

# AWS re:Inforce

JUNE 10 - 12, 2024 | PHILADELPHIA, PA

CFS224

# Amazon Q Developer: Securing your code

## Ron Ledwich

Business Leader, AI Dev Experiences  
AWS Partner COE  
AWS

## Mikhail Shapirov

Principal Solutions Architect, AI Dev  
Experiences, AWS Partner COE  
AWS



# Generative AI stack

## APPLICATIONS THAT LEVERAGE LLMs AND OTHER FMs



Amazon Q  
Business



Amazon Q  
Developer



Amazon Q in  
QuickSight



Amazon Q in  
Connect/Supply Chain

## TOOLS TO BUILD WITH LLMs AND OTHER FMs



Amazon Bedrock

Guardrails

Agents

Customization Capabilities

## INFRASTRUCTURE FOR FM TRAINING AND INFERENCE



GPUs



AWS  
Trainium



AWS  
Inferentia



Amazon SageMaker



Amazon EC2  
UltraClusters



EFA



EC2 Capacity Blocks  
for ML



AWS Nitro  
System



AWS Neuron

# Generative AI stack

## APPLICATIONS THAT LEVERAGE LLMs AND OTHER FMs



Amazon Q  
Business



Amazon Q  
Developer



Amazon Q in  
QuickSight



Amazon Q in  
Connect/Supply Chain

## TOOLS TO BUILD WITH LLMs AND OTHER FMs



Amazon Bedrock

Guardrails

Agents

Customization Capabilities

## INFRASTRUCTURE FOR FM TRAINING AND INFERENCE



GPUs



AWS  
Trainium



AWS  
Inferentia



Amazon SageMaker



Amazon EC2  
UltraClusters



EFA



EC2 Capacity Blocks  
for ML



AWS Nitro  
System



AWS Neuron



# Amazon Q Developer



Reimagines the experience across the entire software development lifecycle (SDLC)

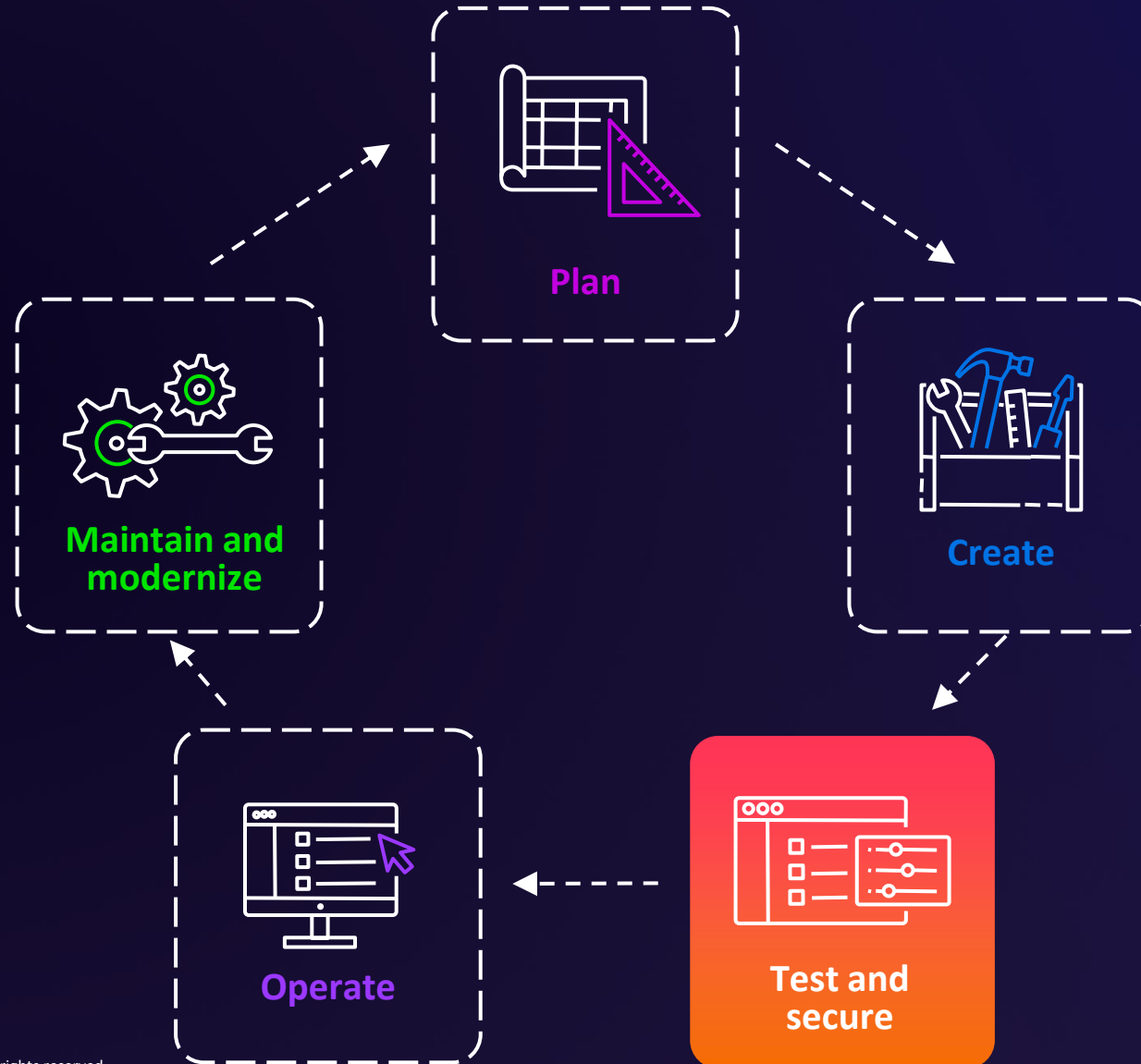
Helps developers and IT professionals build and manage secure, scalable, and highly available applications

Helps you write, debug, test, optimize, and upgrade your code faster

Converses with you to explore new AWS capabilities, learn unfamiliar technologies, and architect solutions

**Amazon Q is built with security and privacy in mind from the start, making it easier for organizations to use generative AI safely**

# Amazon Q supports developers across the SDLC



# Do you know where your code is coming from?

Third-party reference code

Developer forums

Sample projects

Open-source libraries

Package managers



# What types of issues are out there?

Inadvertent resource disclosures

SQL injection

Cross-site scripting

Hardcoded passwords

Database connection strings

Service misconfiguration

Unprotected service endpoints






# Security scanning capabilities





Scan generated and developer-written code to detect security issues

Receive issue remediation suggestions

Scan for hard-to-find security issues

Supports VS Code and JetBrains IDEs for multiple programming languages

 **Security scan completed. 3 issues found.**

 lambda_function.py	user/projects/lambda_function.py
	Not setting the S3 bucket owner condition might introduce a risk of accidentally using a wrong bucket. For example, a configuration error lead to accidentally writing production data into test accounts. [Line 150]
	The elevated privilege level required to perform operations should be immediately after the operation is performed. [Line 160]
	Recreating AWS clients from scratch in each Lambda function invocation is expensive and can lead to availability risks. Clients should be cached across invocations. [Line 190]

# Behind the scenes

POWERED BY AMAZON CODEGURU

## Amazon CodeGuru **Detector Library**

Trained on decades of knowledge and experience across millions of code reviews

Java

 Python

 JavaScript

 TypeScript

 C#

 CloudFormation

 Terraform

 Go

 Ruby

 C

 C++

 PHP

[docs.aws.amazon.com/codeguru/detector-library](https://docs.aws.amazon.com/codeguru/detector-library)

eks-blueprints

EXPLORER

lib

addons

efs-csi-driver

eks-pod-identity-agent

emr-on-eks

external-dns

external-secrets

falco

fluxcd

gpu-operator

grafana-operator

helm-addon

istio-addons

jupyterhub

karpenter

iam.ts

index.ts

keda

index.ts

knative-operator

kube-proxy

kube-state-metrics

kuberay

kubevious

metrics-server

nested-stack

neuron

nginx

opa-gatekeeper

prometheus-node-exporter

OUTLINE

TIMELINE

lib > addons > keda > TS index.ts > KedaAddOn > deploy

68

export class KedaAddOn extends HelmAddOn {

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

...readonly options: KedaAddOnProps;

...constructor(props?: KedaAddOnProps) {

...super({...defaultProps, ...props});

...this.options = this.props as KedaAddOnProps;

...}

...deploy(clusterInfo: ClusterInfo): Promise<Construct> {

...const cluster = clusterInfo.cluster;

...let values: Values = populateValues(this.options);

...values = merge(values, this.props.values ?? {});

...if (this.options.irsaRoles!.length > 0) {

...//Create Service Account with IRSA

...const opts = { name: this.options.kedaOperatorName, namespace: this.options.namespace };

...const sa = cluster.addServiceAccount(this.options.kedaServiceAccountName!, opts);

...setRoles(sa, this.options.irsaRoles!);

...const namespace = createNamespace(this.options.namespace!, cluster);

...sa.node.addDependency(namespace);

...const chart = this.addHelmChart(clusterInfo, values);

...chart.node.addDependency(sa);

...return Promise.resolve(chart);

...} else {

...//Let Keda Create Service account for you. This is controlled by flag helmOptions.createServiceAccount (refe

...const chart = this.addHelmChart(clusterInfo, values);

...return Promise.resolve(chart);

...}

...}

...}

.../\*\*

> ClusterLogg

Aa ab \*

No results

↑ ↓ ≡ ×

bugfix/997\*

1 ↓ 0 ↑

0 0 3 214

0

✓ AWS: IAM Identity Center (d-9a6718f479)

▶ Amazon Q

Ln 95, Col 14

Spaces: 2

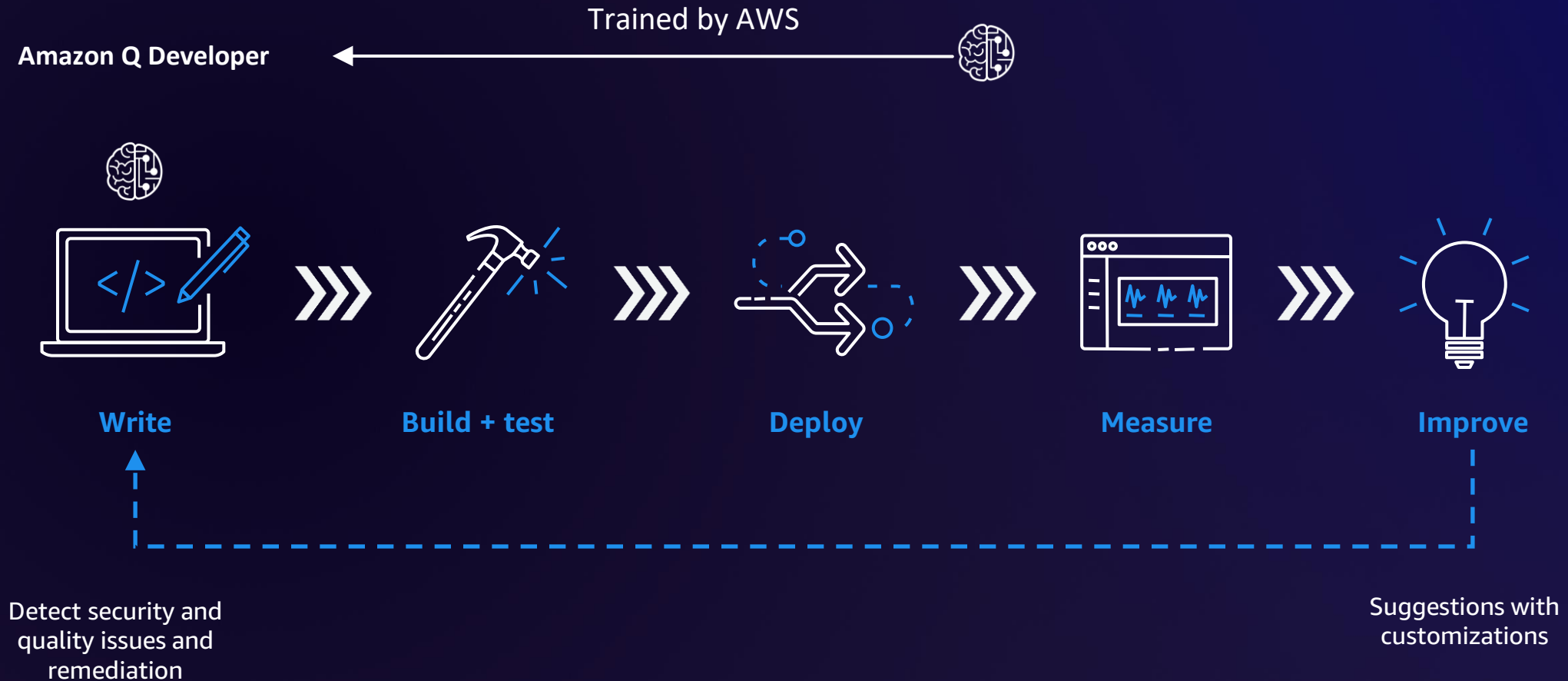
UTF-8

CRLF

{ } TypeScript

22 Spell

# Amazon Q Developer in your software workflow



# What are we scanning

Resource	Auto scans	Project scans
Maximum input artifact size	200 KB	500 MB
Maximum source code size	200 KB	50 MB

# Supported programming languages

	Detection	Automatic code fix
Java – Java 17 and earlier	✓	✓
JavaScript – ECMAScript 2021 and earlier	✓	✓
Python – Python 3.11 and earlier (Python 3)	✓	✓
C# – All versions (.Net 6.0 and later recommended)	✓	✓
TypeScript – All versions	✓	✓
Ruby – Ruby 2.7 and 3.2	✓	
Go – Go 1.18	✓	
Infrastructure as Code		
AWS CloudFormation	✓	✓
Terraform – 1.6.2 and earlier	✓	✓
AWS CDK – TypeScript and Python	✓	*

# Amazon Q Developer security scanning

SERVICE LIMITS · [AWS.AMAZON.COM/Q/DEVELOPER/PRICING](https://aws.amazon.com/q/developer/pricing)

# 50

Security scans per month

**Amazon Q Developer Free Tier**

Free

# 500

Security scans per month  
Automatic scanning included

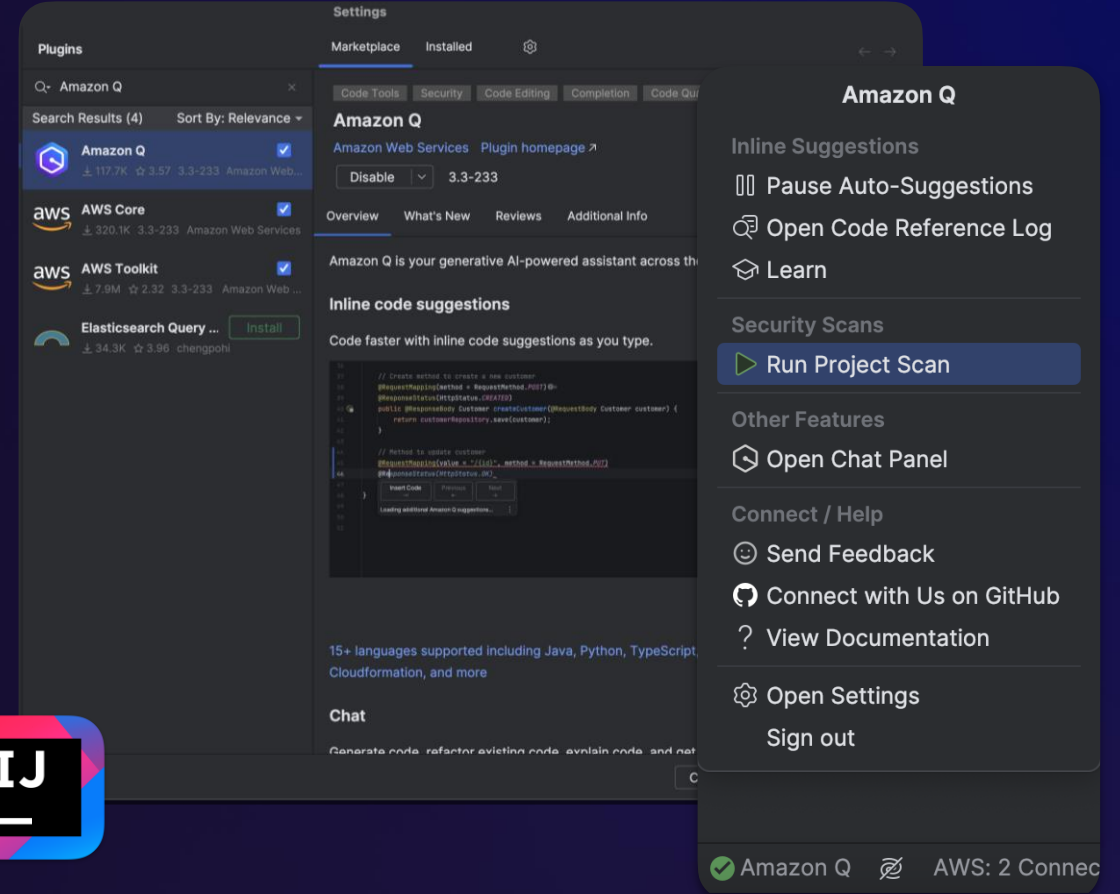
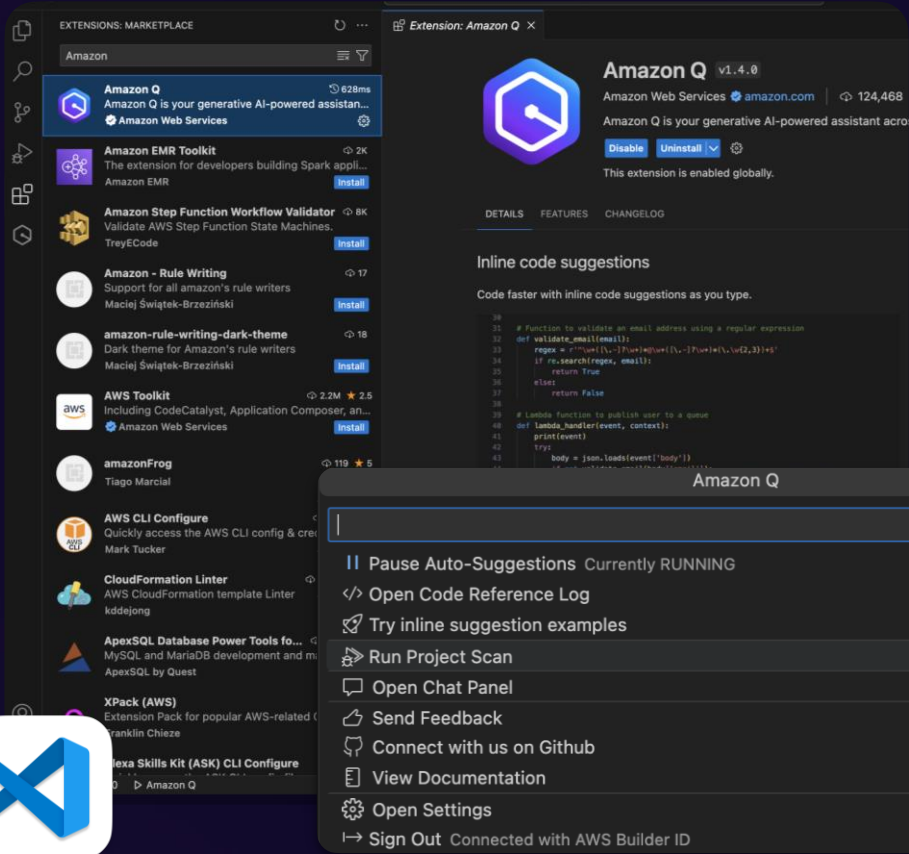
**Amazon Q Developer Pro Tier**

\$19/mo. per user





# Get started today with Amazon Q IDE plugins



Install Amazon Q plugin in VS Code or IntelliJ  
Try out for **free** using AWS Builder ID  
Click **Run Project Scan** to invoke security scanning

