AKEYLESS

Secure the Era of AI Agents

Akeyless AI Agent Identity Security protects autonomous systems with secretless, short-lived identities for secure access everywhere they run.

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. Each agent can generate its own credentials, tokens, and keys 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 appear only when needed and vanish when the task ends, verifying every connection and keeping secrets out of reach so enterprises can move fast with AI and stay 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.
- Secure agent connectivity across clouds and systems.
- Enforce least privilege for every AI interaction.
- 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, uncontrolled access, and lack of visibility across environments.

The solution is built on three key capabilities that work together to remove secrets, verify identity, and enforce least privilege:

- **Secretless AI** replaces hardcoded credentials with real-time, short-lived access. Secrets stay out of code, prompts, and pipelines.
- **AI Agent Identity Provider** gives every agent a verifiable identity that can authenticate securely across clouds, SaaS, and on-prem systems.
- **Privileged AI Agent Access** applies policy-based control and monitoring so AI agents can perform sensitive actions safely and with full visibility.

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

Akeyless AI Agent Identity Security

Secretless AI™

- Eliminate Creds, Certs, Keys
- Real-Time Secrets Retrieval
- Dynamic Identities & Entitlements
- Secret-Zero Removal

AI Agent Identity Provider

- Ephemeral Access (IT & ZSP)
- Identity Federation Across Clouds, Hybrid
- Advanced Authentication Schemes

AI Agent PAM

- Zero Trust Access (Proxy)
- Session Recording
- Rogue Agent Session Termination

Secretless AI

AI agents shouldn't hold credentials. Secretless AI 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.

AI Agent Identity Provider

AI agents need trusted identities to operate safely across systems. The Akeyless AI Agent Identity Provider gives every agent a verifiable, short-lived identity that authenticates securely across clouds, SaaS, and on-prem environments. These ephemeral identities replace hardcoded API keys with policy-based, federated access that scales automatically as agents are deployed. Each identity is issued and verified in real time, ensuring only approved agents can connect and act.

How It Protects

- Provides short-lived, policy-controlled identities for AI agents.
- Federates authentication across cloud, SaaS, and on-prem systems.
- Uses existing IAM roles, certificates, or SPIFFE/SPIRE as identity anchors.
- Enforces access policies and entitlements at the moment of issuance.
- Scales seamlessly as agents multiply across environments.

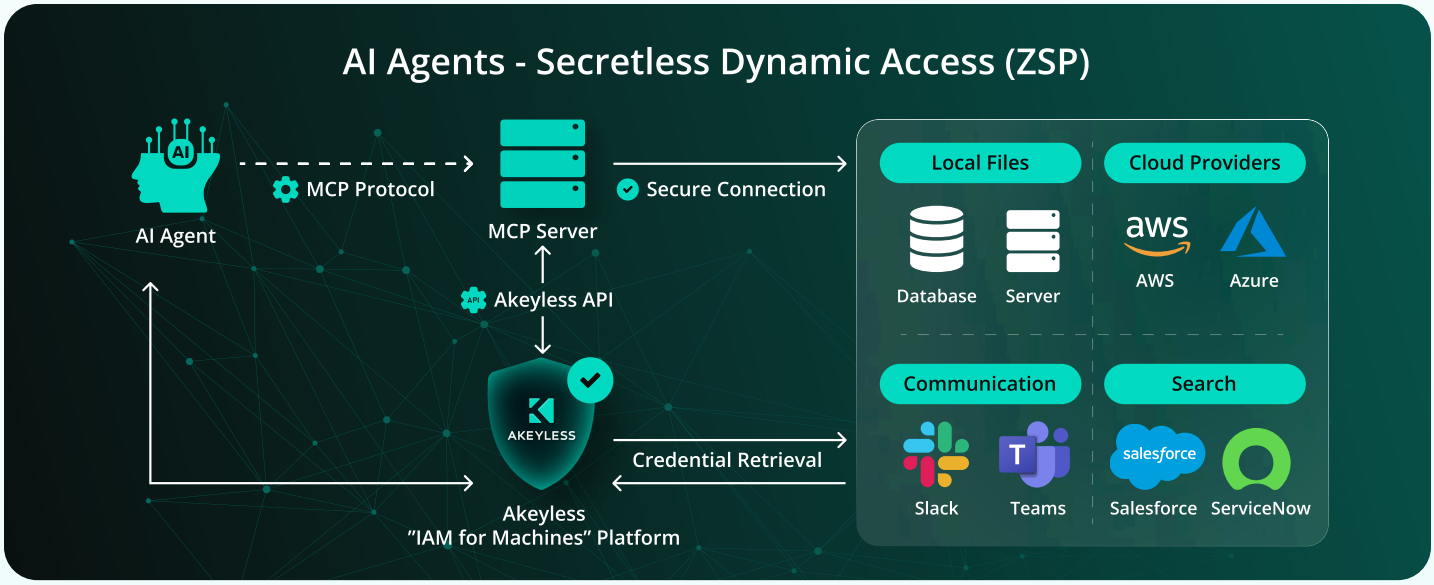
Privileged AI Agent Access

Some AI agents need elevated access to perform sensitive actions such as database updates, infrastructure changes, or code deployment. Privileged AI Agent Access extends Zero Trust controls to these autonomous sessions. Agents connect through secure, policy-enforced channels and only for the time required. All actions are authenticated, recorded, and continuously monitored so security teams can detect and stop anything unusual in real time.

How It Protects

- Grants just-in-time privileged access with zero standing privileges.
- Monitors and records all agent activity for full auditability.
- Detects rogue or unauthorized sessions so they can be terminated instantly.
- Applies least privilege to autonomous systems performing sensitive tasks.
- Provides a single control plane for managing privileged human and machine sessions.

Runtime Flow: Secure Access for AI Agents



1. **AI Agent** → MCP Server: The agent sends a request via the Model Context Protocol
2. **MCP** → Akeyless API: The MCP server authenticates with Akeyless using infrastructure identity (e.g., IAM role, GitHub JWT).
3. **Akeyless** → Target System: Akeyless connects to the endpoint (database, SaaS app, or cloud) and issues a temporary credential back to the MCP server.
4. **MCP Server** → Agent: The credential is used to establish a secure session for the AI agent to complete its task.

Delivers ephemeral, policy-bound access without embedding credentials in the agent.

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.

Your Advantage

- Faster and safer AI adoption with security built in, not bolted on
- Visibility into how every AI agent connects 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

AI-Powered Insights, Detection & Response with Akeyless Jarvis™

As AI agents multiply across environments, visibility and control are critical. Akeyless Jarvis™ delivers AI-driven discovery, detection, and response for autonomous identities. It continuously analyzes behavior to surface unmanaged agents, identify anomalies, and highlight risky or excessive access.

Security teams gain a single view of how AI agents authenticate, what they access, and where exposure exists. Insights integrate with SIEM and SOAR tools, turning identity data into actionable intelligence across both non-human and human identities.

Built for the Most Demanding Environments

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

- FIPS 140-2 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