AKEYLESS

Secure the Era of AI Agents

Akeyless AI Agent Identity Security protects autonomous systems with secretless, short-lived identities and controls what they can do at runtime with intent-based, just-in-time access.

AI Innovation Demands a New Approach to Identity

Organizations are racing to deploy AI agents that automate work, decisions, and communication. These initiatives are now essential to staying competitive. But as AI scales across clouds, data, and development tools, a new challenge has emerged: how to secure autonomous systems that connect without human oversight.

Traditional identity and secrets tools weren't built for this. Credentials, tokens, and keys proliferate across prompts, logs, and pipelines, creating access paths no team can fully see or control.

Akeyless AI Agent Identity Security gives every agent a real identity. It issues secretless, short-lived credentials that vanish when the task ends and ensures agents act only within approved intent and authority. Enterprises can move fast with AI while staying in control of trust.

Key Benefits

- Empower DevOps to deploy AI agents faster and more securely.
- Reduce risk and exposure by removing static credentials.
- Simplify governance with centralized visibility and control.
- Control what AI agents can do at runtime with intent-based access.
- Prevent sensitive data leakage with real-time masking.
- Future-proof security with zero-knowledge, quantum-safe protection.

How Akeyless Secures AI Agents

Akeyless delivers identity and access security purpose-built for autonomous systems. Its platform protects AI agents from credential exposure, enforces controlled access, and brings visibility across environments. The solution is built on three key capabilities that work together to control what agents can do at runtime, how they access systems, and how their activity is tracked over time, with the Akeyless Gateway acting as the centralized enforcement point for all agent interactions:

- **Agentic Identity Intelligence** continuously maps AI agents, the identities they use, and how they access systems and data.
- **SecretlessAI**™ replaces hardcoded credentials with just-in-time, short-lived access. Secrets stay out of code, prompts, and pipelines.
- **Agentic Runtime Authority** controls what AI agents can do by evaluating intent and enforcing policy in real time:

Together, these capabilities create a unified security layer for autonomous systems, helping organizations scale AI securely and with confidence.

Akeyless AI Agent Identity Security

Agentic Identity Intelligence

- Discover AI agents and access paths
- Expose orphaned credentials and excessive privileges
- AI agent data mapping and lineage
- Integration with governance and SIEM tools

SecretlessAI™

- Eliminate static credentials, certificates, and keys
- Access brokered through the Akeyless Gateway
- Just-in-time, task-scoped identities with strict TTL
- Zero Persistent Knowledge (agents never store secrets)

Agentic Runtime Authority

- Intercept and govern agent actions by intent
- JIT, scoped access with zero standing privileges
- Real-time session monitoring and kill switch
- Full traceability from prompt to action

Agentic Identity Intelligence

You can't secure what you can't see. Agentic Identity Intelligence continuously discovers AI agents, the identities they use, and how they access systems and data. It builds a time-aware system of record that maps agent activity, access paths, and data flows across environments. Security teams gain a complete picture of who owns each agent, what it can access, and how data moves through AI-driven workflows. This context continuously informs policy decisions and strengthens runtime enforcement.

How It Protects

- Discovers AI agents, identities, credentials, and entitlements across environments.
- Identifies orphaned credentials, unmanaged agents, and privilege drift.
- Maps data access, movement, and lineage across agent workflows.
- Provides audit-ready evidence for governance, compliance, and investigations.
- Integrates with SIEM, GRC, and data governance tools for continuous monitoring.

SecretlessAI

AI agents shouldn't hold credentials. SecretlessAI replaces static keys and tokens with short-lived access issued at runtime. Agents authenticate with their native identity and receive temporary credentials that expire immediately after use. No secrets appear in code, prompts, or logs, and Akeyless Distributed Fragments Cryptography (DFC) keeps all keys mathematically protected and invisible, even to Akeyless. The result is secure, auditable access across clouds, SaaS, and on-prem systems without slowing development.

How It Protects

- Issues short-lived identities and dynamic credentials at runtime.
- Eliminates secret zero with certificate or cloud IAM–based authentication secured by DFC.
- Removes hardcoded credentials from code, prompts, and pipelines.
- Keeps secrets out of developer workflows through integrations for Cursor, VS Code, n8n, and Copilot via MCP.
- Extends secretless access to legacy and on-prem systems using lightweight gateways.

Agentic Runtime Authority

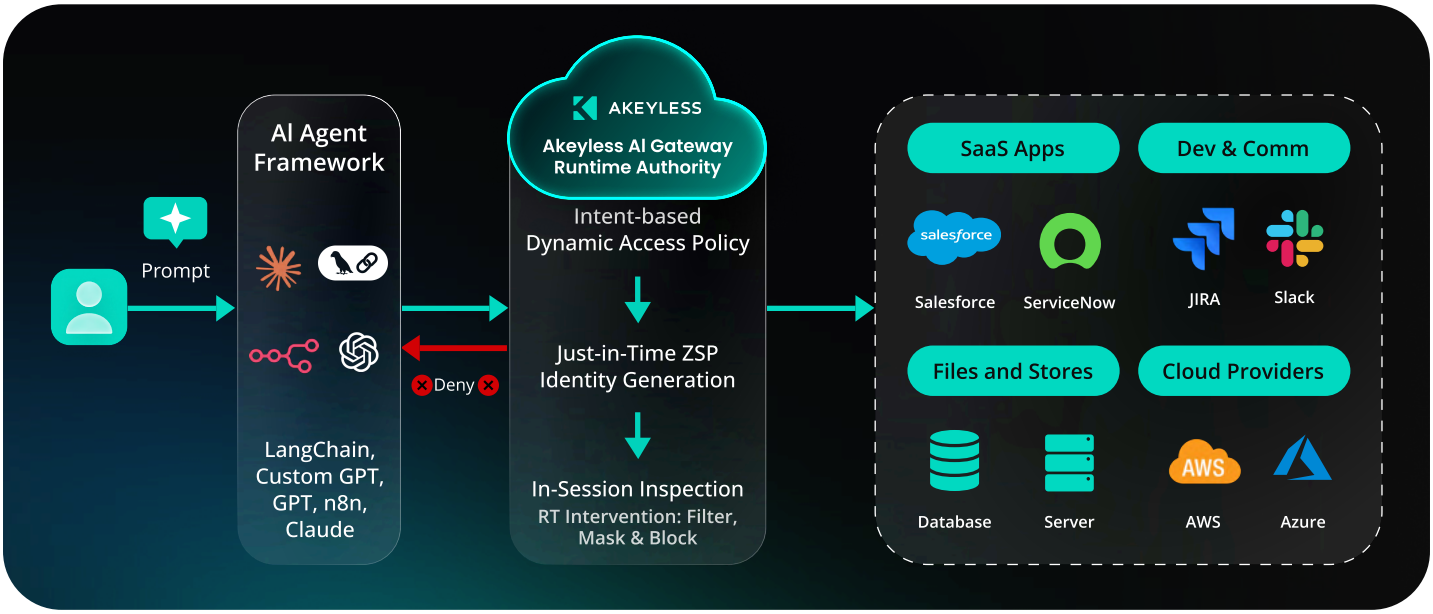
AI agents shouldn't operate unchecked. Agentic Runtime Authority intercepts every request before access is granted, evaluates intent, and enforces policy in real time. Agents have no direct connectivity to target systems, with all access brokered through a controlled execution path.

Instead of relying on static roles or pre-approved permissions, Akeyless determines what an agent is trying to do and allows only actions that align with approved intent. Access is granted just in time and controlled at the command level during execution. Responses are inspected and masked before reaching the agent, and access is revoked immediately when the task is complete or behavior deviates.

How It Protects

- Brokers communication through the Akeyless Gateway so agents have no direct connectivity.
- Intercepts agent requests and evaluates semantic intent before execution.
- Enforces Zero Standing Privilege with just-in-time, task-scoped access.
- Inspects live sessions and blocks unsafe or mismatched actions before reaching systems.
- Provides a real-time kill switch to instantly terminate suspicious activity.
- Inspects and masks sensitive data in responses before it reaches the agent.
- Creates a complete execution trace from prompt → intent → policy → action.

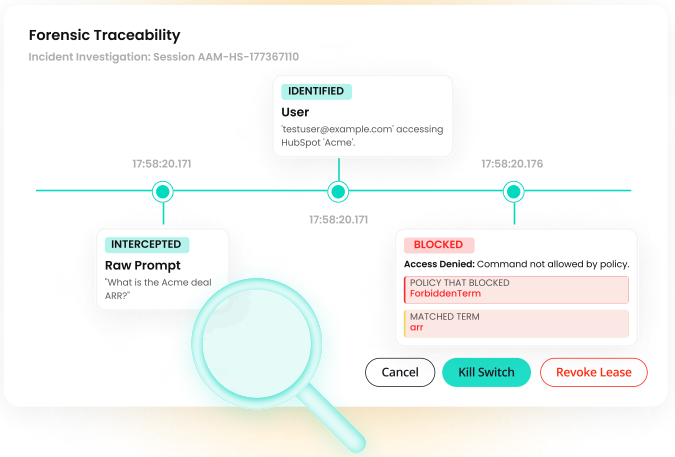
Agentic Runtime Authority In Action

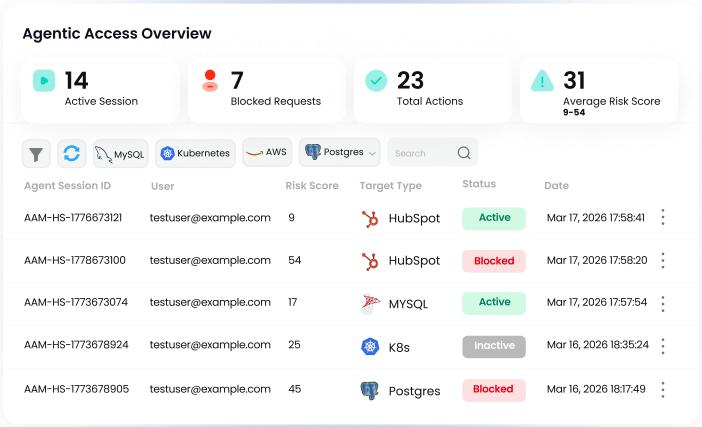


1. A prompt or tool call is initiated from the AI agent framework.
2. The request is intercepted by the Akeyless Gateway, with no direct access to target systems.
3. The request is analyzed against policy to determine what the agent is trying to do and whether it is allowed.
4. A scoped, short-lived identity is generated with Zero Standing Privilege.
5. Commands and responses are monitored and controlled in real time, with unsafe actions immediately blocked and sensitive data masked.
6. Every step, from prompt to policy decision to execution, is captured in a unified audit trail.

Take Control of AI Security Without Losing Speed

You don't have to choose between innovation and protection. Every agent is authenticated, every secret remains hidden, and every action stays visible for full accountability. Powered by the Akeyless Identity Security Platform and its Distributed Fragments Cryptography™ (DFC) foundation, your AI environment gains protection that is private, verifiable, and built for scale. Agent access and actions are controlled from request through execution, with a complete audit trail for full traceability and accountability.





Your Advantage

- Faster and safer AI adoption with security built in, not bolted on
- Visibility into how every AI agent acts and accesses systems
- Simpler governance across clouds, SaaS, and on-prem systems
- Assurance that secrets and keys remain yours alone
- Long-term resilience with zero-knowledge and post-quantum cryptography

Built for the Most Demanding Environments

Akeyless meets the highest standards for security and compliance so you can adopt AI with confidence.

- FIPS 140-3 validated cryptography
- SOC 2 Type II and ISO 27001 certified
- GDPR and PCI DSS aligned
- Designed for regulated and global enterprises

Ready to secure your AI agents?

Request a demo at akeyless.io/demo

Akeyless.io

© 2026 AKEYLESS. All Rights Reserved.