Kiteworks

UNTERNEHMENSÜBERBLICK

Organisationen tauschen täglich sensible Daten über Tausende von Kanälen, Systemen und Partnern aus—dennoch verlassen sich die meisten auf fragmentierte Einzellösungen. Diese schaffen Compliance-Blindstellen, vergrößern die Angriffsfläche und lassen Sicherheitsteams ohne die notwendige Transparenz zurück. Mit der Beschleunigung von Unternehmensprozessen durch KI vergrößert sich die Governance-Lücke: Daten bewegen sich schneller, als Richtlinien folgen können, und Regulierungsbehörden warten nicht länger auf Sicherheitsverletzungen, um Kontrollmängel zu sanktionieren.

ZENTRALE HERAUSFORDERUNGEN

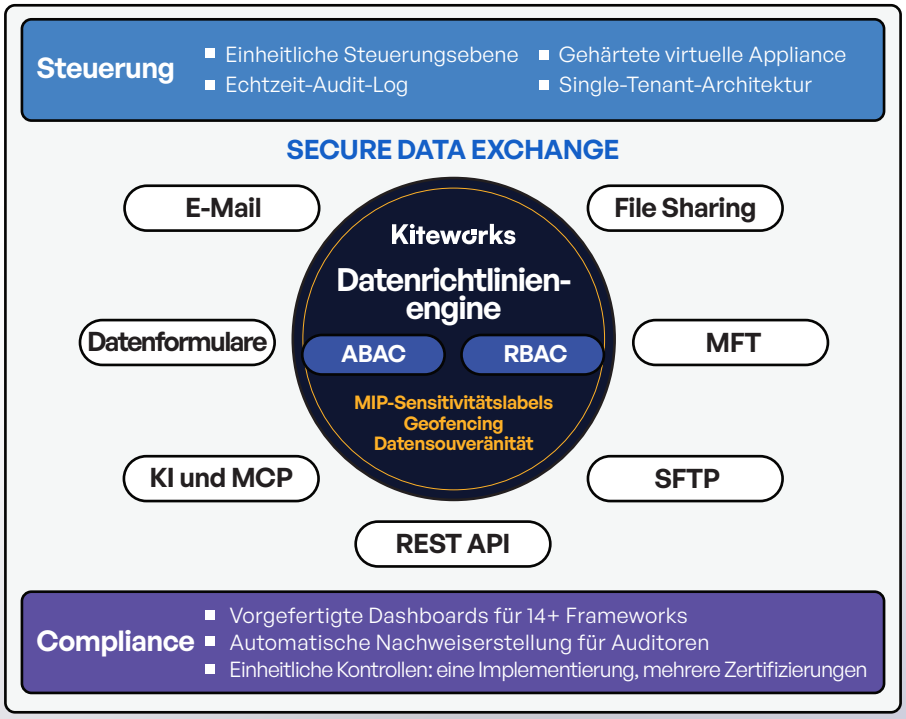
5-10	$4,45 MIO. USD	1 von 3	33 %	63 %
Getrennte Tools für den Austausch privater Inhalte	Durchschnittliche Kosten einer Datenpanne	Vorfälle zur Datensouveränität im vergangenen Jahr	Fehlende revisionssichere Audit-Trails	Keine Durchsetzung von Grenzen für KI- und Agentenzugriffe auf Daten

WAS WIR TUN

Kiteworks ermöglicht es Organisationen, Risiken bei jedem Senden, Teilen, Empfangen und Verwenden sensibler unstrukturierter Daten effektiv zu steuern. Die Plattform ersetzt fragmentierte Einzellösungen durch eine einheitliche Steuerungsebene für sicheren Datenaustausch – eine Richtlinien-Engine, ein Audit-Log, eine Sicherheitsarchitektur. Basierend auf einer gehärteten virtuellen Appliance mit mehrschichtiger Sicherheitsarchitektur bietet Kiteworks einheitliche Governance, Transparenz und Schutz über alle Kanäle hinweg und erweitert gleichzeitig unternehmensweite Kontrollen auf KI-gestützte Workflows.

Ki-Daten-Governance

- Zero-Trust-Zugriff für KI und Agenten auf Daten
- Konformes RAG für Unternehmensdaten
- ABAC-/RBAC-Richtliniendurchsetzung für KI
- Echtzeit-Audit-Trail für KI-Zugriffe
- Kompatibel mit jeder MCP-kompatiblen KI-Plattform



Repository-Konnektoren

Microsoft Office	CIFS/SMB File Shares
SharePoint	OneDrive
SFTP	Box
DropBox	Google Drive
Google Workspace	Google Cloud Storage
Amazon S3	Azure Blob
Wasabi	iManage
Salesforce	*und mehr*

CMMC 2.0 | DSGVO | HIPAA | NIS 2 | DORA | PIPEDA | ITAR | EU AI ACT | PCI DSS | UND MEHR

Schutz: Datenzentrierte Sicherheit (OpenTDF)

- Richtlinien sind in Dateien eingebettet—Schutz reist mit den Daten
- Dauerhafte Zugriffskontrollen unabhängig von Standort oder System
- Zero-Trust-Ansatz: jeder Zugriff wird jedes Mal verifiziert

SafeEDIT: Besitzlos Bearbeiten

- Externe Parteien bearbeiten Dokumente ohne Download
- Next-Gen DRM—Daten verlassen niemals Ihre Umgebung
- Mehrere Bereitstellungsoptionen, einschließlich FedRAMP-Hosting

ZERTIFIZIERUNGEN UND VALIDIERUNGEN

FedRAMP High (in Bearbeitung) | FedRAMP Moderate | SOC 2 Typ II | IRAP
Cyber Essentials Plus | ISO 27001/27017/27018 | FIPS 140-3 | BSI C5