

Top 5 Reasons to Migrate Off MOVEit to Kiteworks



Organizations running MOVEit Automation are absorbing emergency patch cycles at an accelerating cadence. The April 30, 2026 disclosure of CVE-2026-4670 (NVD CVSS 9.8 authentication bypass) and CVE-2026-5174 is the third critical vulnerability wave to hit MOVEit in three years—following the 2023 CIOp mass exploitation that compromised 2,700+ organizations and exposed approximately 95.8 million individuals (Emsisoft, June 2024), and the 2024 authentication bypass pair. It is also the fourth critical MFT vulnerability across vendors in 18 months, after Cleo, CrushFTP, and Wing FTP. Kiteworks consolidates managed file transfer, secure email, file sharing, SFTP, data forms, and AI data channels onto a single hardened, single-tenant virtual appliance with one policy engine and one consolidated audit log—built for the regulatory environment that now surrounds every data exchange surface.

1. End the Emergency Patch Cycle

Each MOVEit disclosure has been a no-workaround, full-installer upgrade with exploitation observed within hours. Organizations have absorbed at least four emergency change windows in three years. Kiteworks ends the cycle with a hardened virtual appliance maintained by Kiteworks, one-click full-system updates, and continuous penetration testing rather than reactive disclosure response.

2. Move From Customer-Managed Infrastructure to a Hardened Virtual Appliance

MOVEit Automation runs on customer-managed infrastructure where security depends on correct OS configuration, network exposure, and command port reachability. Kiteworks deploys as a hardened virtual appliance with embedded network firewall, web application firewall, and intrusion detection—maintained by Kiteworks, with no customer-side security stack to configure. When Log4Shell carried an industry National Vulnerability Database (NVD) CVSS of 10, Kiteworks' layered controls significantly reduced the practical exploitability; Kiteworks' internal assessment estimated the residual exploitability at approximately CVSS 4—an internal estimate, not an NVD-issued score.

3. Single-Tenant Isolation Replaces Shared Infrastructure Risk

Every Kiteworks deployment is single-tenant. Customers do not share databases, file systems, or runtime environments. Cross-tenant attack patterns cannot reach across boundaries that do not exist. Combined with FIPS 140-3 validated encryption and tamper-evident audit logging, the architecture aligns with the controls regulators expect to see documented under HIPAA Security Rule, CMMC Level 2, PCI DSS, and GDPR Article 32.

4. Consolidate the Data Exchange Estate Onto One Audit Log

MFT is one channel. Enterprises also exchange sensitive data through email, web forms, file sharing, SFTP, APIs, and AI assistants. According to the Kiteworks Data Security and Compliance Risk: 2025 MFT Survey Report, 62% of organizations operate fragmented systems across MFT, email, file sharing, and web forms, and 63% have not integrated MFT with their SIEM. Kiteworks unifies these channels under one platform with one policy engine and one consolidated audit log.

5. Migrate Without Rebuilding the Workflows

Migration is a real planning decision, not a forklift. Kiteworks offers a structured migration path from MOVEit Transfer and MOVEit Automation that preserves the underlying business workflows—file transfer schedules, partner endpoints, encryption requirements, audit trail continuity. The architectural end-state is one where the next MFT-class CVE is a routine patch event, evidence-quality audit logs satisfy multiple regulatory regimes simultaneously, and the data exchange surface is governed by controls regulators can recognize.