Kiteworks Delivers the Data-Layer Governance Banks Need to Deploy AI at Scale Without Compounding Regulatory Risk

Kiteworks Compliant AI and Secure MCP Server bring zero-trust governance to AI agents to meet SOX, GLBA, SEC, FINRA, and NY DFS Part 500 standards.

SAN MATEO, CA, UNITED STATES, May 21, 2026 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today detailed how Kiteworks Compliant AI gives financial institutions the data-layer governance they need to deploy AI agents against regulated customer data without compounding regulatory exposure. The company is presenting the framework to senior banking technology, risk, and compliance leaders at the 13th Annual Bank IT USA Conference in New York City on June 1, 2026.

> We extend zero trust to the one place most banks have not yet applied it [the data layer], and we give compliance teams regulator-ready evidence in hours instead of weeks."
>
> *Catia Pereira, Director of Sales Engineering at Kiteworks*

The governance gap is measurable. Fifty-seven percent of organizations operate without a centralized AI data gateway, and seven percent have no dedicated AI data controls at all[1]—even as finance and insurance took 27% of all cyberattacks,[2] and the average cost of a financial services data breach hit $6.08 million.[3] Regulators are applying existing data-governance frameworks—SOX §404, the GLBA Safeguards Rule, SEC AI disclosure requirements, FINRA supervisory expectations, NY DFS Part 500, and OCC third-party risk guidance—directly to AI agent activity, without waiting for new legislation.

"Every bank in the United States has deployed AI. Almost none of them can answer the question a regulator will eventually ask—who authorized each AI interaction with regulated customer data, under what policy, and what was returned," said Catia Pereira, Director of Sales Engineering at Kiteworks. "Model-level guardrails do not answer that question. Guardrails are configuration settings inside the system being attacked. The control that survives when the model is compromised is the one at the data layer—independent of the model, enforcing policy on every request. That is what Kiteworks delivers. We extend zero trust to the one place most banks have not yet applied it, and we give compliance teams regulator-ready evidence in hours instead of weeks."

How Kiteworks Compliant AI makes AI defensible for regulated banking workflows:

- Authenticated Agent Identity, Linked to the Human Authorizer. Every AI agent is cryptographically verified and bound to the human who delegated the workflow before any regulated data access occurs. No shared service accounts. No anonymous agents running against customer PII, financial records, KYC files, or trade data.

- Policy-Enforced Access Evaluated on Every Request. The Kiteworks Data Policy Engine evaluates role-based and attribute-based access control on every operation—not just at connection. Agents inherit the rights of the user they are acting for and cannot exceed them. The standard SOX, GLBA, and FINRA already require for human access, now extended to agents.

- FIPS 140-3 Validated Encryption at Rest and in Transit. Federally validated cryptography protects every piece of regulated data flowing through an AI workflow, with sovereignty controls that keep data in jurisdiction.

- Tamper-Evident Audit Trail, Streamed to the SIEM in Real Time. Every AI interaction is captured with full attribution—who authorized the agent, what was accessed, under what policy, when, and with what outcome. Evidence packages export in hours, not weeks.

- One Control Plane Across Email, File Sharing, SFTP, MFT, Data Forms, APIs, and AI. The same policy engine and audit trail that govern human-mediated data exchange now govern agent-mediated access, consolidating five to 10 solutions onto a single platform.

Catia Pereira will present "The AI Data Governance Gap in Banking" at the 13th Annual Bank IT USA Conference on June 1, 2026, at 2 p.m. EDT in New York City. The session walks senior banking CISOs, CCOs, CIOs, and CROs through the four-pillar framework regulated firms are using to make AI defensible—and the one question every banking regulator will eventually ask.

For attendees seeking to learn more about how Kiteworks secures data exchange for humans and AI agents, reserve time to meet with the Kiteworks team at BankIT USA: https://info.kiteworks.com/bankitmeetingroom

[1] Kiteworks, "Data Security and Compliance Risk: 2026 Forecast Report."
[2] IBM, "X-Force Threat Intelligence Index 2026," February 2026.
[3] IBM and Ponemon Institute, "Cost of a Data Breach Report 2025."

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 secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks 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
+1 203-550-8551
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X
