Kiteworks

TOP 5

# Top 5 Ways Kiteworks *Actually* Supports CMMC 2.0 Compliance in a Sea of Otherwise Empty Vendor Promises

**Kiteworks is the powerhouse** at your back, enabling you to grow your business with the federal government by providing a consistent and comprehensive approach to security; we deliver the gold standard for sensitive content communication and help to reduce the risk of data breaches and other security incidents. Defense industrial base (DIB) companies like General Dynamics Information Technology and MITRE partner with Kiteworks and enjoy the benefits listed below:

1. **Six straight years of achieving FedRAMP Moderate authorization delivers on privacy promises no others can.**

   Take the fast route to CMMC 2.0 compliance with Kiteworks, audited yearly and continuously monitored by a certified third-party assessor, FIPS 140-2 Validated, and FedRAMP Moderate Authorized since 2017. FedRAMP reduces cost, decreases the risk of noncompliance and breaches, and is the security gold standard. As an authorized cloud service provider (CSP), Kiteworks has passed rigorous yearly audits by certified third parties that validate 325 NIST 800-53 security controls, as well as having incidents and configuration changes continuously monitored. Audits and monitoring also encompass plans for vulnerability management, configuration management, contingencies, incident responses, and other categories. **Don't be fooled by vendors** who claim to be "equivalent" and pass the cost and effort of authorization onto you.

2. **Nearly 90% of CMMC 2.0 requirements out-of-the-box provide the fast-path to compliance and revenue.**

   The platform itself checks the boxes for defense in depth, such as built-in hardening, encryption of data, and zero trust between services. We help you meet nearly 90% of Level 2 requirements by staying compliant in practices within Configuration Management, System and Information Integrity, Maintenance, Personal Security, Physical Protection, Security Assessment, and System and Information Integrity. For contractors and subcontractors doing business with the U.S. DoD, this translates into dramatically faster compliance audits and expanded revenue opportunities.

3. **A one-stop console for tracking, no matter the communication channel, makes demonstrating compliance a breeze.**

   Email, file sharing and transfer, automated (managed) file transfer, APIs, and web forms are consolidated into one system. You can retain a firm grasp on all activity with a single point of truth—a clean, consolidated, real-time audit log feeding content, user, location, and time specific information to your SIEM systems. The Kiteworks platform also responds to unexpected activity and sends out live alerts to preidentified key individuals. Authenticate all users with unique IDs, multi-factor authentication including RADIUS, SMS, and authenticator apps.

### 4. Centralized content-based policy controls give unparalleled risk management over malicious exposure of sensitive data.

Define and enforce user access levels for all controlled unclassified information (CUI). Ensure encryption of all content at rest (with AES-256 encryption) to protect CUI from unauthorized access, data corruption, and malware. Kiteworks allows you to have granular policy controls like view-only access and water marking to protect sensitive content and enforce compliance policies yet increases user productivity and collaboration as business owners easily manage content, folders, invitations, and access controls. Kiteworks also allows you to set policies for password complexity while allowing administrators to reset user passwords and enforce password changes during login.

### 5. A hardened single-tenant virtual appliance creates multiple layers of protection for confidence you can "take to the board."

Kiteworks enforces a strict secure software development life cycle including extensive security code reviews, third-party testing, and a bounty program to keep your data protected. The Kiteworks hardened virtual appliance is architected to reduce the number of potential vulnerabilities in its libraries and increase the attack complexity required to exploit them; an embedded network firewall and WAF, zero-trust access, and minimized attack surface all work to significantly reduce security risk. The Private Content Network also invokes multiple layers of protection to reduce the impact on confidentiality, integrity, and availability with AI-based anomaly detection, advanced intrusion detection and alerts, as well as zero-day threat blocking. These internal layers work together to significantly reduce the CVSS security risk impact score. This means better protection for private customer content and a stronger security posture in the face of advanced persistent threats.

Being CMMC 2.0 compliant ensures that an organization's systems and networks meet a high level of cybersecurity hygiene, protecting against cyber threats and data breaches, while simultaneously allowing organizations to bid for U.S. government contracts. Don't leave yourself vulnerable and miss out on this important revenue! Government contractors, subcontractors, systems integrators, and National Institute of Environmental Health Sciences (NIEHS) trust Kiteworks to unify, control, track, and secure sensitive documents and provide them with the gold standard in cybersecurity.

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, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.

www.kiteworks.com

December 2022