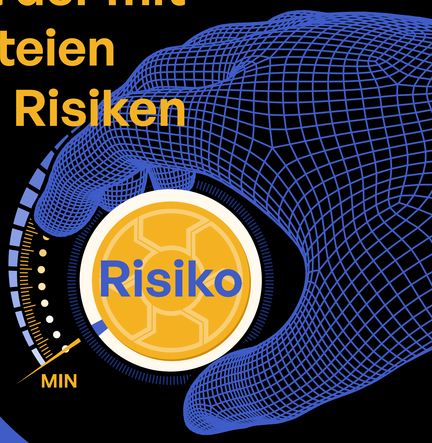
Kiteworks

www.kiteworks.com

# Insights zum Management der mit externen Parteien verbundenen Risiken

**Highlights aus dem 2024 Sensitive Content Communications Privacy and Compliance Report**




## PRÄMISSE

## Sensible Inhalte von externen Parteien und die damit verbundenen Risiken stellen viele Unternehmen vor große Herausforderungen

**66 %**

der Unternehmen **tauschen sensible Inhalte** mit 1.000+ externen Parteien aus

**77 %** In der APAC-Region ist das mit externen Parteien verbundene Risikopotenzial am größten: 77 % tauschen sensible Inhalte mit mehr als 1.000 externen Parteien aus

**51 %** Dienstleistungsunternehmen tauschen vertrauliche Inhalte mit mehr externen Parteien aus als jeder andere Wirtschaftszweig (51 % tauschen Inhalte mit mehr als 2.500 externen Parteien aus oder versenden diese)

**47 %** Das Hochschulwesen weist das zweithöchste Risiko für die Branche auf: 47 % der Befragten teilen und versenden sensible Inhalte an 2.500 externe Parteien

In der EMEA-Region ist die Herausforderung am größten: **45 %** gaben an, dass sie **<50 %** der sensiblen Inhalte nicht kontrollieren und nachverfolgen können, sobald diese ihre Domain verlassen

**69 %** der Hochschuleinrichtungen sind nicht in der Lage, **<50 %** der sensiblen Inhalte zu kontrollieren und nachzuverfolgen, sobald diese ihren Bereich verlassen

Kommunalverwaltungen haben das zweithöchste Risiko: **54 %** der Befragten gaben zu, dass sie den Überblick und die Kontrolle über sensible Daten verlieren, wenn diese die Organisation verlassen

**39 %**

**der Unternehmen gaben an, dass sie nicht in der Lage sind, den Zugriff auf <50 % der sensiblen Inhalte zu verfolgen und zu kontrollieren**

## Wie Kiteworks das Management der mit externen Parteien verbundenen Risiken gewährleistet

Das Kiteworks Private Content Network (PCN) konsolidiert und sichert alle externen Kommunikationskanäle, einschließlich E-Mail, SFTP, Filesharing & Collaboration, Managed File Transfer und Web-Formulare

Echtzeitüberwachung zur Analyse sensibler Inhalte, die in ein Unternehmen eingehen oder es verlassen

Ermöglicht , granulare, skalierbare, auf Attributen basierende Inhaltskontrollen zu definieren und dabei unternehmensgerechte Verschlüsselung sowohl während der Übertragung als auch im ruhenden Zustand zu verwenden

Integrierbar in die bestehende erweiterte Sicherheitsinfrastruktur, einschließlich Data Loss Prevention (DLP), ATP, SIEM, CDR und andere

Nutzt Single-Tenant-Hosting, einschließlich FedRAMP-Installations-optionen, um gesetzliche Anforderungen zu erfüllen und die vollständige Kontrolle über die Server-umgebung zu behalten

**Alle Ergebnisse des 2024 Sensitive Content Communications Privacy and Compliance Report sind ab sofort zum Download verfügbar.**