Kiteworks

TOP 5

Top 5 Reasons Wealth Management Firms Need Kiteworks

Unify, track, control, and secure sensitive content to manage third-party and supply chain risk with Kiteworks. Kiteworks closes the gap between exposure and protection with a unified Private Data Network that governs every channel where sensitive client data moves within, into, and out of your organization.

1. Unified Governance Across Every Data Channel

Wealth managers move sensitive client data through email, file sharing, managed file transfer, SFTP, and data forms—often through disconnected tools with separate logs and separate gaps. Kiteworks consolidates all channels into a single zero-trust platform with one policy engine, one audit trail, and one governance framework. When a regulator or client asks how data is protected, the answer is one system, not six.

2. SEC, GLBA, and SOX Compliance on Demand

SEC examiners keep flagging the same deficiencies: weak access controls, poor DLP, thin vendor oversight, insufficient audit trails. Kiteworks' automated compliance reporting generates preconfigured evidence for SEC, GLBA, SOX, HIPAA, GDPR, CMMC 2.0, and 50+ additional frameworks. Compliance reports gather control evidence automatically—no manual assembly, no six-week scramble before an exam.

3. Granular Access Controls That Match Fiduciary Obligations

Kiteworks' Data Policy Engine enforces role-based (RBAC) and attribute-based (ABAC) access controls dynamically—based on user role, data classification, device posture, and contextual conditions. Advisors see only what they need. External parties access only what policy permits. Every access decision is logged, creating the evidence trail that proves least-privilege enforcement to regulators and auditors.

4. Hardened Vendor Data Exchange for Supply Chain Risk

Wealth managers depend on custodians, clearing firms, fund administrators, tax preparers, and technology vendors—each a potential entry point for attackers. Kiteworks' MFT Server deploys as a hardened virtual appliance with built-in encryption, granular access management, and comprehensive audit logging that do not depend on the counterparty's security practices. Every vendor file exchange is governed, logged, and auditable in one system.

5. Immutable Audit Trails That Prove Control Under Pressure

When a breach occurs, the question is not whether you had a policy. It's whether you can prove you enforced it. Kiteworks' centralized, immutable audit logs capture every file access, every policy enforcement action, and every data movement across all channels—producing exportable evidence artifacts in the format regulators, auditors, courts, and institutional clients expect. The difference is between "we believe we're compliant" and "we can demonstrate it."