

Govern AI Agent Risk from Discovery to Enforcement

Reco Finds the Risk. Kiteworks Governs the Data.

AI Agent Governance

FedRAMP

CMMC 2.0

EU Data Act

GDPR

HIPAA

The Challenge

AI agents are spreading across SaaS platforms faster than security teams can review them. Reco's own research finds 71% of knowledge workers use AI tools without IT approval, and analysts project that 40% of enterprise applications will carry agentic capabilities by the end of 2026. The Kiteworks 2026 Data Security and Compliance Risk Report puts a number on the resulting gap: no AI containment control is deployed by more than 31% of organizations, and 65% of organizations that went looking for shadow AI usage found it. Security teams can see the risk building. Most cannot yet govern it, because visibility and enforcement have lived in separate tools, owned by separate teams, running on separate data.

The Solution

The Reco Platform discovers every agent, app, and identity across your ecosystem, using the largest agent and app catalog in the market so security teams start with real risk profiles instead of a blank slate. The Kiteworks control plane takes that risk signal and enforces policy on the sensitive data those identities can actually reach, across email, file sharing, APIs, managed file transfer, and AI agent workflows. One governed, audited control plane covers both the humans and the agents acting on their behalf, so the gap between finding a risk and closing it collapses from months to minutes.

The Governance Gap, Quantified

Findings from the Kiteworks 2026 Data Security and Compliance Risk Report and Reco's own research into agent and app sprawl.

31%

Highest AI Containment Control Adoption
Rate Measured

65%

Organizations That Found Unapproved AI
Tool Usage

260+

Agent and App Platforms Reco Covers

Key Capabilities



Continuous Identity & Agent Discovery

Reco maps every application, human and non-human identity, and agent, surfacing sprawl and over-permissioned access as it appears. The Reco Graph keeps that inventory current as new tools and agents are adopted.



Real-Time Policy Enforcement

The Kiteworks Data Policy Engine acts on that risk signal instantly: view-only access, SafeEDIT, encryption, or an outright block. Policy decisions apply the moment risk is identified, not at the next audit cycle.



One Control Plane for Humans and Agents

The Kiteworks Secure MCP Server governs AI agents under the same RBAC/ABAC policy, encryption, and audit trail already applied to human users. Security teams manage one policy model instead of a parallel set of rules for machine identities.

Key Capabilities



Possessionless Editing

SafeEDIT lets authorized users edit sensitive data directly in the browser, without ever downloading the file. Sensitive data never leaves the governed environment, even during active collaboration.



Unified Audit Evidence

One audit log spans every access, share, edit, and transfer event, feeding SIEM platforms like Splunk and ArcSight. Compliance teams get one evidence trail instead of reconciling logs across Reco, Kiteworks, and point tools.



Compliance-Grade Foundation

FedRAMP High In Process, building on FedRAMP Moderate Authorized since 2017, and mapped to regulations such as HIPAA, CMMC 2.0, GDPR, and PCI DSS. The same controls that satisfy federal auditors extend automatically to agent-driven data access.

Where This Fits



Agent Sprawl Containment

Bring newly discovered AI agents under governed policy the moment Reco surfaces them, closing the window between discovery and enforcement that most organizations never close today.



Regulated Industry Adoption

Extend agentic AI into healthcare, financial services, and government workloads with audit-ready evidence, without waiting for a compliance exception process to catch up.



SaaS Modernization

Replace fragmented point tools with one connected path from identity risk to enforced data governance, spanning email, file sharing, APIs, and managed file transfer.

Ready to Close the Gap Between AI Agent Discovery and Enforcement?

www.kiteworks.com

Kiteworks

