Kiteworks | CONCENTRIC Ai

SOLUTION BRIEF

Kiteworks + Concentric AI

End-to-End Data Security Governance and Automated Enforcement

Organizations have long struggled to keep their most sensitive data secure at every stage of its journey.

But legacy tools rely on pattern matching and keywords to discover data, which generates endless false positives, and without accurate discovery, everything downstream fails—classification, access controls, and DLP policies. And when data is shared externally with partners, vendors, and customers, security and compliance risks multiply.

Secure Sensitive Data From Discovery to Delivery

Concentric AI secures data at rest, in motion, and across all the GenAI applications users interact with. Its Semantic Intelligence™ AI and data security governance platform autonomously discovers, classifies, continuously monitors, and remediates sensitive data across structured and unstructured sources in cloud and on-premises environments.

The platform uses context-aware deep learning to understand exactly where sensitive data resides and how it's being used—and applies Microsoft Information Protection (MIP) labels based on these insights. When Semantic Intelligence™ classifies data as "Confidential," or when it applies compliance labels such as "HIPAA" or "GDPR," the Kiteworks Data Policy Engine, which is at the heart of a Kiteworks Private Data Network (PDN), ensures that these classifications translate into real-world protection when the data is shared, accessed, and used downstream, including outside the organization. It applies these enforcement policies to email, file sharing and collaboration, SFTP, and MFT, as well as API- and MCI-based automation.

How the Kiteworks Data Policy Engine Mitigates Downstream Risk

Classification Label Ingestion: Automatically enforces policies on documents classified by Concentric AI's Semantic Intelligence™ platform via Microsoft MIP sensitivity labels (tags)

Role- and Attribute-Based Access Controls: Defines policies that intake data attributes such as MIP sensitivity labels, user attributes such as role and location, and user actions, such as edit or download; enforces run-time policies such as view-only, SafeEDIT, block, encrypt, or allow

Possessionless Editing: Enables secure document editing for internal and external users virtually in their browsers, without file downloads, with SafeEDIT Next-gen DRM

End-to-End Encryption: Applies military-grade encryption for data in transit and at rest across email, file sharing, MFT, SFTP, APIs, and forms

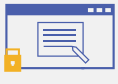
Unified Audit Logs and Reports: Provides SOC and compliance teams with comprehensive, real-time visibility into every access, share, and transfer event, including external data exchanges

Solution Highlights

Context-aware AI discovers, categorizes, and classifies data without rules, regex, or trainable classifiers

Secures data at rest, in motion, and in use

Enforces consistent, auditable governance even outside the organization



Provides complete audit trails for compliance and security analysis

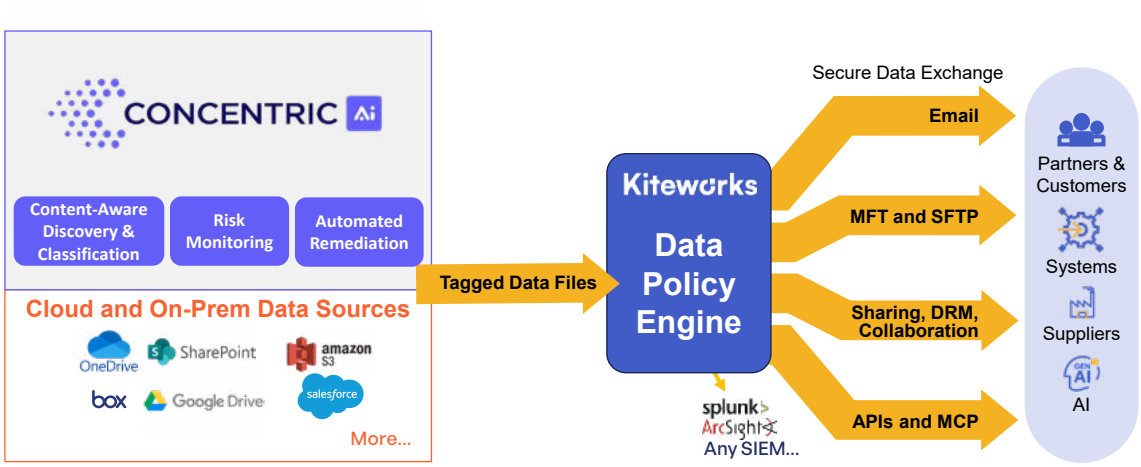


Diagram 1: Enforce Policies Using Concentric AI's Context-Aware Discovery and Classification.

Automate Governance Without Sacrificing Business Process Responsiveness

Kiteworks automatically enforces the right level of protection based on user roles, run-time context, and MIP labels. Business users collaborate seamlessly while high-risk activities are limited or blocked, without constant intervention from security teams

Extend Concentric AI's End-to-End Data Security Governance to Your Supply Chain

Kiteworks extends the upstream benefits of Concentric AI data protection downstream into your supply chain by enforcing MIP-based controls on sensitive data shared externally. It ensures secure, compliant exchanges with vendors and partners, applying encryption, access policies, and audit logging to maintain your data security posture beyond the perimeter.

Confidently Meet Audit and Governance Requirements

- Demonstrate control over **regulated data flows** (e.g., CUI, PCI, PHI, PII)
- Map activity to compliance frameworks like **NIST CSF, GDPR, HIPAA, CMMC, and ISO 27001**
- Export **unified audit logs** and **dedicated reporting** for compliance audits and incident response

Why Concentric AI + Kiteworks?

Concentric AI and Kiteworks help organizations maximize their data security investments with complementary solutions that ensure data discovery and continuous risk insights translate into automated enforcement to protect your most sensitive data wherever it travels. Together, they deliver:

- **Upstream Discovery and Risk Assessment:** Context-aware discovery and categorization to identify sensitive and business-critical data across all your data sources with unprecedented accuracy
- **Downstream Enforcement:** Effectively manage risk for data in motion with consistent, auditable governance that eliminates manual processes and meets the strictest regulatory requirements
- **Unified Protection:** Centralized controls, automated enforcement, and comprehensive visibility from internal repositories to external communications with supply chain partners

January 2026

www.kiteworks.com www.concentric.ai