Kiteworks

SOLUTION BRIEF

Kiteworks Compliant AI

Data-Layer Governance voor AI Agent Toegang tot gereguleerde gegevens

AI-agenten zijn de nieuwe digitale medewerkers—ze krijgen toegang tot financiële gegevens, patiëntgegevens, CUI en handelsgeheimen met machinesnelheid. In tegenstelling tot menselijke medewerkers tonen agenten geen beoordelingsvermogen en zullen ze elke gegevens of functie benaderen die ze niet expliciet wordt verboden.

Regelgeving zoals HIPAA, CMMC/ITAR, PCI DSS, SEC en SOX vereist strikte controles op gegevenstoegang, audittrail en encryptie. Deze verplichtingen gelden evenzeer voor AI-agenten die gereguleerde gegevens benaderen.

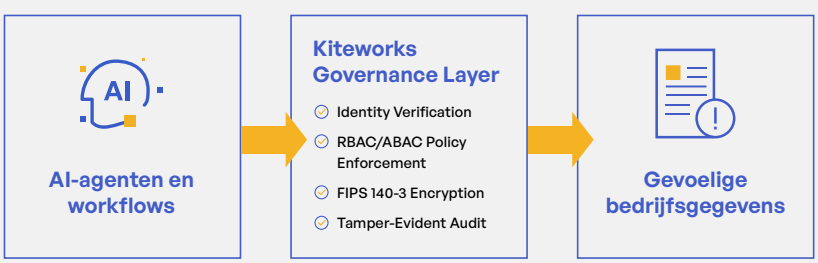
Data-Layer Governance: De enige laag die AI-agenten niet kunnen omzeilen

Kiteworks Compliant AI reguleert agentinteracties op de data layer—niet op de modellayer. Modelprompts en veiligheidsfilters kunnen worden omzeild; handhaving op de data layer niet.

Elke agentinteractie doorloopt vier governance-controlepunten:

- **Geauthenticeerde identiteit:** Agenten worden geverifieerd via OAuth 2.0 en gekoppeld aan de menselijke autorisator die de workflow heeft gedelegeerd.
- **Beleidsafgedwongen toegang (ABAC):** Verzoeken worden in realtime geëvalueerd op basis van agentidentiteit, gegevensclassificatie en context. Minimale noodzakelijke toegang wordt op operationeel niveau afgedwongen.
- **FIPS 140-3 gevalideerde encryptie:** Alle door agenten benaderde gegevens worden versleuteld tijdens transport en in rust met gevalideerde cryptografische modules.
- **Manipulatiebestendige audittrail:** Elke interactie wordt gelogd met volledige toewijzing en in realtime doorgestuurd naar SIEM.

Waar AI compliant wordt



Compliance ingebouwd in de architectuur, niet achteraf toegevoegd

Oplossing Hoogtepunten

- **Reguleert AI-agent toegang tot gevoelige gegevens op de data layer, onafhankelijk van model, prompt of agent framework**
- **FIPS 140-3 gevalideerde encryptie voor alle door agenten benaderde egevens tijdens transport en in rust**
- **FedRAMP Moderate Authorized; FedRAMP High In Process**
- **Drie afzonderlijk aanschafbare Governed Assists via MCP voor gereguleerde workflows**
- **Werkt met Claude, Copilot en elke MCP-compatibele LLM**

Drie Governed Assists: Compliance-Ready AI Workflows

Kiteworks Compliant AI levert drie Governed Assists—afzonderlijke, aanschafbare mogelijkheden aangedreven door het Model Context Protocol (MCP) en van begin tot eind gereguleerd door de Kiteworks Data Policy Engine. Elke operatie is identiteit-geverifieerd, ABAC-geëvalueerd, FIPS 140-3 versleuteld en manipulatiebestendig gelogd.

Governed Folder Operations Assist: AI-agenten navigeren, maken aan, hernoemen, verplaatsen en verwijderen mappenhiërarchieën met natuurlijke taal—waarbij elke operatie wordt gereguleerd door de Data Policy Engine. Mappenstructuren erven automatisch RBAC/ABAC-controles, waarmee wordt voldaan aan CUI-segregatie (CMMC), dossiersegregatie (HIPAA) en vereisten voor auditwerkruimtevoorziening.

Toepassingen: Structurering van klantportefeuilles · CUI-mappensegregatie · Auditwerkruimtevoorziening · Litigation hold werkruimtes · Documentatie van klinische studies

Governed File Management Assist: AI-agenten beheren de volledige levenscyclus van gegevens—uploaden, downloaden, lezen, aanmaken, verplaatsen, hernoemen en verwijderen van bestanden—met elke operatie afgedwongen door de Data Policy Engine. Voldoet aan bewaarschema's (NARA, SOX), minimale noodzakelijke toegang (HIPAA) en vereisten voor verwijdering (PCI).

Toepassingen: SOX-bewaarscans · CUI-markering verificatie · Verpakking van meldingen van ongewenste gebeurtenissen · Generatie van privilege logs · Handhaving van recordschema's

Governed Forms Creation Assist: AI-agenten genereren gereguleerde gegevensverzamelingsformulieren op basis van natuurlijke taalbeschrijvingen—waardoor de handmatige last van formuliercreatie wordt weggenomen en alle inzendingen automatisch naar beleidsgereguleerde opslag met geërfde RBAC/ABAC-controles worden geleid.

Toepassingen: KYC/CDD intake · FISMA-incidentrapportage · HIPAA-autorisatieformulieren · Leverancierskwalificatievragenlijsten · Whistleblower-rapportage

Voldoe vol vertrouwen aan audit- en governancevereisten

- Toon controle aan over gereguleerde gegevensstromen (CUI, PCI, PHI, PII, SEC-gereguleerde content)
- Koppel AI-agentactiviteiten aan compliance frameworks zoals HIPAA, CMMC, PCI DSS, SEC/SOX, GDPR, NIST CSF en ISO 27001
- Exporteer uniforme audit logs en speciale AI-compliancerapportages voor audits en incidentrespons
- Stel snel direct bruikbare AI-bewijspakketten samen voor de raad van bestuur

Naadloze integratie met elk AI-platform

Kiteworks Compliant AI werkt met elk MCP-compatibel AI-platform—Claude, Copilot en elke toekomstige LLM die het Model Context Protocol ondersteunt. De AI Data Gateway biedt REST API's voor RAG-pijplijnen en programmatische AI-workflows. Zet in op elke omgeving—cloud, on-premises of hybride—met cross-platform ondersteuning voor Windows, macOS en Linux. Standaardgebaseerde, leveranciersneutrale governance die uw investering beschermt, ongeacht welke AI-platforms uw organisatie gebruikt.