Kiteworks

SOLUTION BRIEF

# Kiteworks Sichere Managed File Transfer (MFT):

## Wenn Sie absolut, definitiv, die modernste und sicherste MFT-Lösung benötigen

### Kiteworks MFT: Die einzige moderne und sichere Managed File Transfer-Lösung

Die erste Generation von MFT-Anbietern entwickelte ihre Architekturen in den 1990er und 2000er Jahren. Doch heute leben wir in einer Welt, in der Advanced Persistent Threat (APT) Angriffe zum Geschäftsmodell geworden sind, und es reicht nicht mehr aus, nur die Übertragungen zu verschlüsseln und Zugangskontrollen auf Verzeichnisse zu setzen. Aus diesem Grund hat Kiteworks MFT mit einer modernen, gehärteten Virtual Appliance-Architektur, die um einen Next-Generation-Flow-Engine herum entwickelt wurde, neu erfunden. Wir haben Enterprise Scale-Out und Hochverfügbarkeit für weltweite Cluster in der Cloud, On-Premises oder Hybrid hinzugefügt. Wir haben Skalierbarkeit und Effizienz weiter ermöglicht mit zugangskontrolliertem Multi-User-Authoring und Operations-Management, einschließlich einem grafischen Flow-Designer, intuitiven Fehlersuche-Traces und Timing-Diagrammen zur Maximierung des Durchsatzes. Und natürlich, Sicherheit, Sicherheit und noch mehr Sicherheit.

### Gehärtete Virtual Appliance hindert APT Angreifer mit Schichten des Schutzes

Kiteworks MFT wird in einer gehärteten virtuellen Appliance eingesetzt, die durch unübertroffene Sicherheitsschichten Ihren Inhalt und Ihre Metadaten schützt. Diese gehärtete virtuelle Appliance, die darauf ausgelegt ist, Ausnutzungsmöglichkeiten zu minimieren, hat sich gegenüber großen Schwachstellen wie Log4Shell aus dem Jahr 2022 als widerstandsfähig erwiesen. Der Härtungsprozess beginnt bereits bei der Produktentwicklung und nutzt Sicherheitsbestpraktiken wie OWASP, defensive und offensive Strategien, Penetrationstests durch Dritte und Bounty-Programme für umfassende Sicherheit durch Design. Die im System eingebettete Firewall und WAF schützen den Perimeter, während die angenommene Sicherheitsarchitektur gegen erweiterte Bedrohungen absichert. Schlüsselverwaltungsoptionen, doppelte Verschlüsselung für ruhende Daten und verschiedene Intrusion-Detection-Systeme (IDS) stärken Ihre Abwehr weiter. Vertrauen Sie auf Kiteworks, Ihren ultimativen Schutz gegen Cyber-Bedrohungen.

### Rasche Identifizierung von Bedrohungen und Nachweis der Compliance mit einem vereinheitlichten Audit-Log

Unsere Managed File Transfer-Lösung nutzt die Kraft eines zentralisierten, umfassenden Audit-Logs, um eine konsolidierte Übersicht über alle Aktivitäten auf allen Kiteworks-Kommunikationskanälen und Systemdiensten zu bieten. Sie ist darauf ausgelegt, Bedrohungen schnell zu identifizieren, was eine umgehende Abhilfemaßnahme und gründliche Forensik ermöglicht. Füttern Sie fortlaufend standardisierte, vorgereinigte Logs in Ihr SIEM, um Ihrem SecOps-Team unübertroffene Sichtbarkeit und Kontrolle zu bieten, was eine sofortige Abhilfemaßnahme und beschleunigte Forensik ermöglicht. Und wenn es Zeit für eine weitere Compliance-Prüfung ist, können Sie sich auf integrierte Berichte und Exporte verlassen, um die Vorbereitungen zu beschleunigen und eine starke Compliance-Haltung zu gewährleisten. Mit Kiteworks verfolgen Sie nicht nur Downloads, Bearbeitungen, Konfigurationsänderungen und Berechtigungszuweisungen - Sie schützen proaktiv Ihre sensiblen Inhalte und stellen die regulatorische Compliance sicher.

## Durchsetzung granularer Richtlinien zentral zur Optimierung von Sicherheit und Compliance

Die Lösung ermöglicht leistungsstarke Produktivitäts- und Compliance-Vorteile durch die zentrale Durchsetzung von Richtlinien. Kiteworks-Administratoren definieren und setzen Richtlinien im gesamten System durch, um eine konsistente Anwendung von Sicherheitsmaßnahmen und Compliance-Regeln zu gewährleisten und Audits zu vereinfachen. Dieser zentrale Ansatz eliminiert das Risiko von Richtlinienlücken und Inkonsistenzen, die durch ein Flickwerk von separaten Kontrollen für jeden Kommunikationskanal entstehen können. Mit Kiteworks setzen Sie nicht nur Richtlinien durch - Sie schaffen eine robuste, sichere und konforme digitale Umgebung.

## Vertrauen Sie der einzigen MFT-Plattform, die robust genug für FedRAMP und IRAP ist Glauben Sie nicht einfach unserem Wort

Fragen Sie die akkreditierte Drittprüfungsorganisation (3PAO), die die Sicherheit von Kiteworks getestet und sie gegen 325 Sicherheitskontrollen für NIST 800-53 geprüft hat. Die daraus resultierende FedRAMP-Autorisierung der US-Bundesregierung ermöglicht den Einsatz von Kiteworks-gehosteten Systemen durch Bundesbehörden. Und machen Sie sich keine Sorgen, dass unsere Sicherheitslage seit der ersten Autorisierung nachgelassen hat: Kiteworks muss den Test- und Prüfprozess jährlich wiederholen, um die Autorisierung aufrechtzuerhalten. Ebenso hat ein IRAP-registrierter Prüfer eine Beurteilung des in der Cloud gehosteten Kiteworks gegen 816 PROTECTED Level-Sicherheitskontrollen durchgeführt, um australischen Regierungsbehörden die Nutzung zu ermöglichen. Kein anderer MFT-Anbieter kann Ihnen die Beruhigung bieten, die mit diesen rigorosen, fortlaufenden Drittpartei-Sicherheitsbewertungen einhergeht.