



How AWS is Securing the Future of Generative AI

Generative AI is fueling massive organizational growth

The rapid growth of generative artificial intelligence (AI) has been top of mind for most organizations across the globe with widespread adoption—with 100+ million people in the US on track to use Gen AI barely two months after the release of ChatGPT¹. That's more than 2x the number of smartphone and tablet users, respectively.² Significantly, 56% of workers are also already using generative AI on the job.³



The challenges of the generative AI security landscape

As with all new technologies, the growth and adoption of generative AI has outpaced its guardrails.

71% of senior IT leaders feel generative AI will introduce new security risks

There has been a minimal increase in organizations' mitigation of AI-related risks **1-4%**⁴

51% of workers are either unaware of a generative AI policy or don't have one in their organization

How to approach generative AI security

Organizations are already aware of this challenge with 92% of companies planning to use AI to power their security efforts. However, compounding the challenges around lack of generative AI security policies and compliance framework is the fact that it requires a multi-pronged approach to address successfully.

Amazon Web Services (AWS) has developed a comprehensive generative AI security strategy, resting on three key pillars:



1 Secure generative AI

2 Secure against generative AI

3 Develop generative AI for security

SECURE GENERATIVE AI

AWS can help your organization to protect its data and intellectual property



Build generative AI apps securely



Amazon Bedrock



Fine-tune machine learning models securely



Amazon SageMaker Jumpstart



As few as

20

labeled examples are sufficient to fine-tune FMs securely with Amazon Bedrock

SECURE AGAINST GENERATIVE AI-BASED THREATS

Deploy end-to-end security with 300+ cloud security services from AWS



Discover and protect sensitive data



Amazon Macie



Protect network traffic



AWS Network Firewall



Security groups in Amazon VPCs



100,000+

customers use AWS for ML

DEVELOP GENERATIVE AI FOR SECURITY

Enhance your security with generative AI-powered services



Detect security alerts and automate threat responses



Amazon GuardDuty



Finding Groups in Amazon Detective



Scan for vulnerabilities to generate more secure code



Amazon CodeWhisperer



Developers using Amazon CodeWhisperer were

57%

faster than those who did not use it

The future of generative AI is secure—with AWS

[Download the ebook to learn more >](#)

1. Reuters, "ChatGPT sets record for fastest-growing user base", 2023.
2. Insider Intelligence, 2023.
3. The Conference Board, September 2023.
4. McKinsey, "The state of AI in 2022—and a half decade in review", December 2022.
5. Mimecast, "The State of Email Security", 2023.