

Kiteworks integriert Cyera, um Datenklassifizierungen durchzusetzen

Cyera-Klassifizierungen versehen Dateien in Kiteworks mit Tags, sodass die Data Policy Engine steuern kann, wie Menschen, Maschinen und KI-Agenten auf sensible Daten zugreifen und sie austauschen

Data Policy Engine

SafeVIEW

Sovereign Edit

Sovereign Edit – Streaming

Audit-Nachweise

Die Herausforderung

Die Erkennung zeigt, wo sensible Daten liegen, und die Klassifizierung, wie sensibel sie sind. Das Risiko entsteht, sobald diese Daten sich bewegen: als E-Mail-Anhang, bei der Freigabe für einen Partner, beim Abruf durch einen automatisierten Workflow oder auf Anfrage eines KI-Agenten. Unternehmen brauchen einen Weg, die Erkennung und Klassifizierung sensibler Daten bis zur Durchsetzung der Richtlinien zu verlängern, die Daten in Bewegung steuern und schützen.

Die Lösung

Kiteworks baut auf Ihren jahrelangen Investitionen in die Datenklassifizierung auf und wandelt die Klassifizierungen von Cyera in Kiteworks-Tags um. Bei jeder Anfrage zum Zugriff auf Daten oder zu ihrer Bewegung wertet die Data Policy Engine den Tag und die Attribute des Benutzers in Echtzeit aus und wendet Vorgaben an wie zulassen, blockieren, Genehmigung verlangen oder einschränken, für Menschen, Maschinen und KI-Agenten gleichermaßen.

So funktioniert die Integration

1

HOCHLADEN

Eine Datei gelangt in Kiteworks

Eine Person, ein automatisierter Prozess oder ein KI-Agent lädt eine Datei über Dateifreigabe, SFTP, E-Mail-Anhänge, Formulare, APIs, MCP oder Managed File Transfer hoch.

2

ABFRAGEN

Kiteworks fragt Cyera ab

Kiteworks sucht die Datei anhand einer eindeutigen Datei-ID im Cyera-Inventar, ohne Dateidaten oder Metadaten preiszugeben.

3

TAGGEN

Die Datei erhält einen Tag

Befindet sich die Datei im Cyera-Inventar, liefert Cyera ihre Sensitivitätsklassifizierung zurück, und Kiteworks versieht die Datei mit einem Tag.

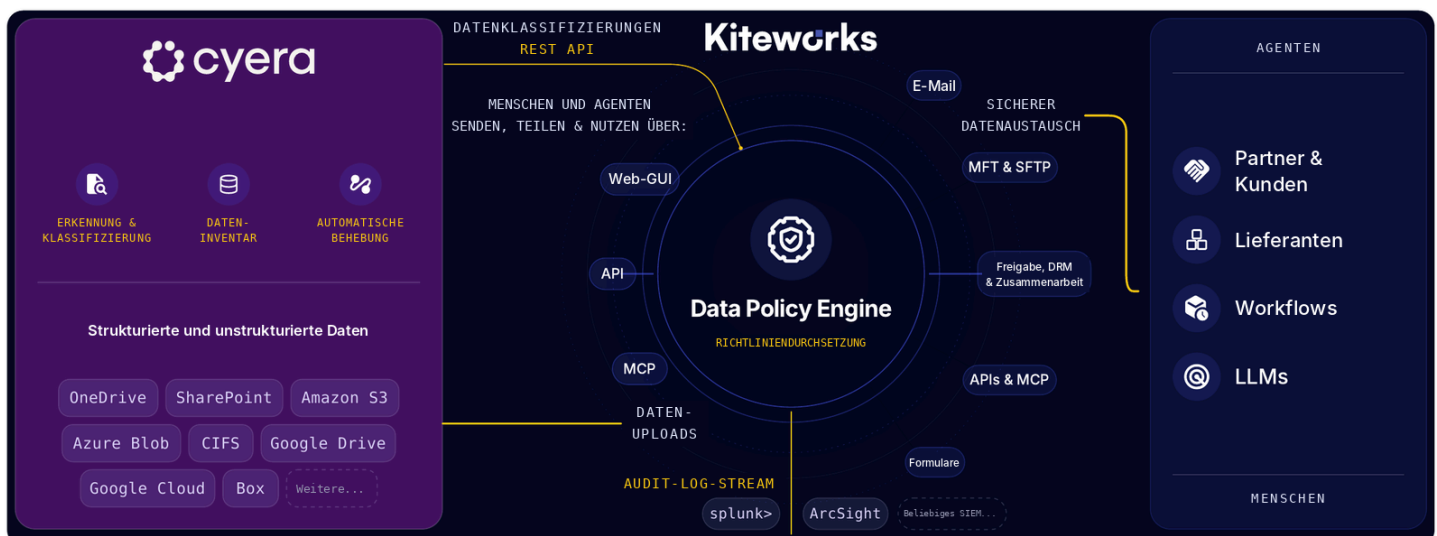
4

DURCHSETZEN

Die Richtlinie entscheidet

Versucht später jemand oder etwas, diese Daten zu bewegen, wendet die Data Policy Engine die von Ihnen festgelegten Regeln an, abhängig vom Tag, vom Benutzer und von der angeforderten Aktion.

Architektur von Cyera und Kiteworks



Was Sie mit einer Cyera-Klassifizierung tun können



Klassifizierungsgesteuerte Richtlinien

Definieren Sie anhand von Datenklassifizierungen Regeln, mit denen Sie Ihre Vorgaben nach NIST CSF, CMMC, HIPAA, NIS 2, PCI-DSS und weiteren Standards umsetzen.



Menschen und KI-Agenten, eine Control Plane

Die Kiteworks Control Plane steuert Zugriff, Nutzung und Austausch von Daten für Menschen, Maschinen und KI-Agenten nach denselben Richtlinien.



Jeder Kanal

Wenden Sie Richtlinien über E-Mail, Dateifreigabe, SFTP, Managed File Transfer, APIs, MCP und Formulare hinweg an.



SafeVIEW und Sovereign Edit

Beschränken Sie eine sensible Datei auf die Ansicht mit Wasserzeichen oder auf die Bearbeitung im Browser ohne Download.



Genehmigungen und Begründungen

Verlangen Sie vor dem Senden oder Freigeben eine Genehmigung oder ein Formular, das eine Begründung im Audit-Log festhält.



Audit-Nachweise

Erfassen Sie die angeforderte Aktion, den Benutzer, die Tags und die betroffenen Dateien, mit Berichten für CMMC 2.0, DSGVO und HIPAA, die Audit- und Governance-Anforderungen unterstützen.

Wer profitiert



Sicherheitsteams

Wenden Sie die Klassifizierungen, denen Sie bereits vertrauen, auf Dateien an, sobald sie in Kiteworks eintreffen, damit eine sensible Datei so behandelt wird, wie es die Richtlinie vorsieht.



Compliance- und Governance-Teams

Zeigen Sie Prüfern, welche Richtlinie für welche Datei galt, für welche Person, Maschine oder welchen KI-Agenten, mit einem Audit-Eintrag zu jeder Aktion.



KI- und Datenteams

Halten Sie KI-Agenten innerhalb derselben klassifizierungsgesteuerten Richtlinien wie Menschen, mit einem einheitlichen Regelwerk für E-Mail, Dateifreigabe, SFTP, Managed File Transfer, APIs, MCP und Formulare.

Über Cyera

Cyera ist die KI-Sicherheitsplattform für das Zeitalter der Agenten. Unternehmen wie Paramount, Chipotle und Valvoline nutzen Cyera, um genau zu steuern, auf welche Daten ihre KI zugreifen kann – und um zu regeln, was danach geschieht. Die Plattform schützt Daten im Ruhezustand, in Bewegung und in Nutzung, ob sie von Menschen oder KI-Agenten berührt werden. Mit 9 Milliarden US-Dollar bewertet und mit über 1,7 Milliarden US-Dollar von Accel, Blackstone, Cyberstarts, Georgian, Lightspeed und Sequoia unterstützt. Schützen Sie Ihre Daten. Sichern Sie KI.

Sehen Sie Ihre Cyera-Klassifizierungen in Kiteworks durchgesetzt

www.kiteworks.com

Kiteworks



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.