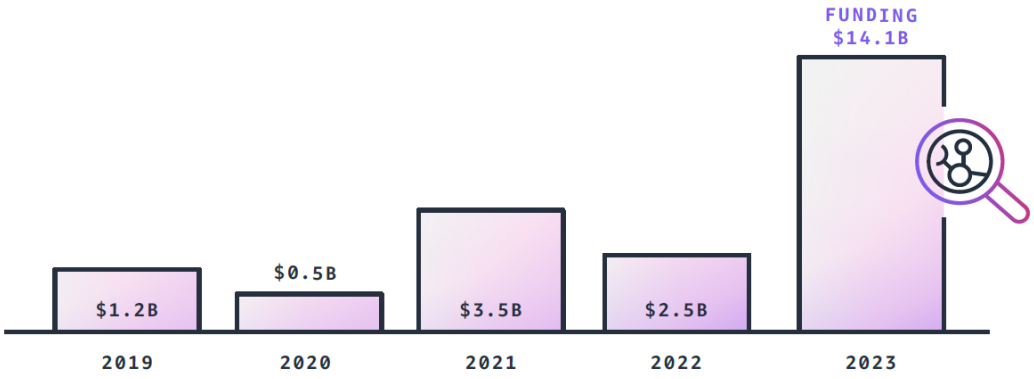
aws startups

Generative AI security: Top 4 questions startup founders should ask

With the majority of venture capital (VC) funding and big-tech investment directed to generative AI in 2023, and Goldman Sachs predicting that the technology will add $7 trillion to the global GDP in the next decade,[1] generative AI has become a cornerstone of startup success.

But, questions about generative AI security can leave some startup founders feeling lost in space. In this infographic, we address those questions and concerns—so your startup can confidently pursue its biggest generative AI ideas.

Investor interest in generative AI market soared in 2023

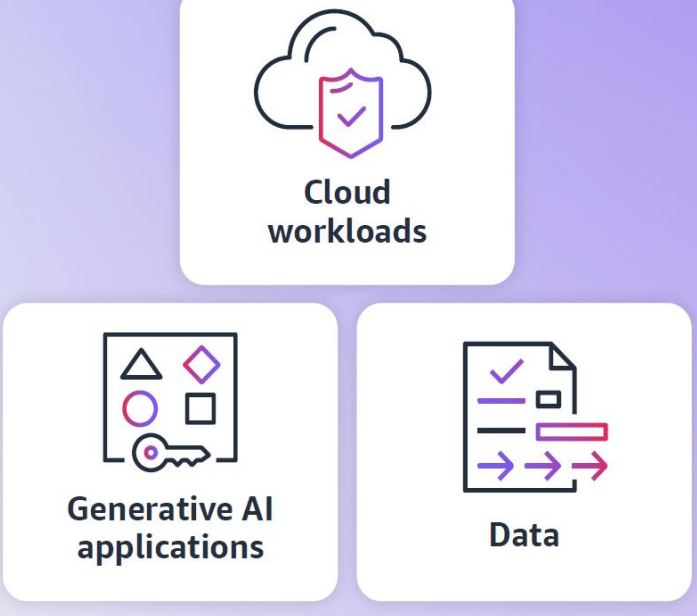


2023 was a record year for investment in generative AI startups. The total value of funding quadrupled between 2022 and Q2 2023, fueled by fewer, larger deals.[2]

QUESTION 1

What do you need to protect?

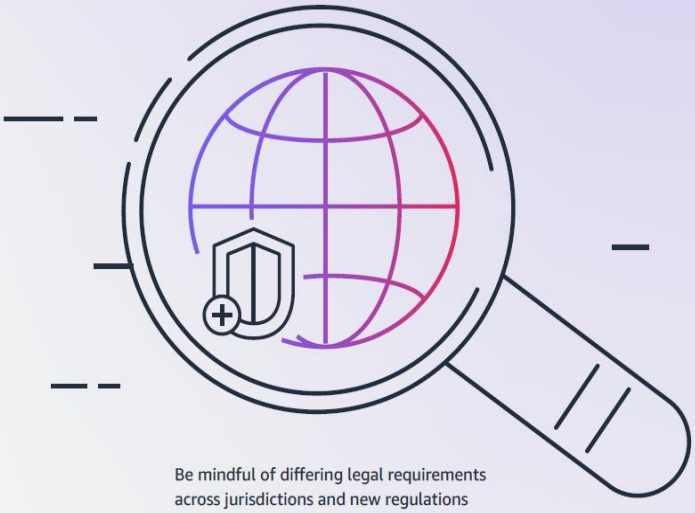
Generative AI security involves protection across three key areas:



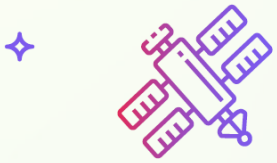
QUESTION 2

How do you maintain regulatory compliance?

The first and most important step is to engage your legal advisors. This may involve vetting your legal rights to use specific data and models and determining the applicability of laws around privacy, biometrics, antidiscrimination, and other use case-specific regulations.



Be mindful of differing legal requirements across jurisdictions and new regulations proposed around the world.



QUESTION 3

How do you ensure your models perform as intended?

Startups can use **Amazon Bedrock** to create foundation models (FMs), which are highly accurate, private, and secure. Start with one of many industry-leading FMs—then fine-tune it to your specific use case. You can even use your unlabeled datasets to customize the FM for your domain or industry. Amazon Bedrock creates a private, customized copy of the base FM for you, and none of your data is used to train the original models.

OTHER WAYS TO HELP IMPROVE MODEL PERFORMANCE AND REDUCE RISK INCLUDE:

Responsible AI policies

Consider how AI will affect your users, customers, and employees.

LEARN MORE ›

Guardrails

Add guardrail models to identify and filter toxicity.

LEARN MORE ›

Model disgorgement

Practice "machine unlearning" to remove bias or sensitive data.

LEARN MORE ›

Model sharding

Break large models into sub-models to train on specific data.

LEARN MORE ›

Content moderation

Combine automation and human review to block harmful content.

LEARN MORE ›

Explainability and auditability

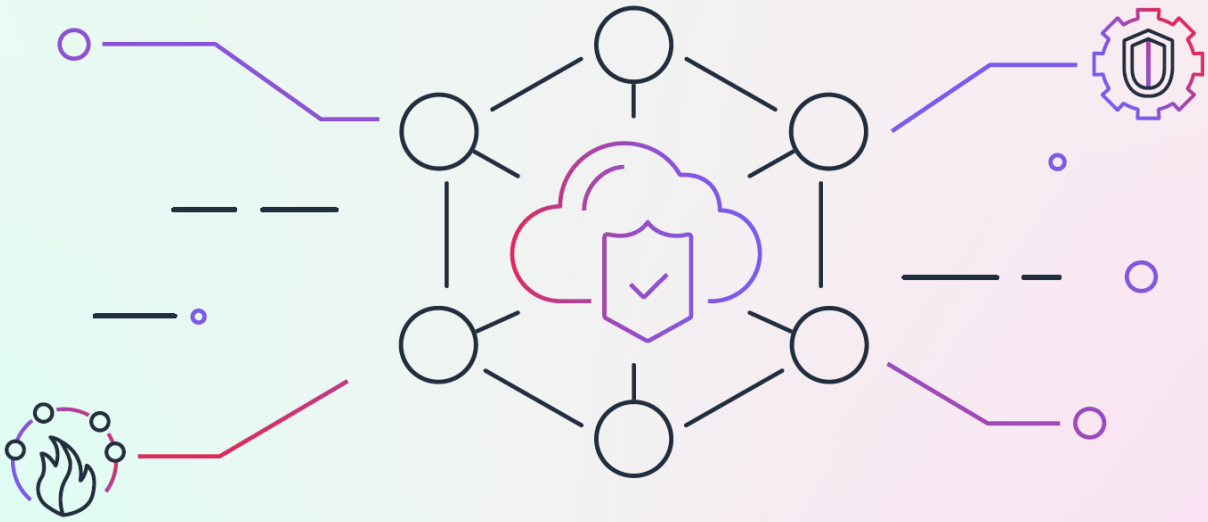
Establish a traceable record and document everything you do.

LEARN MORE ›

QUESTION 4

Where should you start?

Working with the right partners and tools can make your path to generative AI security much clearer. Amazon Web Services (AWS) is architected to be the world's **most secure cloud computing environment**, offering many security features at the hardware level and as services. Plus, Amazon Bedrock helps keep your data and applications secure and private as you fine-tune and customize FMs for generative AI.



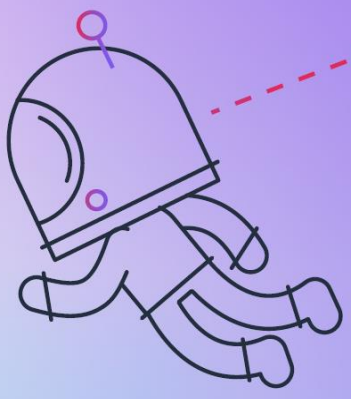
AWS OFFERS
300+ CLOUD SECURITY TOOLS AND FEATURES

aws startups

Deploy generative AI securely

AWS can provide the deep insights and specific guidance your startup needs to innovate beyond limits with generative AI—all while helping to protect your data, your customers, and your business.

- **Learn more about generative AI for startups ›**
- **Get started quickly with Amazon Bedrock ›**
- **Elevate your cloud security ›**
- **Build responsible AI ›**



[1] "Generative AI could raise global GDP by 7%," Goldman Sachs, April 2023

[2] "The state of generative AI in 7 charts," CB Insights, August 2023