

2024

Forecast for Managing Private Content Exposure Risk



Understanding Private Content Exposure Risk

Managing your data privacy and compliance risks becomes increasingly more difficult by the year due to increased cybercrime, evolution and growth in compliance regulations and standards, and increased complexity in technology.

Based on Kiteworks 2024 Sensitive Content Communications Forecast Report

12 File and Email Data Communication Privacy and Compliance Predictions for 2024



1. Data Privacy and Compliance Risk of AI LLMs

Nearly two-thirds of companies are either experimenting (29%) or expanding (33%) their use of GenAI today.

However, only 20% of organizations have processes to mitigate PII risks in GenAI.



2. Data Privacy and AI LLM Regulations and Standards

The White House Executive Order aims to monitor and regulate AI risks while harnessing its potential.

The EU AI Act takes effect in stages through 2026, defining AI risk levels.



3. Need for a Modern MFT Approach

12% of data breaches last year involved the software supply chain.

A couple of the most notable cyber breaches in 2023 were the result of MFT supply chain attacks.



4. Need for a Modern Email Protection Gateway

Email phishing attacks surged 47% in the past year.

Traditional email encryption methods have gaps and users instigate risky workarounds.



5. Growth in Data Privacy Regulations and Standards

Data privacy regulations will cover 75% of the global population by the end of 2024.



6. Rising Importance of Data Sovereignty

70% of countries regulate how companies collect, store, and use citizen data.



7. Increased Fines for Data Privacy Violations

More GDPR fines in first half of 2023 than 2019–2021 combined, reaching over \$1.8 billion.



8. Adoption of FedRAMP Authorized Sensitive Content Communication Solutions

The 2023 NDA codifies FedRAMP requirements, boosting cloud adoption.



9. Emergence of Digital Rights Management to Protect Sensitive Content

DRM market potentially reaching over \$5 billion by 2024.



10. Integration of Advanced Security Into Sensitive Content Communications

Adoption of DLP, CDR, and ATP are predicted to grow rapidly.



11. Centralizing Sensitive Content Communications and the PCN

Nearly 75% of organizations say measurement of sensitive content communications needs improvement.



12. Growth in Communications of Very Large Files Containing Sensitive Content

Many orgs have sensitive content communication tools with size limits under 250 GB, creating challenges for large sensitive files.



Prepare for 2024 by scheduling a **custom-tailored demo** of Kiteworks **today.**