

Security in the Age of Frontier AI



Adobe

Today's speakers



Aanchal Gupta

Chief Security Officer

Adobe



Abhigyan Modi

Senior Vice President,
Document Cloud and
Country Manager

Adobe India



Lori DeFurio

Principal Business
Solutions Technologist

Adobe



Mahrya Dakubu

Head of GTM Strategy
for Corporate Business
Professionals

Adobe

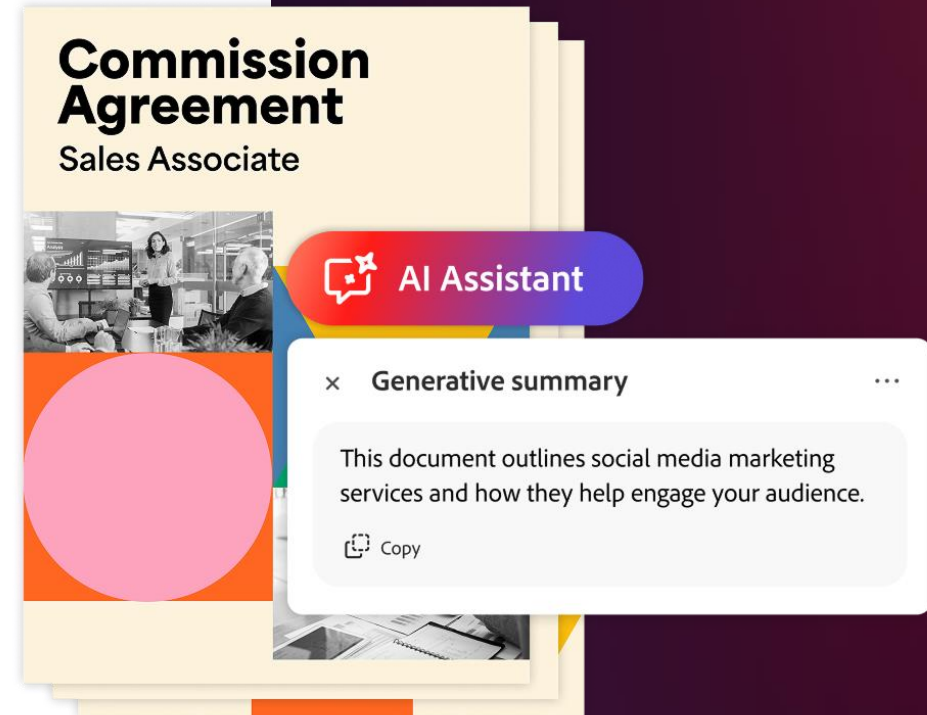
Agenda

State of the landscape: Protecting at AI speed

Trust, verified: AI inside your documents

New capabilities: Knowledge Base and Analyzer in Acrobat Studio

Q&A



State of the landscape: Protecting at AI speed



Aanchal Gupta

Chief Security Officer

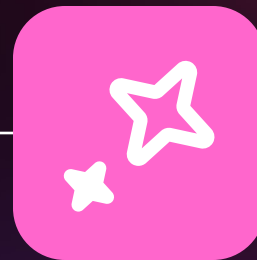
Adobe

Speed changes the game

The gap between a vulnerability going public and being exploited is now measured in days, not years; response timelines need to be built around that reality.



Years
(Before AI)



Days
(With AI)

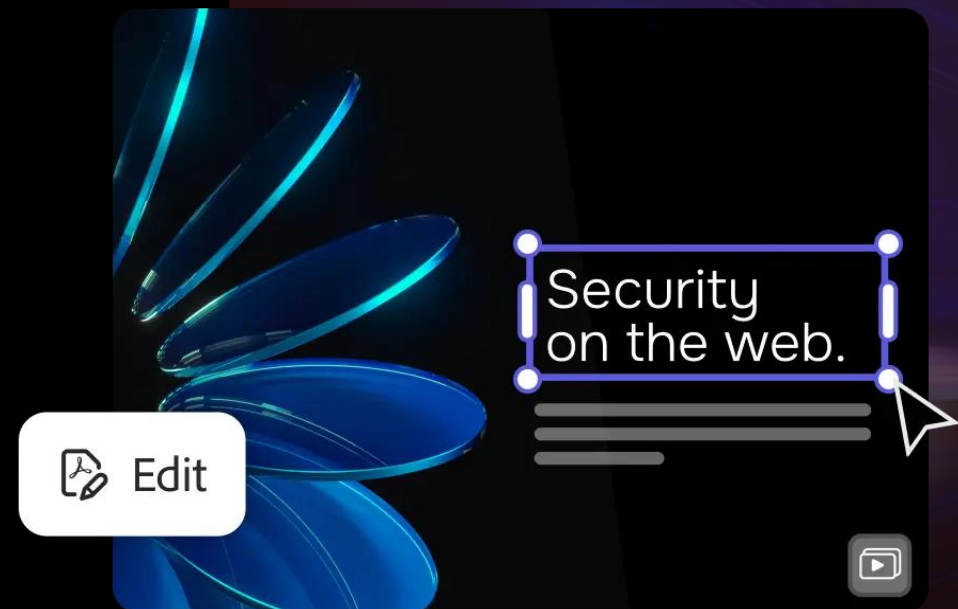


Hours
(soon)

Visibility + AI = a defender's edge

Adobe's own AI test harness turns insider visibility into a faster, more thorough defense.

- Build an AI test harness to scan your own code first
- Fix confirmed vulnerabilities within SLA, then deploy fast
- Use your source-code visibility — attackers only see a black box
- Measure speed to remediation, not just speed to detection



Speed multiplies fundamentals, it doesn't replace them

Use AI to deepen your core security investments.

Do our NDAs cover third-party subcontractors?



Syncing



Field Readiness Collection

3,998
documents indexed



Knowledge Base collections

Yes — same confidentiality terms apply, if listed in Exhibit A.



Master NDA Template

Section 4



 AI recommendation

■ CSE - 360K

■ Affiliate - 249K

■ Paid TM - 189K

Learn by doing

Give teams real problems and the freedom to experiment with AI hands on, because firsthand experience builds adoption in a way that policy alone never will.

Visibility before restriction

You can only secure what you can see, so pair deep environment visibility with layered defenses like sandboxing for untrusted files.

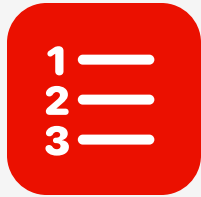


-2026 Data Breach Investigations Report, Verizon

Three pillars of security strategy

When priorities feel endless, organize your strategy around these three:

Operational excellence



**Strong
foundations**



**Safe
space for
innovation**



**Tight identity
and access
management**

Trust, verified: AI inside your documents



Abhigyan Modi

Senior Vice President,
Document Cloud and Country Manager

Adobe India

AI radically expands what document security means

Security now has to cover not just the document, but the AI's interaction with the information inside that document.

1



**Precise
attribution**

2



**No LLM training
on customer
content**

3



**Content
filtering**

4



**Enterprise
governance**

5



**Deliberate
document
inclusion**

Trace every answer back to its source

Attribution is more than a convenience, it fosters:



Trust

+



Transparency

Attribution is more than protecting against incorrect answers; it protects against incorrect answers compounding.



Richer sharing starts with the same foundation

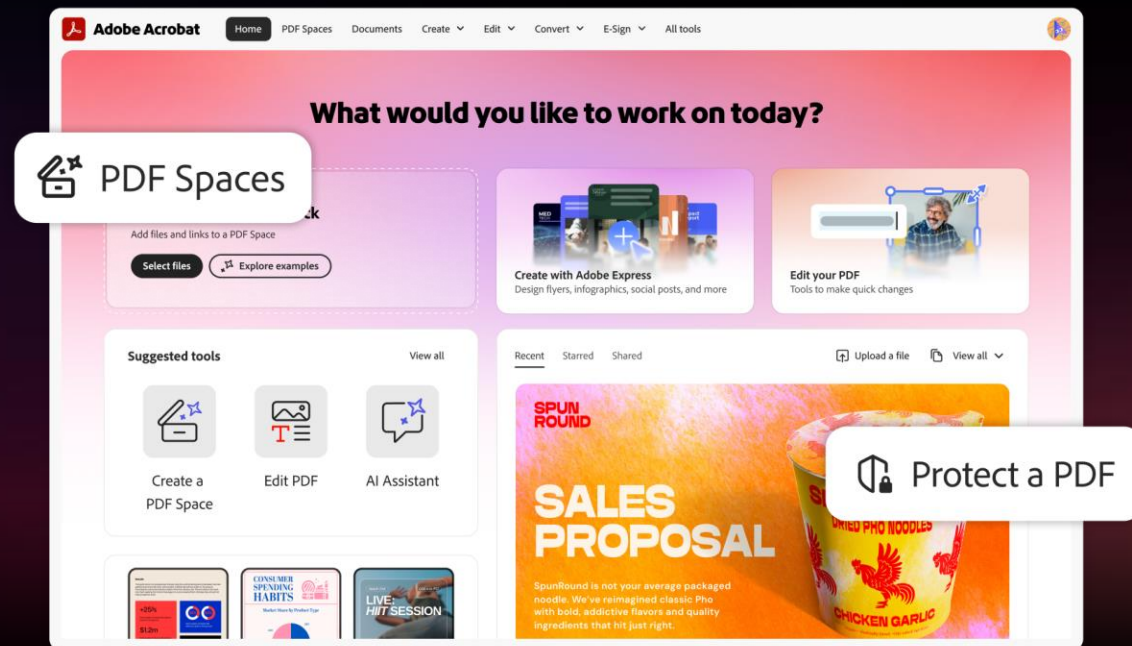
PDF Spaces extends documents into shared, interactive experiences without changing the rules.



The future of information sharing is richer, requiring more context and more information shared



PDF Spaces is the next step for businesses that care about the effectiveness of that information



Knowledge Base and Analyzer in Acrobat Studio

Acrobat Studio expands everyday productivity and adds enterprise document intelligence.

Adobe Acrobat Studio

Acrobat Pro

Now easier to use via **conversational AI**

Create PDFs

Edit PDFs

Sign PDFs

Redact PDFs

Secure PDFs



EVERYDAY PRODUCTIVITY

AI Assistant

Understand & action on documents

PDF Spaces

Collaborate around documents with shared context

Express

Create polished, on-brand deliverables from documents

ENTERPRISE INTELLIGENCE

Knowledge Base

Transform curated document collections into trusted answers

NEW

Analyzer

Turn document collections into structured data for business processes

NEW

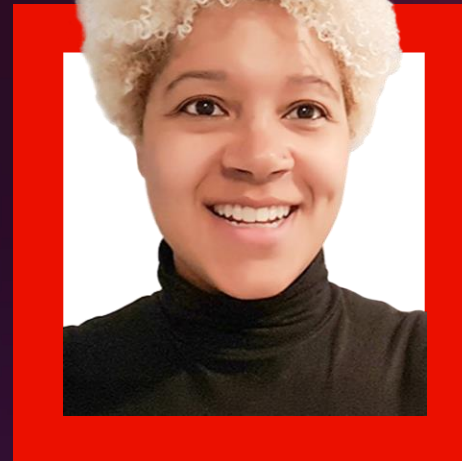
Q&A



Aanchal Gupta

Chief Security Officer

Adobe



Mahrya Dakubu

Head of GTM Strategy
for Corporate Business
Professionals

Adobe

The risk framework is the same

Don't reinvent your risk framework for AI.

1



Classification

2



Encryption

3



Storage

4



**Identity
Management**

5



**Access
Management**

You are in control of your data.

1

Customer data is not used to train language models.

2

Acrobat AI Assistant and PDF Spaces only look at the documents you tell it to.

3

Customer has controls and discretion to enable and disable storing chat history & documents in the cloud.*

4

Responses with verifiable citations to specific points in the source documents.

5

Enterprise controls to manage who has AI access in the company.**

6

Easy to deploy across the enterprise.**

Evaluate AI vendors

When evaluating an AI vendor, look for documented certifications and alignment with reliable AI frameworks, not just general security claims.

Look for:



ISO 42001



NIST AI
Framework

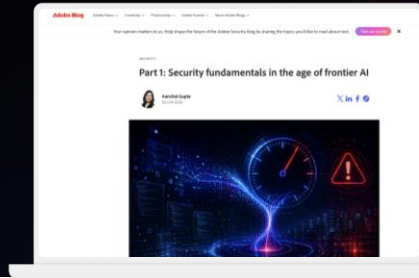


CCF AI Framework

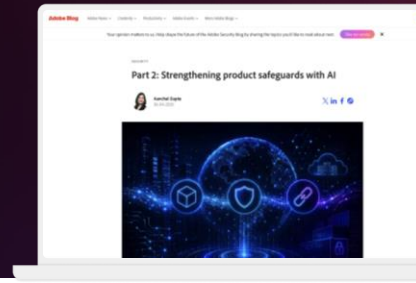


Resources

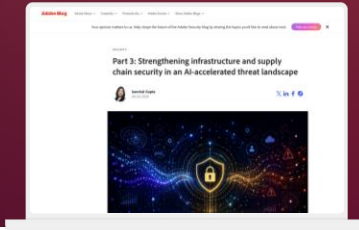
Part 1: Security fundamentals in the age of frontier AI



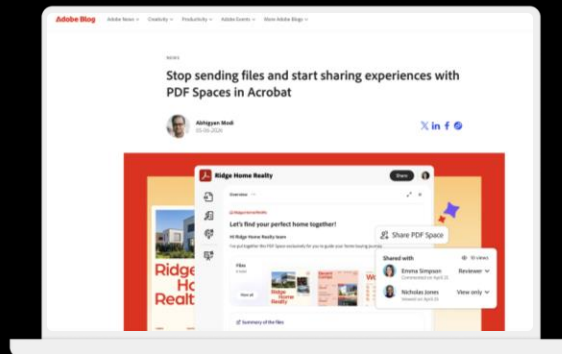
Part 2: Strengthening product safeguards with AI



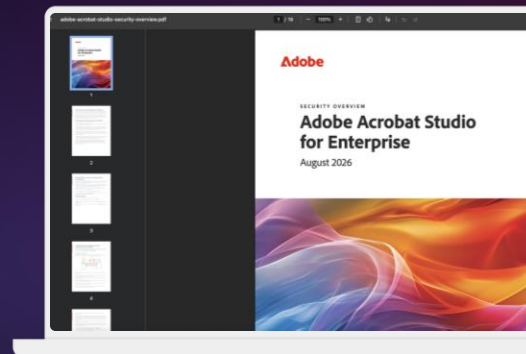
Part 3: Strengthening infrastructure and supply chain security in an AI-accelerated threat landscape



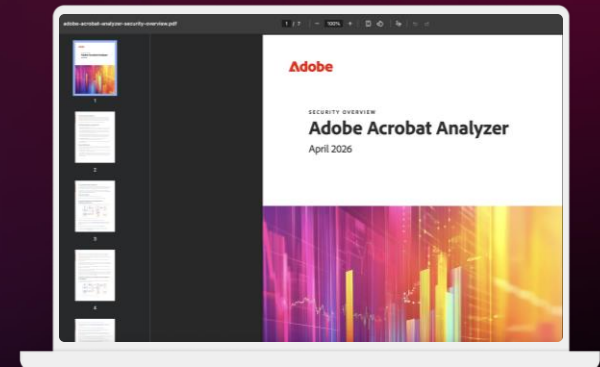
Stop sending files and start sharing experiences with PDF Spaces in Acrobat



Security Overview: Adobe Acrobat Studio for Enterprise

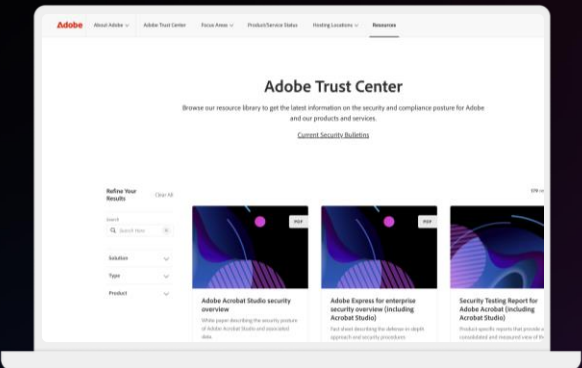


Security Overview: Analyzer in Acrobat

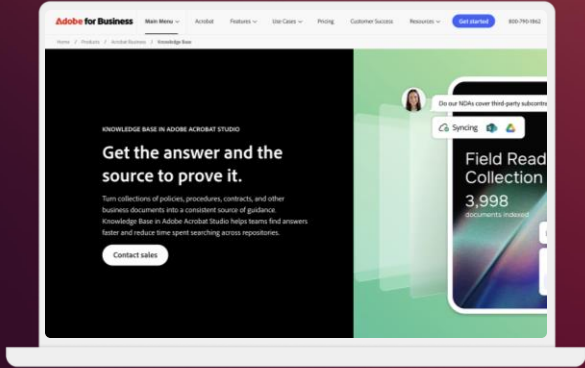


Resources

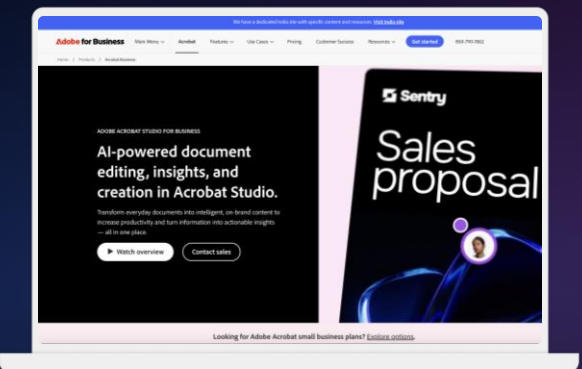
Adobe Trust Center



Knowledge Base in Adobe Acrobat Studio



Adobe Acrobat Studio for Business



Security Overview: Knowledge Base in Acrobat



Adobe