Kiteworks

FEATURE BRIEF

Kiteworks Comparison: FedRAMP High vs. Moderate

The Platinum and Gold Standards for Security

FedRAMP High builds directly on FedRAMP Moderate but represents a major increase in security depth, continuous monitoring frequency, data protection, and operational complexity. To achieve FedRAMP High, an organization must satisfy everything required at Moderate, meeting significantly more frequent or stringent requirements across at least 100 of those controls, plus meet 96 additional controls focused on high-impact scenarios.

	Kiteworks FedRAMP Service Offering	
Aspect	**Kiteworks Federal Cloud Moderate Authorized Status**	**Kiteworks Secure Gov Cloud High In Process Status**
Number of Controls (NIST SP 800-53 Rev. 5)	**325 controls**	**421 controls**
Target Data Sensitivity	**Controlled unclassified information (CUI); moderate risk data**	**Highly sensitive/critical data (emergency services, financial, law enforcement)**
MFA	✔ For privileged access	★ For all users
Audit Event Logging	✔ Logging and review	★ Granular, near real-time audit logging
Encryption	✔ Strong	★ FIPS-validated encryption everywhere
Supply Chain Risk NIST 800-53 "SR" Controls	✔ Partial coverage	★ Full SR family validated
Continuous Monitoring	✔ Monthly/periodic scans ✔ Periodic log reviews	★ Near real-time monitoring ★ More immediate remediation deadlines
Assessment & Documentation	✔ Detailed assessments ✔ Penetration testing ✔ Detailed documentation	★ More rigorous assessments ★ Deeper penetration testing ★ More detailed documentation
Personnel Screening	✔ For select roles	★ Enhanced screening, more frequent background checks, more roles included
Incident Response	✔ Reporting, testing, and integration	★ Automated detection and response ★ Coordination with external teams ★ Deeper testing
Boundary/Access Controls	✔ Network segmentation, firewall, least-privilege controls	★ Additional boundary protections, advanced filtering, error handling, protection against DoS
Developer Security Architecture		★
Component Authenticity		★
Automated Flaw Remediation		★
Architecture for DNS		★

Moderate and High Impact Use Case Examples

FedRAMP Moderate covers the majority of federal cloud use cases (around 80%) involving sensitive but unclassified data where a breach would cause serious harm (e.g., PII, routine CUI, most agency records). FedRAMP High is reserved for the government's most sensitive unclassified information—data that if compromised could lead to loss of life, threats to national security, or catastrophic damage (e.g., emergency services, law enforcement intel, defense communications, ITAR data).

Use Case	FedRAMP Moderate Examples	FedRAMP High Examples
Defense Industrial Base (CUI, ITAR)	Contractors handling CUI (e.g., supply chain, schematics). File transfer or collaboration tools, SFTP, and managed file transfer. Impact: Program delays, IP theft.	Handling ITAR-regulated data (e.g., weapons specs). Requires U.S.-only storage/personnel. Impact: Regulatory violation, national security loss.
Defense & Intelligence Agencies	DoD systems storing non-critical logistics or training CUI. Secure collaboration or email apps. Impact: Operational disruption.	Mission-critical DoD/IC systems transferring unclassified but vital intel or military data. Secure collaboration or email apps. Impact: National security threat.
Technology and Manufacturing Exporters (EAR/Dual Use Items)	Documentation, classification records, and licensing files subject to EAR. Apps include secure file sharing, managed file transfer, and email. Impact: Export violation fines, loss of export privileges.	Encryption software, advanced semiconductors, or other EAR-controlled items subject to enhanced BIS scrutiny. Requires strict access controls, audit logging, and U.S.-person oversight of sensitive technical data. Impact: Severe regulatory penalties, reputational damage, and loss of export privileges.
Personally Identifiable Information (PII)	Civilian agencies managing HR systems or public portals with basic PII (e.g., contact info). Apps include email, file-sharing portals, and managed file transfer. Impact of breach: Privacy violation or fraud.	Intelligence or law enforcement with highly sensitive PII (e.g., undercover agents). Apps include email, file-sharing portals, and managed file transfer. Impact of breach: Life or mission endangerment.
Protected Health Information (PHI)	VA or HHS systems handling medical records or patient portals. Used for storing and transmitting PHI. Impact: Privacy harm or service disruption.	Emergency response or medical control systems (e.g., device data or dispatch). Impact: Life-threatening if data is unavailable or altered.
Emergency Services & Law Enforcement	Admin systems (e.g., payroll, non-critical reporting) in local/federal agencies. File-sharing and internal portals. Impact: Reputational or operational harm.	Operational systems like 911 dispatch or federal law enforcement database reporting information. Real-time, mission-critical apps. Impact: Public safety risks.
Financial Data (Government & Contractors)	Systems transmitting agency budgets, invoices, or payrolls, such as secure file sharing and email apps. Impact: Financial fraud or data loss.	National financial systems (e.g., fund transfers or benefits). Impact: Severe financial loss or public confidence crisis.