

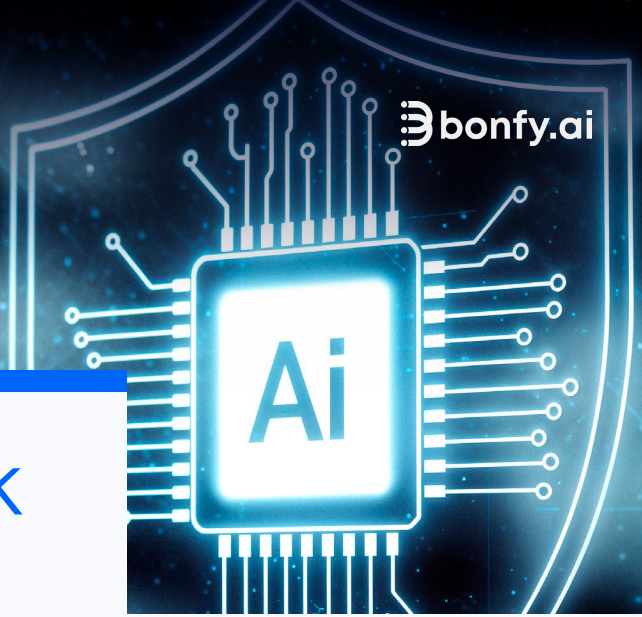


Bonfy ACS™ for AI Agent Security



AI agents are rapidly moving from experiments to production, orchestrating complex workflows across SaaS apps, data stores, and external services. They read, write, and act on behalf of users and systems, often outside traditional security controls. Bonfy ACS™ provides adaptive content security for AI agents, protecting enterprise data across agent grounding, reasoning, and outputs without slowing innovation.

The AI Agent Risk Surface



As organizations adopt system-level agents (e.g., Microsoft Copilot Studio, Salesforce Agentforce, ServiceNow agents), agentic coworkers (e.g., Claude Code and Cowork), and browser-based agents, information now flows through multi-hop chains of LLMs, MCP servers, APIs, and SaaS systems with new demands for data surface visibility and posture management. Traditional DLP, DSPM, and endpoint tools were never designed to see or govern these flows.

Key AI agent risks include:

- Excessive grounding data: Agents are granted access to broad repositories (SharePoint, Google Drive, CRM, file stores), exposing sensitive and regulated content to LLMs.
- Unmonitored tool calls (MCP/other APIs): Agents send content to external tools and services that may mishandle PII, client data, or IP.
- Hallucinated or repurposed content: LLMs can generate outputs that combine confidential, customer-specific, or regulated information in unexpected ways.
- Shadow agents and shadow AI: Employees adopt unsanctioned agent frameworks and browser-based agents that impersonate the user and access corporate data without governance.
- Lack of visibility and attribution: Security teams cannot easily see which agents accessed which content, what they did with it, or who/what generated risk.

The result:

Organizations are “flying blind” as agents access, transform, and share sensitive content across systems the security stack does not monitor effectively.

Bonfy ACST™: Data-Centric Security for AI Agents

Bonfy ACST™ is an AI data security platform that protects unstructured data across email, files, SaaS apps, collaboration tools, AI systems, and AI agents. Its entity-aware Knowledge Graph engine understands the business, people, customers, and consumers behind the data to deliver high-accuracy detection and true policy enforcement across both human and agentic workflows.

For AI agents, Bonfy ACS delivers three core protections:

- **Control what agents can see**
Bonfy limits which sensitive content agents can access so prompts and grounding data stay within business and trust boundaries.
- **Control what agents can do with data**
Bonfy lets agents check content safely during reasoning and execution to prevent misuse of PII, regulated data, and customer-specific information.
- **Control what leaves the organization**
Bonfy inspects agent outputs across email, SaaS, and collaboration tools to block risky messages and files before they leak sensitive data.

Key Capabilities for AI Agent Security

Bonfy ACS extends its multi-channel platform to AI agents with the following capabilities:

- **Unified multi-channel coverage:**
One platform monitors data in motion, at rest, and in use across email, SaaS, collaboration tools, AI systems, and agents—eliminating blind spots.
- **Context-aware intelligence:**
A knowledge graph maps your organizational entities and relationships for precise detection and fewer false positives.
- **Centralized policy and automation:** A single control plane streamlines discovery, labeling, remediation, and enforcement across all workflows.
- **Entity-level risk management:**
Agents are modeled as first-class entities with cross-channel correlation and risk scoring.
- **Flexible deployment:** Delivered as cloud-native SaaS (multi-tenant, single-tenant, or BYOC) and integrates with Microsoft, Google, Salesforce, Slack, and more.

Outcomes

With Bonfy ACS, organizations can:



Adopt AI agents faster by enabling automated AI data governance.



Maintain strong privacy, regulatory, and contractual controls across agent workflows.



Reduce tool sprawl by consolidating AI data security into a single, high-accuracy platform.



Provide executives and boards with clear evidence that AI-related data risks are understood and controlled.

Contact Us

For inquiries or additional information, please contact us at info@bonfy.ai

bonfy.ai

 /bonfy-ai

 bonfy.bsky.social