Kiteworks

SOLUTION BRIEF

Kiteworks + Data Security Posture Management (DSPM)

Extend Data Modernization, Governance, and Control Beyond the Enterprise

Leverage DSPM Data Classification to Mitigate Risk of Data in Motion and in Use

Data Security Posture Management (DSPM) platforms discover and classify sensitive data, uncover shadow data, and identify overexposure risks. Inside the enterprise, they enforce policies on data at rest using APIs and interfaces into your applications. But as soon as the **data is in motion or in use**, visibility and control vanish, whether moving downstream via email, file transfers, APIs, or collaboration.

The Data Policy Engine at the heart of a Kiteworks Private Data Network (PDN) **leverages classification labels** from your upstream DSPM solution and enforces consistent, auditable governance over how sensitive documents are shared, accessed, and used downstream—**even outside your organization.** It applies these policies to email, file sharing and collaboration, SFTP, MFT, and API-based automation.

How the Kiteworks Data Policy Engine Mitigates Downstream Risk

Classification Label Ingestion: Automatically enforce policies on documents labeled by DSPM tools via Microsoft Purview or integrated APIs

Role- and Attribute-Based Access Controls: Define policies that intake data attributes such as MIP sensitivity labels, user attributes such as role and location, and the user's action, such as edit or download, and enforce a run-time policy such as view-only, SafeEDIT, block, encrypt, or allow

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

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

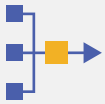
Unified Audit Logging and Reports: Provide the SOC and compliance teams with comprehensive, real-time visibility into every access, share, and transfer event, including external data exchanges

Enhances DLP: Integrate with DLP servers via ICAP, using DLP responses in policy decisions to block or allow data movement, or to limit usage to SafeEDIT or view-only modes

Automate Governance Without Sacrificing Business Process

Solution Highlights

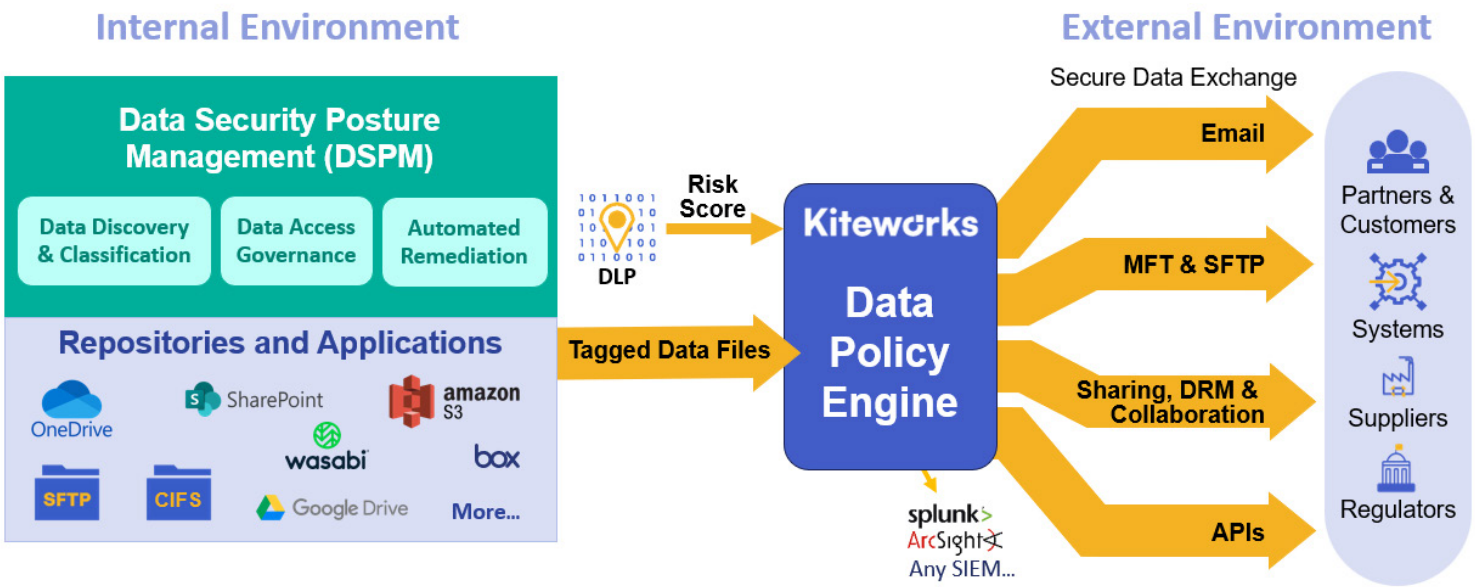
Protects in use, in motion, and at rest



Leverages DSPM data classifications

Enforces even outside your enterprise

Possessionless editing for secure collaboration



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 DSPM Data Security to Your Supply Chain

Kiteworks extends the upstream benefits of DSPM 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.

Simplify Compliance

- 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 the **unified audit log** and **dedicated reporting** for compliance audits and incident response

Seamless Integration With Any DSPM Platform

Regardless of the DSPM solution you are using, Kiteworks acts as a downstream **enforcement layer** for its data classification. It ensures your **sensitive data stays protected**—no matter where it travels—and multiplies the value of your DSPM and DLP investment.

How Kiteworks Leverages DSPM Classifications and Enhances DLP

DSPM	DLP	Kiteworks
Data at Rest		
Discovers and **classifies data** • Identifies where sensitive data exists • Classifies data by sensitivity • Maps data flows and lineage • Assesses risk posture		
Data in Motion		
	Integrates with data flow products • Endpoint agents • Email gateway integration • Web gateway integration • Legacy file server agents • ICAP and API integration	**Executes** data flows • File sharing/collaboration • Email clients and gateway • SFTP and MFT servers • Repositories gateway • Web forms
	Scans/inspects data for sensitive patterns • All data from integration points	**Detects sensitive data** via **rules and tags** • All corporate-wide email, inbound and outbound • All in-platform transfers, uploads, downloads, edits
	Leverages DSPM **classifications**	Leverages DSPM **classifications**
	Enforces policies via **integrations** • Block, encrypt, require user justification, restrict access ...	**Enforces policies** in **platform** and **mail stream** • SafeEDIT, view-only, block, encrypt, require approval or justification, apply tags ...
		Governs data in **third-party automated workflows** • SFTP, MFT, APIs
Data in Use		
		Governs data in **third-party collaboration** • View-only access • Agentless, possessionless editing (SafeEDIT Next-gen DRM) • Restriction of permission grants • Secure remote access

Use Case Examples

Defense Contractor CMMC Level 2 Certification

- **Challenge:** Mid-sized defense contractor with controlled unclassified information (CUI) stored across on-premises systems, AWS S3, and Microsoft 365 needs CMMC Level 2 certification. To help comply with this regulation, they have a corporate policy of keeping CUI off all end-user desktops.
- **DSPM Role:** Discovers and classifies CUI across hybrid environments, maps data flows, monitors access patterns, and provides compliance gap analysis for CMMC controls.
- **DLP Role:** Leverages DSPM data labels to identify CUI and prevents unauthorized CUI uploads to the cloud via CASB and Web Gateway integrations.
- **Kiteworks Role:** Leverages DSPM data labels to identify CUI in corporate repositories. Policies prevent downloads of CUI to end-user desktops but enable downloads of non-sensitive information. To enable CUI editing for users with appropriate privileges, it provides SafeEDIT possessionless editing so they edit virtually in their browsers without downloading CUI files. Policies prevent emailing CUI to unallowed recipients, and ensure encryption, authentication, and forwarding restrictions on emails to approved recipients.

  Detects CUI in incoming email, attachments, and uploads based on sender attributes, applies CUI tags to the files, and then handles the data according to the CUI policies. Passes non-CUI email through to normal processing. Creates an audit log of all inbound and outbound transmissions and internal and external downloads of sensitive data and feeds it to ArcSight and CMMC 2.0 compliance reports.

Multi-Site Healthcare System PHI Protection for HIPAA Compliance

- **Challenge:** Hospital network with Epic EHR, cloud-based imaging systems, and third-party billing platforms needs to secure PHI across 15 locations.
- **DSPM Role:** Discovers PHI in unstructured data (physician notes, lab reports), tracks data lineage from patient intake to billing, identifies shadow IT applications storing health data.
- **DLP Role:** Endpoint DLP prevents unauthorized PHI transmission via personal email, and blocks screenshots of patient records. DLP server scans inbound email files forwarded by Kiteworks and returns a risk score based on PHI and PII discovered in the file.
- **Kiteworks Role:** Leverages DSPM data labels to identify PHI and implement policies to prevent transmission to external parties via corporate web email, execute secure SFTP transmission of reports to specific regulatory agency systems, enable downloads of PHI files to designated employees and non-sensitive files to specified users, execute secure MFT transmissions to care data to specific insurance company systems, and encrypt email transmissions to approved child protective services and law enforcement organizations.

  Forwards email attachments to DLP for risk scoring and uses the score to apply tags that drive policies on downstream processing and usage. Creates an audit log of all incoming and outgoing transmissions and internal and external downloads of sensitive data and feeds it to Splunk and HIPAA compliance reports.