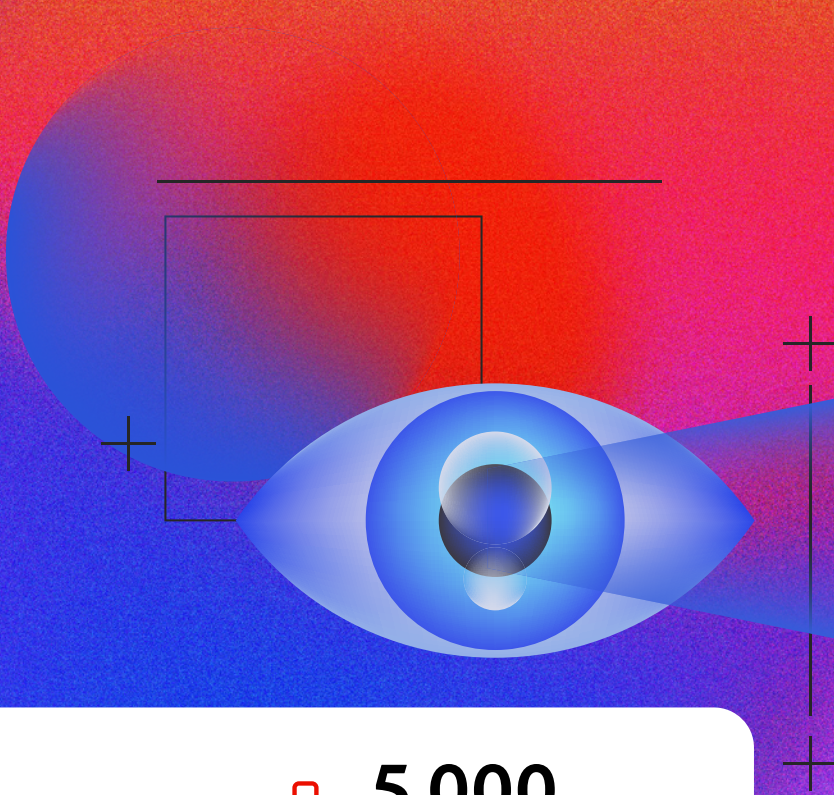


Adobe

DICKER
DATA

Secure documents. Govern AI. Stay in control.

Protect documents,
control AI use and simplify



The Risk Landscape

Cyber threats and data breaches are rising, with over 5,000 publicly reported incidents in EMEA in 2025 alone and an average global breach cost of \$4.88 million. At the same time, as organisations accelerate AI adoption, the pressure on IT and security teams continues to grow.

90% of successful cyber-attacks start with a phishing email, and PDFs sit at the heart of everyday business workflows. But like any widely used file type, they can be exploited if opened without the right protections. Threat actors often disguise malicious content inside documents or phishing emails, and it's important that the environment you open your PDFs in is secure.



5,000

publicly reported incidents
in EMEA in 2025



\$4.88M

average global breach cost



90%

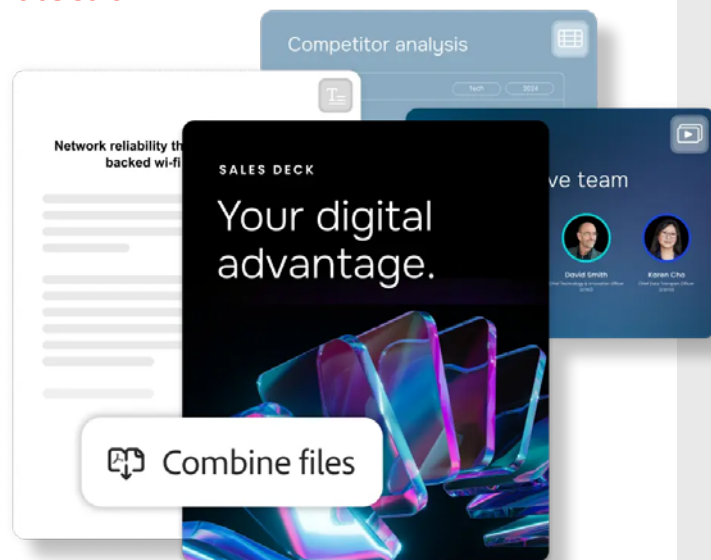
of successful cyber-attacks
start with a phishing email

Application Security & Information Protection

Full sandboxing and built-in information protection

Document security must begin at the application layer. Adobe Acrobat Studio provides full sandboxing capabilities that isolate all PDF processing, including scripts, fonts and embedded content, inside a highly restricted execution environment. Even if a file contains malicious code, it is contained and prevented from accessing the wider system. This best-in-class defence reduces endpoint risk before damage can occur.

Built-in information protection features, including encryption in transit and at rest, sensitivity labels, document certification and permanent redaction, ensure confidential data remains secure throughout its lifecycle. Meanwhile, secure cloud sharing replaces risky email attachments with controlled links, reducing exposure while maintaining oversight.





Your Document



AI Assistant



Safe Business
Output

AI Services / LLM Governance

Governed AI services built for enterprise use

Adobe's responsible AI framework includes robust testing for harm and bias, while Acrobat Studio's generative AI capabilities are designed with enterprise governance in mind.

AI Assistant analyses only user-selected documents and does not use customer data to train foundation models. Outputs are commercially safe and indemnified, providing organisations with added assurance when deploying AI-generated content.

Azure OpenAI is configured with logging and abuse monitoring disabled, while content filtering remains enabled. This controlled configuration enables organisations to adopt AI capabilities while protecting sensitive information and maintaining compliance.

Centralised Management & Enterprise Controls

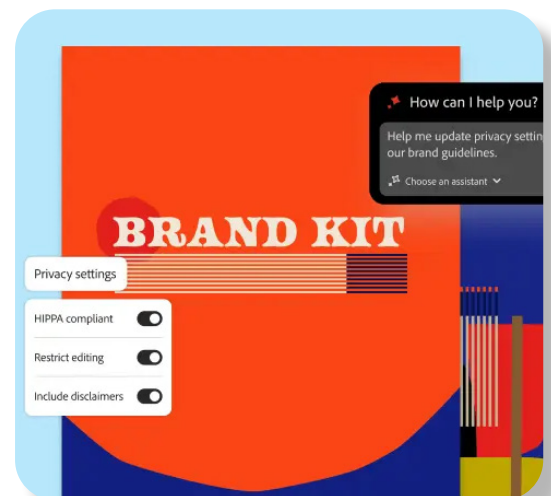
Policy-driven control at organisational scale

Acrobat Studio gives IT teams the oversight needed to enforce consistent security and access policies across the organisation.

Centralised controls include:

- ✓ Prevention of unauthorised user-driven installations
- ✓ Enterprise mobile management for secure access across devices
- ✓ Control over document sharing, including the ability to disable public links
- ✓ Dedicated key encryption to protect sensitive data

Together, these controls provide visibility, enforce policy compliance and support secure document and AI workflows at scale.



In a landscape of rising cyber threats and accelerating AI adoption, document security must be deliberate and enforceable. Acrobat Studio combines application-level defence, governed AI processing and centralised policy control to help organisations reduce risk without slowing innovation. With visibility across users, devices and AI interactions, IT teams can maintain compliance while enabling secure, scalable digital transformation.

Discover how Acrobat Studio secures and governs AI-ready document workflows.

Adobe.sales@dickerdata.com.au

Adobe

DICKER
DATA