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

PRT276

SPONSORED BY TREND MICRO

Simplify and accelerate security for simple storage: Case studies

Mike Milner (he/him)

VP Cloud Technology
Trend Micro

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

Agenda

- Benefits of Amazon Simple Storage Service (Amazon S3)
- AWS shared responsibility model for Amazon S3 security
- Challenges: Implementing security
- Customer use cases & architecture examples
- Closing & questions

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

Amazon S3



- Durable
- Simple
- Low cost
- Extendable

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

Durable storage

- 99.999999999% (11 9s)
- Amazon S3 Replication
- S3 Versioning
- S3 Object Lock



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

Low cost

- $0.023/GB per month

  (first 50 TB, S3 Standard, based on US East [Ohio] Region)
- $0.15/GB at launch in 2006
- Higher volume tiers
- S3 Standard-Infrequent Access
- S3 Glacier Flexible Retrieval
- https://aws.amazon.com/s3/pricing/



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

Simple

Object storage



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

AWS shared responsibility Model

CUSTOMER

Responsible for security **IN** the cloud

CUSTOMER DATA		
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT		
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION		
CLIENT-SIDE DATE ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

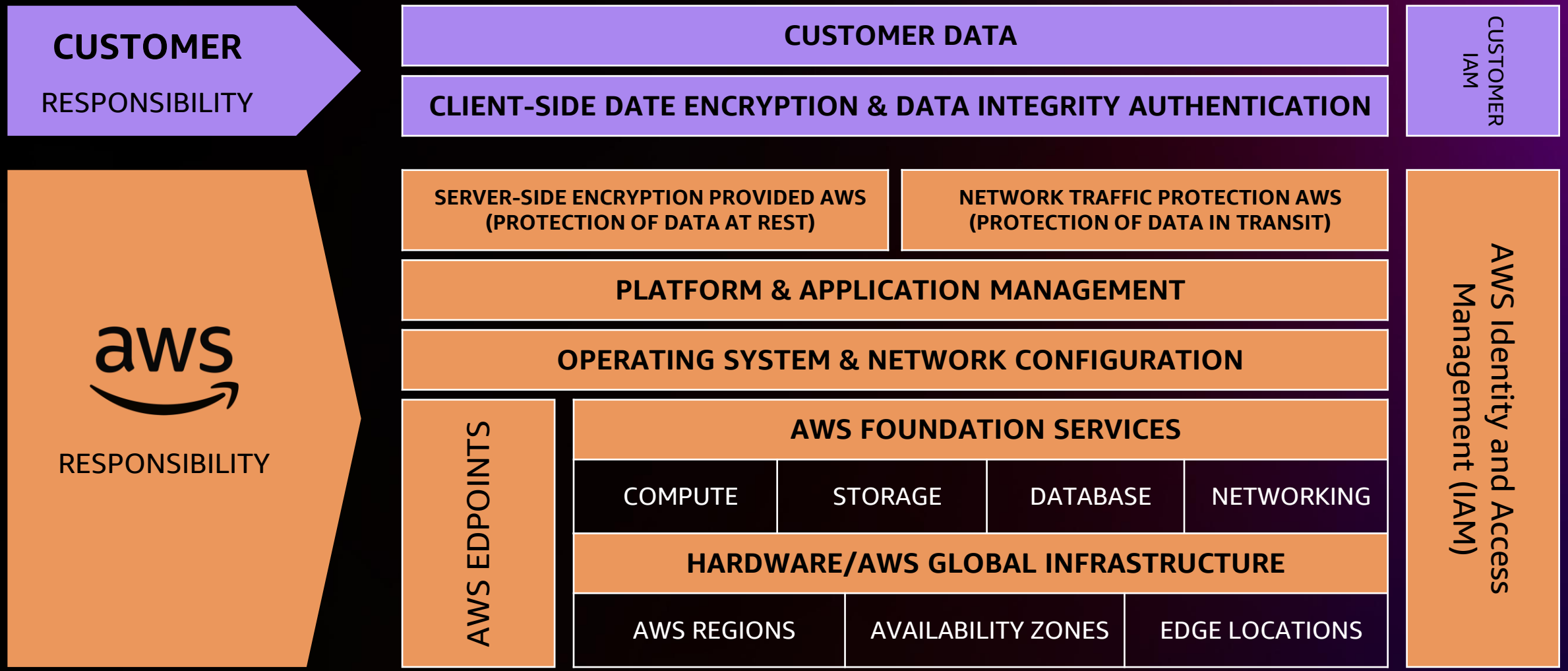


Responsible for security **OF** the cloud

SOFTWARE			
COMPUTE	STORAGE	DATABASE	NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE			
AWS REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS	

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

Shared responsibility model for Amazon S3



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

Common requirements for securing S3

01	02	03	04	05	06
DEFINE the least-privileged access to the bucket and continuously review those permissions across all the buckets	**ENABLE** encryption and data recovery to help meet compliance requirements	**DEFINE** tags for better labelling, collecting & organizing resources available within your AWS environment	**ENABLE** S3 Block Public Access for buckets that should never be public	**ENSURE** the logging access is activated to track access requests	**VALIDATE** information being stored is safe and does not contain malicious code like malware or ransomware

aws

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

Questions to ask yourself

- How can we audit and validate that these security policies and controls have been implemented?
- Do users have visibility when changes occur that would violate a policy or compliance mandate?
- How can our development teams be aligned with our architects' policies?
- How do we introduce scanning of malicious content without affecting the current workflow's performance or availability?

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

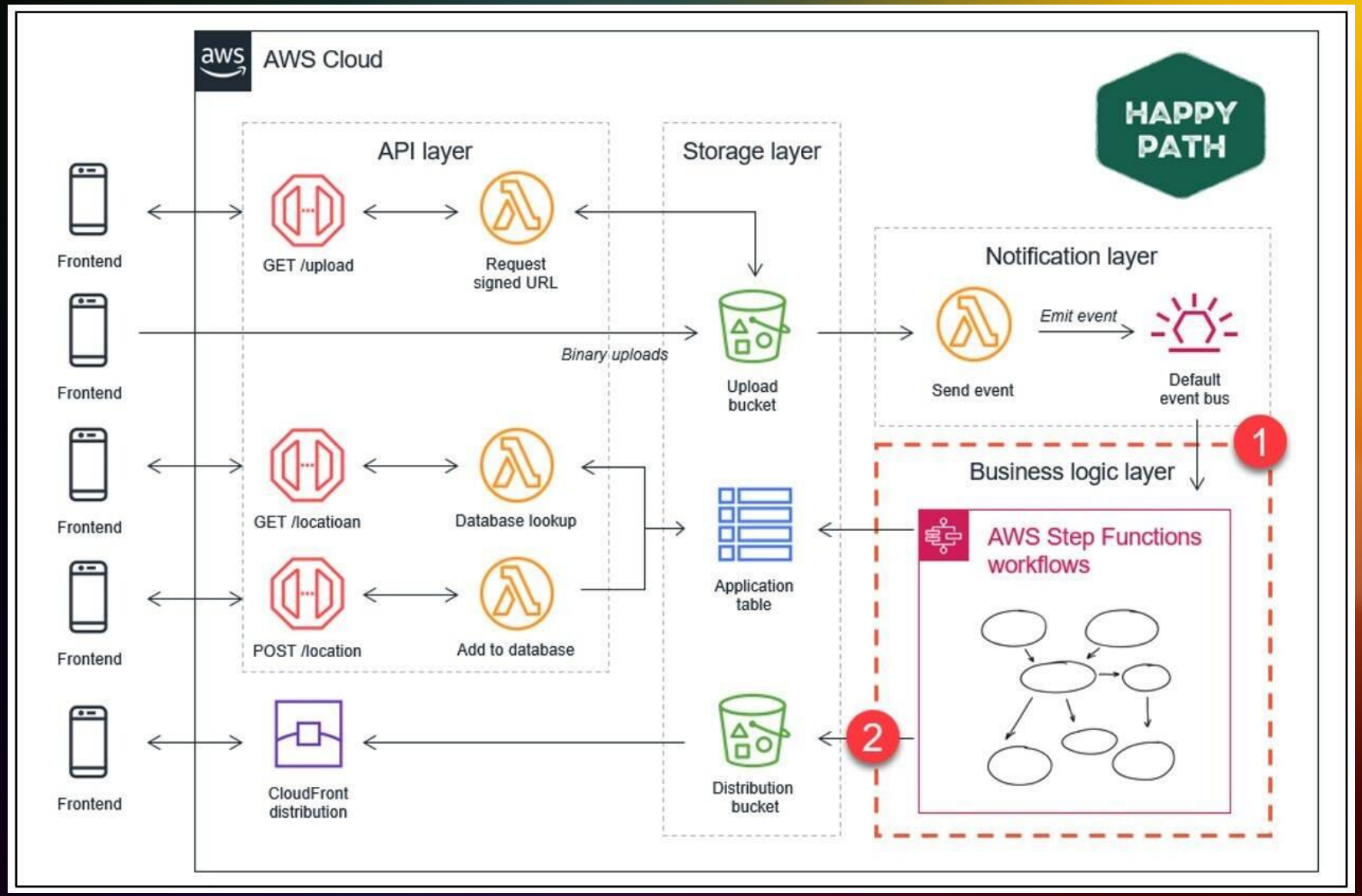
Shift left, swipe right

- Automate the visibility of misconfigurations with a cloud security posture management (CSPM) tool
- Choose a tool that embraces **shift-left** security, allowing developers to integrate into their infrastructure-as-code workflows with AWS CloudFormation templates
- Remediate issues early in the pipeline – this saves time and money and reduces risk to the business

aws

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

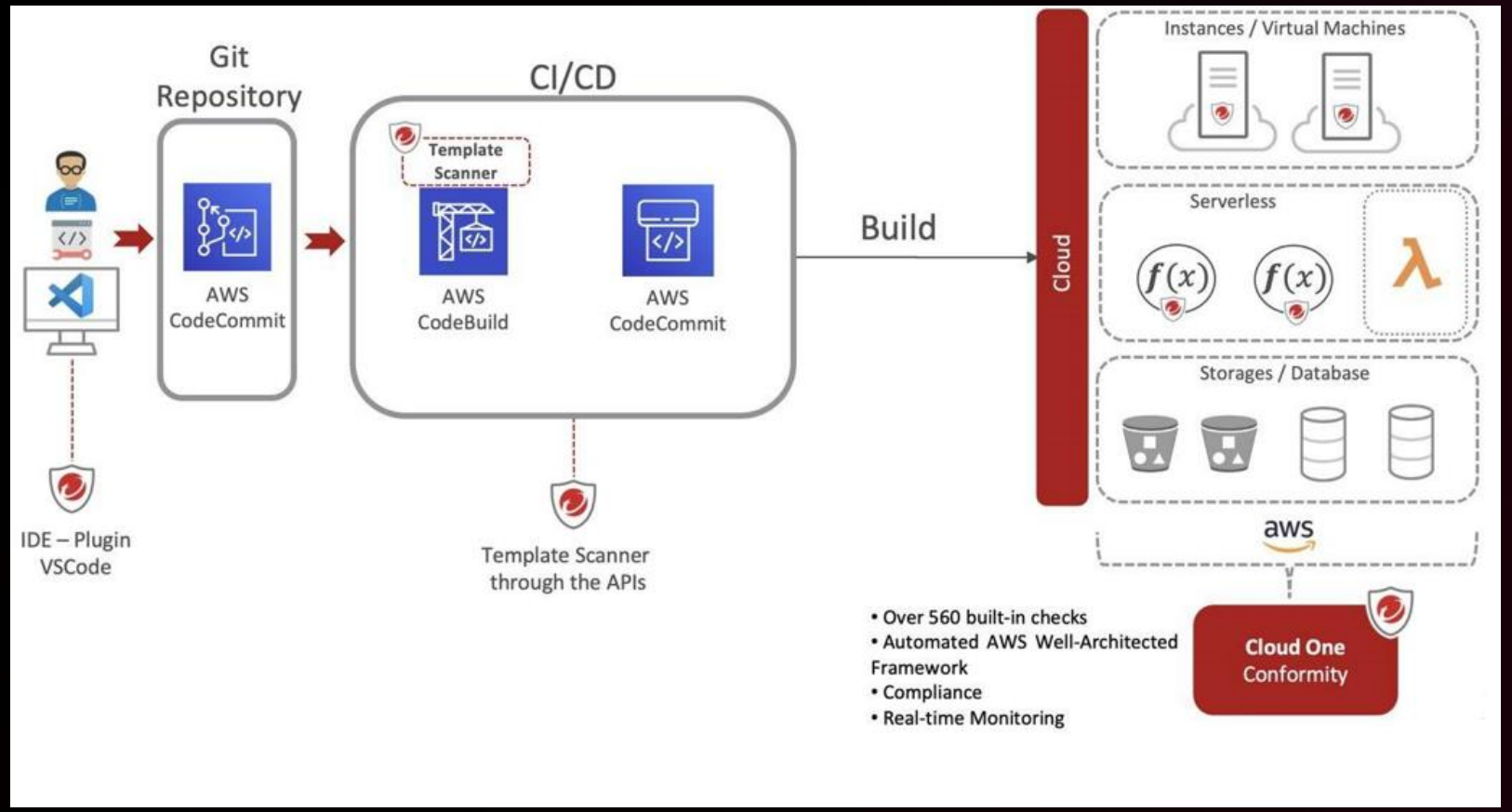
Happy Path architecture



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

Gaining visibility into misconfigurations

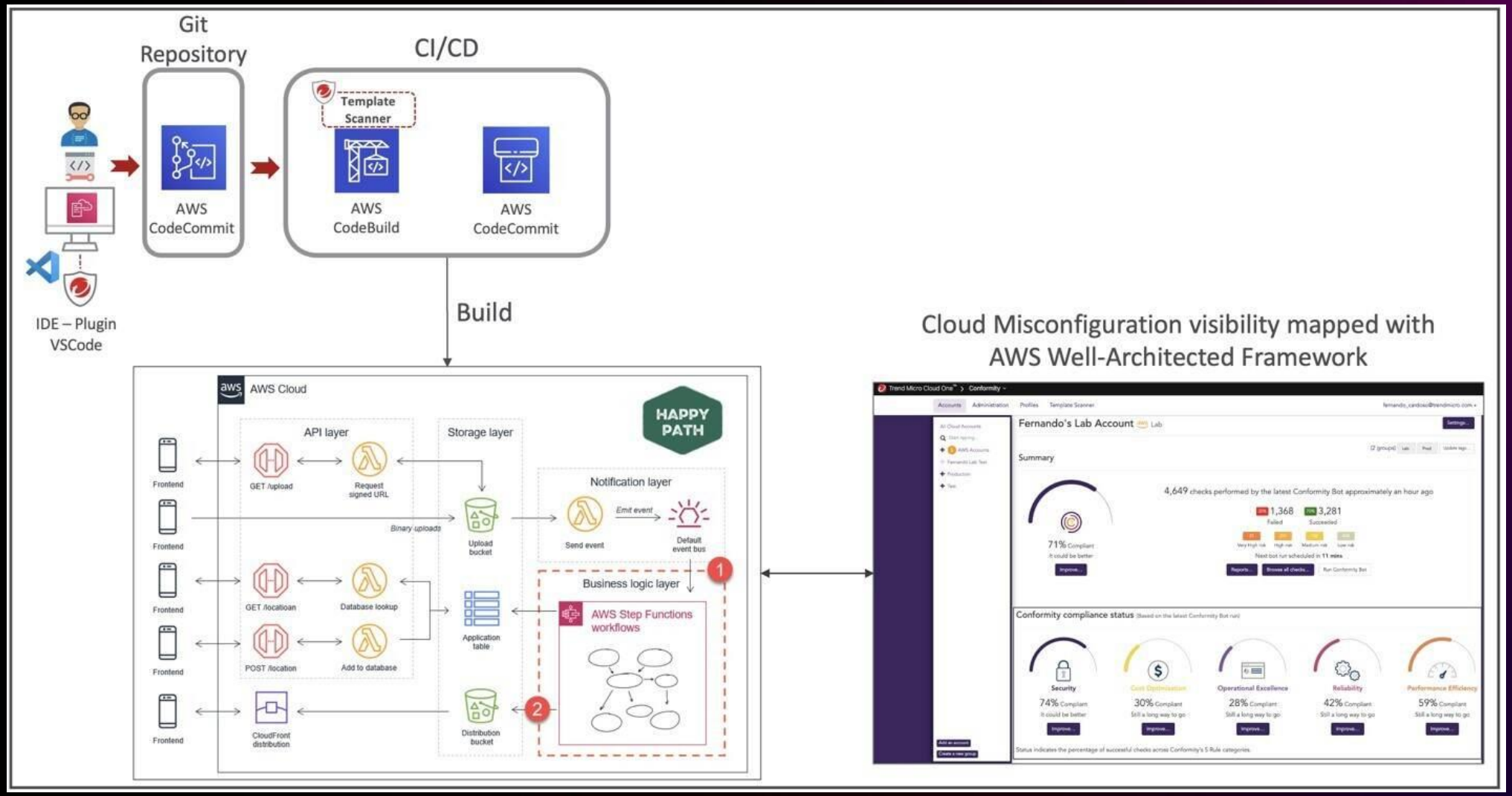
INFRASTRUCTURE AS CODE: PIPELINE AS SECURITY



- Check your resources against compliance mandates, including
  - PCI DSS
  - HIPAA
  - HITRUST
  - NIST 800-53
  - AWS Well-Architected Framework
- Integrate into your AWS CodeBuild pipeline to automate and remediate findings

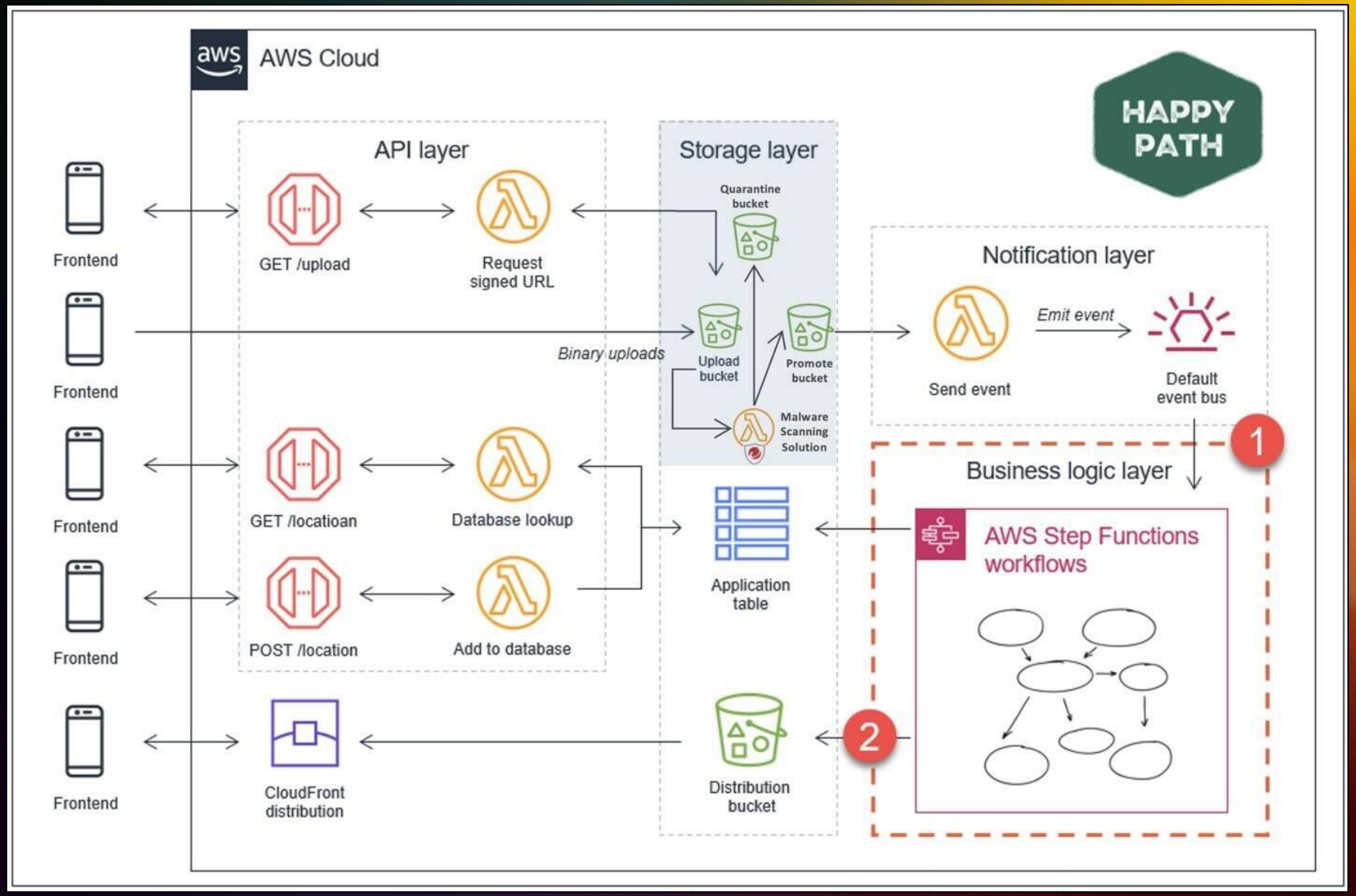
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing security to the Happy Path build



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

Happy Path architecture with content scanning



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

Downsides of scanning with infrastructure

- Files need to be transferred onto Amazon EC2 instances for scanning
- Maintenance costs to operate virtual machines (patching)
- Cost of running infrastructure even when not scanning
- Performance concerns when handling large file types

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

FOX Sports: Serverless huge file scanning



Live video feeds



S3 bucket

FOX SPORTS

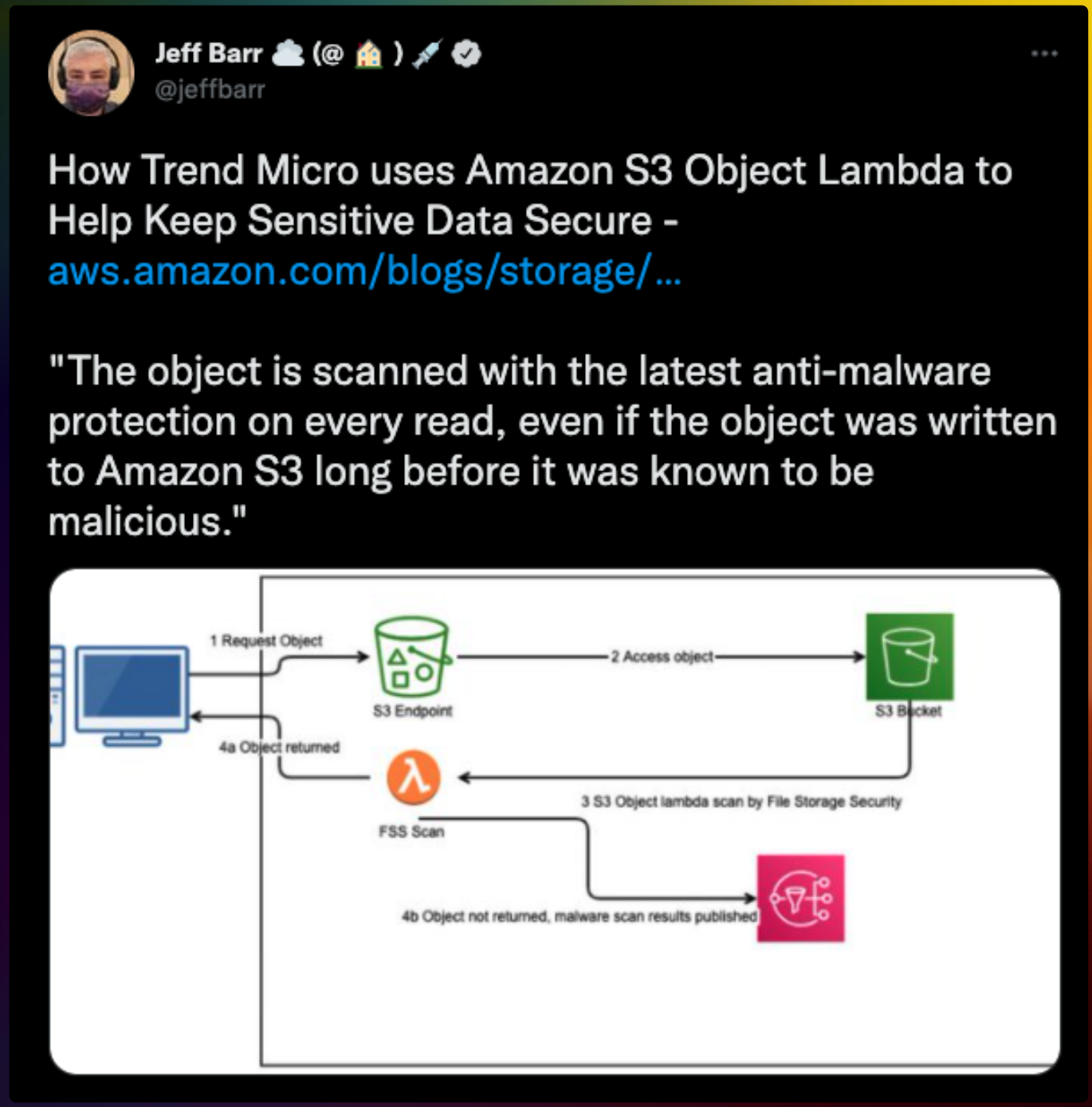
aws

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

Use case: Education

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

Cloud-native malware protection

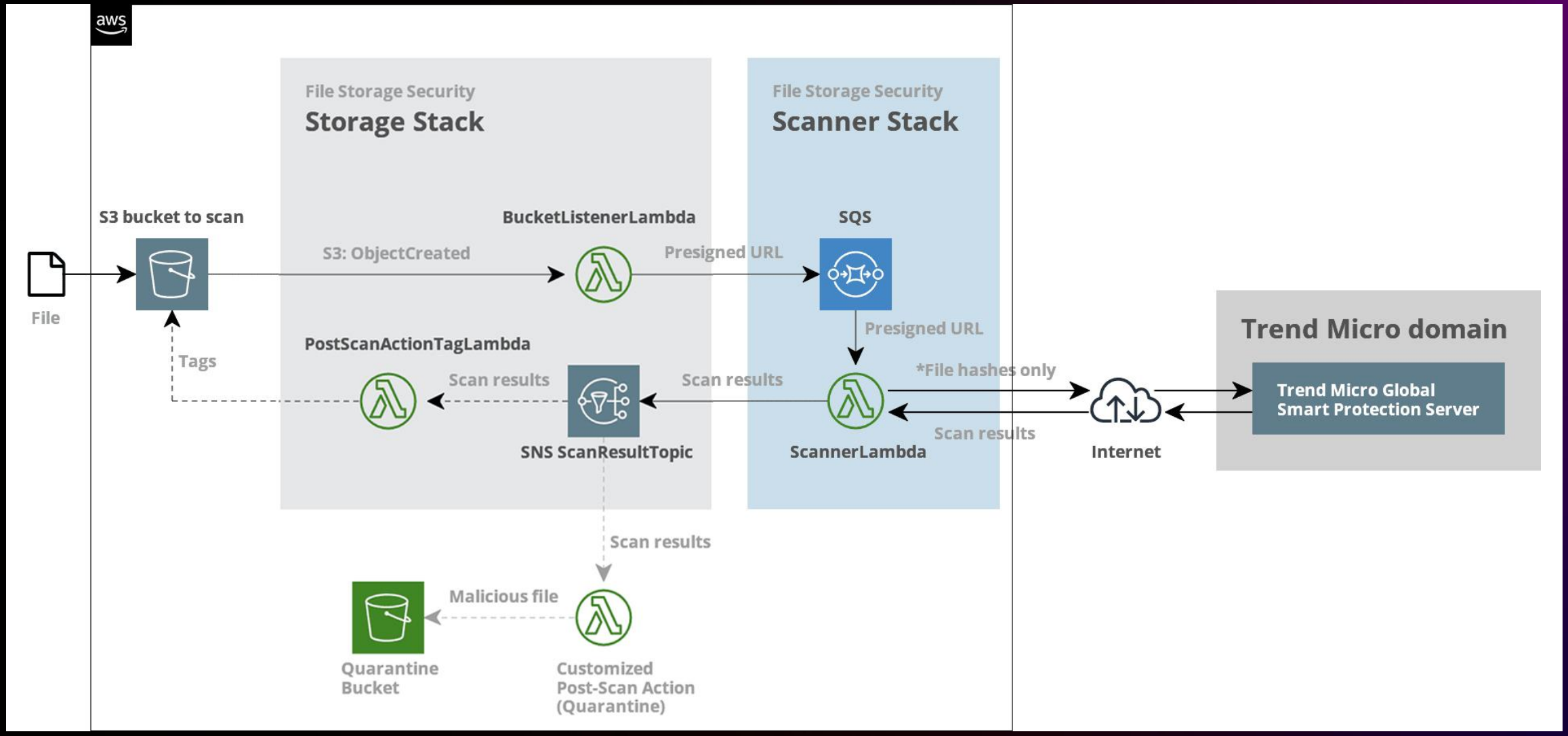


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case: Finan¢e

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

File storage security: Serverless architecture



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

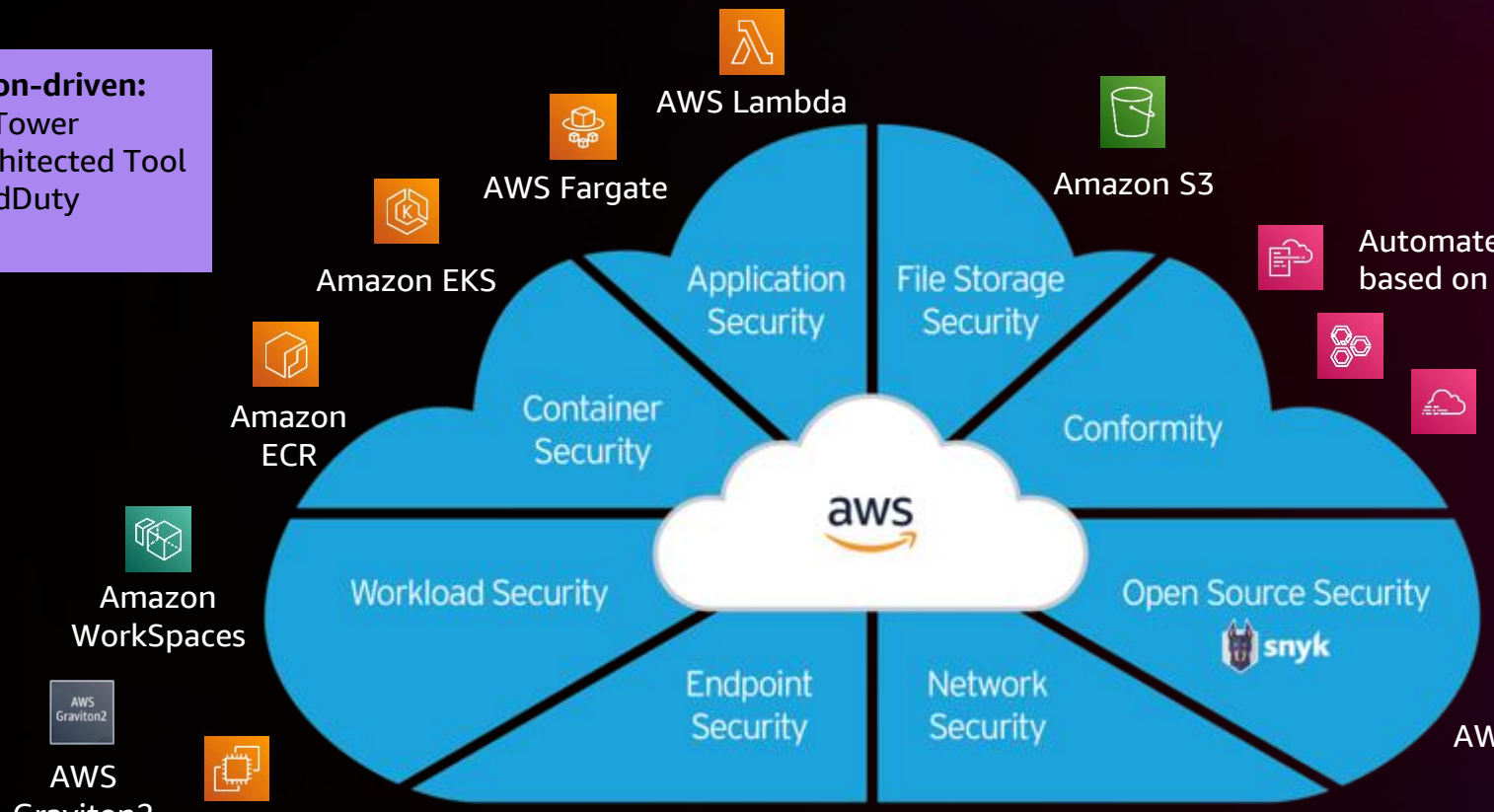
Advantages: File storage security

- Just like Amazon S3 – flexibility; any file, any size
- Performance – lowered FOX Sports scan times from many minutes to a few seconds
- Elimination of running infrastructure that requires maintenance
- Not billed when not scanning
- Scan on PUT or GET
  - Useful for web content or file repositories
  - Protect your upstream workflows and downstream customers/brand
- Integrate into your AWS services already in use, like AWS CodeBuild, AWS Security Hub, and more

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

Choose the flexible, all-in-one, security services platform built on AWS

API- and integration-driven:
- AWS Control Tower
- AWS Well-Architected Tool
- Amazon GuardDuty
- And more

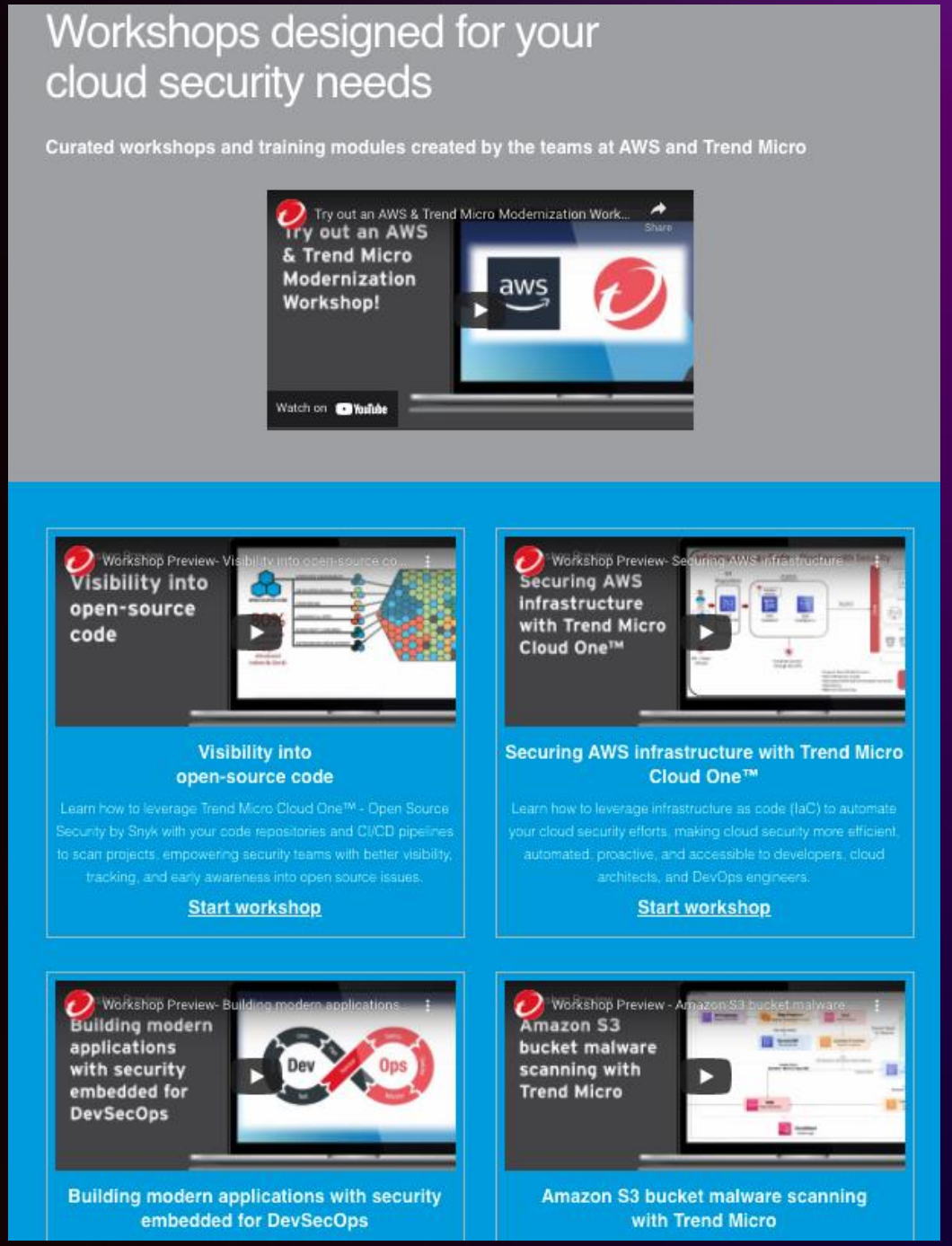


Trend Micro Cloud One

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

AWS & Trend Micro self-guided workshops

trendmicro.com/awsworkshops



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

Thank you!

Mike Milner
mike_milner@trendmicro.com
Mike Milner



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

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