Kiteworks | reco

LÖSUNGSÜBERSICHT

FÜR SECURITY- UND COMPLIANCE-TEAMS

KI-Agenten-Risiken Von Der Erkennung Bis Zur Durchsetzung Steuern

Reco Findet Das Risiko. Kiteworks Kontrolliert Die Daten.

KI-Agenten-Governance | FedRAMP | CMMC 2.0 | EU Data Act | DSGVO | HIPAA

Die Herausforderung

KI-Agenten verbreiten sich schneller über SaaS-Plattformen, als Sicherheitsteams sie überprüfen können. Recos eigene Untersuchungen zeigen, dass 71 % der Wissensarbeiter KI-Tools ohne Freigabe der IT nutzen, und Analysten gehen davon aus, dass bis Ende 2026 40 % der Unternehmensanwendungen über agentische Fähigkeiten verfügen werden. Der Kiteworks 2026 Data Security and Compliance Risk Report beziffert die daraus entstehende Lücke: Keine einzige KI-Eindämmungskontrolle wird von mehr als 31 % der Unternehmen eingesetzt, und 65 % der Unternehmen, die gezielt nach Schatten-KI-Nutzung gesucht haben, sind fündig geworden. Sicherheitsteams sehen das Risiko wachsen. Die meisten können es jedoch noch nicht steuern, weil Transparenz und Durchsetzung bislang in getrennten Tools lagen, von unterschiedlichen Teams verantwortet wurden und auf unterschiedlichen Datenbeständen liefen.

Die Lösung

Die Reco-Plattform erkennt jeden Agenten, jede Anwendung und jede Identität in Ihrem gesamten Ökosystem – gestützt auf den größten Agenten- und App-Katalog am Markt, sodass Sicherheitsteams mit echten Risikoprofilen starten, statt bei null anzufangen. Die Kiteworks Control Plane nimmt dieses Risikosignal auf und setzt Richtlinien für die sensiblen Daten durch, auf die diese Identitäten tatsächlich zugreifen können – über E-Mail, File Sharing, APIs, Managed File Transfer und KI-Agenten-Workflows hinweg. Eine einzige, zentral gesteuerte und auditierte Control Plane deckt sowohl Menschen als auch die in ihrem Auftrag handelnden Agenten ab, sodass sich die Zeitspanne zwischen dem Auffinden und dem Schließen eines Risikos von Monaten auf Minuten verkürzt.

Die Governance-Lücke in Zahlen

Ergebnisse aus dem Kiteworks 2026 Data Security and Compliance Risk Report und Recos eigener Untersuchung zur Ausbreitung von Agenten und Anwendungen.

31%
Höchste gemessene Adoptionsrate einer KI-Eindämmungskontrolle

65%
Unternehmen, die nicht genehmigte Tool-Nutzung fanden

260+
Von Reco abgedeckte Agenten- und App-Plattformen

Kernfunktionen

Kontinuierliche Identitäts- und Agentenerkennung

Reco erfasst jede Anwendung, jede menschliche und nicht-menschliche Identität sowie jeden Agenten und deckt Wildwuchs sowie übermäßig berechtigten Zugriff auf, sobald sie entstehen. Der Reco Graph hält dieses Inventar aktuell, während neue Tools und Agenten eingeführt werden.

Richtliniendurchsetzung in Echtzeit

Die Kiteworks Data Policy Engine reagiert sofort auf dieses Risikosignal: Zugriff nur zum Anzeigen, SafeEDIT, Verschlüsselung oder eine vollständige Sperrung. Richtlinienentscheidungen greifen in dem Moment, in dem das Risiko erkannt wird – nicht erst beim nächsten Audit-Zyklus.

Eine Control Plane für Menschen und Agenten

Der Kiteworks Secure MCP Server steuert KI-Agenten nach denselben RBAC-/ABAC-Richtlinien, derselben Verschlüsselung und demselben Audit-Trail, die bereits für menschliche Nutzer gelten. Sicherheitsteams verwalten so ein einziges Richtlinienmodell, statt ein paralleles Regelwerk für maschinelle Identitäten zu pflegen.

Possessionless Editing

Mit SafeEDIT können autorisierte Nutzer sensible Daten direkt im Browser bearbeiten, ohne die Datei jemals herunterzuladen. Sensible Daten verlassen die kontrollierte Umgebung selbst während aktiver Zusammenarbeit nie.

Einheitliche Audit-Nachweise

Ein einziges Audit-Log erfasst jeden Zugriffs-, Freigabe-, Bearbeitungs- und Übertragungsvorgang und speist SIEM-Plattformen wie Splunk und ArcSight. Compliance-Teams erhalten so einen einzigen Nachweispfad, statt Protokolle aus Reco, Kiteworks und Einzellösungen abgleichen zu müssen.

Compliance-taugliches Fundament

FedRAMP High befindet sich im Zulassungsverfahren – aufbauend auf der FedRAMP-Moderate-Autorisierung seit 2017 – und ist auf Regularien wie HIPAA, CMMC 2.0, DSGVO und PCI DSS abgestimmt. Dieselben Kontrollen, die Bundesauditoren erfüllen, gelten automatisch auch für agentengesteuerte Datenzugriffe.

Einsatzbereiche

Eindämmung der Agenten-Ausbreitung

Neu entdeckte KI-Agenten werden in dem Moment, in dem Reco sie aufdeckt, unter kontrollierte Richtlinien gestellt – und schließen damit die Lücke zwischen Erkennung und Durchsetzung, die die meisten Unternehmen heute nie schließen.

Einführung in regulierten Branchen

Agentische KI lässt sich mit audit-fähigen Nachweisen in Gesundheitswesen, Finanzdienstleistungen und Behörden-Workloads ausweiten, ohne auf einen Compliance-Ausnahmeprozess warten zu müssen.

SaaS-Modernisierung

Fragmentierte Einzellösungen weichen einem durchgängigen Pfad von Identitätsrisiko bis zu durchgesetzter Daten-Governance – über E-Mail, File Sharing, APIs und Managed File Transfer hinweg.

Bereit, die Lücke zwischen KI-Agenten-Erkennung und -Durchsetzung zu schließen?

www.kiteworks.com

Kiteworks | reco

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.