Kiteworks

TOP 5

Top 5 Gründe für den Umstieg von MOVEit auf Kiteworks

Organisationen, die MOVEit Automation einsetzen, bewältigen Notfall-Patch-Zyklen in immer kürzeren Abständen. Die Veröffentlichung von CVE-2026-4670 (NVD CVSS 9,8, Authentifizierungsumgehung) und CVE-2026-5174 am 30. April 2026 ist die dritte kritische Schwachstellenwelle, die MOVEit in drei Jahrentrifft – nach der massenhaften Cl0p-Ausnutzung von 2023, die mehr als 2.700 Organisationen kompromittierte und rund 95,8 Millionen Personen offenlegte (Emsisoft, Juni 2024), und dem Authentifizierungsumgehungs-Paar von 2024. Es ist zugleich die vierte kritische MFT-Schwachstelle herstellerübergreifend innerhalb von 18 Monaten, nach Cleo, CrushFTP und Wing FTP. Kiteworks konsolidiert Managed File Transfer, sichere E-Mail, Dateifreigabe, SFTP, Datenformulare und KI-Datenkanäle auf einem einzigen gehärteten, mandantenreinen virtuellen Appliance mit einer Richtlinien-Engine und einem konsolidierten Audit-Protokoll – entwickelt für das regulatorische Umfeld, das heute jede Datenübertragungsfläche umgibt.

1. Beenden Sie den Notfall-Patch-Zyklus

Jede MOVEit-Veröffentlichung war ein Upgrade mit Vollinstaller ohne Behelfslösung, wobei die Ausnutzung innerhalb von Stunden beobachtet wurde. Organisationen haben in drei Jahren mindestens vier Notfall-Änderungsfenster bewältigt. Kiteworks beendet diesen Zyklus mit einem von Kiteworks gewarteten gehärteten virtuellen Appliance, Komplett-System-Updates per Mausklick und kontinuierlichen Penetrationstests statt einer reaktiven Reaktion auf Veröffentlichungen.

2. Von kundenverwalteter Infrastruktur zu einem gehärteten virtuellen Appliance

MOVEit Automation läuft auf kundenverwalteter Infrastruktur, bei der die Sicherheit von korrekter Betriebssystemkonfiguration, Netzwerkexposition und Erreichbarkeit des Befehlsports abhängt. Kiteworks wird als gehärtetes virtuelles Appliance mit eingebetteter Netzwerk-Firewall, Web Application Firewall und Intrusion Detection bereitgestellt – von Kiteworks gewartet, ohne kundenseitig zu konfigurierenden Sicherheits-Stack. Als Log4Shell in der National Vulnerability Database (NVD) der Branche einen CVSS von 10 trug, begrenzten die mehrschichtigen Kontrollen von Kiteworks die Exposition; die interne Bewertung von Kiteworks schätzte die verbleibende Ausnutzbarkeit auf etwa CVSS 4 – eine interne Schätzung, kein von der NVD ausgestellter Wert.

3. Mandantenreine Isolation ersetzt das Risiko gemeinsam genutzter Infrastruktur

Jede Kiteworks-Bereitstellung ist mandantenrein. Kunden teilen sich keine Datenbanken, Dateisysteme oder Laufzeitumgebungen. Mandantenübergreifende Angriffsmuster können Grenzen, die nicht existieren, nicht überwinden. In Kombination mit FIPS-140-3-validierter Verschlüsselung und manipulationssicherer Audit-Protokollierung entspricht die Architektur den Kontrollen, die Aufsichtsbehörden dokumentiert sehen wollen – gemäß HIPAA Security Rule, CMMC Level 2, PCI DSS und DSGVO Artikel 32.

4. Konsolidieren Sie den Datenökosystem auf ein einziges Audit-Protokoll

MFT ist nur ein Kanal. Unternehmen tauschen sensible Daten auch über E-Mail, Webformulare, Dateifreigabe, SFTP, APIs und KI-Assistenten aus. Laut dem Bericht Kiteworks Data Security and Compliance Risk: 2025 MFT Survey Report betreiben 62 % der Organisationen fragmentierte Systeme über MFT, E-Mail, Dateifreigabe und Webformulare hinweg, und 63 % haben MFT nicht in ihr SIEM integriert. Kiteworks vereint diese Kanäle auf einer Plattform mit einer Richtlinien-Engine und einem konsolidierten Audit-Protokoll.

5. Migrieren Sie, ohne die Workflows neu aufzubauen

Migration ist eine echte Planungsentscheidung, kein Komplettaustausch. Kiteworks bietet einen strukturierten Migrationspfad von MOVEit Transfer und MOVEit Automation, der die zugrunde liegenden Geschäftsabläufe bewahrt – Dateiübertragungspläne, Partner-Endpunkte, Verschlüsselungsanforderungen und Audit-Kontinuität. Der architektonische Endzustand ist einer, in dem die nächste MFT-Schwachstelle ein routinemäßiges Patch-Ereignis ist, beweisfähige Audit-Protokolle mehrere regulatorische Regime gleichzeitig erfüllen und die Datenübertragungsfläche durch Kontrollen geregelt wird, die Aufsichtsbehörden anerkennen können.