Kiteworks

SOLUTION BRIEF

FOR CISOS, COMPLIANCE, AND SECURITY TEAMS

Govern Every Sensitive Data Exchange With the Data Policy Engine

Define Policy Once. Enforce It on Every Sensitive Data Exchange, for People and AI Agents.

CMMC 2.0 | HIPAA / HITECH | GDPR / NIS 2 | ITAR / EAR | SOC 2 Type II | ISO 27001, 27017, 27018

FedRAMP Class D Agency Auth In Process (formerly High In Process) | FedRAMP Class C Certified (formerly Moderate Authorized)

The Challenge

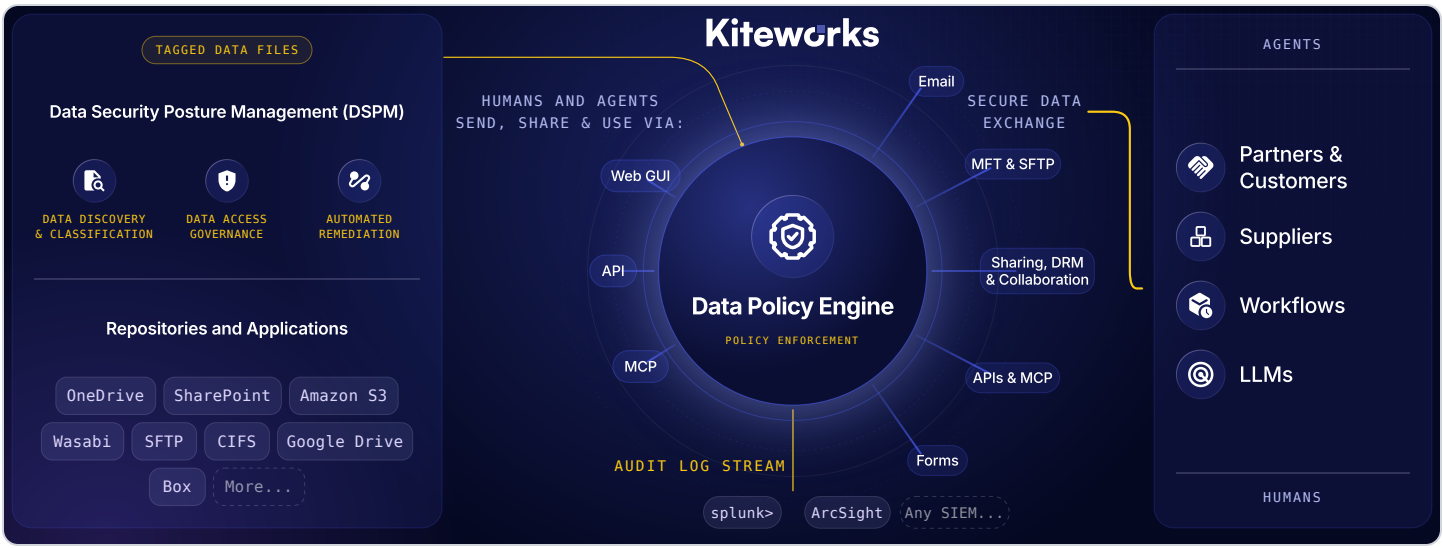
AI agents, employees, and external parties request sensitive data through the same MCP, API, email, forms, SFTP, file sharing, and MFT channels. Traditional tools each provide their own policies and their own logs. Enforcement drifts from one channel to the next, gaps open between them, and proving compliance means stitching evidence together from every system before an audit.

The Solution

The Kiteworks Data Policy Engine (DPE) lets admins define data policies once and enforces them at runtime across every channel. Each decision weighs the attributes of the data, the actor (a person or an AI agent), and the action requested, then allows it, blocks it, requires approval, or limits the user to protected viewing or editing. Every agent or user action goes to one audit log.

One Control Plane for Every Sensitive Data Exchange

Whether a request comes from an employee, a partner, or an AI agent, the Data Policy Engine evaluates the same data, actor, and action attributes, and enforces the same policies across APIs, AI agents, email, file sharing, and other channels.



How the Data Policy Engine Decides

1 DATA

Evaluate the Data

Attributes such as classification tags, folder, and email keywords describe what is being exchanged.

2 ACTOR

Identify the Actor

Context such as email address, domain, profile, and geolocation defines the requesting user or agent.

3 ACTION

Weigh the Action

Accessing, sending, sharing, or uploading each triggers its own set of responses.

4 ENFORCE

Apply the Directive

The matching rule enforces automatically, in real time, with no manual step.

Policy Control Without the Complexity

IF-THEN rules built from data, user or agent, and action conditions. Start from a pre-built template or build from scratch.

Unified AND/OR Policy Rules

One rule logic across user attributes, data attributes, and actions, applied uniformly to MCP, API, web, and all other data exchange channels.

Pre-Built Policy Templates

Start from templates such as blocking data from leaving the organization or requiring approval to share.

Classification-Aware Policies

Control access for people and AI agents based on Kiteworks tags, Cyera AI tags, or Microsoft Purview labels. Policies can also tag data at upload.

Sovereign Edit

Policy can require certain users and partners to edit in the browser while the file stays on Kiteworks, never downloaded, extracted, or sent to the Microsoft cloud.

Approval Flows and Justification

Require approval before a share, or a justification form before an access or upload.

Granular RBAC and Expiration

Least-privilege roles, folder-level access, and time-based expiration for files and shared links.

Govern Every Data Request From Agents and Humans in Real Time

Access

Block, SafeVIEW, Sovereign Edit, justification form, or allow.

Share or Send

Block, require manager approval, or allow.

Upload

Block, apply a Kiteworks tag, require a justification form, or allow.

Enforce Agent and Human Compliance Automatically and Prove It

One Immutable Audit Log

Every agent and human action is centrally logged and feeds compliance reporting and SIEM integrations.

Policy Reporting and Dashboards

Evaluate the performance of a policy before enabling it, and measure its impact in operation.

Framework Mapping

DPE rules provide broad and granular support for regulations such as CMMC 2.0, HIPAA, GDPR, FedRAMP, ITAR, NIS 2, PCI DSS, and PIPEDA.

Ready to Govern Every Sensitive Data Exchange?

www.kiteworks.com sales@kiteworks.com

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.

Copyright © 2026 Kiteworks.