Kiteworks

CAPABILITY BRIEF | FINANCIAL SERVICES

Securing Financial Services Data Exchange in the AI Era

Unifying Data Governance, AI Control, and Compliance Across Every Channel a Financial Institution Uses to Exchange Sensitive Data

Executive Summary

Financial services operates under the tightest regulatory stack of any sector, faces sustained adversary focus, and has moved AI into production faster than its governance can keep up. Regulators are now applying every existing framework -- SOX, GLBA, FINRA, NY DFS Part 500, DORA -- to AI agent activity, without waiting for new rules.

Kiteworks closes the exposure at the data layer: one platform unifying email, file sharing, MFT, SFTP, data forms, APIs, and AI workflows under a single policy engine, audit log, and security architecture.

The Challenge

AI is in production across loan origination, advisor workflows, underwriting, and customer service. The data layer those workflows consume is the layer most institutions have not extended their governance to.

Most financial institutions operate 5 to 10 separate tools for sensitive data exchange -- each with its own policies, audit logs, and gaps. When AI agents reach into all of those channels, fragmentation that was already a compliance liability becomes an AI governance crisis. When an examiner asks who authorized each AI interaction with regulated customer data, the answer becomes a multi-week investigation across fragmented logs and shared service accounts.

The Kiteworks Solution

Kiteworks is the secure data exchange for financial services. One platform. One policy engine. One audit log. Built on a hardened virtual appliance with FIPS 140-3 validated cryptography, single-tenant isolation, and tamper-evident audit streamed in real time to the institution's SIEM.

Control

Policy-enforced access and complete attribution across email, file sharing, MFT, SFTP, data forms, APIs, and AI -- one examiner-ready record of every interaction with regulated data, human or agent.

At a Glance

60% of financial services firms have no centralized AI data gateway[1]

Only 33% of organizations have complete knowledge of where their data is stored[2]

Attacks via public-facing apps up 44% year over year[3]

97% of AI-related breaches involved organizations lacking AI access controls; average U.S. breach cost exceeds $10 million[4]

Kiteworks unifies email, file sharing, MFT, SFTP, data forms, APIs, and AI workflows under one platform with FedRAMP Moderate Authorization and FIPS 140-3 validated cryptography

AI Governance

Through Kiteworks Compliant AI, including Secure MCP Server, AI agents are cryptographically authenticated, bound to the human authorizer, and governed by attribute-based access on every request. Independent of model, vendor, or model-level guardrails.

Compliance

Pre-mapped to SOX, GLBA, FINRA, SEC, NY DFS Part 500, OCC Bulletin 2023-17, PCI DSS 4.0, DORA, NIS 2, GDPR, and ISO 27001. Evidence assembles in hours, not weeks.

Anticipated Outcomes

- **Unified governance.** Replace 5 to 10 fragmented tools with one control plane.
- **AI without compounding regulatory risk.** Authenticated identity, policy-enforced access, FIPS 140-3 encryption, and full audit applied to every AI workflow.
- **Audit trails examiners can read.** Real-time SIEM streaming with full attribution.
- **Evidence in hours, not weeks.** On-demand exports ready for SOX, GLBA, FINRA, SEC, NY DFS, OCC, PCI, and DORA examinations.
- **Sovereignty for cross-border operations.** In-jurisdiction key custody, geofencing, and data residency.

Sources

[1] Kiteworks, Data Security and Compliance Risk: 2026 Forecast Report, December 2025.
[2] Thales, 2026 Thales Data Threat Report, 2026.
[3] IBM X-Force, 2026 X-Force Threat Intelligence Index, February 25, 2026.
[4] IBM Security and Ponemon Institute, Cost of a Data Breach Report 2025: The AI Oversight Gap, 2025.

Kiteworks