
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC217

Detecting vulnerabilities in AWS Lambda functions using Amazon Inspector

Rick Anthony
General Manager, Amazon Inspector
Amazon Web Services (AWS)

Kashish Wadhwa
Principal Product Manager, Amazon Inspector
Amazon Web Services (AWS)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- What is Amazon Inspector?
- What customer problems does Amazon Inspector solve?
- How Amazon Inspector works
- Security for serverless functions
- What’s new?
- Demo
- Q&A

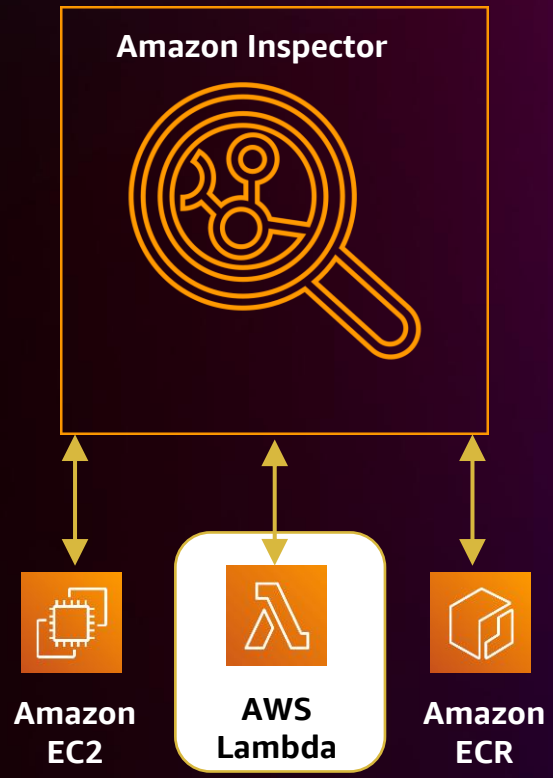
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Inspector: Continual vulnerability management at scale

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Amazon Inspector?

Amazon Inspector is an automated vulnerability management service that **continually** scans workloads for software vulnerabilities and unintended network exposure

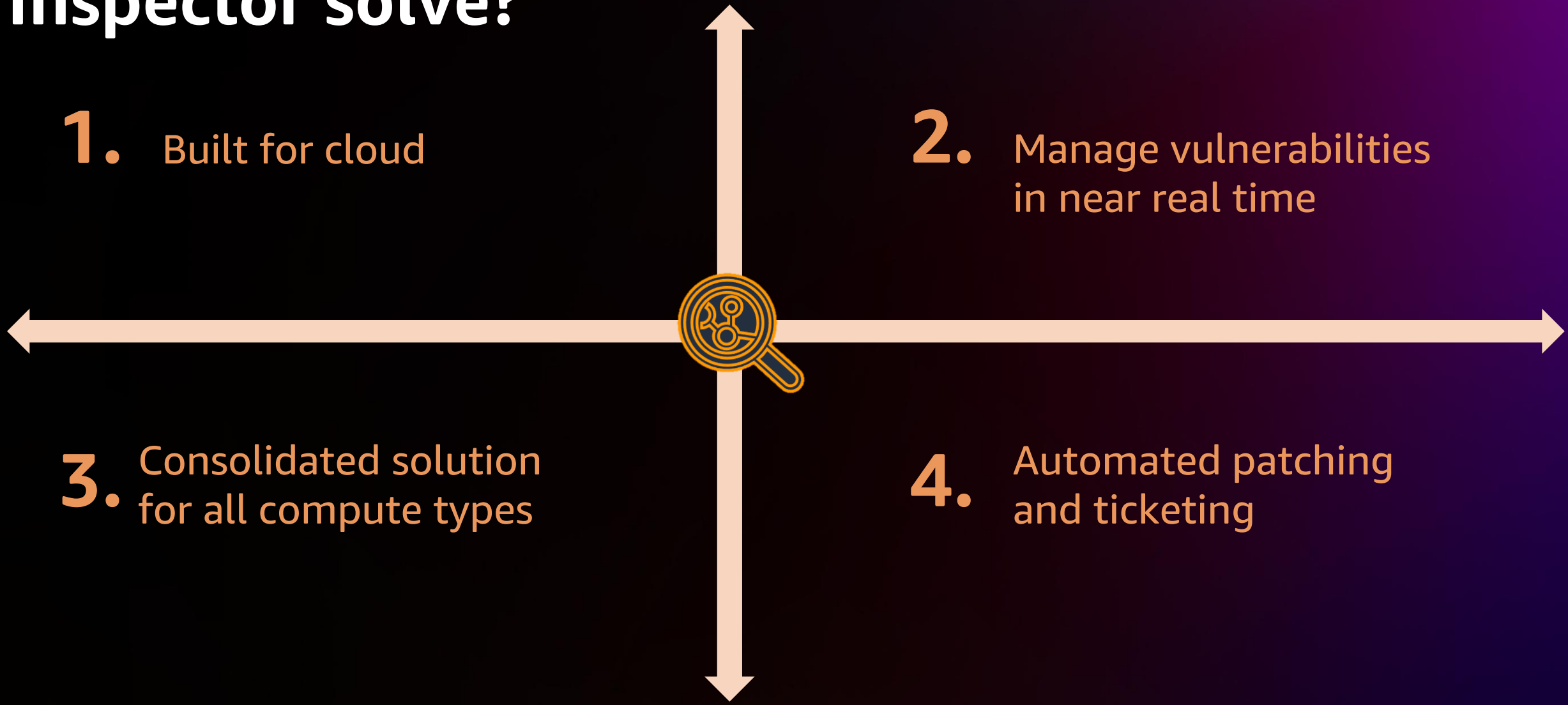


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What customer problems does Amazon Inspector solve?

1. Built for cloud

2. Manage vulnerabilities in near real time



3. Consolidated solution for all compute types

4. Automated patching and ticketing

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How Amazon Inspector works



Frictionless activation and management



Continual vulnerability monitoring



Prioritized and contextualized results

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How Amazon Inspector works

1. Frictionless activation and management

- ✓ One-click activation
- ✓ Integration with AWS Organizations
- ✓ Auto-activation of new accounts
- ✓ Security by default with simple organization level configuration
- ✓ Centralized view for the administrator account, while individual accounts can view their account-specific information

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How Amazon Inspector works

2. Continual vulnerability monitoring

- ✓ Automated discovery of all resources
- ✓ Findings in real time through continual vulnerability and network reachability scanning
- ✓ Intelligent algorithm determines what to scan, when to scan, or how often to scan based on event triggers:
  - ✓ A new software package is installed
  - ✓ An instance is patched
  - ✓ A new CVE is published that impacts resources

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

**The shortened time between when a vulnerability is disclosed and when it is exploited in the wild—a 71% drop over 2020 – Rapid7 report*

How Amazon Inspector works

3. **Prioritized and contextualized results**

- ✓ Amazon Inspector risk score is calculated for each finding by correlating CVE metadata with the customer's environmental factors such as:
  - ✓ Network exposure of an instance
  - ✓ Exploitability details
  - ✓ Potential security threats
- ✓ Remediation details with fixed-in package details
- ✓ Exploitability information with last known exploitation date

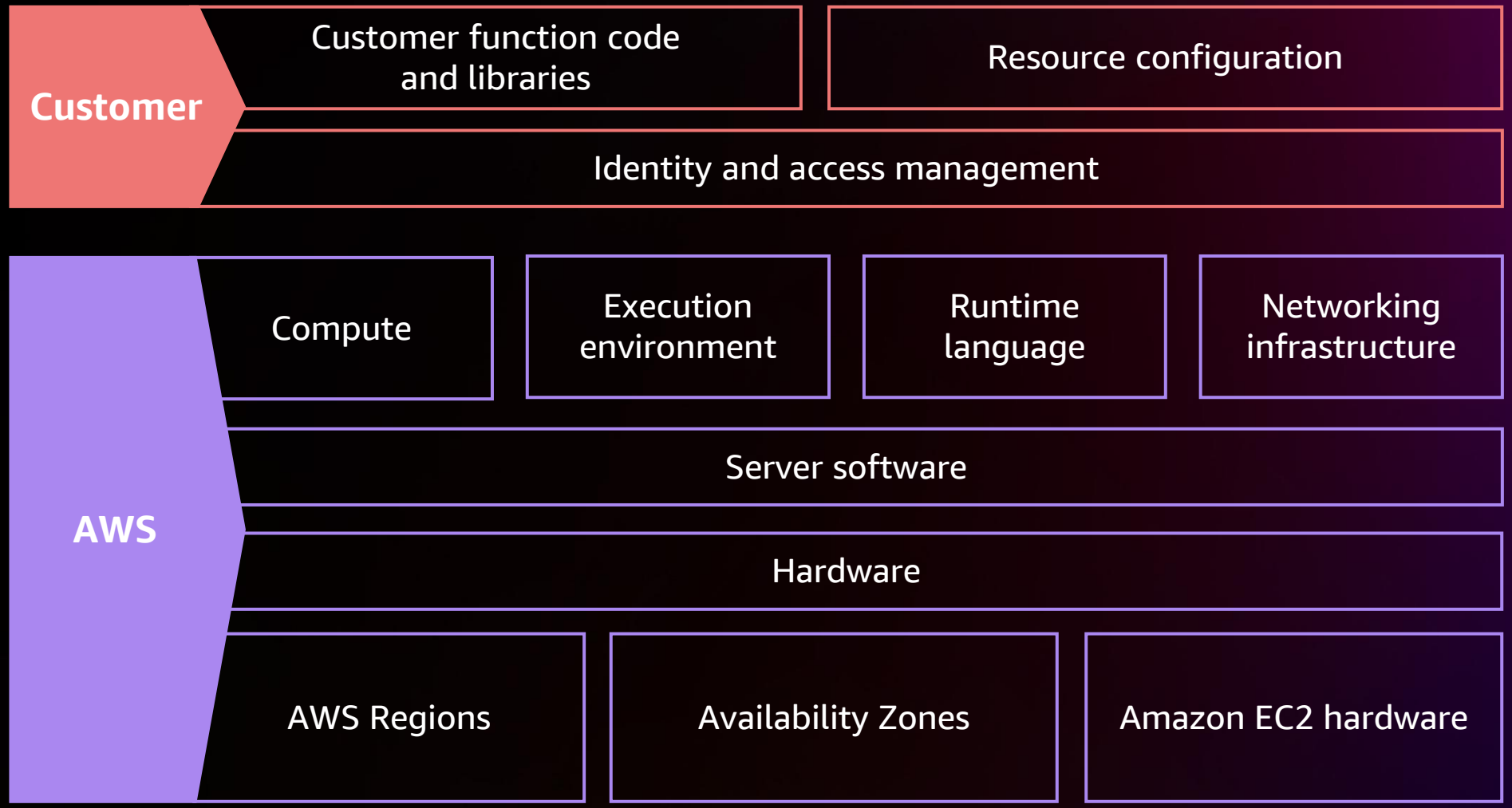
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security for serverless functions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model for serverless functions



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What’s new?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Added support for Lambda functions

With this expanded capability, Amazon Inspector now identifies software vulnerabilities (CVEs) in application package dependencies used in the Lambda function code and associated layers

Simplified one-click activation and multi-account support with AWS Organizations

Automated discovery and continuous monitoring of all functions

- ✓Automated discovery upon deployment
- ✓Continuous scanning based on
  - ✓Updates to the function
  - ✓New CVEs being published
- ✓No agents needed

Easy prioritization and remediation with exploitability and fixed-in package details

Automation through integration with Amazon EventBridge



A single pane of glass for vulnerabilities across all resources

- ✓ Lambda functions
- ✓ Amazon EC2 instances
- ✓ Container images in Amazon ECR

Note: Automated exclusion of stale functions that have not been invoked in 90 days plus manual tag-based exclusion available

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pricing for Lambda scanning

Priced **per Lambda function per month (prorated by hour of Amazon Inspector coverage)**: **$0.30 per function per month** in US East (N. Virginia) Region

*Amazon Inspector coverage hours are a defined time duration from when a function is discovered to the time when it's deleted or excluded from scanning

Pricing example:
You enter a new billing month for your US East (N. Virginia) Region with 20 Lambda functions deployed. Amazon Inspector charges in US East (N. Virginia) would be calculated as follows:

- 10 Lambda functions scanned for all 30 days at $0.30 per function = $3.00
- 10 Lambda functions scanned for only 15 days (i.e., deleted after 15 days) at $0.30 per function = $1.50
- There is no additional charge for rescanning
- For the month, your Amazon Inspector bill would be $4.50

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Important blogs and other useful resources

1. Manage container deployment: go.aws/3gsV0W7

2. Automating vulnerability management and patching using Amazon Inspector and AWS Systems Manager Patch Manager
   Part 1: go.aws/3EUaMT7
   Part 2: go.aws/3GH7cNv

3. Introducing the new Amazon Inspector: go.aws/3ECa1wR

Other blogs and demo videos: go.aws/3i9QzQa

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Rick Anthony
linkedin.com/in/rick-anthony

Kashish Wadhwa
linkedin.com/in/kashishwadhwa

Learn more at
aws.amazon.com/inspector

Start with a free 15-day trial:
console.aws.amazon.com/inspector



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.