

KITEWORKS SECURE MCP SERVER

Unlock AI-Powered Workflows For Regulated Industries

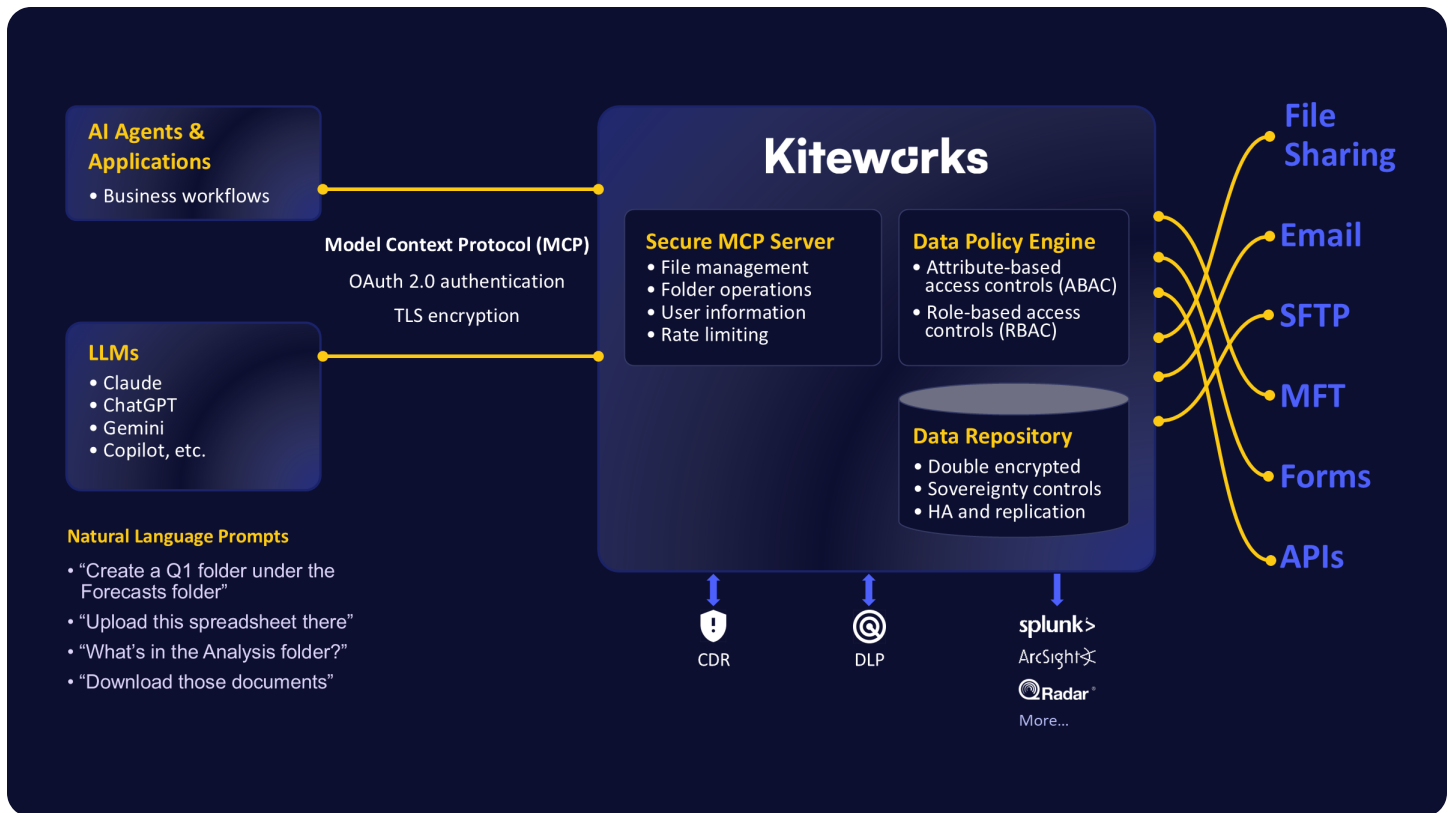
The Challenge

Enterprises across regulated industries are racing to adopt AI to accelerate productivity, automate insight generation, and enhance decision-making. Yet most face an unrelenting dilemma: how to leverage AI models like Claude, Gemini, and ChatGPT without losing control of sensitive data. Conventional AI integrations force organizations to expose internal files, customer records, and intellectual property to external systems—each query risking data leakage, compliance violations, and unauthorized access.

The Solution

The Kiteworks Secure MCP Server creates a governance-controlled connection between large language models and your organization's data, letting teams work in natural language through familiar AI clients like Claude and Copilot. Built on the Model Context Protocol (MCP), it evaluates every request against your role-based (RBAC) and attribute-based (ABAC) access controls—so an AI client receives only the data that policy deems appropriate for it, while information too sensitive for the model is kept out of its reach. Every file access, folder operation, and data retrieval is authorized, enforced, and logged inside your Kiteworks control plane for secure data exchange.

How The Kiteworks Secure MCP Server Works



Every file access, folder operation, and data retrieval flows through the Secure MCP Server and Data Policy Engine—governed by RBAC and ABAC and captured in a unified audit trail.

AI Without Compromise

Kiteworks Secure MCP Server enables secure AI interaction with enterprise data while ensuring that sensitive information never leaves your trusted environment. Employees gain AI-powered efficiency, while the security team retains complete oversight. Every AI operation is logged for compliance and forensics, preserving data integrity, trust, and auditability.

Governance That Scales With AI

- OAuth 2.0 authentication ensures every AI operation inherits the user's existing permissions.
- ABAC dynamically enforces data-handling policies based on classification, sensitivity, and context.
- A comprehensive audit log captures every AI exchange for continuous visibility and compliance.
- Kiteworks is FedRAMP Authorized and IRAP assessed to the PROTECTED level.

Enterprise-Grade Security By Design



Access Token Protection

Stores tokens in the encrypted OS keystore instead of environment variables.



OAuth 2.1 Hardening

Dynamic client registration, authorization code with PKCE, JWT access and refresh tokens, and automatic token rotation.



FIPS 140-3 Cryptography

AES-256-GCM, RSA with SHA-256, and TLS 1.3 with NIST-approved curves.



Post-Quantum Forward Secrecy

Hybrid X25519 + ML-KEM-768 TLS key exchange (FIPS 203).



Rate Limiting Controls

Configurable global, per-user, and per-session quotas.



Path Traversal Protection

Normalize and validate all filesystem paths.



Data and Secret Isolation

Never expose credentials or transferred payloads to the LLM.



TLS Authenticity

Enforce certificate validation and hostname verification to prevent man-in-the-middle attacks.

Build Compliant Forms in Seconds—Just Ask Claude

With the Kiteworks Secure MCP Server, your teams can generate sophisticated Secure Data Forms in seconds simply by asking Claude. Point Claude at a PDF, image, or text description, and it drafts and previews a complete form as structured JSON, delivered straight to a governed Kiteworks folder. Every new form inherits your platform's role-based and attribute-based access controls, double encryption, and unified audit log—turning AI-accelerated form building into a fully compliant, governance-first data collection workflow.

Connecting To Your Private Kiteworks MCP Server

Every Kiteworks customer runs its own private Kiteworks cloud instance, so each organization deploys its own private Kiteworks MCP server. Setup takes two steps:

1

INSTALL & CONFIGURE

Install & Configure Your Server

Follow the [Kiteworks MCP Installation & Setup](#) guide to stand up a local server for a developer or an HTTP server for your organization.

2

CONNECT

Connect as an End User

Each user opens the Connector Marketplace in their Claude Desktop client and connects to Kiteworks.

Learn more about the Kiteworks Secure MCP Server at [Kiteworks MCP Server Overview](#).

The Result: Secure, Compliant AI Productivity

Kiteworks Secure MCP Server enables enterprises to safely integrate AI into daily operations while protecting sensitive data and meeting regulatory requirements. By enforcing governance and security at every layer, it delivers responsible AI adoption that accelerates innovation without risking exposure or compliance gaps—so organizations can confidently put their sensitive data to work in AI workflows, securely and intelligently, without compromise.

Ready to unlock AI without compromise?

www.kiteworks.com

Kiteworks



Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, through, and out of the organization; significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.