Kiteworks

TOP 5

Top 5 razones para migrar de MOVEit a Kiteworks

Las organizaciones que utilizan MOVEit Automation están absorbiendo ciclos de parches de emergencia a un ritmo acelerado. La divulgación del 30 de abril de 2026 de CVE-2026-4670 (NVD CVSS 9,8, omisión de autenticación) y CVE-2026-5174 es la tercera oleada de vulnerabilidades críticas que afecta a MOVEit en tres años, tras la explotación masiva de Cl0p en 2023 que comprometió más de 2700 organizaciones y expuso aproximadamente 95,8 millones de personas (Emsisoft, junio de 2024), y el par de omisiones de autenticación de 2024. Es también la cuarta vulnerabilidad crítica de MFT entre proveedores en 18 meses, después de Cleo, CrushFTP y Wing FTP. Kiteworks consolida la transferencia gestionada de archivos, el correo seguro, el uso compartido de archivos, SFTP, formularios de datos y los canales de datos de IA en un único dispositivo virtual reforzado y de inquilino único, con un solo motor de políticas y un único registro de auditoría consolidado, diseñado para el entorno regulatorio que ahora rodea cada superficie de intercambio de datos.

1. Ponga fin al ciclo de parches de emergencia

Cada divulgación de MOVEit ha sido una actualización con instalador completo, sin solución alternativa, con explotación observada en cuestión de horas. Las organizaciones han absorbido al menos cuatro ventanas de cambio de emergencia en tres años. Kiteworks pone fin al ciclo con un dispositivo virtual reforzado mantenido por Kiteworks, actualizaciones completas del sistema con un solo clic y pruebas de penetración continuas, en lugar de una respuesta reactiva a las divulgaciones.

2. Pase de una infraestructura gestionada por el cliente a un dispositivo virtual reforzado

MOVEit Automation se ejecuta en una infraestructura gestionada por el cliente, donde la seguridad depende de la correcta configuración del sistema operativo, la exposición de la red y la accesibilidad del puerto de comandos. Kiteworks se implementa como un dispositivo virtual reforzado con firewall de red, firewall de aplicaciones web y detección de intrusiones integrados, mantenido por Kiteworks, sin pila de seguridad que el cliente deba configurar. Cuando Log4Shell tuvo un CVSS de 10 en la National Vulnerability Database (NVD) del sector, los controles en capas de Kiteworks contuvieron la exposición; la evaluación interna de Kiteworks estimó la explotabilidad residual en aproximadamente CVSS 4, una estimación interna, no una puntuación emitida por la NVD.

3. El aislamiento de inquilino único reemplaza el riesgo de la infraestructura compartida

Cada implementación de Kiteworks es de inquilino único. Los clientes no comparten bases de datos, sistemas de archivos ni entornos de ejecución. Los patrones de ataque entre inquilinos no pueden cruzar límites que no existen. Combinada con cifrado validado FIPS 140-3 y registros de auditoría a prueba de manipulaciones, la arquitectura se alinea con los controles que los reguladores esperan ver documentados conforme a la Regla de Seguridad de HIPAA, CMMC Nivel 2, PCI DSS y el Artículo 32 del RGPD.

4. Consolide el patrimonio de intercambio de datos en un único registro de auditoría

MFT es un solo canal. Las empresas también intercambian datos sensibles a través del correo electrónico, formularios web, uso compartido de archivos, SFTP, API y asistentes de IA. Según el informe Kiteworks Data Security and Compliance Risk: 2025 MFT Survey Report, el 62 % de las organizaciones operan sistemas fragmentados entre MFT, correo electrónico, uso compartido de archivos y formularios web, y el 63 % no ha integrado MFT con su SIEM. Kiteworks unifica estos canales en una sola plataforma con un único motor de políticas y un único registro de auditoría consolidado.

5. Migre sin reconstruir los flujos de trabajo

La migración es una decisión de planificación real, no un traslado forzado. Kiteworks ofrece una ruta de migración estructurada desde MOVEit Transfer y MOVEit Automation que preserva los flujos de trabajo empresariales subyacentes: programaciones de transferencia de archivos, puntos de conexión de socios, requisitos de cifrado y continuidad del registro de auditoría. El estado final de la arquitectura es aquel en el que la próxima CVE de tipo MFT es un evento de parche rutinario, los registros de auditoría con calidad probatoria satisfacen varios regímenes regulatorios de forma simultánea, y la superficie de intercambio de datos se rige por controles que los reguladores pueden reconocer.