Kiteworks Launches Compliant AI—the Industry's First Data-Layer Compliance Solution for AI Agent Governance

Solution enforces ABAC, encryption, and audit logs for every AI agent interaction with regulated data—independent of the model, prompt, or agent framework.

SAN MATEO, CA, UNITED STATES, March 23, 2026 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today announced Kiteworks Compliant AI—the industry's first data-layer governance solution that enforces attribute-based access control (ABAC), FIPS 140-3 validated encryption, and tamper-evident audit logging for every AI agent interaction with regulated data, independent of the model, prompt, or agent framework. The announcement includes three purpose-built Governed Agent Assists: compliance-ready workflows that enable AI agents to manage folders, handle files, and create data collection forms across regulated environments, all with regulatory policies enforced by the Kiteworks Data Policy Engine (DPE). Kiteworks is showcasing its Compliant AI capabilities at Booth S-0335, themed Evil Breach 2: AI Agent Nightmare Begins!

> "No other platform delivers this combination of controls at the data layer for AI agents. That's not a feature—it's an architecture."
>
> *Yaron Galant, Chief Product Officer at Kiteworks*

The launch addresses an acute and widening governance gap. According to the Kiteworks 2026 Data Security and Compliance Risk Forecast Report, 100% of organizations surveyed have agentic AI on their roadmap and 51% already have agents in production—yet 63% cannot enforce purpose limitations on those agents, and 60% cannot terminate a misbehaving agent. The World Economic Forum's Global Cybersecurity Outlook 2026 confirms that 87% of organizations now rank AI-related vulnerabilities as the fastest-growing cyber risk. Meanwhile, a 2026 red-team study by researchers from Harvard, MIT, Stanford, and Carnegie Mellon documented AI agents autonomously exfiltrating data and triggering unauthorized operations with no effective kill switch. Organizations are deploying agents they cannot constrain, audit, or stop.

"AI agents are the new digital employees—and like all employees, they access, handle, share, and act on regulated data," said Yaron Galant, Chief Product Officer, Kiteworks. "The difference is that

AI agents exercise zero independent ethical judgment. They will access any data they are not explicitly prevented from touching. HIPAA does not care whether a human or an AI agent accessed that patient record. Kiteworks Compliant AI governs the data layer—not the model—so every agent interaction is authenticated, ABAC policy-governed, FIPS 140-3 encrypted, and logged in a tamper-evident audit trail before any regulated data is touched. No other platform delivers this combination of controls at the data layer for AI agents. That's not a feature—it's an architecture."

Data-Layer Governance: The Only Layer AI Agents Cannot Bypass
Unlike model-level guardrails that can be circumvented by prompt injection, Kiteworks enforces governance at the point of data access through four checkpoints:

- Authenticated Identity: Every agent is authenticated and linked to the human authorizer who delegated the workflow, satisfying HIPAA, CMMC, and SOX requirements.

- Policy-Enforced Access (ABAC): Every request is evaluated against agent identity, data classification, request context, and operation type. Minimum necessary access is enforced at the operation level.

- FIPS 140-3 Validated Encryption: All agent-accessed data is encrypted in transit and at rest using FIPS 140-3 validated cryptographic modules.

- Tamper-Evident Audit Trail: Every interaction is logged with full attribution—who, what, when, and why—and fed directly into the organization's SIEM.

Three Governed Assists: Compliance-Ready AI Workflows
Kiteworks Compliant AI ships three Governed Assists—discrete capabilities powered by the Model Context Protocol (MCP) and governed end-to-end by the Data Policy Engine.

- Governed Folder Operations Assist: AI agents navigate, create, move, and delete folder hierarchies via natural language, with every operation governed by policy and inheriting RBAC/ABAC controls.

- Governed File Management Assist: AI agents control the full data life cycle—upload, download, read, create, move, delete—satisfying retention schedules (NARA, SOX), minimum necessary access (HIPAA), and disposal requirements (PCI).

- Governed Forms Creation Assist: AI agents generate governed data collection forms from natural language, with all submissions routed to policy-governed storage for KYC/CDD, HIPAA authorization, and FISMA incident reporting.

Why It Matters: The Evidence Gap
Kiteworks 2026 Forecast Report identifies audit trails as the keystone capability for AI

governance: 33% of organizations lack evidence-quality audit trails entirely, and those organizations are 20 to 32 points behind on every AI maturity metric—including purpose binding, impact assessments, and human-in-the-loop controls. Meanwhile, 61% are running fragmented data exchange infrastructure that cannot produce actionable evidence. Kiteworks Compliant AI closes this gap by embedding governance directly into the data access architecture.

“The question is no longer whether AI will be regulated,” said Tim Freestone, Chief Strategy Officer, Kiteworks. “It’s whether your organization can produce the evidence when the audit arrives. With Compliant AI, organizations can generate a complete evidence package—delegation chains, ABAC policy records, encryption certificates, tamper-evident audit exports—in hours, not weeks. Compliance becomes the AI accelerator, not the bottleneck.”

Experience Kiteworks Compliant AI at RSAC 2026
Visitors to Booth S-0335 will enter the world of Evil Breach 2: AI Agent Nightmare Begins—where attendees can see live demonstrations of Kiteworks Compliant AI governing real-time agent interactions, speak with experts about AI governance for their industry, and discover how Kiteworks MCP-powered Governed Assists deliver compliant file operations at enterprise scale.

About 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 thousands of global enterprises and government agencies.

David Schutzman
Kiteworks
203-550-8551
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X