Kiteworks

TOP 5

Top 5 redenen om te migreren van MOVEit naar Kiteworks

Organisaties die MOVEit Automation gebruiken, verwerken noodpatchcycli in een steeds hoger tempo. De bekendmaking van 30 april 2026 van CVE-2026-4670 (NVD CVSS 9,8, omzeiling van authenticatie) en CVE-2026-5174 is de derde golf van kritieke kwetsbaarheden die MOVEit in drie jaar treft – na de massale Cl0p-exploitatie van 2023 die meer dan 2.700 organisaties trof en ongeveer 95,8 miljoen personen blootstelde (Emsisoft, juni 2024), en het authenticatie-omzeilingspaar van 2024. Het is ook de vierde kritieke MFT-kwetsbaarheid bij verschillende leveranciers in 18 maanden, na Cleo, CrushFTP en Wing FTP. Kiteworks consolideert managed file transfer, beveiligde e-mail, bestandsdeling, SFTP, dataformulieren en AI-datakanalen op één gehard, single-tenant virtueel appliance met één beleidsengine en één geconsolideerd auditlogboek – gebouwd voor de regelgevende omgeving die nu elke gegevensuitwisseling omringt..

1. Beëindig de noodpatchcyclus

Elke MOVEit-bekendmaking was een upgrade met volledig installatieprogramma zonder tijdelijke oplossing, waarbij exploitatie binnen enkele uren werd waargenomen. Organisaties hebben in drie jaar minstens vier noodwijzigingsvensters verwerkt. Kiteworks beëindigt de cyclus met een door Kiteworks onderhouden gehard virtueel appliance, volledige systeemupdates met één klik en doorlopende penetratietests in plaats van een reactieve respons op bekendmakingen.

2. Ga van door de klant beheerde infrastructuur naar een gehard virtueel appliance

MOVEit Automation draait op door de klant beheerde infrastructuur, waarbij de beveiliging afhangt van de juiste OS-configuratie, netwerkblootstelling en bereikbaarheid van de commandopoort. Kiteworks wordt ingezet als gehard virtueel appliance met ingebouwde netwerkfirewall, web application firewall en inbraakdetectie – onderhouden door Kiteworks, zonder beveiligingsstack die de klant moet configureren. Toen Log4Shell een CVSS van 10 had in de National Vulnerability Database (NVD) van de sector, beperkten de gelaagde controles van Kiteworks de blootstelling; de interne beoordeling van Kiteworks schatte de resterende exploiteerbaarheid op ongeveer CVSS 4 – een interne schatting, geen door de NVD uitgegeven score.

3. Single-tenant-isolatie vervangt het risico van gedeelde infrastructuur

Elke Kiteworks-implementatie is single-tenant. Klanten delen geen databases, bestandssystemen of runtime-omgevingen. Cross-tenant-aanvalspatronen kunnen grenzen die niet bestaan niet overschrijden. In combinatie met FIPS 140-3-gevalideerde versleuteling en manipulatiebestendige auditregistratie sluit de architectuur aan op de controles die toezichthouders gedocumenteerd willen zien onder de HIPAA Security Rule, CMMC Level 2, PCI DSS en AVG Artikel 32.

4. Consolideer het gegevensuitwisselingslandschap op één auditlogboek

MFT is één kanaal. Ondernemingen wisselen gevoelige gegevens ook uit via e-mail, webformulieren, bestandsdeling, SFTP, API's en AI-assistenten. Volgens het rapport Kiteworks Data Security and Compliance Risk: 2025 MFT Survey Report gebruikt 62 % van de organisaties gefragmenteerde systemen voor MFT, e-mail, bestandsdeling en webformulieren, en heeft 63 % MFT niet geïntegreerd met hun SIEM. Kiteworks verenigt deze kanalen op één platform met één beleidsengine en één geconsolideerd auditlogboek.

5. Migreer zonder de workflows opnieuw op te bouwen

Migratie is een echte planningsbeslissing, geen complete vervanging. Kiteworks biedt een gestructureerd migratiepad vanaf MOVEit Transfer en MOVEit Automation dat de onderliggende bedrijfsworkflows behoudt – schema's voor bestandsoverdracht, partnereindpunten, versleutelingsvereisten en auditcontinuïteit. De architecturale eindtoestand is er een waarin de volgende MFT-kwetsbaarheid een routinematige patchgebeurtenis is, auditlogboeken van bewijskwaliteit meerdere regelgevende regimes tegelijk vervullen, en de gegevensuitwisseling wordt beheerst door controles die toezichthouders kunnen herkennen.