

The Kiteworks Control Plane for Secure Data Exchange

One policy and audit framework for every send, share, receive, and use of sensitive data.

Who we are

Kiteworks governs every send, share, receive, and use of sensitive data through a single Control Plane covering email, file sharing, managed file transfer, SFTP, data forms, APIs, and AI agent exchanges. Agents join people as governed identities, so one set of controls and one audit trail cover human collaboration and machine workflows alike.

MISSION

Empower organizations to manage risk in every exchange of private data — governance, compliance, and protection unified in one control plane.

Company facts

2,700+

Enterprise and government customers

100M+

Users across 83 countries

90+

Compliance frameworks mapped

1.75M

Seats at largest single customer

130M+

Secure files shared monthly

70M+

Emails controlled monthly

\$456M

Raised, led by Insight Partners and Sixth Street

Channels governed by one control plane

Every channel enforces the same attribute- and role-based policy, and writes to the same audit log.



Email

Policy-based encryption, retention, and full delivery audit.



File sharing

Governed internal and external collaboration with granular access.



Managed file transfer

Automated, high-volume transfers under the same evidence model.



SFTP and APIs

Machine-to-machine exchange and embedded integrations, fully logged.



Data forms

Data forms intake that keeps regulated submissions inside governed boundaries.



AI agents and MCP

Compliant AI and Secure MCP Server govern how people and agents use data.

How the control plane delivers

Control

One Control Plane with a real-time audit log on a hardened, single-tenant virtual appliance — policy and evidence in one place.

Compliance

Pre-built dashboards for 14+ of the most-audited frameworks, plus automated evidence generation for assessors.

Sovereignty

Single-tenant deployment with Data Policy Engine geo-fencing keeps data in-region and out of reach of extraterritorial access.

AI

Compliant AI and the Secure MCP Server govern data access and use for people and agents alike, under one policy and audit trail.

One control plane. Every channel. One audit trail.

See how Kiteworks governs sensitive data exchange across email, file sharing, MFT, APIs, and AI agents.

kiteworks.com/contact

Key trends shaping sensitive data exchange

- **AI adoption has outrun AI governance**

83% of enterprises already use AI in daily operations, but only 13% have strong visibility into how it is being used (Cyera Research Labs, 2025 State of AI Data Security Report).
- **Sensitive data is still undiscovered and unclassified**

Only a third of organizations know where all their data is stored, and just 39% can classify all of it (Thales, 2026 Data Threat Report) — the answer both DSPM programs and regulatory reporting depend on.
- **Third-party exchange is the top risk concentration**

65% of large companies by revenue name third-party and supply chain vulnerabilities their single greatest challenge, up from 54% a year earlier (World Economic Forum, Global Cybersecurity Outlook 2026).
- **Tool sprawl multiplies blind spots**

Organizations run an average of seven data protection tools plus six AI security tools, yet only 39% feel confident they understand them (Thales, 2026 Data Threat Report).
- **Regulators now expect continuous evidence**

Under the July 2026 Digital Omnibus, EU AI Act high-risk obligations apply from December 2, 2027, and transparency duties have been live since August 2, 2026. Fines reach €15M or 3% of global turnover for high-risk and transparency breaches, and €35M or 7% for prohibited practices — on top of NIS2, DORA, CMMC 2.0, and GDPR.

Global operations

GLOBAL HQ San Mateo, California — Silicon Valley.	EMEA HQ Zurich, Switzerland.	REGIONAL OFFICES Portsmouth NH; UK; Netherlands; Germany; Romania; Bulgaria; Australia; Singapore.	ECOSYSTEM 52 product integrations and 7 acquisitions.
---	--	--	---

Certifications and validations

✓ FedRAMP High In Process	✓ FedRAMP Moderate Authorized	✓ SOC 2 Type II	✓ IRAP (PROTECTED)
✓ ISO 27001/17/18	✓ FIPS 140-3 Validated	✓ BSI C5 Type 2 Attestation	✓ UK Cyber Essentials Plus