

How AWS is Securing the Future of Generative Al

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% general new se

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

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.

Organizations are already aware of this challenge with

generative AI security strategy, resting on three key pillars:

Amazon Web Services (AWS) has developed a comprehensive



- Secure generative AI
- 2 Secure against generative AI
 - Develop generative AI for security

SECURE GENERATIVE AI

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



apps securely

Build generative AI



Amazon Bedrock

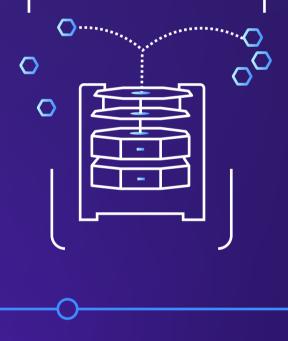


models securely

Fine-tune machine learning



Amazon SageMaker Jumpstart



labeled examples are sufficient to fine-tune

As few as

FMs securely with Amazon Bedrock

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

SECURE AGAINST GENERATIVE AI-BASED THREATS

Discover and protect sensitive data





AWS Network Firewall

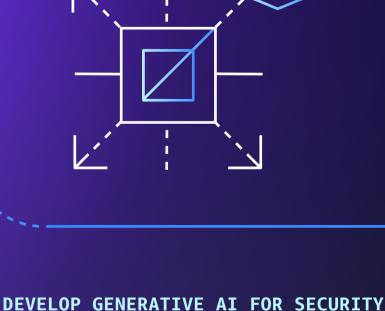
Amazon Macie



Protect network traffic



Security groups in Amazon VPCs



for ML

customers use AWS

generative Al-powered services

Enhance your security with

Detect security alerts and automate threat responses



Scan for vulnerabilities to



Finding Groups in Amazon Detective

Amazon GuardDuty



generate more secure code



Developers using Amazon

CodeWhisperer were

Amazon CodeWhisperer

faster than those who did not use it

-----: ------:

The future of generative AI is secure—with AWS

Download the ebook to learn more >

- Reuters, "ChatGPT sets record for fastest-growing user base", 2023.
- Insider Intelligence, <u>2023</u>.
 The Conference Board, <u>September 2023</u>.
 McKinsey, "The state of Al in 2022—and a half decad

4. McKinsey, "The state of AI in 2022—and a half decade in review", <u>December 2022</u>.
5. Mimecast, "The State of Email Security", <u>2023</u>.
© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.