Kiteworks

LÖSUNGSÜBERBLICK

FÜR CISOS, COMPLIANCE- UND SICHERHEITSTEAMS

Jeden sensiblen Datenaustausch mit der Data Policy Engine steuern

Einmal Richtlinien festlegen. Bei jedem sensiblen Datenaustausch durchsetzen, für Menschen und KI-Agenten.

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

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

Die Herausforderung

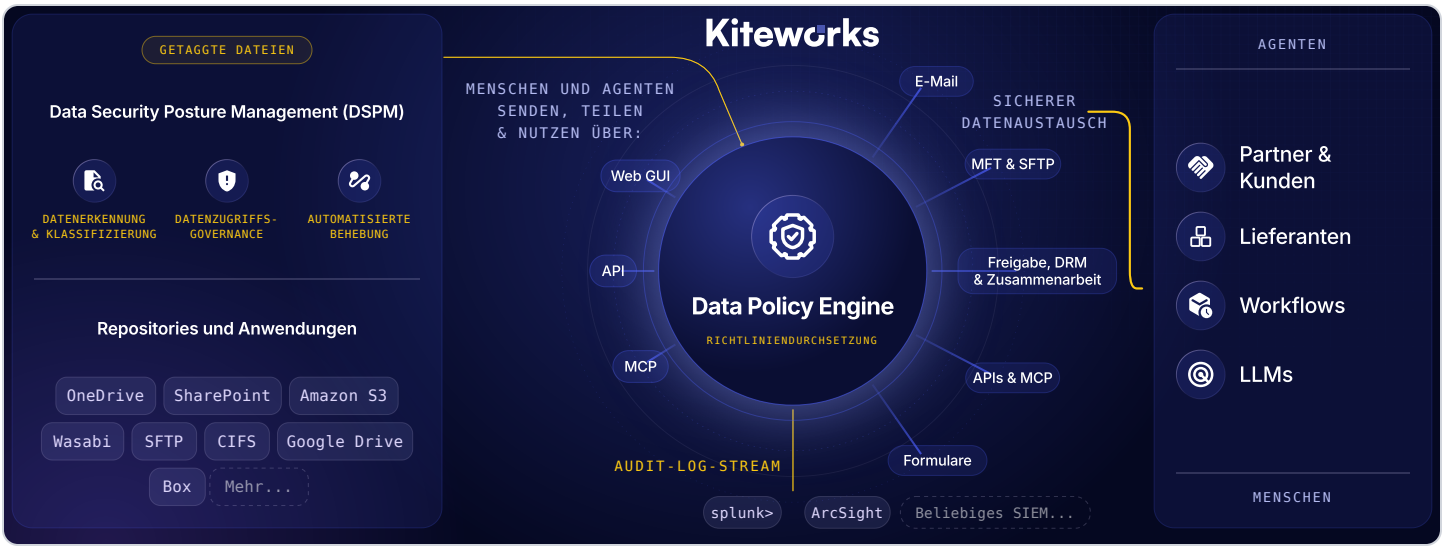
KI-Agenten, Mitarbeitende und externe Parteien fordern sensible Daten über dieselben MCP-, API-, E-Mail-, Formular-, SFTP-, Dateifreigabe- und MFT-Kanäle an. Herkömmliche Tools haben jeweils eigene Richtlinien und Protokolle. Die Durchsetzung driftet von Kanal zu Kanal auseinander, Lücken entstehen, und der Compliance-Nachweis heißt: vor jedem Audit Belege aus allen Systemen sammeln.

Die Lösung

Mit der Kiteworks Data Policy Engine (DPE) legen Admins Datenrichtlinien einmal fest und setzen sie zur Laufzeit in jedem Kanal durch. Die Entscheidung bewertet Daten, Akteur (Person oder KI-Agent) und Aktion: erlauben, blockieren, Genehmigung verlangen oder auf geschütztes Anzeigen und Bearbeiten beschränken. Jede Agenten- und Benutzeraktion landet in einem Audit-Log.

Eine Kontrollebene für jeden sensiblen Datenaustausch

Ob die Anfrage von einem Mitarbeitenden, einem Partner oder einem KI-Agenten kommt: Die Data Policy Engine bewertet dieselben Daten-, Akteur- und Aktionsattribute und setzt dieselben Richtlinien durch, über APIs, KI-Agenten, E-Mail, Dateifreigabe und weitere Kanäle.



So entscheidet die Data Policy Engine

1 DATEN

Daten bewerten

Attribute wie Klassifizierungs-Tags, Ordner und E-Mail-Schlüsselwörter beschreiben, was ausgetauscht wird.

2 AKTEUR

Akteur identifizieren

Kontext wie E-Mail-Adresse, Domain, Profil und Standort bestimmt den anfragenden Benutzer oder Agenten.

3 AKTION

Aktion abwägen

Zugriff, Versand, Freigabe und Upload lösen jeweils eigene Reaktionen aus.

4 DURCHSETZEN

Vorgabe durchsetzen

Die passende Regel greift automatisch und in Echtzeit, ganz ohne manuellen Schritt.

Richtliniensteuerung ohne Komplexität

WENN-DANN-Regeln aus Daten-, Benutzer- oder Agenten- und Aktionsbedingungen. Mit Vorlage starten oder von Grund auf bauen.

Einheitliche Regellogik

Eine UND/ODER-Logik für Benutzer, Daten und Aktionen, einheitlich angewendet auf MCP, API, Web und alle weiteren Kanäle des Datenaustauschs.

Vorgefertigte Vorlagen

Vorlagen, etwa um den Datenabfluss aus dem Unternehmen zu blockieren oder für Freigaben eine Genehmigung zu verlangen.

Klassifizierungsbasiert

Zugriff für Menschen und KI-Agenten per Kiteworks-Tags, Cyera-KI-Tags oder Microsoft-Purview-Labels steuern. Richtlinien können Daten beim Upload taggen.

Sovereign Edit

Bestimmte Benutzer und Partner bearbeiten per Richtlinie im Browser; die Datei bleibt in Kiteworks, ohne Download, Extraktion oder Microsoft-Cloud-Versand.

Freigabe und Begründung

Verlangen Sie eine Genehmigung vor der Freigabe oder ein Begründungsformular vor Zugriff oder Upload.

RBAC mit Ablaufdatum

Fein abgestufte Rollen nach dem Prinzip minimaler Rechte, Zugriff auf Ordnerebene und zeitbasiertes Ablaufdatum für Dateien und Links.

Jede Datenanfrage von Agenten und Menschen in Echtzeit steuern

Zugriff

Blockieren, SafeVIEW, Sovereign Edit, Begründung einholen oder erlauben.

Freigabe oder Versand

Blockieren, Genehmigung durch Vorgesetzte verlangen oder erlauben.

Upload

Blockieren, Kiteworks-Tag setzen, Begründung verlangen oder erlauben.

Compliance für Agenten und Menschen automatisch durchsetzen und nachweisen

Ein unveränderliches Audit-Log

Jede Aktion von Agenten und Menschen wird zentral protokolliert, speist Compliance-Reporting und SIEM-Integrationen.

Richtlinien-Reporting und Dashboards

Bewerten Sie die Wirkung einer Richtlinie vor der Aktivierung und messen Sie ihren Effekt im Betrieb.

Zuordnung zu Regelwerken

DPE-Regeln unterstützen Vorschriften wie CMMC 2.0, HIPAA, DSGVO, FedRAMP, ITAR, NIS 2, PCI DSS und PIPEDA umfassend und granular.

Bereit, jeden sensiblen Datenaustausch zu steuern?

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.