Kiteworks

UNTERNEHMENSÜBERBLICK

Die Kiteworks Control Plane für den sicheren Datenaustausch

Ein einheitliches Regelwerk für Richtlinien und Audits – für jedes Senden, Teilen, Empfangen und Verwenden sensibler Daten.

Wer wir sind

Kiteworks steuert jedes Senden, Teilen, Empfangen und Verwenden sensibler Daten über eine einzige Control Plane, die E-Mail, Dateifreigabe, Managed File Transfer, SFTP, Datenformulare, APIs und den Austausch mit KI-Agenten abdeckt. KI-Agenten treten dabei wie Menschen als kontrollierte Identitäten auf, sodass ein einheitliches Regelwerk und ein einheitlicher Audit-Trail sowohl die menschliche Zusammenarbeit als auch maschinelle Workflows abdecken.

MISSION

Organisationen befähigen, Risiken bei jedem Austausch privater Daten zu steuern – Governance, Compliance und Schutz vereint in einer Control Plane.

Unternehmenszahlen

2.700+
Unternehmens- und Behördenkunden

100 Mio.+
Nutzer in 83 Ländern

90+
Abgebildete Compliance-Frameworks

1,75 Mio.
Lizenzen beim größten Einzelkunden

130 Mio.+
Sicher geteilte Dateien pro Monat

16 TB
Maximale sicher übertragene Dateigröße

456 Mio. $
Eingesammeltes Kapital, angeführt von Insight Partners und Sixth Street

Von einer Control Plane gesteuerte Kanäle

Jeder Kanal setzt dieselbe attribut- und rollenbasierte Richtlinie durch und schreibt in dasselbe Audit-Log.

E-Mail
Richtlinienbasierte Verschlüsselung, Aufbewahrung und vollständige Zustellprüfung.

Dateifreigabe
Kontrollierte interne und externe Zusammenarbeit mit granularen Zugriffsrechten.

Managed File Transfer
Automatisierte Übertragungen mit hohem Volumen im selben Nachweismodell.

SFTP und APIs
Maschine-zu-Maschine-Austausch und eingebettete Integrationen, vollständig protokolliert.

Datenformulare
Erfassung über Datenformulare, die regulierte Einreichungen innerhalb kontrollierter Grenzen hält.

KI-Agenten und MCP
Compliant AI und der Secure MCP Server regeln, wie Menschen und Agenten Daten nutzen.

Was die Control Plane leistet

Kontrolle
Eine Control Plane mit Echtzeit-Audit-Log auf einer gehärteten Single-Tenant-Appliance – Richtlinien und Nachweise an einem Ort.

Compliance
Vorgefertigte Dashboards für mehr als 14 der am häufigsten geprüften Frameworks sowie automatisierte Nachweiserstellung für Prüfer.

Datenhoheit
Single-Tenant-Bereitstellung mit Geofencing durch die Data Policy Engine hält Daten in der Region und außerhalb der Reichweite extraterritorialen Zugriffs.

KI
Compliant AI und der Secure MCP Server regeln den Datenzugriff und die Datennutzung gleichermaßen für Menschen und Agenten – unter einem einheitlichen Regelwerk und Audit-Trail.

Wichtige Trends im Umgang mit sensiblen Daten

Die KI-Einführung ist der KI-Governance vorausgeeilt
83 % der Unternehmen nutzen KI bereits im Tagesgeschäft, doch nur 13 % haben einen verlässlichen Überblick darüber, wie sie eingesetzt wird (Cyera Research Labs, 2025 State of AI Data Security Report).

Sensible Daten bleiben unentdeckt und unklassifiziert
Nur ein Drittel der Organisationen weiß, wo sich sämtliche ihrer Daten befinden, und lediglich 39 % können sie vollständig klassifizieren (Thales, 2026 Data Threat Report) – genau die Antwort, auf die sowohl DSPM-Programme als auch die regulatorische Berichterstattung angewiesen sind.

Der Austausch mit Drittparteien ist die größte Risikokonzentration
65 % der nach Umsatz größten Unternehmen nennen Schwachstellen bei Drittparteien und in der Lieferkette als ihre größte Herausforderung – ein Anstieg gegenüber 54 % im Vorjahr (World Economic Forum, Global Cybersecurity Outlook 2026).

Tool-Wildwuchs vervielfacht blinde Flecken
Organisationen setzen im Schnitt sieben Datenschutz-Tools und sechs KI-Sicherheitstools gleichzeitig ein, doch nur 39 % fühlen sich sicher, diese wirklich zu verstehen (Thales, 2026 Data Threat Report).

Aufsichtsbehörden erwarten heute durchgängige Nachweise
Gemäß dem Digital Omnibus vom Juli 2026 gelten die Hochrisiko-Pflichten des EU AI Act ab dem 2. Dezember 2027, während die Transparenzpflichten bereits seit dem 2. August 2026 in Kraft sind. Verstöße gegen Hochrisiko- und Transparenzpflichten werden mit bis zu €15 Mio. oder 3 % des weltweiten Umsatzes geahndet, verbotene Praktiken mit bis zu €35 Mio. oder 7 % – zusätzlich zu NIS2, DORA, CMMC 2.0 und der DSGVO.

Globale Präsenz

GLOBALER HAUPTSITZ
San Mateo, Kalifornien, Silicon Valley.

EMEA-HAUPTSITZ
Bahnhofstrasse 29, 6300 Zug, Schweiz.

REGIONALBÜROS
Portsmouth (NH); Großbritannien; Niederlande; Deutschland; Rumänien; Bulgarien; Australien; Singapur.

ÖKOSYSTEM
52 Produktintegrationen und 8 Akquisitionen.

Zertifizierungen und Validierungen

- **FedRAMP High** In Bearbeitung
- **FedRAMP Moderate** Autorisiert
- **SOC 2 Type II**
- **IRAP (PROTECTED)**
- **ISO 27001/17/18**
- **FIPS 140-3 validiert**
- **BSI C5 Type 2** Testat
- **UK Cyber Essentials Plus**

Kiteworks

Die Mission von Kiteworks ist es, Organisationen zu befähigen, Risiken bei jedem Senden, Teilen, Empfangen und Verwenden sensibler Daten wirksam zu steuern. Die Kiteworks-Plattform bietet Kunden einen sicheren Datenaustausch, der Data Governance, Compliance und Schutz in einer einheitlichen Control Plane vereint. Kiteworks vereinheitlicht, verfolgt, kontrolliert und schützt sensible Daten, die innerhalb, in und aus der Organisation heraus bewegt werden, verbessert dadurch das Risikomanagement erheblich und stellt die regulatorische Compliance bei allen sensiblen Datenaustauschen sicher. Mit Hauptsitz im Silicon Valley schützt Kiteworks über 100 Millionen Endnutzer sowie Tausende globale Unternehmen und Behörden.

Copyright 2026 Kiteworks.