



Access alone is not access-controlled

Authentication decides who gets in. Delinea decides what happens next.

The problem is not getting access; it is everything that happens after.

The challenge

Even when access is legitimate, little governs what an identity can do once inside. That gap between authentication and execution is where damage happens; lateral movement, privilege escalation and blast radius all grow where enforcement does not reach, and breakouts now happen in minutes, not days.

AI agents, humans and machines share the same weaknesses: credentials that never expire, privileges that outlast the task, and actions traditional controls cannot evaluate as they happen. AI agents act at machine speed, so exposure compounds before anyone notices. The discipline is not new; the speed is. The result is standing privilege, unclear accountability, and no control over what any identity does after login. Access alone is not control.

Secure AI agents, humans, and machines without slowing the business

Standing privilege is your largest unmanaged risk across AI agents, humans and machines. Delinea reduces it without disrupting operations by enforcing Zero Standing Privilege (ZSP) where risk demands it, securing credentials and continuously authorizing sessions, queries and tool calls through one platform.

90%

of security teams report pressure to loosen controls to keep AI initiatives moving

59%

of organizations say they lack a viable alternative to standing privilege for machine and AI agents

80%

of organizations say they are unable to understand why a non-human identity took a privileged action

Source: 2026 Identity Security Report

Benefits



Agents stay in scope.

Each agent gets only what its task requires, so a compromised or misused agent has far less to reach.



Agents never hold credentials.

In a brokered session, the credential is injected at the proxy at the moment of use and never reaches the agent.



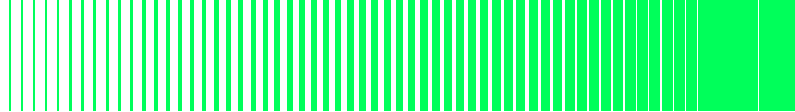
Every action is cleared before it happens.

Policy is evaluated at the moment of execution. An action that is not permitted does not run, so problems are prevented rather than flagged afterward.



Every decision is defensible.

Each action is tied to a named identity and recorded, so when a board or a regulator asks when happened and why, the answer is already there.



I How Delinea closes the gap

Reduce standing privilege and enforce control at the moment of action

Static credentials and standing access are the entry points attackers depend on most. Delinea removes them and keeps enforcing policy from the point of access to the moment of action.

- ✓ Credentials are vaulted, rotated automatically and injected at the moment of use, never left dormant in scripts or pipelines.
- ✓ Elevated access is granted just-in-time for a specific task and window, then revoked.
- ✓ Each session, query and tool call is evaluated and controlled at the moment it happens across databases, servers, Kubernetes, cloud consoles and MCP-brokered connections. Lateral movement and privilege escalation are stopped before they succeed.
- ✓ Every privileged session across AI agents, humans and machines is recorded and tied to a named identity. One record serves both the audit trail and the risk signals.

Govern identity and connections under one policy

Fragmented tools create the gaps attackers look for. Delinea applies one consistent policy across every identity type and access path, including on-premise, cloud and SaaS.

- ✓ Remote sessions for admins, contractors and vendors are authorized, recorded and tied to a named identity. Third-party access becomes a governed, auditable activity instead of a blind spot.
- ✓ Least-privilege endpoint controls block ransomware and privilege escalation before a workstation becomes a foothold.
- ✓ Segregation of duties and sensitive access rulesets monitor user risk continuously within ERP and connected applications. Automated user and role access reviews support SOX, HIPAA, and PCI-DSS requirements without manual review cycles or spreadsheet reconciliation.

Outcomes you can report on:

70%
reduction

*in standing privileges
across cloud and on-
premises (ROI study)*

33%
decrease

*in security incidents or
breaches (ROI study)*

49%
improvement

*in the ability to
detect threats and
anomalies (ROI study)*

44%
decrease

*in unauthorized remote
access by employees
and vendors (ROI study)*



Analyst call out: Analysts agree: a Leader in the [2025 Gartner Magic Quadrant for PAM](#), seventh consecutive time, and an Overall Leader in the [KuppingerCole Leadership Compass for PAM \(2026\)](#) and [NHI Management \(2025\)](#).

Delinea extends the PAM you already own into a continuous authorization model: just-in-time access, and each action authorized as it happens, for AI agents, humans and machines, under one model and one audit trail. No rip and replace; apply ZSP where risk demands it, deploy in weeks, run at 99.995% uptime and with up to 90% fewer resources than legacy alternatives.

One platform. One audit trail. Each decision defensible. See it in action at delinea.com.



Delinea

Delinea is an identity security platform governing what AI agents, humans and machines can do, and for how long. Just-in-time authorization extends privileged access management from access to action, cutting standing privilege across on-premise, multi-cloud and ephemeral infrastructure. Its platform scores identity risk and keeps access decisions auditable. Over 9,000 organizations, including two-thirds of the Fortune 100, rely on Delinea. Learn more at delinea.com.