# token

# *Identity-First* AI Agent Security

AI agents are becoming first-class actors in the enterprise with highly privileged identities. They write code, access sensitive data, call APIs, and make decisions at machine speed. Token Security is the first platform to secure AI agents by understanding their intent, giving organizations complete confidence in how agents are created, governed, and operated without slowing innovation.
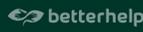
bloomreach    betterhelp    Hewlett Packard Enterprise    HiBob    dayforce

---

## Unseen. Unsecured. Out of Control.

As AI use explodes, enterprises face a new class of identity threat: intelligent, autonomous agents with unchecked access to critical systems. Traditional Identity and Access Management (IAM) programs weren't designed for this new class of identity, but without comprehensive visibility, intent-based permissioning, and continuous governance, enterprises risk losing control over how AI agents access and act within critical environments. AI agents are difficult to secure because they are:

### Everywhere & Exploding

AI Agent and non human identitites span across on-prem, cloud and AI platforms, while outnumbering human identities by 50:1

### Complex & Connected

A single compromised agent can trigger cascading damage across every connected system it touches.

### Impossible to Remediate

Without understanding the context and usage of each AI agent and identity, security and IAM teams fear breaking production systems.

---

The Solution

## How Token Security Solves AI Agent Security Challenges

Token Security helps security and identity teams manage the full AI agent identity lifecycle, so they can adopt agentic AI quickly, without losing control.
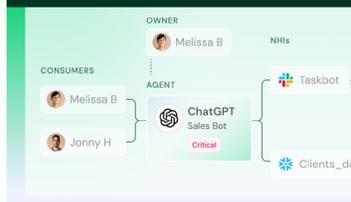
### Shadow AI & MCP Server Discovery

Automatically discover and inventory every AI agent, custom GPT, and coding agent using MCP servers.

### AI Agent Ownership and Accountability

Assign clear ownership for each AI agent to eliminate orphaned accounts that pose long-term risk.

### AI Agent Access Control and Right-Sizing

Continuously evaluate AI agent access and right-size permissions according to scoped agent intent.
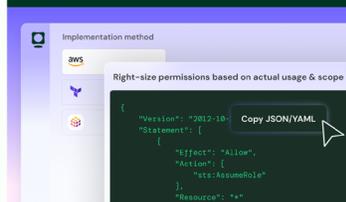
### Traceability in a Multi-Agent Ecosystem

Log every AI agent action to maintain an audit trail for compliance evidence and forensics investigation.
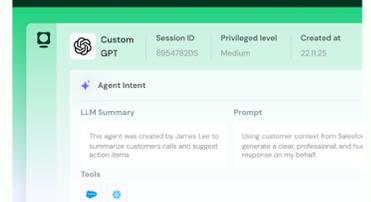
# *The Token* **Security Platform**

Token Security is the AI Agent Security Platform built to secure AI agents by treating identity as the control plane, delivering end-to-end security across the AI agent lifecycle.



Databases   Identity Providers   Critical SaaS   Vaults

Cloud Accounts   Code and CI/CD   On-prem

---
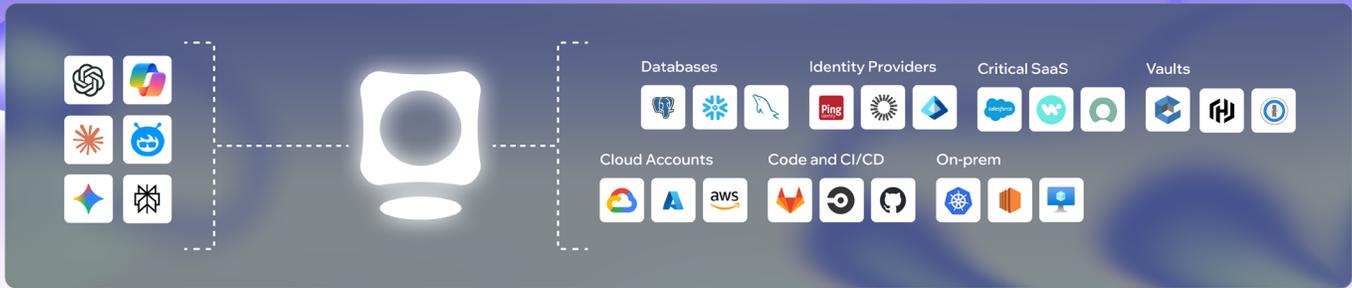
→ *Discover*

## Know Every AI Agent, Everywhere

You can't secure what you can't see. Token provides deep, contextual visibility into all AI agents across cloud environments, SaaS platforms, internal tools, and custom frameworks.

→ *Understand*

## Enforce Least Privilege for AI Agents

By analyzing massive amounts of identity and telemetry data, Token provides contextual awareness for AI agents, enabling you to understand agent intent, who owns agents, and what agents can access.

→ *Enforce*

## Set the Rules for AI Agent Trust

As AI agents become core to business operations, Token enables security and identity teams to move from ad-hoc controls to automated remediation and formal governance based on intent-based access policies.

---

`Why Token Security`

# Created for today's AI, not yesterday's IAM.

**01**

## Built for Agentic AI

Token treats agents as first-class identities that require continuous discovery, governance, and control, moving beyond bolted-on policies on legacy, human-centric tools.

**02**

## Identity is the Control Plane

Guardrails and prompt security fail when access is granted. Token secures agents at the identity level, where control is possible.

**03**

## Deep Identity Intelligence

Token correlates AI agents, humans, secrets, permissions, and data in a unified identity graph, revealing the blast radius and enabling remediation at scale.

**04**

## End-to-End AI Agent Identity Lifecycle Governance

Agents fail over time, not just at creation. Token enforces ownership, intent, access, and governance from an AI agent's creation through retirement.

**05**

## Intent-Based Least-Privilege Enforcement

Token applies intent-aware least-privilege to agents, ensuring they have only the permissions needed for their purpose, and only for the time required.

---

www.token.security →

**token**