Authorization is continuous

Policy is evaluated on every tool call throughout the session, not only when it starts. If an action is not permitted, it does not run.

Every session is recorded

Policy is evaluated on every tool call throughout the session, not only when it starts. If an action is not permitted, it does not run.

Benefits

Contained blast radius

A compromised or misbehaving agent stays contained instead of moving laterally across the environment. Access can be revoked network-wide.

Audit and incident response

Every action ties to a named identity, so incident response teams know what an agent ran and when, not just that a connection occurred.

No standing credentials

Credentials are injected at the moment of access and removed when the task ends. Nothing sits exposed between tasks.

Just-in-time, context-bound access

Policy gates every agent by identity and by context, such as resource sensitivity or task scope. Access ends automatically once the task completes.

Runtime authorization reads the protocol layer, not just the connection.

Keeping the credential out of an agent's reach and injecting it at the point of access is a useful starting point. It closes off one class of risk. But confirming a connection opened doesn't answer what happened inside it. It doesn't record the query, the command or the tool call the agent made, and it can't authorize individual actions before they run. The Delinea proxy goes further. It is both session-aware and identity-aware: it knows a connection occurred, who the agent was, what it ran and whether each action was permitted.

What runtime authorization enforces

Per-action authorization
Policy is evaluated on every tool call, not once at session start. An action that isn't permitted does not run.

Identity attribution
Human-initiated sessions are logged under the named developer's identity. Autonomous agents are logged under a dedicated service account. Every action has an owner.

Full session recording
The tool call or query is tied to a named identity for every session, not just confirmation that a connection occurred.

One enforcement point
MCP, SSH, Kubernetes, databases and cloud consoles are brokered through the same proxy, producing a consistent policy and audit record across protocols.

Instant, network-wide revocation
Access can be revoked without disrupting other services or human workflows sharing the same environment.

Where runtime authorization applies

Developer AI tools
The agent connects through a named identity. It holds no credential, and every tool call is evaluated against policy before it runs. Every action is logged under the named identity for incident response.

Autonomous agents on infrastructure
The agent operates under a dedicated service account running on cloud and on-premise infrastructure, not a human credential. No static token sits on the host. Access can be revoked network-wide without disrupting other services.

Runtime authorization covers databases, SSH hosts, Kubernetes clusters, cloud consoles and MCP-brokered connections.

Learn more about Delinea runtime authorization. Contact our experts.

Delinea

Delinea is the identity security platform that governs what humans, machines, and AI agents do once they have access. It enforces just-in-time authorization at the moment of action, not just when access is first granted, reducing reliance on standing privilege across on-premises, multi-cloud, and ephemeral infrastructure. Built on deep privileged access management expertise, the Delinea Platform continuously discovers identities, analyzes risk, and enforces least privilege, so every access decision is defensible. This gives organizations the visibility and control to adopt AI with confidence. Learn more at **delinea.com**.