

FOR SECURITY, COMPLIANCE, AND AI GOVERNANCE TEAMS

Kiteworks Integrates with Cyera to Enforce Data Classifications

Cyera Classifications Tag Files in Kiteworks, So the Data Policy Engine Can Govern How People, Machines, and AI Agents Access and Exchange Sensitive Data

Data Policy Engine

SafeVIEW

Sovereign Edit

Sovereign Edit – Streaming

Audit Evidence

The Challenge

Discovery tells you where sensitive data lives, and classification tells you how sensitive it is. The risk appears when that data moves: attached to an email, shared with a partner, pulled by an automated workflow, or requested by an AI agent. Organizations need a way to extend sensitive data discovery and classification into enforcement of the policies that govern and protect data in motion.

The Solution

Kiteworks builds on your years of investment in data classification by turning Cyera's classifications into Kiteworks tags. For every data access or movement request, the Data Policy Engine evaluates the tag and the user's attributes in real time and applies directives such as allow, block, require approval, or restrict, for people, machines, and AI agents alike.

How the Integration Works

1

UPLOAD

A File Enters Kiteworks

A person, an automated process, or an AI agent uploads a file through file sharing, SFTP, email attachments, forms, APIs, MCP, or managed file transfer.

2

LOOK UP

Kiteworks Checks Cyera

Kiteworks looks the file up in Cyera's inventory using a unique file identifier, exposing no file data or metadata.

3

TAG

The File Is Tagged

If the file is in Cyera's inventory, Cyera returns its sensitivity classification and Kiteworks tags the file.

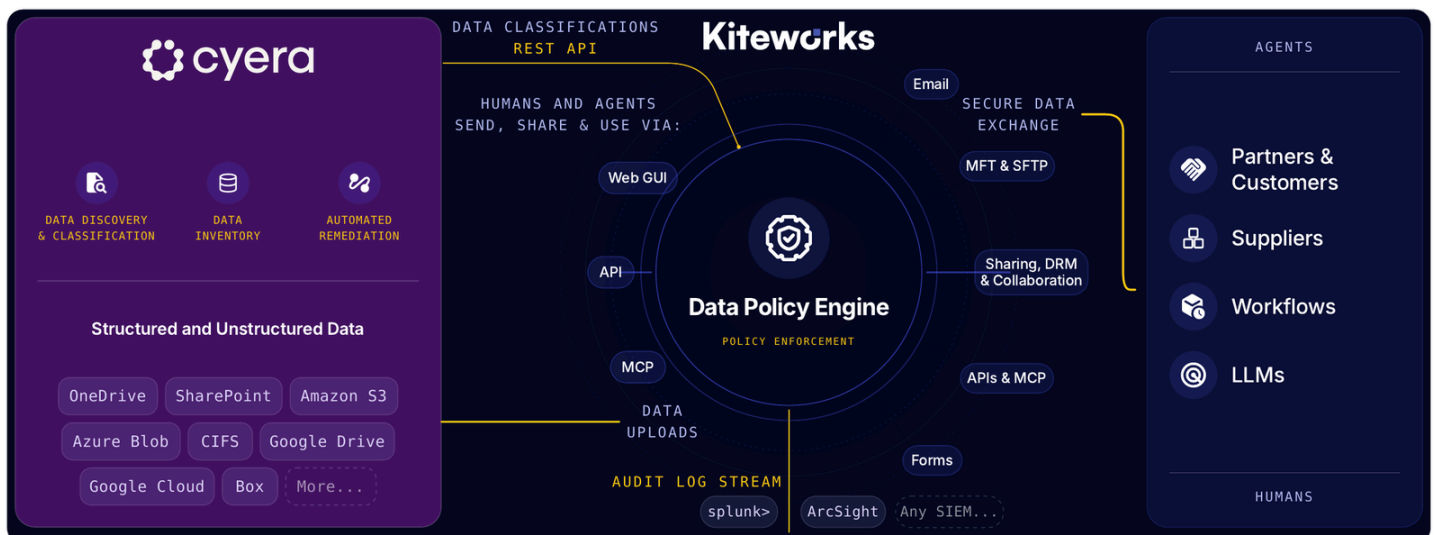
4

ENFORCE

Policy Decides

Later, when anyone or anything tries to move that data, the Data Policy Engine applies the rules you set, based on the tag, the user, and the action requested.

Cyera and Kiteworks Architecture



What You Can Do with a Cyera Classification



Classification-Driven Policy

Use data classifications to define rules that implement your NIST CSF, CMMC, HIPAA, NIS 2, PCI-DSS, and other policies.



People and AI Agents, One Control Plane

The Kiteworks Control Plane governs data access, use, and exchange for people, machines, and AI agents under the same policies.



Every Channel

Apply policy across email, file sharing, SFTP, managed file transfer, APIs, MCP, and forms.



SafeVIEW and Sovereign Edit

Restrict a sensitive file to watermarked viewing, or to editing in the browser without a download.



Approvals and Justifications

Require approval before a send or share, or a form that records a justification in the audit log.



Audit Evidence

Record the action requested, the user, the tags, and the files affected, with reports for CMMC 2.0, GDPR, and HIPAA that support audit and governance requirements.

Who Benefits



Security Teams

Apply the classifications you already trust to files as they enter Kiteworks, so a sensitive file is handled the way policy says it should be.



Compliance and Governance Teams

Show auditors which policy applied to which file, for which person, machine, or AI agent, with an audit record of each action.



AI and Data Teams

Keep AI agents inside the same classification-driven policies as people, with one policy set across email, file sharing, SFTP, managed file transfer, APIs, MCP, and forms.

About Cyera

Cyera is the AI Security Platform built for the age of agents. Enterprises like Paramount, Chipotle, and Valvoline use Cyera to control exactly what data their AI can reach – and govern what happens next. The platform secures data at rest, in motion, and in use, whether touched by humans or AI agents. Valued at \$9 billion and backed by over \$1.7 billion from Accel, Blackstone, Cyberstarts, Georgian, Lightspeed, and Sequoia. Protect your data. Secure AI.

See Your Cyera Classifications Enforced in Kiteworks

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.