Die Top 7 Gründe, warum Sie Kiteworks gegenüber ShareFile den Vorzug geben sollten

Content-Risiko-Management und Compliance auf höchstem Niveau

Unabhängig davon, ob Sie Ihre sensiblen Daten in der Cloud oder in Ihren eigenen Räumlichkeiten speichern, Kiteworks kombiniert die höchste Produktivität mit dem stärksten Schutz vor den Risiken von Datenschutzverletzungen und der Nichteinhaltung von Vorschriften, selbst bei der Zusammenarbeit mit externen Parteien.

1. Kein Zugriff auf Metadaten oder Inhalte durch den Anbieter, zu keinem Zeitpunkt

Die gehosteten und On-Premises-Systeme von Kiteworks sind so geschützt, dass weder die Mitarbeiter von Kiteworks - noch externe Angreifer - Zugriff auf Ihre Inhalte oder Metadaten haben. Mit ShareFile hat der Anbieter Zugriff auf Ihre Metadaten, die Ihre Dateien, Richtlinien und Anwender beschreiben - selbst wenn Sie On-Premises StorageZones verwenden - und er kann auf Ihre Inhalte zugreifen, wenn diese in seiner Cloud gehostet werden.

2. Eingebaute Schutzmechanismen zum Schutz vor Insidern und Angreifern

Kiteworks bietet eine unübertroffene Härtung der virtuellen Appliance mit integrierter Netzwerk-Firewall, WAF und Intrusion Detection. Ein laufendes Bounty-Programm und regelmäßige Pen-Tests sowie Appliance-Updates mit einem Klick minimieren Schwachstellen. Die On-Premises StorageZone Controller von ShareFile bieten jedoch keine Härtung zum Schutz des Systems vor internen oder externen Angreifern, so dass Administratoren Zugriff auf Dateien, Betriebssystem und Anwendungscode haben. Updates müssen für jede Komponente manuell durchgeführt werden, was die Wartungskosten erhöht und das Risiko erhöht, dass Sicherheitspatches fehlen.

3. Umfassendes Audit-Protokoll für SecOps- und Compliance-Teams

Kiteworks fasst alle Komponentenprotokolle in einem einzigen, kontinuierlichen Datenstrom zusammen, der an Ihr Security Information and Event Management (SIEM) System weitergeleitet wird, um Bedrohungen zu erkennen und zu entschärfen sowie bereichsspezifische und benutzerdefinierte Berichte zu erstellen. Das detaillierte Audit-Protokoll hilft Ihnen, Compliance-Audits mit minimalem Aufwand zu bestehen. Im Gegensatz dazu bietet ShareFile nur eine Reihe separater thematischer Berichte, die von Administratoren geplant, ausgeführt und exportiert werden müssen. Es gibt keinen Live-Feed zu Splunk, Datadog, ArcSight oder anderen SIEM-Systemen.

4. CMMC- und Behörden-konforme U.S. Federal Compliance

Die Verschlüsselung von Kiteworks hat den strengen NIST FIPS 140-2 Validierungs-Zertifizierungsprozess bestanden, und das Cloud-gehostete Produkt und die Prozesse werden jährlichen FedRAMP-Audits und einer kontinuierlichen Überwachung durch einen zertifizierten externen Prüfer (3PAO) unterzogen. ShareFile hat keine FedRAMP-Zertifizierung und keine NIST-Validierung für FIPS 140-2.

5. Risikobewältigung bei der Zusammenarbeit durch eigentumslose Bearbeitung

Kiteworks SafeEDIT, ein Digital Rights Management (DRM) der nächsten Generation, ermöglicht die Bearbeitung aller Arten von gemeinsam genutzten Dateien durch interne und externe Parteien in einer virtuellen Browser-Benutzeroberfläche, während die Datei selbst auf dem Kiteworks Server-Cluster geschützt bleibt. Es werden keine Agenten oder Plugins benötigt. Mit ShareFile müssen Sie externen Parteien Zugriff auf Ihre sensiblen Inhalte gewähren, um diese zu bearbeiten, sei es über die Microsoft 365 Cloud oder per Download.

6. Absoluter Datenschutz mit Single Tenant Cloud Hosting

Reduzieren Sie das Risiko eines unbeabsichtigten oder unbefugten Zugriffs auf Inhalte mit einer unabhängigen privaten Kiteworks-Cloud für jeden Kunden, ohne Vermischung von Daten, Metadaten oder gemeinsam genutzten Anwendungsressourcen. Im Gegensatz dazu vermischt die Multi-Tenant Cloud von ShareFile Ihre Daten und Metadaten mit denen anderer Kunden, was im Falle von Software-Bugs oder Konfigurationsfehlern zu einem Sicherheitsrisiko zwischen den Mandanten führen kann.

7. Sicherer Austausch großer Dateien für gesetzeskonforme Produktivität

Zuverlässiges und sicheres Verschlüsseln, Senden, Freigeben, Empfangen, Scannen, Anzeigen und Speichern großer Bilddateien, CAD-Dateien und anderer Dateitypen bis zu 16 Terabyte. Bei Netzwerkausfällen wird die Übertragung an der Stelle fortgesetzt, an der sie unterbrochen wurde. Die Größenbeschränkung von ShareFile auf 100 GB führt dazu, dass Nutzer auf andere, unsichere Kommunikationsformen ausweichen, wenn ihre Geschäftsprozesse größere Dateien erfordern.