Kiteworks

SOLUTION BRIEF

Kiteworks Compliant AI

Data-Layer Governance for AI Agent Access to Regulated Data

AI agents are the new digital employees—accessing financial records, patient data, CUI, and trade secrets at machine speed. Unlike human employees, **agents exercise no judgment** and will access any data or execute any function they are not explicitly prevented from invoking.

Regulations such as HIPAA, CMMC/ITAR, PCI DSS, SEC, and SOX require strict controls for data access, audit trails, and encryption. These obligations apply equally to AI agents accessing regulated data.

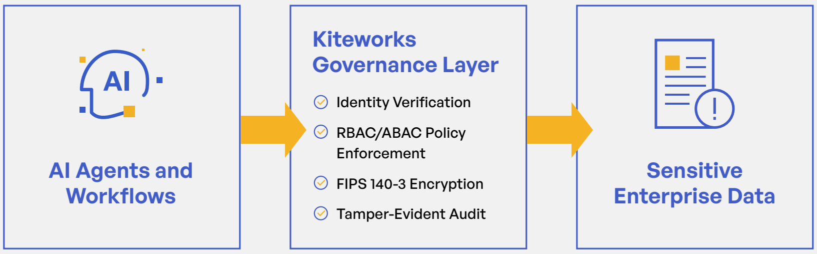
Data-Layer Governance: The Only Layer AI Agents Cannot Bypass

Kiteworks Compliant AI governs agent interactions at the data layer—not the model layer. Model prompts and safety filters can be bypassed; data-layer enforcement cannot.

Every agent interaction passes through four governance checkpoints:

- **Authenticated Identity:** Agents verified via OAuth 2.0 and linked to the human authorizer who delegated the workflow.
- **Policy-Enforced Access (ABAC):** Requests evaluated in real time against agent identity, data classification, and context. Minimum necessary access enforced at the operation level.
- **FIPS 140-3 Validated Encryption:** All agent-accessed data encrypted in transit and at rest with validated cryptographic modules.
- **Tamper-Evident Audit Trail:** Every interaction logged with full attribution and streamed to SIEM in real time.

Where AI Becomes Compliant



Compliance built into the architecture, not bolted on after deployment

Solution Highlights

Governs AI agent access to sensitive data at the data layer, independent of model, prompt, or agent framework

FIPS 140-3 validated encryption for all agent-accessed data in transit and at rest

FedRAMP Moderate Authorized; FedRAMP High In Process

Three purchasable Governed Assists via MCP for regulated workflows

Works with Claude, Copilot, and any MCP-compatible LLM

Three Governed Assists: Compliance-Ready AI Workflows

Kiteworks Compliant AI ships three Governed Assists—discrete, purchasable capabilities powered by the Model Context Protocol (MCP) and governed end-to-end by the Kiteworks Data Policy Engine. Every operation is identity-verified, ABAC-evaluated, FIPS 140-3 encrypted, and tamper-evident logged.

Governed Folder Operations Assist: AI agents navigate, create, rename, move, and delete folder hierarchies using natural language—with every operation governed by the Data Policy Engine. Folder structures inherit RBAC/ABAC controls automatically, satisfying CUI segregation (CMMC), records segregation (HIPAA), and audit workspace provisioning requirements.

Use cases: Client portfolio structuring · CUI folder segregation · Audit workspace provisioning · Litigation hold workspaces · Clinical trial documentation

Governed File Management Assist: AI agents control the full data life cycle—upload, download, read, create, move, rename, and delete files—with every operation enforced by the Data Policy Engine. Satisfies retention schedules (NARA, SOX), minimum necessary access (HIPAA), and disposal requirements (PCI).

Use cases: SOX retention sweeps · CUI marking verification · Adverse event report packaging · Privilege log generation · Records schedule enforcement

Governed Forms Creation Assist: AI agents generate governed data collection forms from natural language descriptions—removing the manual burden of form creation while ensuring all submissions route to policy-governed storage with inherited RBAC/ABAC controls.

Use cases: KYC/CDD intake · FISMA incident reporting · HIPAA authorization forms · Supplier qualification questionnaires · Whistleblower report intake

Confidently Meet Audit and Governance Requirements

- Demonstrate control over **regulated data flows** (CUI, PCI, PHI, PII, SEC-regulated content)
- Map AI agent activity to compliance frameworks including **HIPAA, CMMC, PCI DSS, SEC/SOX, GDPR, NIST CSF, and ISO 27001**
- Export **unified audit logs** and **dedicated AI compliance reporting** for audits and incident response
- Produce board-ready AI evidence packages quickly

Seamless Integration With Any AI Platform

Kiteworks Compliant AI works with any MCP-compatible AI platform—Claude, Copilot, and any future LLM that supports the Model Context Protocol. The AI Data Gateway provides REST APIs for RAG pipelines and programmatic AI workflows. Deploy in any environment—cloud, on-premises, or hybrid—with cross-platform support for Windows, macOS, and Linux. Standards-based, vendor-neutral governance that protects your investment regardless of which AI platforms your organization adopts.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a Private Data Network that delivers data governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and over 1,500 global enterprises and government agencies.