Kiteworks

SOLUTION BRIEF

Kiteworks Compliant AI

Datenebenen-Governance für KI-Agenten Zugriff auf regulierte Daten

KI-Agenten sind die neuen digitalen Mitarbeiter – sie greifen mit Maschinengeschwindigkeit auf Finanzdaten, Patientendaten, CUI und Geschäftsgeheimnisse zu. Im Gegensatz zu menschlichen Mitarbeitern treffen Agenten keine eigenen Entscheidungen und greifen auf alle Daten zu oder führen jede Funktion aus, sofern sie nicht explizit daran gehindert werden.

Regelungen wie HIPAA, CMMC/ITAR, PCI DSS, SEC und SOX verlangen strikte Kontrollen für Datenzugriff, Audit-Trails und Verschlüsselung. Diese Anforderungen gelten gleichermaßen für KI-Agenten, die auf regulierte Daten zugreifen.

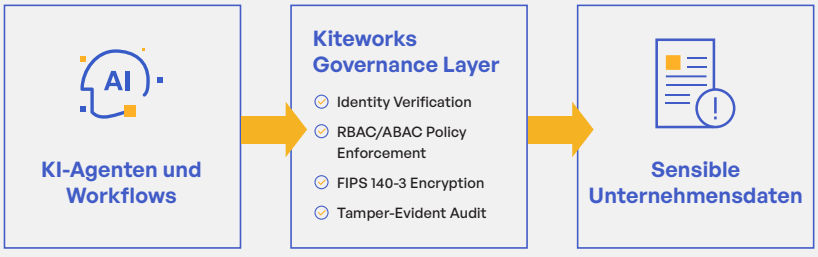
Datenebenen-Governance: Die einzige Ebene, die KI-Agenten nicht umgehen können

Kiteworks Compliant AI steuert Agenteninteraktionen auf der Datenebene – nicht auf der Modellebene. Modell-Prompts und Sicherheitsfilter lassen sich umgehen; die Durchsetzung auf der Datenebene jedoch nicht.

Jede Agenteninteraktion durchläuft vier Governance-Prüfpunkte:

- **Authentifizierte Identität:** Agenten werden über OAuth 2.0 verifiziert und mit dem menschlichen Autorisierer verknüpft, der den Workflow delegiert hat.
- **Richtlinienbasierter Zugriff (ABAC):** Anfragen werden in Echtzeit anhand der Agentenidentität, Datenklassifizierung und des Kontexts bewertet. Minimal notwendiger Zugriff wird auf Operationsebene durchgesetzt.
- **FIPS 140-3-validierte Verschlüsselung:** Alle von Agenten genutzten Daten werden während der Übertragung und im ruhenden Zustand mit validierten kryptografischen Modulen verschlüsselt.
- **Manipulationssicherer Audit-Trail:** Jede Interaktion wird mit vollständiger Zuordnung protokolliert und in Echtzeit an SIEM gestreamt.

Wo KI konform wird



Compliance ist in die Architektur integriert, nicht nachträglich angebaut

Lösung

Steuert den Zugriff von KI-Agenten auf sensible Daten auf der Datenebene – unabhängig von Modell, Prompt oder Agenten-Framework

FIPS 140-3-validierte Verschlüsselung für alle von Agenten genutzten Daten während der Übertragung und im ruhenden Zustand

FedRAMP Moderate zertifiziert; FedRAMP High in Vorbereitung

Drei käufliche Governed Assists über MCP für regulierte Workflows

Kompatibel mit Claude, Copilot und jedem MCP-kompatiblen LLM

Drei Governed Assists: Compliance-fähige KI-Workflows

Kiteworks Compliant AI liefert drei Governed Assists – eigenständige, käufliche Funktionen, die vom Model Context Protocol (MCP) bereitgestellt und durch die Kiteworks Data Policy Engine Ende-zu-Ende gesteuert werden. Jede Operation ist identitätsverifiziert, ABAC-geprüft, FIPS 140-3-verschlüsselt und manipulationssicher protokolliert.

Governed Folder Operations Assist: KI-Agenten navigieren, erstellen, benennen um, verschieben und löschen Ordnerhierarchien per natürlicher Sprache – jede Aktion wird durch die Data Policy Engine gesteuert. Ordnerstrukturen übernehmen automatisch RBAC/ABAC-Kontrollen und erfüllen so CUI-Segmentierung (CMMC), Aktensegmentierung (HIPAA) und Anforderungen an Audit-Workspaces.

Anwendungsfälle: Strukturierung von Kundenportfolios · CUI-Ordnersegmentierung · Bereitstellung von Audit-Workspaces · Litigation-Hold-Workspaces · Dokumentation klinischer Studien

Governed File Management Assist: KI-Agenten steuern den gesamten Datenlebenszyklus – Hochladen, Herunterladen, Lesen, Erstellen, Verschieben, Umbenennen und Löschen von Dateien – jede Aktion wird durch die Data Policy Engine durchgesetzt. Erfüllt Aufbewahrungsfristen (NARA, SOX), minimal notwendigen Zugriff (HIPAA) und Anforderungen an die Datenlöschung (PCI).

Anwendungsfälle: SOX-Aufbewahrungsprüfungen · CUI-Markierungsüberprüfung · Erstellung von Berichten zu unerwünschten Ereignissen · Generierung von Privilegienprotokollen · Durchsetzung von Aufbewahrungsplänen

Governed Forms Creation Assist: KI-Agenten erstellen gesteuerte Datenerfassungsformulare aus natürlichen Sprachbeschreibungen – der manuelle Aufwand für die Formularerstellung entfällt, während alle Einreichungen in richtliniengesteuerten Speicher mit vererbten RBAC/ABAC-Kontrollen geleitet werden.

Anwendungsfälle: KYC/CDD-Erfassung · FISMA-Vorfallmeldungen · HIPAA-Einwilligungsformulare · Lieferantenqualifizierungsfragebögen · Whistleblower-Berichte

Audit- und Governance-Anforderungen souverän erfüllen

- Nachweis der Kontrolle über regulierte Datenflüsse (CUI, PCI, PHI, personenbezogene Daten, SEC-regulierte Inhalte)
- Abbildung der KI-Agentenaktivitäten auf Compliance-Frameworks wie HIPAA, CMMC, PCI DSS, SEC/SOX, DSGVO, NIST CSF und ISO 27001
- Export einheitlicher Audit-Logs und dedizierte KI-Compliance-Berichte für Audits und Incident Response
- Schnelle Bereitstellung von prüfungsfähigen KI-Nachweispaketen für den Vorstand

Nahtlose Integration mit jeder KI-Plattform

Kiteworks Compliant AI funktioniert mit jeder MCP-kompatiblen KI-Plattform – Claude, Copilot und jedem zukünftigen LLM, das das Model Context Protocol unterstützt. Das AI Data Gateway stellt REST-APIs für RAG-Pipelines und programmatische KI-Workflows bereit. Einsatz in jeder Umgebung – Cloud, On-Premises oder Hybrid – mit plattformübergreifender Unterstützung für Windows, macOS und Linux. Standardbasierte, herstellerunabhängige Governance schützt Ihre Investition – unabhängig davon, welche KI-Plattformen Ihr Unternehmen nutzt.