InfoBrief, sponsored by Adobe | January 2025

Ensuring Document Security

Navigating AI, Flexible Work, and Trust in a Connected World

Holly Muscolino
Group Vice President,
Workplace Solutions, IDC

Grace Trinidad, PhD, MPH, MS
Research Director,
Trust Measurement and Metrics, IDC

Navigating This InfoBrief

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

In This InfoBrief

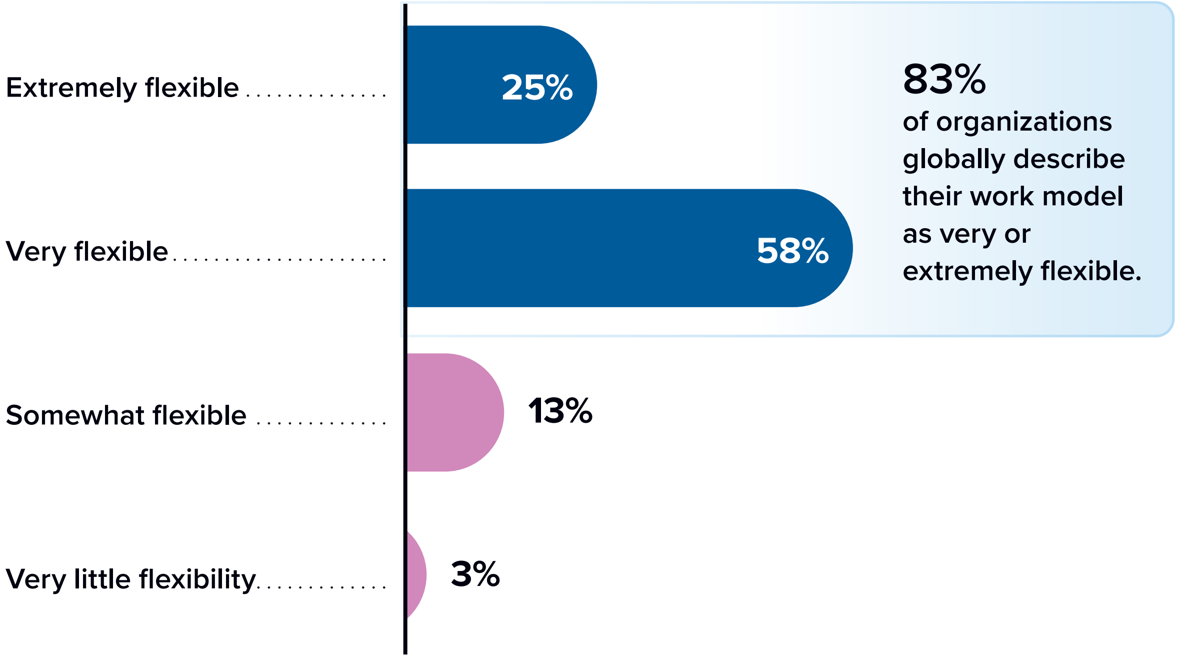
In an era of integrated technology platforms, generative AI (GenAI), distributed organizations, and flexible work, **organizations are reviewing, rethinking, and revising their approach to security and governance. This review must include document security.**

This IDC InfoBrief reviews an often-overlooked aspect of an organization's security strategy: document security. IDC analysts spoke with three senior decision-makers to understand how they approach security and compliance at their organizations. This InfoBrief also includes a review of IDC's research related to organizational security in the era of flexible work models and GenAI.

Flexible Work Grows Alongside Security Concerns

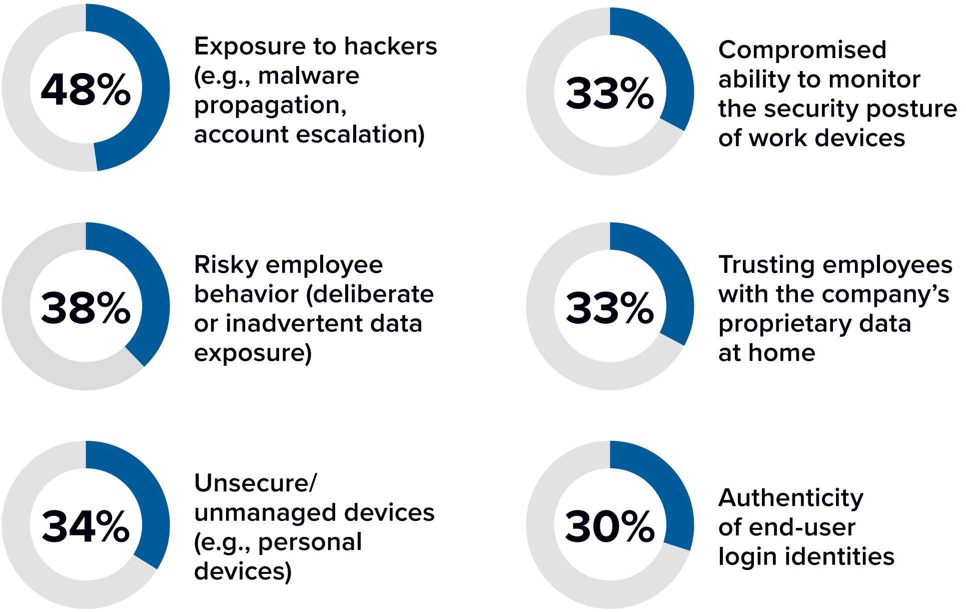
Leaders believe that employee systems are more prone to hacking in flexible work models, and they find it challenging to mitigate security threats.

How would you describe your company's work model?



83% of organizations globally describe their work model as very or extremely flexible.

What are your biggest security concerns related to flexible work models?



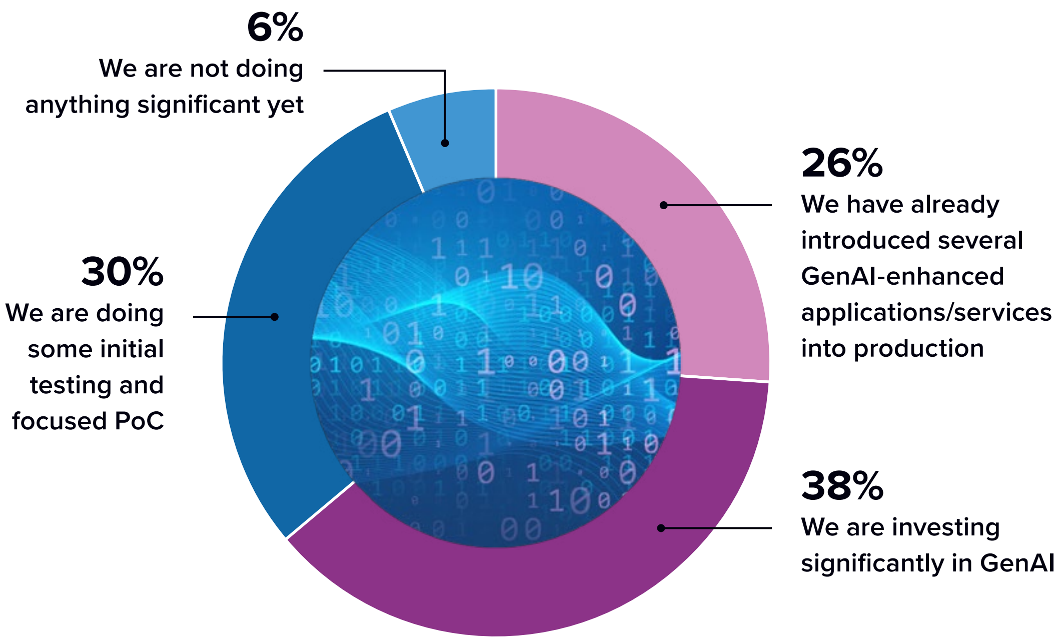
Note: Totals may not sum to 100% due to rounding. n = 1,269; Source: IDC's *Worldwide Future of Work Survey*, June 2024

Flexible work models introduce increased (or new) security concerns for organizations.

GenAI Adds a New Dimension to Security Concerns

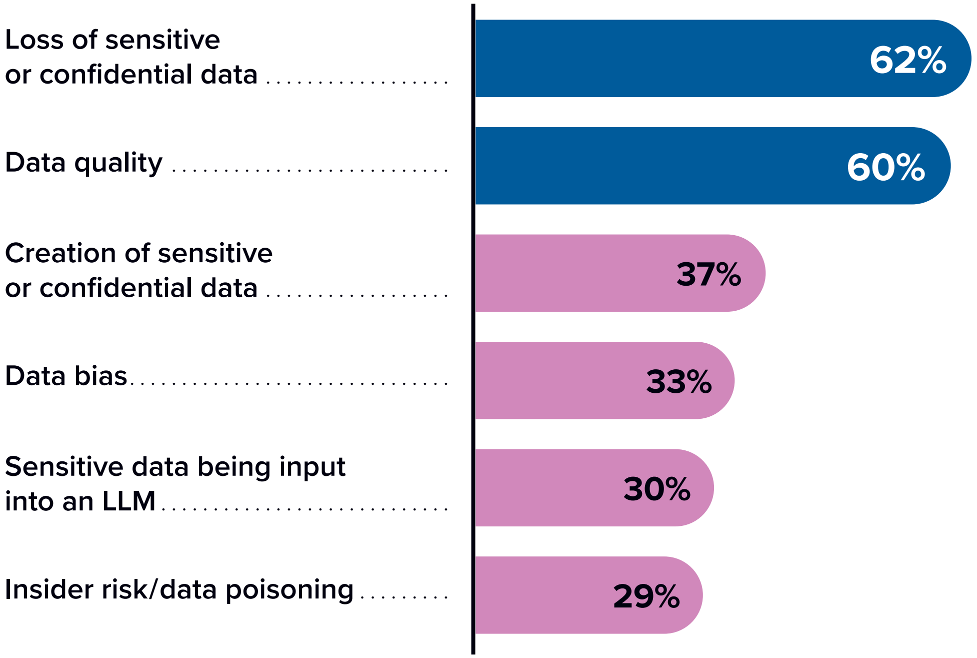
63% of organizations are heavily investing in GenAI or have already deployed GenAI solutions, which introduces **new security and compliance** concerns.

What is your organization's current state of evaluating or using GenAI?



Note: Totals may not sum to 100% due to rounding. n = 891; Source: IDC's *Future Enterprise Resiliency & Spending Survey Wave 7,* July 2024

What are your biggest data security concerns when it comes to privately interfacing with GenAI models?



Note: LLM = Large language model. n = 619; Source: IDC's *Data Privacy Survey,* March 2024

Documents Drive Business

80%–90% of enterprise data is unstructured and most business processes are reliant on some type of document. Yet document security is an often-overlooked aspect of an organization's overall security strategy.

Sales

- Contracts and agreements
- Proposals and quotes

Legal

- Contract management
- Nondisclosure agreements

Finance

- Budget approvals
- Travel/spend authorization
- Invoice approval

Remote Work

- Applications
- Policy changes
- Contracts and agreements

Product Management

- Change authorization
- Requirement acceptance
- Road map approval

IT

- Vendor agreements
- Asset management
- Change requests

Marketing

- Customer onboarding
- Self-service
- Marketing contracts
- Release forms

HR

- Offer packages
- Employee onboarding
- Benefits enrollment
- Self-service

Challenges with Document Security

Document security is a central challenge for organizations. The rise of flexible work models has exacerbated these challenges

Documents as Attack Vector

Although any file type can be used (e.g., .doc, .xls, .ppt, .jpg, .png), PDF files are a popular choice for attackers because of their widespread use. Between 2019 and 2020, Palo Alto Networks **identified a 1,160% increase in malicious PDFs.**

(Source: unit42.paloaltonetworks.com/phishing-trends-with-pdf-files)

Unauthorized Access or Sharing

Because documents and PDFs are easily shared, **overprovisioned access controls can lead to unauthorized sharing or unauthorized access to key documents.** ISO 27001 guidance “Control A.9.2.1” requires the restriction of user access to information and applications.

Data Extraction Risks, Protecting IP

Attackers and benign individuals within an organization **can put the organization at risk of unauthorized and harmful data extraction.** Compromised metadata, selectable text, embedded objects and links, and form data can be hidden in any document type.

Compliance

Existing security regulations and frameworks place an **emphasis on pseudonymization and encryption to protect PII.** GDPR Article 32(1) states: “implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: [the] pseudonymisation and encryption of personal data.”

> “… Identifying data and being able to act on it appropriately is a huge concern I have internally … every time data gets passed from one system to another, we’re trying to make sure that we know exactly what that data is …”
>
> Director, Application Development
> at a large insurance firm

ADDRESSING THE CHALLENGES: Documents as Attack Vectors

Common document types, such as PDFs, have become a popular vector for attack due to their flexibility, their widespread use across platforms, and the ease with which users and attackers can embed content via encoded streams, JavaScript code, executable files, and other methods.

In 2022, Sophos Labs discovered that a variant of Locky Ransomware was being launched by a VBA macro hidden in a Word document that was hidden again inside a PDF file. If the unsuspecting user followed the document's directions and enabled editing, the VBA macro would download and run the crypto-ransomware.

> "… you have got to layer security … You need encryption in transit. You need encryption in place. You need a document that you know [is secure] depending on what you use that document for … PDF is the gold standard."
>
> Director, Application Development at a large insurance firm

ADDRESSING THE CHALLENGES: Documents as Attack Vectors (continued)

Commonly Exploited Document Types

- PDF
- MS Office Documents (.docx, .pptx, .xlsx)
- Compressed files (.zip, .rar)
- Image files (.jpg, .png, .gif)
- Executable attachments (.exe, .msi)

Common Attack Vectors

- Malicious scripts or macros
- Encoded streams, images, executable files
- Vulnerabilities in PDF readers, MS software
- Phishing via deceptive content

Security Control Options

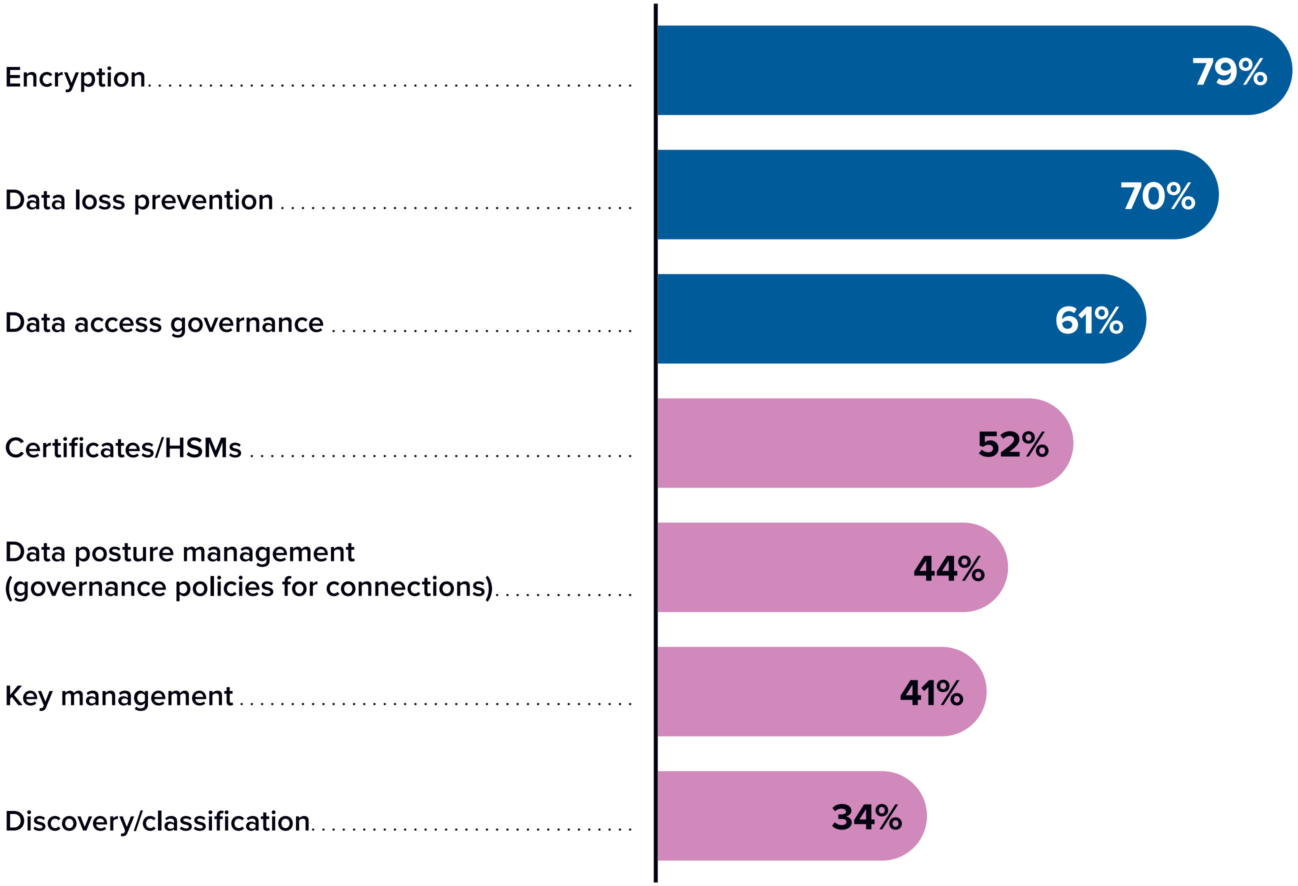
- Education and awareness training
- Attachment sandboxing
- File-type restrictions
- Encrypted email
- Endpoint anti-virus and anti-malware

ADDRESSING THE CHALLENGES: Unauthorized Access or Sharing

Key Security Technologies

- Authentication and privileged locations
- Access controls
- Application security (sandboxing, JavaScript security)
- Compliance certifications
- Digital rights management
- Digital signatures
- Encryption
- Information protection labels
- Redaction
- Secure link sharing, allowlist for links
- Secure storage
- Third-party security testing

What data security technologies are being used to demonstrate privacy/compliance worldwide?



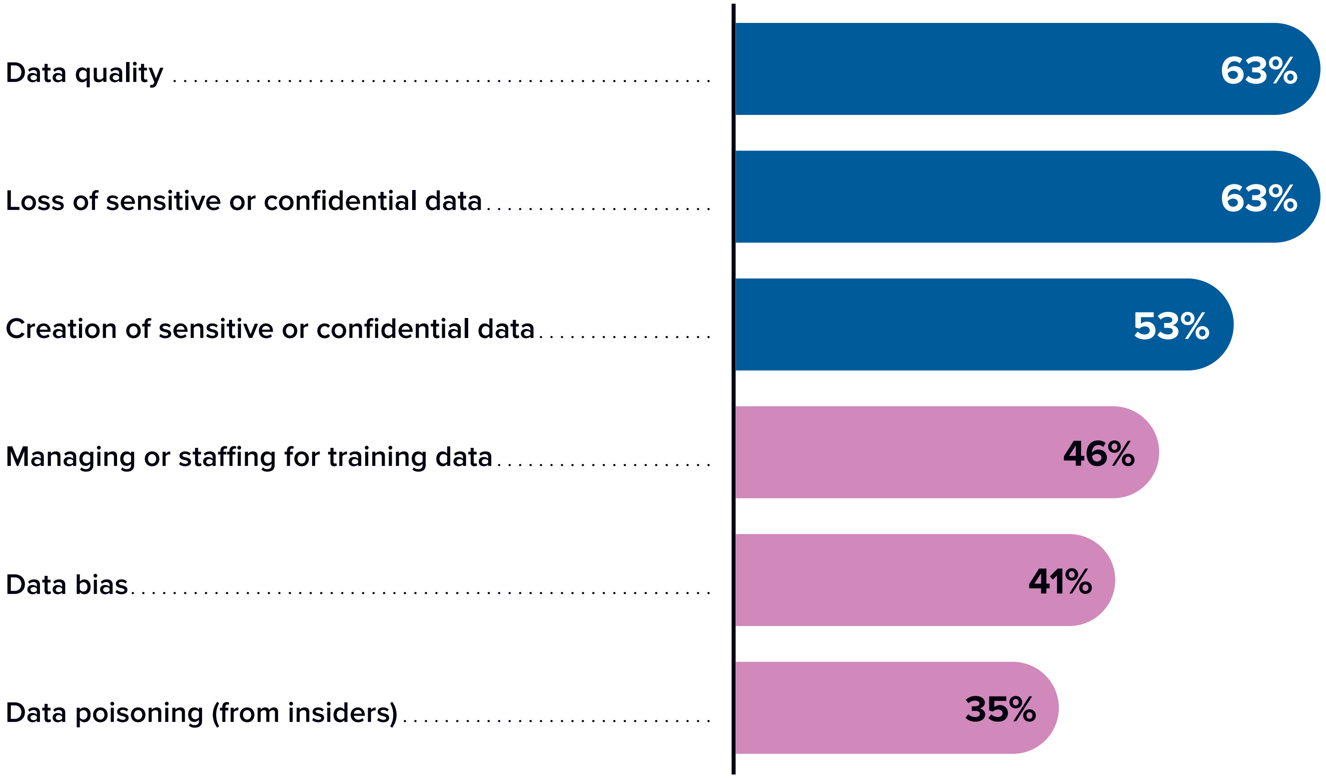
Note: HSM = Hardware security module. n = 227; Source: IDC's *North America eSignature Market Survey*, November 2021

ADDRESSING THE CHALLENGES: Data Extraction and Risks to IP

GenAI presents increased risks of unauthorized access to sensitive data.

> “We’re looking at the most responsible uses for generative AI. Being able to access that unstructured data … I can tell you that [they] spent [nearly] $1 billion over a 10-year period trying to organize our data, putting it into Hadoop data lakes … And when generative AI came out, they scrapped the whole Hadoop data lake. They said this is no longer needed.”
>
> Director, Application Development
> at a large insurance firm

What are your biggest data security concerns when it comes to using public GenAI models?

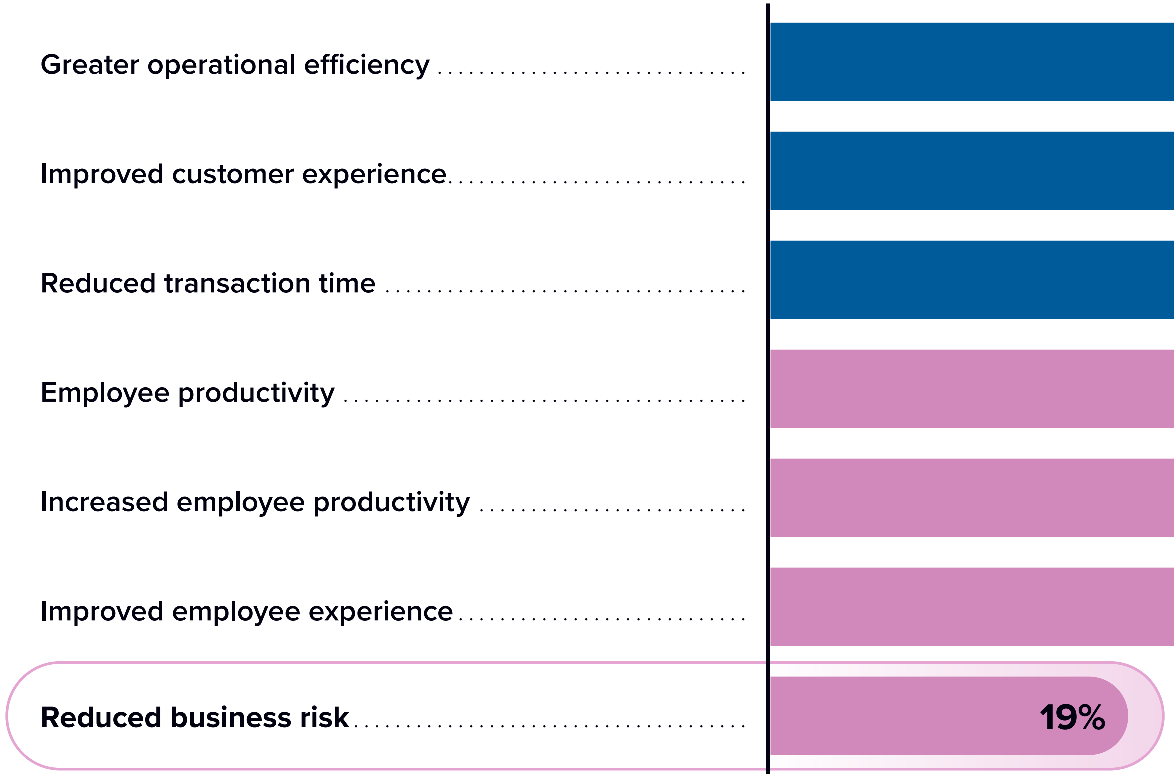


n = 610; Source: IDC’s *Data Privacy Survey*, March 2024

ADDRESSING THE CHALLENGES: Document Integrity

Securing the signing of workflows with electronic and digital signatures proves to be efficient.

Which of the following business benefits did your organization experience or expect to experience as a result of deploying intelligent digital workspace technologies and/or services?



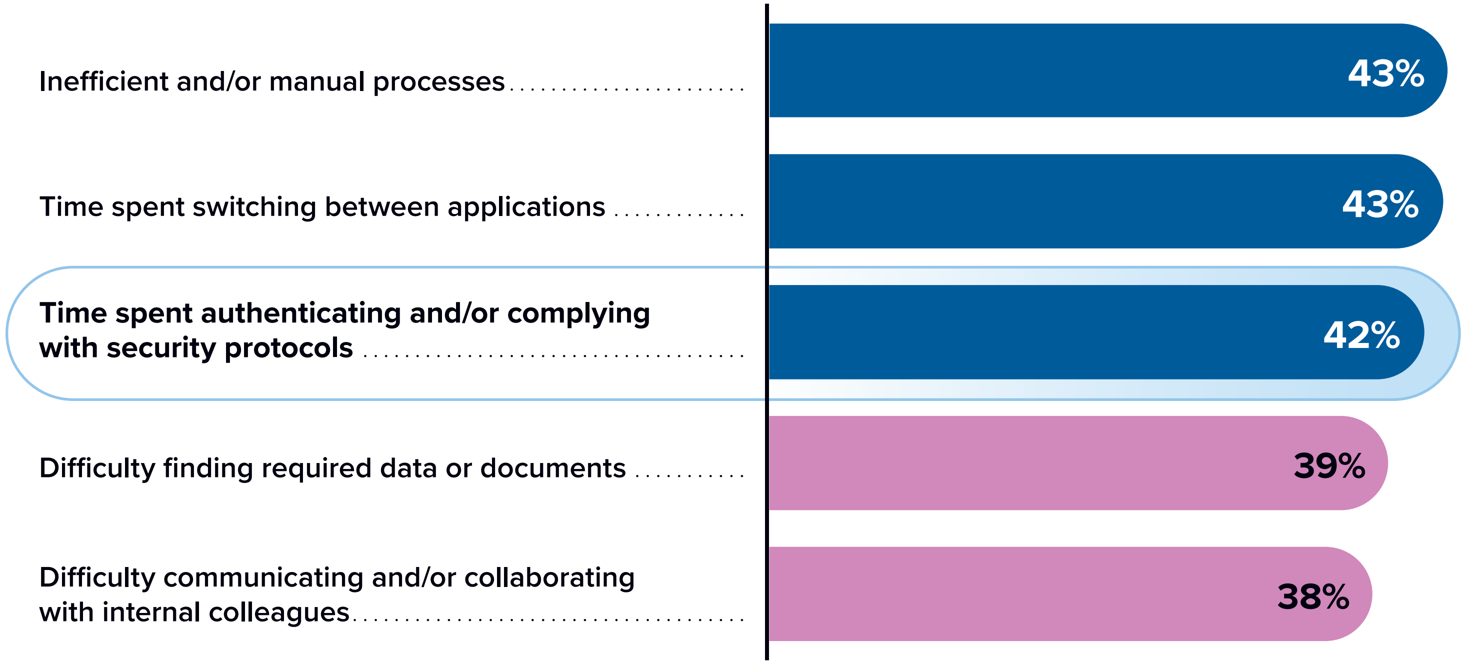
> “Right now, we have two people managing 32,000 electronic signatures per year. With electronic signatures, we can manage all electronic signatures with one primary person and a manager who just steps in occasionally. It’s extremely efficient.”
>
> Director, Application Development at a large insurance firm

n = 227; Source: IDC’s *North America eSignature Market Survey*, November 2021

One More Challenge to Consider: Cultural Change

Time spent complying with security protocols is one of the five primary challenges that prevent employees from working as efficiently as possible.

What are the five primary challenges that prevent employees from working as efficiently as possible?



> "... it's very relevant to me ... that we take a people-centric approach to security. I think it is incredibly important that we as a security team actually represent the people that we serve."
>
> CISO, large software firm

n = 609; Source: IDC's *Intelligent Digital Workspace Market Survey*, May 2022

Essential Guidance

With trillions of documents and PDFs in the market and more being created every day, **senior decision-makers should ensure that secure document workflows are part of their organization's overall security strategy.**

- **Deploy document-centric applications** that are secure by default, with features such as attachment sandboxing, file-type restrictions, and encryption.
- **Establish policies and procedures** to mitigate unauthorized access or sharing, along with the appropriate authentication and identity and access management controls.
- **Understand the risks and novel security threats** that AI presents, and adjust your security strategy to mitigate these risks.
- **Don't overlook the human factor** — establish a security-first mindset throughout the organization; bear in mind both onsite and remote employee workflows and policies, and make it easy for workers to comply.
- Finally, **partner with document technology vendors** that can assist with the above recommendations and that understand that they are one link in a broader operational supply chain.

Appendix: Glossary

Flexible work: A dynamic work model in which workers conduct business at diverse locations — on premises, in the field, or at a remote location, depending on company policy and business needs. Also referred to as **hybrid work.**

- **Not flexible:** There is no formal strategy to support a flexible work model.
- **Very little flexibility:** Some managers are enabling a flexible model on an as-needed, ad hoc basis, but there is no formal strategy in place.
- **Somewhat flexible:** Executive leadership has provided provisional guidance allowing some flexible/hybrid work.
- **Very flexible:** We have flexible work policies enabling workers to work onsite and remotely across multiple departments as per business needs.
- **Extremely flexible:** We have a flexible work strategy allowing workers to switch between remote and flexible work with no technical/policy challenges.

About the IDC Analysts

Holly Muscolino

Group Vice President, Workplace Solutions, IDC

Holly Muscolino is the group vice president, Workplace Solutions, responsible for research related to innovation and transformation in content solutions, including intelligent document processing, esignature, imaging and printing, and other content workflow services. Holly's core coverage also includes work transformation, technology and digital skills research, and the role of technology in driving the Future of Work.

More about Holly Muscolino

Grace Trinidad, PhD, MPH, MS

Research Director, Future of Trust, IDC

Grace Trinidad is research director in IDC's Security and Trust research practice responsible for the Future of Trust research program. In this role she provides strategic guidance and research support on approaches to trust that include risk, security, compliance, privacy, ethics, and social responsibility. Dr. Trinidad has published peer-reviewed research on privacy and trust, exploring public attitudes towards commercial use of personal health information. Other areas of Dr. Trinidad's research include the ethics of artificial intelligence and data sharing, trust in healthcare providers and in healthcare organizations, genomic database use and accessibility, and data equity.

More about Grace Trinidad

Message from the Sponsor

Adobe

Deliver great experiences with trust.

With Adobe Acrobat, organizations can deliver trusted document experiences that transform, scale, and grow their business.

- Securely work anywhere with enterprise-grade security and compliance.
- Utilize high-quality document AI with verifiable insights to accelerate work.

Get Adobe Acrobat today

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com

@idc

@idc