S&P Global
Market Intelligence
451 Research
Business Impact Brief

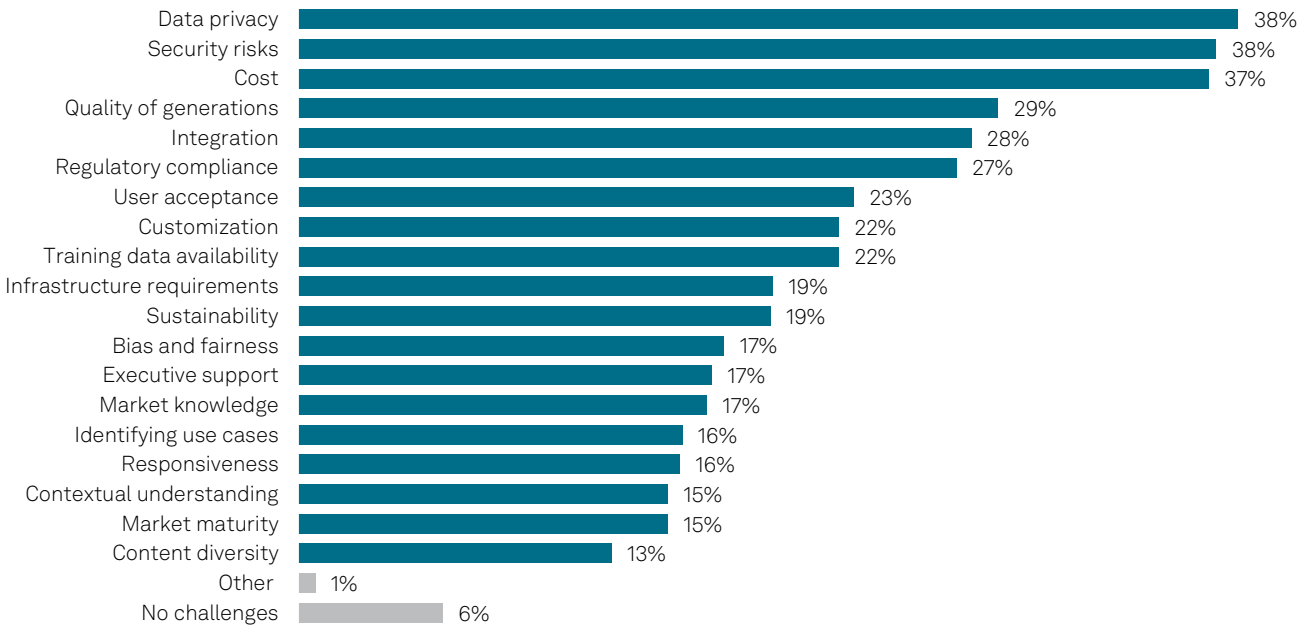
Security is the secret ingredient for GenAI transformation in document productivity

The Take

Recent technological advancements have enhanced document productivity, including real-time collaboration, e-signatures and increasingly sophisticated automation of document processing and workflows. The rise of generative AI is further transforming how individuals and organizations interact with documents, with the potential to categorize and process large volumes of information to unlock the full value of critical information often held in those documents, delivering tailored insights and recommendations, and making related processes much more effective. Two in five organizations (39%) have adopted AI for document use cases such as summarization, analysis, auto-fill, translation and research, according to our Voice of the Enterprise: AI & Machine Learning, Use Cases 2025 survey.

However, this new potential also introduces novel security challenges, particularly concerning data privacy, confidentiality, authenticity and accountability. New types of phishing and social engineering attacks, tampering with document metadata such as authorship and revision histories, inaccuracies and misleading information from generated content, and insufficient access controls on AI-generated documents all pose significant risks to organizations looking to adopt GenAI. Barriers to GenAI adoption include concerns about data privacy, security and regulatory compliance (see Figure 1). As organizations embrace GenAI, they must prioritize security to ensure that advancements in document productivity do not compromise sensitive information or violate compliance regulations.

Figure 1: Barriers to generative AI adoption



Q. Which of the following areas present challenges to your organization's adoption of generative AI? Please select all that apply.
Base: All respondents (n=999).
Source: 451 Research's Voice of the Enterprise: AI & Machine Learning, Use Cases 2025.

S&P Global
Market Intelligence

451 Research
Business Impact Brief

Business impact

Technological advances require comprehensive security postures: GenAI's ability to process a massive volume of documents and information compels organizations to invest in document technologies with comprehensive security controls. Role-based access control combined with AI-powered discovery of personally identifiable information and dynamic data masking can restrict access to critical data to authorized personnel, while enhanced audit trails and monitoring ensure accountability. Data encryption protects information both at rest and in transit, and AI-driven anomaly detection can identify unusual user behavior. Additionally, advanced content filtering can help to automate document classification, further strengthening security.

Guardrails are needed to govern AI usage: Tools with robust security features empower employees to confidently leverage AI applications in their document workflows, driving productivity gains through task automation, insight generation, and improved collaboration and decision-making. However, this empowerment must be carefully managed. Alongside security controls, organizations should educate employees on responsible use of AI, including understanding and applying data sensitivity labels, recognizing potential security threats and adhering to compliance requirements. Additionally, it is crucial to include attributions and citations for AI-generated content to mitigate risks associated with inaccuracies, such as from hallucinations. To further enhance governance, organizations may form a GenAI committee to oversee AI initiatives and conduct audits to ensure compliance and effectiveness. Human oversight is essential to balance automation and accountability. Implementing guardrails for AI usage and strong security controls can enable employees to integrate AI into their document productivity while safeguarding against misuse and compliance violations.

Measures must be taken to mitigate corporate risk: The adoption of private large language models (LLMs) and the enforcement of stringent security protocols significantly reduce the risk of exposing corporate or client data. By ensuring that proprietary information does not inadvertently become part of a public dataset, organizations can protect their intellectual property and maintain compliance with data protection regulations. This proactive approach to security is essential for preserving the integrity of sensitive information.

Looking ahead

Organizations should anticipate an increase in regulations mandating that organizations seek secure solutions from the outset to preempt potential legal challenges. This will necessitate a proactive approach by vendors to ensure security in their document productivity tools and integrate compliance into the development and deployment of their technologies. In addition, there will likely be a heightened emphasis on secure data extraction methods, enabling organizations to safely export information from documents into LLMs and automation systems. This will require stringent security provisions to protect sensitive data during the extraction process, ensuring that information remains confidential and secure.

As organizations strive to convert large volumes of text into actionable insights, security will play a crucial role. Tailoring structured document processes to specific personas and workflows will necessitate careful consideration of security protocols and controls specific to those personas to ensure that sensitive information is handled appropriately and in compliance with company policies and regulations. Documents such as PDFs will remain valuable knowledge repositories within organizations. Implementing robust security measures, including capabilities such as sandboxing that protect users' systems from malicious code in untrusted documents, will be essential to meet compliance standards, uphold organizational policies and protect proprietary information from unauthorized access or breaches. By prioritizing security, organizations can ensure that their knowledge assets remain secure and accessible only to authorized personnel.