Kiteworks

TOP 5

Top 5 Reasons to Use Kiteworks Instead of GCC High

For most defense contractors and federal agencies, Kiteworks runs alongside Microsoft 365 GCC High. A narrower segment faces a different reality. For ITAR-heavy contractors with foreign-owned subsidiary complexity, intelligence community contractors with explicit key custody requirements, pre-decision organizations, federal agencies preparing for ATO renewal under post-ProPublica scrutiny, and existing GCC High customers experiencing documented operational pain, the architectural exposure inside GCC High cannot be mitigated by coexistence. Kiteworks consolidates managed file transfer, secure email, file sharing, SFTP, data forms, and AI data channels onto a single hardened, single-tenant virtual appliance — purpose-built for the regulatory environment GCC High was retrofitted into.

1 Eliminate the FedRAMP Cover Memo From Your Authorization Record

On December 26, 2024, FedRAMP authorized GCC High with a cover report documenting deficiencies and unknown risks. The review team wrote into the official record: "There is a lack of confidence in assessing the system's overall security posture." ProPublica's March 2026 investigation documented 480 hours of review, 18 technical deep dives, and an unresolved data flow diagram dispute. Kiteworks is FedRAMP Moderate Authorized continuously since June 2017 and FedRAMP High In Process (2026) — no cover memo, no asterisk.

2 Hold Your Own Encryption Keys and Remove CLOUD Act Exposure

Microsoft documents an "availability key" mechanism allowing the company to access customer data when customer-side key management is unavailable. Under the U.S. CLOUD Act, the same provider can be lawfully compelled to produce decrypted customer data — the FBI has obtained BitLocker recovery keys from Microsoft. Kiteworks supports customer-controlled key custody: the customer holds the keys, the vendor holds the ciphertext, and there is no mechanism for the platform to decrypt customer data.

3 Replace Multi-Tenant Logical Separation With Single-Tenant Physical Isolation

GCC High runs in a multi-tenant environment with logical separation — the same architecture pattern that produced the 2023 Chinese state-sponsored infiltration of Microsoft's lower-tier GCC. Every Kiteworks deployment is single-tenant: no shared databases, file systems, or runtime environments. Combined with FIPS 140-3 validated encryption and tamper-evident audit logging, the architecture aligns directly with controls regulators expect to see documented under CMMC Level 2, NIST 800171, DFARS 252.204-7012, and ITAR cloud handling requirements.

4 Replace the 72-Hour Throttled Audit Log With Real-Time Tamper-Evident Capture

Microsoft 365 audit logs throttle during high-activity periods, delay up to 72 hours, and fragment across Exchange, SharePoint, Teams, OneDrive, and the security and compliance center. Per Kiteworks Data Security and Compliance Risk: 2026 Forecast Report, 33% of organizations lack evidence-quality audit trails and 61% have fragmented logs. Kiteworks delivers real-time, single tamper-evident audit capture across every channel — email, file share, SFTP, MFT, data forms, APIs, and AI agents. The platform satisfies nearly 90% of the 110 CMMC Level 2 practices.

5 Migrate Without Rebuilding the Workflows — and End the Architectural Risk in One Move

Migration is a planning decision, not a forklift. Kiteworks offers a structured migration path that preserves underlying business workflows — file transfer schedules, partner endpoints, encryption requirements, audit trail continuity, and the user experience employees already understand. The architectural end-state: the FedRAMP cover memo no longer sits underneath the authorization record, customer-controlled keys close the CLOUD Act pathway, single-tenant isolation eliminates cross-tenant exposure, and real-time evidence-quality audit logs satisfy multiple regulatory regimes simultaneously.

www.kiteworks.com

June 2026