Kiteworks

2024 Forecast for Managing Private Content Exposure Risk

12 Predictions for Sensitive Content Communications Based on Cybercrime, Cybersecurity, and Compliance Trends

REPORT

Introduction: Understanding Private Content Exposure Risk

Managing your data privacy and compliance risks becomes increasingly more difficult by the year. Cybercriminals continue to evolve their strategies and approaches, making it more difficult to identify, stop, and mitigate the damages of malicious attacks.[1] Recognizing they can breach hundreds, or even thousands, of companies and millions of records with one successful attack, many rogue nation-states and cybercriminals have turned to the supply chain, a trend we believe will increase in 2024. Third-party vendors, including technology providers, represented 15% of all successful data breaches last year.[2] And as generative artificial intelligence (GenAI) large language models (LLMs) take the digital landscape by storm, tracking and controlling our sensitive content became even harder.

In response, regulatory bodies are evolving their existing data privacy regulations and adding new ones. They also ratcheted up fines and penalties targeting regulatory violations. This "reactionary movement" will not slow down but continue to pick up pace in the coming year. All of this means organizations must track and control content access and generate more audit log reports to demonstrate compliance with relevant compliance requirements.

Kiteworks' Sensitive Content Communications Forecast 2024 Report examines key trends from the past year and maps those to what we expect to see in the coming year. Certainly, managing the privacy and compliance of your sensitive content communications—email, file sharing, managed file transfer (MFT), SFTP, and web forms—is a difficult undertaking with many of the tools you use residing in siloes. In addition, as many of those tools were developed a decade or more ago, they lack the advanced security capabilities needed to protect sensitive content from malicious cyberattacks. Some serious data breaches occurred this year as a result. Organizations are paying attention, and many are assessing their current file and email data communication tools and evaluating alternatives. Rather than keeping these tools in separate silos, growing numbers of organizations will look to centralize them in one platform in 2024 (imagine having only one audit log and consolidated policy management in one place).

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

1. Data Privacy and Compliance Risk of AI LLMs

Despite bans and restrictions, the number of employees and third parties using GenAI LLMs will likely double from 2023 levels as the competitive advantages become too significant to ignore. For example, 15% of employees regularly post company data into GenAI LLMs, and one-quarter of that data is considered sensitive.[3] This will expand the threat surface and potential for IP, PII, PHI, financial documents, merger and acquisition (M&A) communications, and other sensitive content, including AI prompts, to be inadvertently or intentionally exposed, ratcheting up risks of sensitive data leakage and the corresponding implications around brand damage, regulatory fines and penalties, and legal costs.

Even with advances in security controls, data breaches stemming from GenAI LLM misuse will rise in 2024. High-profile examples threatening customer trust and drawing regulatory scrutiny are likely. This will force data security to be a central part of GenAI LLM strategies. Organizations slow to adapt will face brand reputation damage, lost revenue opportunities, potential regulatory fines and penalties, and ongoing litigation costs.

To mitigate risks, leading organizations will implement content-defined zero-trust models to control access and collaboration based on data sensitivity, adding granular access controls and least-privilege access, by default, and eliminating non-authenticated access. This move to zero trust at the content layer also includes integration of real-time data loss prevention (DLP) policies and logging and monitoring of all content access and movement.

Mature data loss prevention capabilities leveraging deep content inspection and adaptive risk scoring will expand from devices and emails to real-time monitoring of GenAI LLM interactions. Usage of digital rights management (DRM) for particularly high-risk content will increase dramatically, enabling collaboration while preventing data extraction. Investments in data security awareness training will also increase to help educate employees on responsible GenAI LLM use. Those acting now to secure unstructured data and to institute strict governance and security tracking and controls will reduce their security and compliance risks.

Nearly two-thirds of companies are either experimenting (29%) or expanding (33%) with GenAI today.[4]

Only 20% of organizations have instituted processes to mitigate PII being used in generative AI LLMs.[5]

2. Data Privacy and AI LLM Regulations and Standards

As noted, the emergence of GenAI LLMs creates significant data privacy and compliance risks for organizations, and regulatory agencies are rushing to put AI regulations and standards in place.

At the forefront of these regulatory activities is the White House Executive Order (EO) from October 30 that aims to monitor and regulate the risks of AI while also harnessing its potential. The EO calls on Congress to act as well and specifically asks federal agencies to act over the next year. The EO establishes new standards for AI safety and security, protects the data privacy of U.S. citizens, and promotes a fair, open, and competitive ecosystem and marketplace for AI and related technologies.[6] The executive order relies on guidance from the National Institute of Standards and Technology (NIST) and imposes requirements for the U.S. federal government's use, evaluation, and procurement of AI software and systems.[7] In addition to a focus on AI disruption to the labor market, the EO will require developers of powerful AI systems to share results of their safety tests with the federal government before they are released to the public. The EO is the first step in the federal government's plan to address AI, and we likely will begin to see legislation at the federal and state levels in 2024. Currently, at least 25 U.S. states are considering AI-related legislation, and 15 passed laws or resolutions.[8]

Outside of the U.S., the EU is working on an AI Act, which will take effect in stages by 2026.[9] The act aims to provide AI developers, deployers, and users with clear requirements and obligations regarding specific uses of AI while reducing administrative and financial burdens for businesses, particularly small and medium-sized enterprises (SMEs). The act defines four levels of risk in AI: unacceptable risk, high risk, limited risk, and minimal or no risk. High-risk AI systems will be subject to strict obligations before they can be put on the market.

One area where AI standards are emerging is the National Institute of Standards and Technology (NIST). Specifically, the NIST AI RMF Playbook emphasizes establishing policies to address risks from third-party systems, testing security and resilience through red team exercises, implementing data governance and privacy controls, enabling transparency and recourse mechanisms, documenting system traceability, empowering oversight functions, and integrating risk management into policies and procedures.[10] In 2024, organizations using the NIST AI RMF will continue to focus on managing sensitive content risks through robust technical controls combined with responsible AI practices like explainability, accountability, and transparent risk communication.

As security requirements and standards emerge, organizations will need to be able to demonstrate compliance with regulatory standards easily and quickly, and having governance tracking, such as detailed audit logs, will be important. Experts believe the latter half of 2024 will be the earliest when AI standards would be implemented and mandated; the governance structures to do so will take time to create and make operational.

Forrester predicts there will be at least three data breaches connected to insecure AI-generated code, and at least one company will be fined for its handling of PII.[11]

3. Need for a Modern MFT Approach

Many managed file transfer (MFT) solutions are based on decades-old technology that have inherent security deficiencies. On-premises deployments that are preferred by many customers are comprised of disparate capabilities that reside in silos and lack vendor-provided hardening; customers must define and implement a hardening strategy such as network and web application firewalls, intrusion detection, removal of unused services and code, and antivirus technologies. The siloed approach also puts the onus of vulnerability management on the customer, detecting the need to update code, finding compatible versions of all the siloed components, integration-testing updated components, and then migrating to production. In addition, legacy MFT solutions often lack advanced security technology such as data loss prevention (DLP), advanced threat prevention (ATP), and content disarm and reconstruction (CDR).

Organizations in 2024 will seek a modern virtual appliance approach that enables a one-click application of a unified update provided by the MFT provider. They will also look for MFT solutions that integrate advanced security capabilities to address unprecedented cyber-threat complexity and volume.

MFT tools are used for the digital transfer of data in an automated, reliable, and secure manner internally and with third parties using governance tracking and controls for regulatory compliance. As part of the software supply chain, the risk of legacy MFT solutions is dramatic. For the past several years, we've witnessed a spiraling escalation of cyberattacks on the software supply chain by rogue nation-states and cybercriminals. Earlier this year, IBM revealed in its Cost of a Data Breach Report that 12% of data breaches involve the software supply chain. At the same time, third parties, which comprise the software supply chain, are an important risk element with 15% of data breaches tied back to third parties.[12]

Two major MFT tools experienced zero-day exploits in 2023 that were targeted by Clop, a Russian cyber gang with a history of targeting MFT tools. In both instances, multiple zero-day vulnerabilities were targeted—a remote code execution (RCE) in the case of Fortra GoAnywhere that impacted over 130 organizations[13] and a SQL injection in the case of MOVEit that affected over 2,000 organizations and 62 million individuals.[14]

If the two MFT attacks in 2023 are any indication, rogue nation-states and cybercriminals will continue to exploit zero-day vulnerabilities in legacy MFT solutions in 2024. When an MFT tool is breached, the supply chain impact can expose sensitive data for hundreds or even thousands of organizations representing millions of individuals. The regulatory impact can be dramatic in terms of fines and penalties, legal costs, class-action lawsuits, and brand damage, among other issues.

12% of data breaches last year involved the software supply chain.[15]

4. Need for a Modern Email Protection Gateway

Email remains the number one attack vector due to malware and phishing. Malware attacks instigated through email shot up 29% in the past year, while phishing attacks also grew 29% and business email compromise (BEC) spiked 66%.[16] The Verizon Data Breach Investigations Report found that BEC attacks doubled over the previous year and the median amount stolen per attack hit $50,000.[17] For phishing and BEC attacks, lack of robust filters and visibility into the context of emails makes it difficult to detect and block sophisticated attacks that use social engineering tactics. More than 8 in 10 of data breaches target humans as their first line of access using social engineering strategies.[18] Further, traditional email security approaches are ineffective against zero-day attacks and rely on user awareness to detect and report suspicious emails; the problem is users can be fooled easily by sophisticated attacks.

Like legacy MFT solutions, legacy email systems lack modern security capabilities. The good news is that we have seen a significant improvement in email encryption. A survey of IT executives found that 90% prioritize the protection of documents and information they communicate in email with other organizations.[19] When these are shared internally, the numbers are not as good: 79% of businesses indicate they share sensitive business data over email without encryption.[20] Further, while organizations employ encryption on their emails, a recent study revealed that only 35% of businesses said they have extensive encryption deployed.[21]

There are several reasons why organizations continue to struggle with email encryption. One reason is that it can be complex and difficult to use.[22] There are different types and levels of encryption (e.g., PGP, S/MIME, DANE, STARTTLS), and the exchange of public keys can be a hassle and often creates risk. For example, when encrypted email cannot be decrypted, organizations must revert to less-than-ideal (and less-than-secure) options, such as signing up for a free but unauthorized email service to transmit the content, asking the sender to use an unencrypted but unpublished shared drive link, or asking the sender to send a password-encrypted Zip file.

Other email security deficiencies certainly exist, such as lack of digital rights management (DRM), data loss prevention (DLP), and advanced threat detection, insecure cloud storage that lacks encryption and access controls, poor identity and access management, and outdated or misconfigured on-premises mail servers.

Based on the above evidence, email security will continue to be a challenge for many organizations in 2024. Until organizations embrace an email protection gateway where email is sent, received, and stored using zero-trust policy management with single-tenant hosting, email security will remain a serious risk factor—both in terms of data privacy as well as regulatory compliance.

Phishing attacks surged 47.2% in the past year, with education and financial services the top industry targets.[23]

5. Growth in Data Privacy Regulations and Standards

2023 witnessed continued growth in data privacy regulations and standards. Gartner predicts that personal data for three-quarters of the world's population will be covered by data privacy regulations by the end of 2024, and the average annual budget for privacy in a company will exceed $2.5 million.[24] Expansion of privacy regulation efforts across dozens of jurisdictions will occur over the next two years. For example, in addition to California, four additional U.S. states enacted data privacy laws in 2023, and another 10 to date passed data privacy laws and their enactment will take place in 2024 and 2025. Numerous other states have data privacy laws at various states of legislative deliberation.

Data privacy is not simply a U.S. phenomenon. It's a global concern, and 2024 is certain to reflect further emphasis on data privacy regulations. For example, with GDPR, multiple EU legislations are in the pipeline, including the Digital Markets Act, Digital Services Act, and AI Regulation.

In July 2023, the EU approved the new Data Privacy Framework that facilitates data transfers from the EU, U.K., and Switzerland to the U.S., outlining the self-certification process for organizations to participate. To participate, a U.S. company must self-certify compliance to the Department of Commerce and commit to following the principles of the relevant framework(s). Compliance is compulsory once an organization self-certifies. The Department of Commerce maintains a public list of participating organizations. An organization must be on the list to claim participation and receive personal data under the frameworks. If an organization is removed from the list, it must cease claims of participation and compliance. However, it must continue applying the principles to data previously received. The frameworks facilitate transatlantic data flows that are critical for businesses while providing safeguards for personal data.

The NIST Privacy Framework was released in 2020 and has proven to be a valuable guide. Based on the draft updates to the NIST Cybersecurity Framework (CSF), the Privacy Framework will likely expand in 2024 to further address enterprise risk management across legal, financial, and privacy domains. This will better position organizations to evaluate and mitigate privacy risks holistically. The Privacy Framework's alignment with proposed federal privacy law indicates it will be an important compliance tool as regulations evolve. Updates we likely will see in 2024 include enhanced integration with the NIST Cybersecurity Framework to better address privacy as an enterprise risk alongside other domains like finance and legal, expanded guidance on managing privacy risks across entire organizations, not just IT systems,[25] and alignment with emerging data privacy regulations to support compliance.[26]

Anticipated changes to the NIST Cybersecurity Framework (CSF) are also worth noting. NIST released a draft update to the CSF in August 2023 and has plans to publish the final CSF 2.0 in early 2024.[27] The updated framework aims to appeal to a broader range of organizations while elevating risk management practices. Key changes include emphasizing continuous risk assessments, prioritizing continuous improvement, strengthening supply chain risk management, and providing more implementation examples. Demonstrating compliance with evolving and emerging data privacy regulations remains a challenge for many organizations. Look for more organizations to centralize governance and use of audit logs used for tracking and reporting in 2024. But with many organizations still reporting siloed sensitive content communication approaches, this can be a difficult undertaking.

6. Rising Importance of Data Sovereignty

Data localization is a growing trend that makes data sovereignty a challenge for organizations in 2024.[28] The United Nations Conference on Trade and Development reports that 70% of countries regulate how companies collect, store, and use data about their citizens.[29] Many emerging privacy laws require organizations to control the country where data resides, which can be a significant challenge for multinational organizations. At the same time, data democratization, the practice of making data accessible and consumable for everyone in an enterprise regardless of technical skill, is a trend that will impact data sovereignty. This trend will require organizations to ensure that data is accessible to all stakeholders while maintaining data sovereignty. Data sovereignty applies to all types of data, including personally identifiable information (PII), as well as other data related to the activities and operations of a business.

Organizations across all sectors of the economy, including government, technology, healthcare, and financial services, are increasingly prioritizing data sovereignty initiatives due to the myriad benefits that come with it. Data sovereignty empowers organizations to maintain compliance with local and international data regulations, which minimizes legal risks, establishes a reputation for responsible data handling, and helps companies avoid hefty fines. By prioritizing data sovereignty, organizations can build trust with customers and stakeholders, enhance brand reputation, and avoid costly legal issues.

Decisions on how to deploy applications are deeply influenced by data sovereignty requirements, particularly in countries with stringent laws, like Germany and China. The United States CLOUD Act, which mandates U.S. companies to provide data under warrant or subpoena regardless of where it is stored, complicates international operations, potentially breaching regulations such as the GDPR. Multitenant hosting options can complicate compliance with data sovereignty and make it more difficult for organizations to demonstrate compliance with data localization laws.

Customers demanding data sovereignty often prefer to engage with vendors that host services domestically. For cloud-based services, in-country hosting zones may suffice unless affected by legislation like the US CLOUD Act. In more complex scenarios, companies will increasingly opt for hosting on their own soil or utilize data sovereignty features within their applications to manage multi-country deployments, although this may pose challenges during compliance audits.[30]

When application clusters span multiple countries, data sovereignty zone functionality is a valuable capability. To offset the above in 2024, watch for companies to turn to single-tenant hosting, which simplifies data sovereignty and the ability of companies to demonstrate such.

Companies will increasingly opt for hosting on their own soil or utilize data sovereignty features within their applications to manage multi-country deployments, although this may pose challenges during compliance audits.

7. Increased Fines for Data Privacy Violations

Fines and penalties associated with data privacy violations increased the past two years, including record-setting fines for GDPR violations, and are projected to continue increasing in 2024. Some of note from 2023 include $1.3 billion issued against Meta (Facebook) by the Irish Data Protection Commission, $391.5 million against Google settling with 40 U.S. states, $61.7 million against Amazon by the FTC, and $2.1 million against Uber, also by the FTC.

Regulators are focused on enforcement of privacy laws and levying fines when violations occur. Lax governance and security make companies an easier target for regulators to make an example of with harsh penalties. For example, recent major fines, like those against Marriott and British Airways under GDPR, were in large part due to lapses in data security. This precedent indicates regulators will come down hard on companies that negligently expose personal data. As additional data privacy laws are passed, both by individual U.S. states and globally, remunerative repercussions will continue to grow.

Enforcement of data protection regulations will not let up in 2024 with most the world's population now covered by data privacy regulations. With the growing focus on data protection, more organizations will create dedicated data privacy practices. For organizations operating in multiple countries, this necessitates a new approach to the design and acquisition of cloud across service models to accommodate different localization strategies in 2024.

More GDPR fines were imposed in the first half of 2023 than in 2019, 2020, and 2021 combined—reaching over $1.8 billion.[31]

75% of the global population will have its personal data covered under privacy regulations by the end of 2024.[32]

8. Adoption of FedRAMP Authorized Sensitive Content Communication Solutions

The James M. Inhofe National Defense Authorization Act (NDAA) for fiscal year 2023, signed into law by President Joe Biden, codifies the FedRAMP program within the General Services Administration and implements important changes in the FedRAMP program that appear designed to further streamline the processes for adoption and use of cloud services by the government. The Office of Management and Budget (OMB) also released draft guidance for modernizing FedRAMP to address today's cloud challenges, which includes a plan to scale FedRAMP, strengthen its approach to security review, and accelerate the secure adoption of cloud products and services in the federal government.[33]

By 2024, FedRAMP Authorization, which is achieved through a rigorous annual audit process annually, will likely be a basic requirement for any cloud service provider wanting to work with the U.S. federal government. For defense industrial base (DIB) contractors, the Cybersecurity Maturity Model Certification (CMMC) 2.0 includes FedRAMP requirements, and having file and email data communications that are FedRAMP Authorized makes demonstrating compliance much easier for DIB contractors. As more DIB contractors push to obtain CMMC Level 2 certification in 2024, DIB contractors will look to use technology solutions, including those used for file and email data communications.

9. Emergence of Digital Rights Management to Protect Sensitive Content

Digital rights management (DRM) adoption will accelerate as organizations aim to protect sensitive content and comply with expanding regulations.[34] Market research predicts strong DRM growth, potentially reaching over $5 billion by 2024.[35] Gartner indicates integrating DRM with wider technology trends will be impactful and certainly will be a growing focus for organizations in 2024.[36] For content-defined policy management, organizations will turn to security standards like the NIST Cybersecurity Framework (CSF) and NIST 800-53.

Key drivers include rising cyber threats, data privacy laws, and demand for controlling internal and external content sharing. Next-generation DRM is crucial for data privacy, providing persistent protection of sensitive data when it leaves the perimeter of the organization. To succeed with DRM, organizations need unified tracking, control, and visibility across their digital ecosystems. This requires following best practices around governance, workflows, and access controls.

For 2024, data classification and DRM policy management will drive organizations to institute data protection using least-privilege access and watermarks for low-risk data, view-only DRM for moderate-risk data, to safe video-streamed editing that blocks downloads and copy and paste for high-risk data. Highly regulated industry sectors will be the biggest adopters of next-generation DRM. For example, healthcare, which is one of the most targeted industries when it comes to cyberattacks, must protect immense amounts of PII and PHI data that is shared, sent, received, and stored within their organizations and with countless third parties. Financial services institutions, manufacturers, law firms, government agencies, and educational institutions also fall into the list of industries with high-risk, high-consequence file and email data exchanges. In turn, they will begin to look to next-generation DRM to manage their data privacy and compliance risks.

Only 22% of organizations have policies and systems in place to track and control access to sensitive content and to whom it is sent and shared.[37]

10. Integration of Advanced Security Into Sensitive Content Communications

Advanced cybersecurity tools like cloud data loss prevention (DLP), advanced threat prevention (ATP) for next-generation antivirus and sandbox detonation, and content disarm and reconstruction (CDR) can integrate into solutions for sending, sharing, and storing sensitive content. In 2024, organizations will embrace advanced cybersecurity technologies to allow policies, scanning, and sanitization to apply to data in transit and at rest. With DLP, organizations can scan outgoing emails and attachments to prevent accidental leaks of sensitive data. CDR can sanitize incoming documents by removing active content for safety. MFT platforms often natively support DLP, antivirus, sandboxing, and advanced protections. Integrating these capabilities into the content transfer process improves security. It prevents data leakage and loss by blocking transfers that violate policies. Malware is blocked from entering the environment through antivirus scanning and sandbox detonation. Incoming content is sanitized for safety through CDR.

In 2024, organizations will seek greater visibility into content flows to enhanced monitoring and detailed audit logs. Enforcing security policies becomes simplified when consolidated into centralized platforms like MFT. Sensitive content communication tools like email, file sharing, MFT, and web forms all benefit from having ATP tightly integrated.

The content disarm and reconstruction (CDR) market is forecast to grow at a 15.7% CAGR through 2026 due to the cost of data breaches and stricter regulation and compliance for content security.[38]

The data loss prevention (DLP) market is expected to grow at a CAGR of 22.3% through 2030 due to a focus on data discovery, policy enforcement, data classification, and incident response.[39]

11. Centralizing Sensitive Content Communications and the PCN

Traditional zero-trust architectures focus on securing the network perimeter and verifying users and devices trying to connect. But content lives beyond the perimeter, and networks do not understand content sensitivity. This is where the paradigm of Private Content Networks (PCNs) comes into play, emphasizing the importance of content sensitivity over network topology. A PCN leverages content-defined trust principles, assigning sensitivity labels to content and enforcing appropriate protection measures such as encryption and access control based on these tags. This ensures that the security measures are commensurate with the content's level of sensitivity and not merely its location within the network infrastructure.

The PCN architecture transcends traditional zero-trust models by integrating comprehensive policy management that dynamically adjusts to the content's sensitivity classification. This system automatically enforces risk policies that consider the user's role, content classification, and intended actions, thereby determining the legitimacy and extent of access or transfer permissions. Such granularity in policy enforcement is crucial for maintaining stringent security postures, especially when dealing with sensitive data that necessitates additional verification steps like justification forms or managerial signoffs.

The PCN also facilitates a robust logging mechanism that meticulously records all content interactions, thereby providing an extensive audit log for regulatory compliance and internal review. This visibility into the flow and usage of sensitive data is a cornerstone of the zero-trust approach, which predicates on the principle of never trust, always verify.

Momentum to extend security and compliance to the content layer will gain further momentum in 2024. Organizations will seek the increased protections and efficiencies of managing sensitive content communication channels in a unified PCN platform using zero-trust security and compliance policies.

Nearly 75% of organizations indicate their measurement and management of sensitive content communications requires either significant or some improvement.[40]

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

Challenges surrounding the handling of large files containing sensitive content will become increasingly pressing for organizations. The expansion of existing use cases for large files is notable in several rapidly evolving fields. For instance, the biotech industry is witnessing an explosion in the size of DNA sequence data files as genetic research and personalized medicine gain traction. Similarly, advancements in design and engineering are leading to larger and more complex CAD files. In law enforcement, the use of video evidence is becoming more prevalent, requiring secure and efficient storage and transfer solutions. Marketing departments are leveraging high-resolution video and graphics to make an impact, while in the realms of economics, financial trading, science, and medical research, the analytics files are ballooning in size and sensitivity. These growing file sizes necessitate robust solutions for secure handling and storage.

As noted above, another area to monitor is the training datasets for private LLMs, a nascent yet rapidly developing field. As these models become more advanced and tailored to specific organizational needs, the datasets they train on will grow in size and confidentiality. This trend suggests a future where the management of large, sensitive training datasets becomes a critical operational concern.

The customer service aspect of products containing software has brought to light the importance of handling large log and HTTP Archive (HAR) files, which contain a wealth of sensitive information. The Okta breach is a stark reminder of the vulnerabilities these files can present.[41] This challenge is compounded by employees who may resort to unsanctioned and insecure methods for transferring these large files, thereby heightening privacy risks. While business-focused cloud storage solutions like Microsoft 365 and Box have increased file size limits to accommodate up to 250 GB, these are still insufficient when compared to the demands of the use cases mentioned. These platforms, and others, will continue to face pressure to support the secure transfer and storage of ever-larger files, as traditional product limits lag behind the needs of modern data-intensive operations.

Many organizations encounter operational challenges when sharing and transferring sensitive data due to limitations of 250 GB or less on many file sharing and file transfer solutions.

Conclusion: Takeaways From Our 12 Predictions

The landscape of sensitive content communication is rapidly transforming due to technological innovations and increasing regulatory measures. Businesses are under heightened strain to protect confidential data amidst escalating cyber threats and to ensure adherence to burgeoning international regulatory standards.

Our 2024 Forecast Report identifies pivotal trends that will influence the security and regulatory compliance of sensitive content in 2024. Some of the key takeaways in the report include:

- Advanced AI technologies, including generative large language models, present new challenges for data privacy and compliance that require stringent governance, comprehensive security measures, and ethical AI utilization.
- Upcoming regulations, such as the EU's AI Act and anticipated U.S. federal legislation, will enforce novel standards for personal data management that organizations will need to effectively implement.
- The spread of data localization mandates necessitates the redesign of apps and cloud setups to meet data sovereignty requirements.
- Increasing fines and penalties for breaches in data privacy call for enhanced governance and security frameworks to prevent infractions.
- Advancement of DRM is essential for the ongoing protection of confidential information.
- Assimilation of sophisticated security technologies, including cloud-based data loss prevention, advanced threat protection, and content disarm and reconstruction, into sensitive content infrastructures helps bridge security voids.
- Consolidation of solutions for communication channels like email, file sharing, managed file transfer, and web forms into a cohesive PCN streamlines security and regulatory adherence.
- Emerging applications across various sectors generate exceptionally large files, challenging the capacity of traditional systems.

Outdated, siloed sensitive content communication tools are insufficient, lacking the necessary advanced functionalities, integrated defenses, and holistic governance to cope with the changing threat environment. By adopting zero-trust architectures, detailed security models based on content, strong access management, and integrated DRM, data loss prevention, and other leading-edge security measures, organizations can mitigate risks and uphold compliance amid growing regulations. And as you plan for 2024, you should do a reset on your sensitive content communication strategies and work to ensure you have the right technologies in place to protect your file and email data communications.

References

[1] "Cybersecurity Forecast 2024: Insights for future planning," Google Cloud, November 2023.

[2] "Sensitive Content Communications Privacy and Compliance 2023 Report," Kiteworks, August 2023.

[3] Stephanie Schappert, "Workers regularly post sensitive data into ChatGPT," cybernews, June 16, 2023.

[4] Matthew Guarini, "Predictions 2024: Tech Leaders Boost Ops To Grow With AI," Forrester Blog, October 24, 2023.

[5] "The state of AI in 2023: Generative AI's breakout year," McKinsey, August 1, 2023.

[6] "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," The White House, October 30, 2023.

[7] Shiva Aminian, et al., "President Biden Issues Long-Awaited Artificial Intelligence Executive Order," Akin, October 30, 2023.

[8] "Artificial Intelligence 2023 Legislation," National Conference of State Legislatures, September 27, 2023.

[9] "Regulatory framework proposal on artificial intelligence," European Commission, accessed November 8, 2023.

[10] "NIST AI RMF Playbook," NIST, accessed November 8, 2023.

[11] Phil Muncaster, "Forrester: GenAI Will Lead to Breaches and Fines in 2024," Forrester, November 2, 2023.

[12] "Cost of a Data Breach Report 2023," IBM, May 2023.

[13] Becky Bracken, "Clop Keeps Racking Up Ransomware Victims With GoAnywhere Flaw," DARKREADING, March 27, 2023.

[14] Wes Davis, "MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023," The Verge, November 10, 2023.

[15] "Cost of a Data Breach Report 2023," IBM, May 2023.

[16] "Worldwide 2022 Email Phishing Statistics and Examples," Trend Micro, May 31, 2023.

[17] "Data Breach Investigations Report 2023," Verizon, March 2023.

[18] "Worldwide 2022 Email Phishing Statistics and Examples," Trend Micro, May 31, 2023.

[19] "90% of Organizations Prioritizing Email Encryption," Echoworx Blog, May 4, 2021.

[20] "Survey: 83 Percent of U.S. Organizations Have Accidentally Exposed Sensitive Data," Egress Press Release, February 21, 2019.

[21] "How to Protect Your Sensitive Information With Email Encryption," Pulse Technology, September 18, 2023.

[22] "Why Is Email Encryption Not Widely Used," Trustifi, February 8, 2021.

[23] Deepen Desai, et al., "2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year," Zscaler Blog, April 18, 2023.

[24] "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner, May 31, 2022.

[25] "NIST Drafts Major Update to Its Widely Used Cybersecurity Framework," NIST, August 8, 2023.

[26] Valdez Ladd, "NIST's Privacy Framework for Proposed US Federal Privacy Law," ISACA, February 15, 2023.

[27] "NIST Drafts Major Update to Its Widely Used Cybersecurity Framework," NIST, August 8, 2023.

[28] "How to Achieve Data Compliance in 2024," Exadel, October 16, 2023.

[29] "Data Sovereignty: Definition, Requirements, and How To Ensure It," Spanning, accessed November 8, 2023.

[30] "Understanding the Implications of Data Sovereignty and Why Data Residency may be a Better Choice for Your Business," Trustwave, October 27, 2023.

[31] Alexis Porter, "Lessons Learned From GDPR Fines in 2023," CPO Magazine, August 2, 2023.

[32] "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner Press Release, May 31, 2022.

[33] Billy Mitchell, "With draft guidance, OMB kickstarts effort to modernize FedRAMP for today's cloud challenges," FEDSCOOP, October 27, 2023.

[34] Katie Walsh, "13 Key Digital Asset Management Best Practices for 2024," Brandfolder, October 26, 2023.

[35] "Digital Rights Management Market Research Report 2024-2030 | 98 Pages Report," Market Reports World, November 3, 2023.

[36] Rick Dagley, "Gartner Predicts Top 10 Strategic Technology Trends for 2024," ITProToday, October 16, 2023.

[37] "Sensitive Content Communications Privacy and Compliance Report 2023," Kiteworks, July 2023.

[38] "Content Disarm and Reconstruction Market by Component (Solutions and Services), Application Area (Email, Web, FTP, and Removable Devices), Deployment Mode, Organization Size, Vertical, and Region—Global Forecast to 2026," MarketsandMarkets, February 2022.

[39] "Data Loss Prevention Market to be Worth $9.33 Billion by 2030," Grand View Research, July 17, 2023.

[40] "Sensitive Content Communications Privacy and Compliance Report 2023," Kiteworks, July 2023.

[41] Bob Ertl, "How the Okta Customer Support Hack Exposed Sensitive Data and Access Credentials," Kiteworks Blog, October 28, 2023.