AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET320

Observability with Amazon CloudFront and AWS WAF

Samrat Karak
Senior Product Manager
Amazon CloudFront

Diana Alvarado
Technical Account Manager
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Amazon CloudFront and AWS WAF overview

Need for observability at the edge

Metrics, console reports, logs (standard and real-time)

Observability examples

Q & A

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudFront: Secure, Performant, and Programmable

- Service fundamentals – **Security, Availability, Performance**
- Secure and programmable – **Edge compute**
- Self-service full control configurations and reporting – **DevOps focused**
- AWS integrations – **DevExp** and **cost-effective**

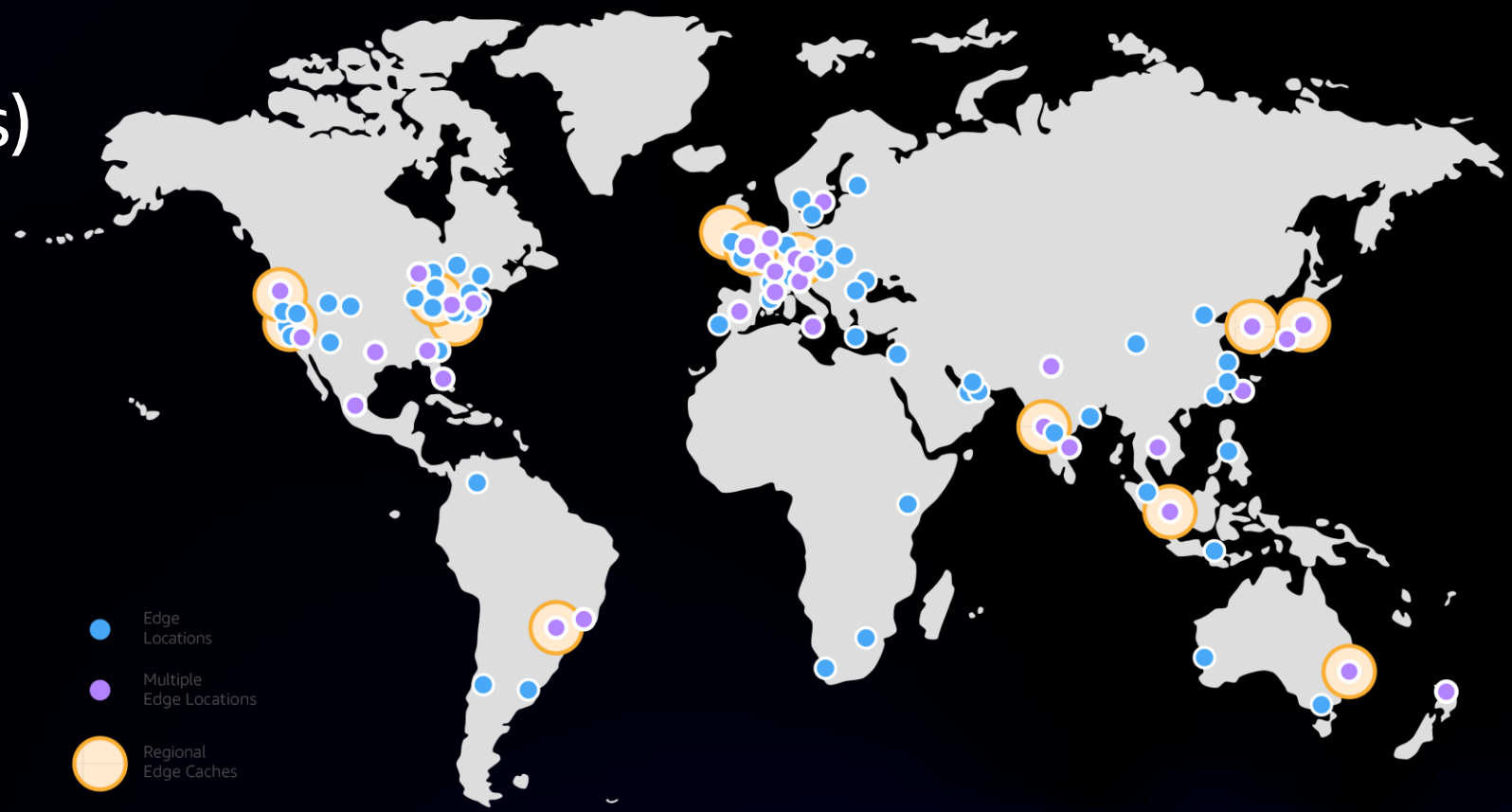
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudFront

300+ point of presence

(90+ cities in 47 countries)

Low latency, high throughput, and highly reliable AWS backbone



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protecting the application perimeter



AWS Shield Standard

Protects AWS services against common DDoS attacks



AWS WAF

Protects web applications by allowing you to write custom rules or choose managed rules from AWS or the AWS Marketplace



AWS Shield Advanced

Managed threat protection that blocks DDoS attacks, vulnerability exploitation, and bad bots

Includes **AWS WAF & AWS Firewall Manager** at no additional cost

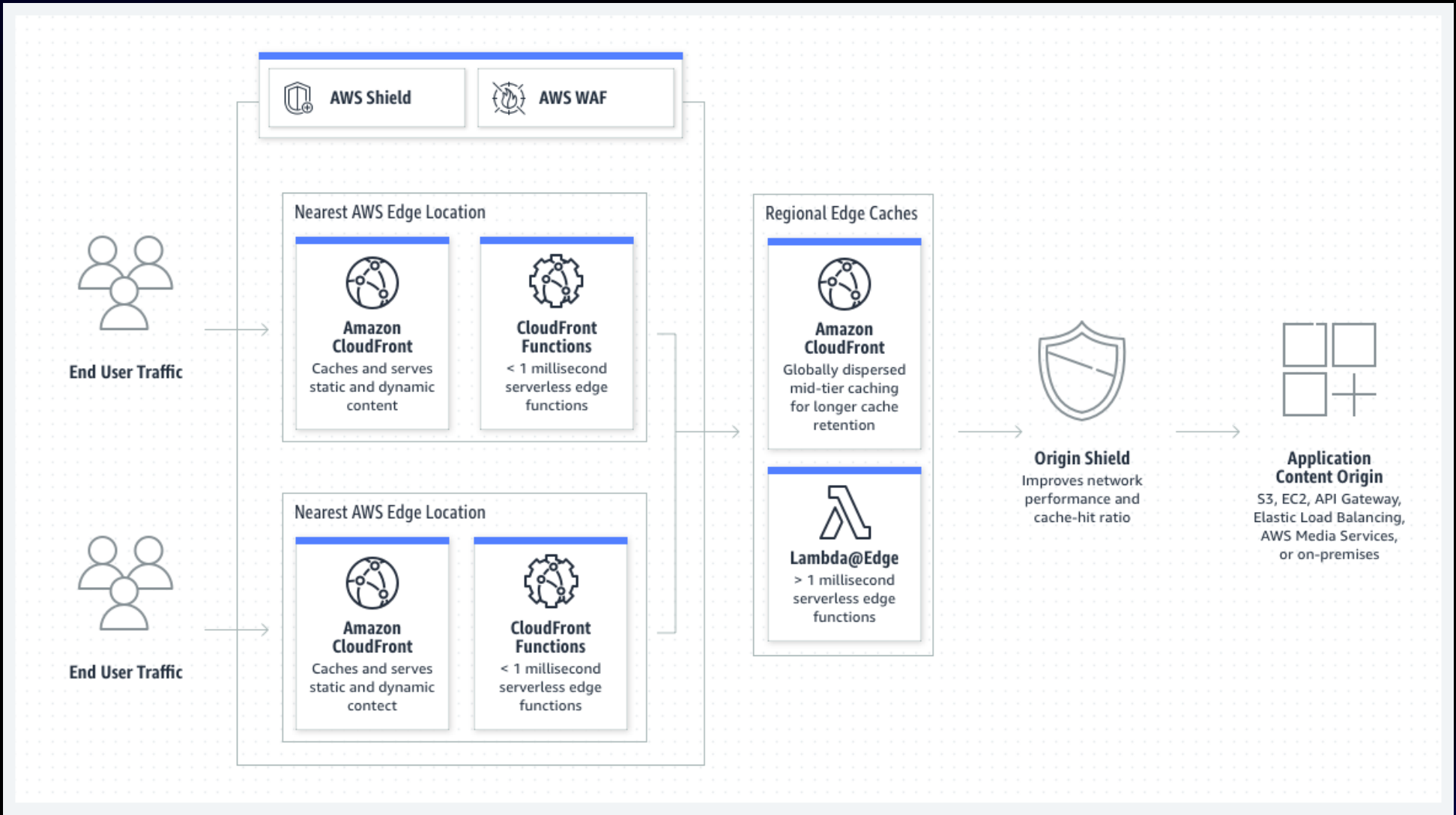


AWS Firewall Manager

Centrally configure and manage security rules across accounts and applications

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Secure application running at the edge



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What can be observed at the edge?

- Receiving requests – human/bot, legit/malicious traffic
- Responses from origin
- Cached responses (normal and error responses)
- Blocked requests (malicious patterns and high rate requests)
- Edge customized responses, WAF custom responses



Amazon CloudFront



AWS WAF

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why do you need observability?



Monitor traffic and configure alarms

- Get notification for traffic anomalies
- Metrics available in Amazon CloudWatch



Understand usage patterns

- Analyze viewer traffic or most popular objects
- Reports available in Amazon CloudFront console



Real-time dashboards

- Investigate performance in real-time
- Real-time logs in Amazon Kinesis Data Streams

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

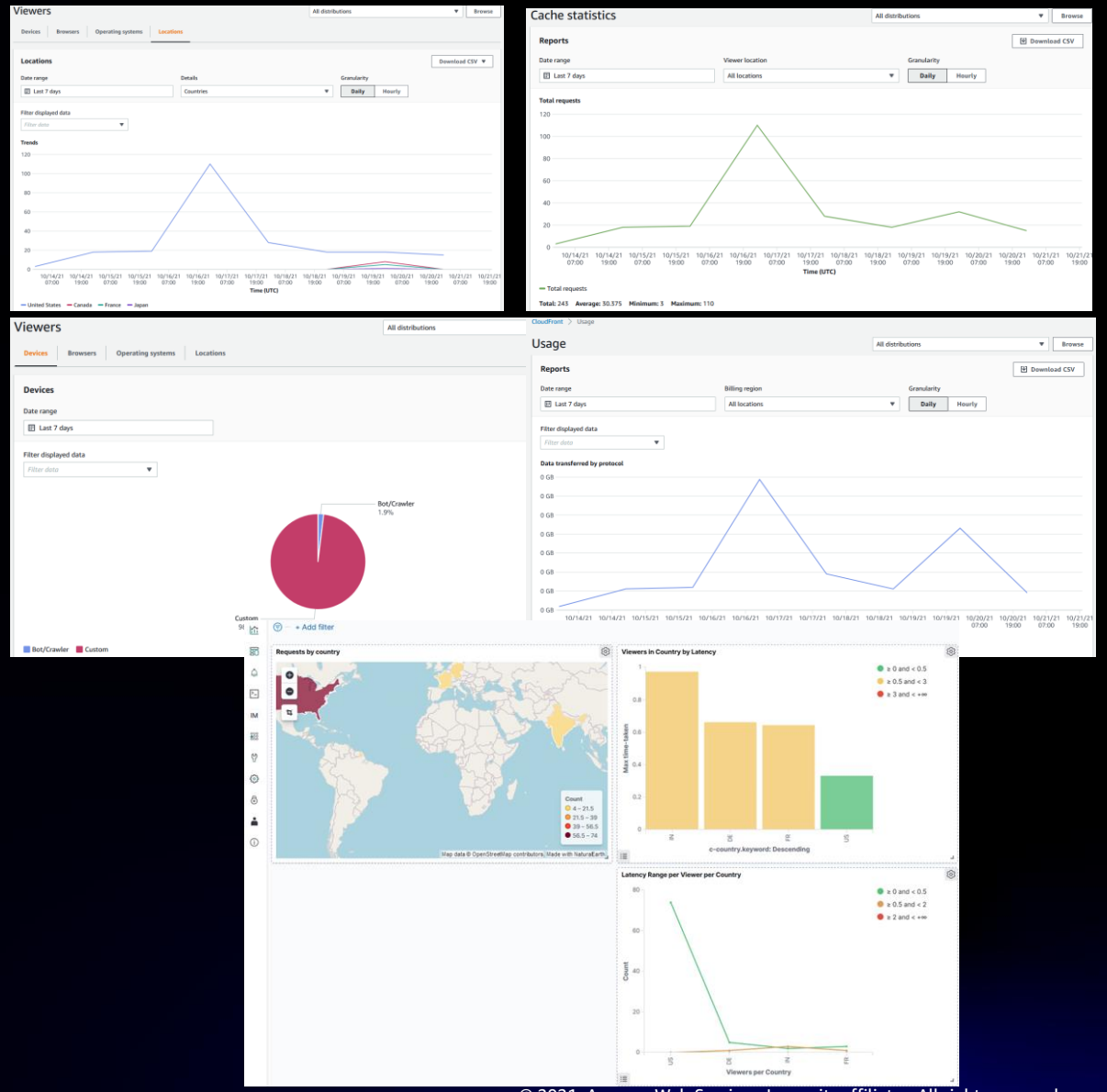
Observability on CloudFront

Metrics through AWS Management Console and CloudWatch

- Requests
- BytesDownloaded
- BytesUploaded
- TotalErrorRate
- Granular 4xx and 5xx ErrorRate
- Cache Hit Ratio
- Origin latency

Detailed access logs

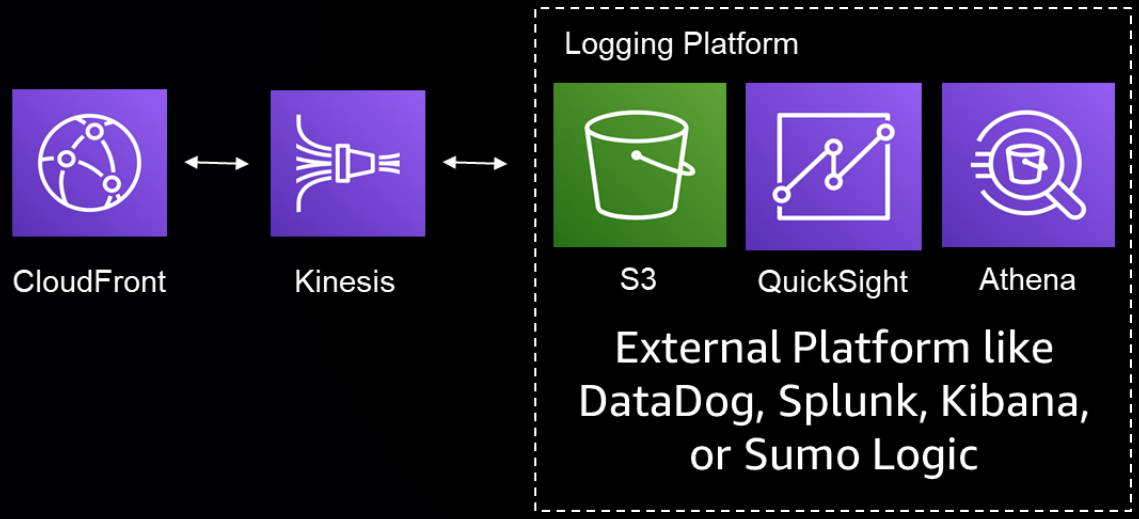
- Standard logs – delivered to S3: Optimized for completeness, 5–10 min latency
- Real-time logs
- Log connectors to various 3P – SumoLogic, DataDog, Splunk, etc
- Console logging available with L@E and CF functions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront real-time logs

- Receive logs within 10 seconds
- Ability to configure the log delivery
  - ✓ Choose log fields
  - ✓ Define sampling rates
  - ✓ Set up logging per cache behavior
- Logs delivered to a Kinesis data stream to any custom HTTP endpoint





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Observability on WAF

Web ACL metrics

- AllowedRequests
- BlockedRequests
- CountedRequests
- PassedRequests

Bot control metrics

- AllowedRequests
- BlockedRequests
- CountedRequests

Rule group and rule dimensions

- Region
- Rule
- RuleGroup
- WebACL

Bot visibility metrics

- SampledAllowedRequests
- SampledBlockedRequests

Logs

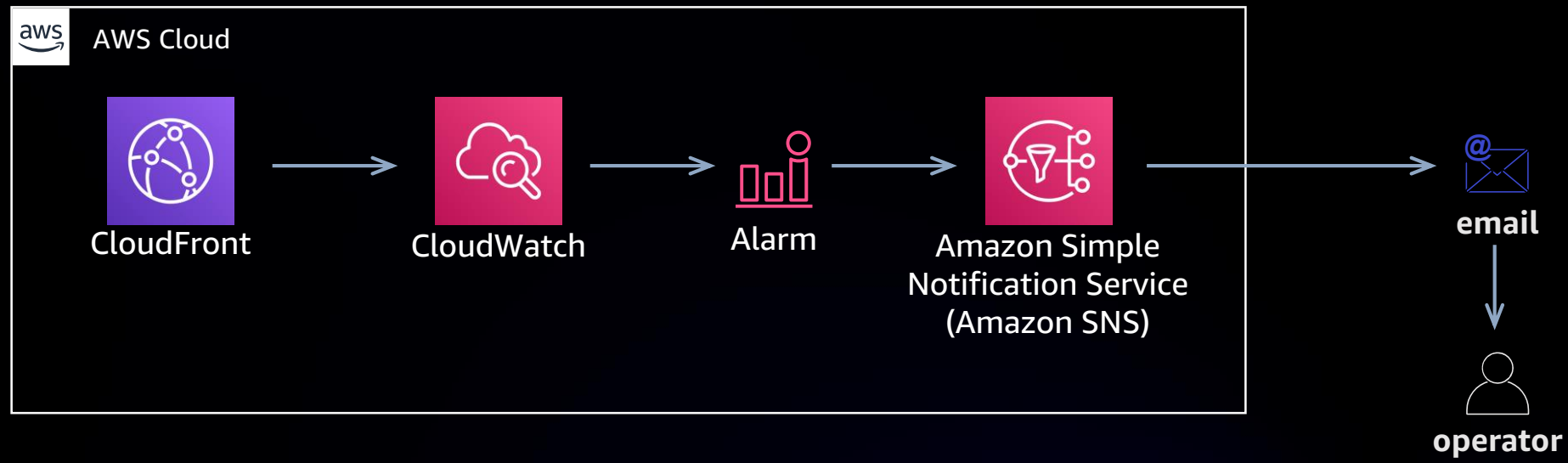
- CloudTrail logs : Record of actions taken by a user, role, or an AWS service in AWS WAF
- Logs in Kinesis Data Firehose with filter criteria
- Example log fields: action, args, clientIP, excludedRules, headers, maxRateAllowed, rateBasedRuleList, labels, etc.

Console: View sample requests

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitor for traffic and error anomalies

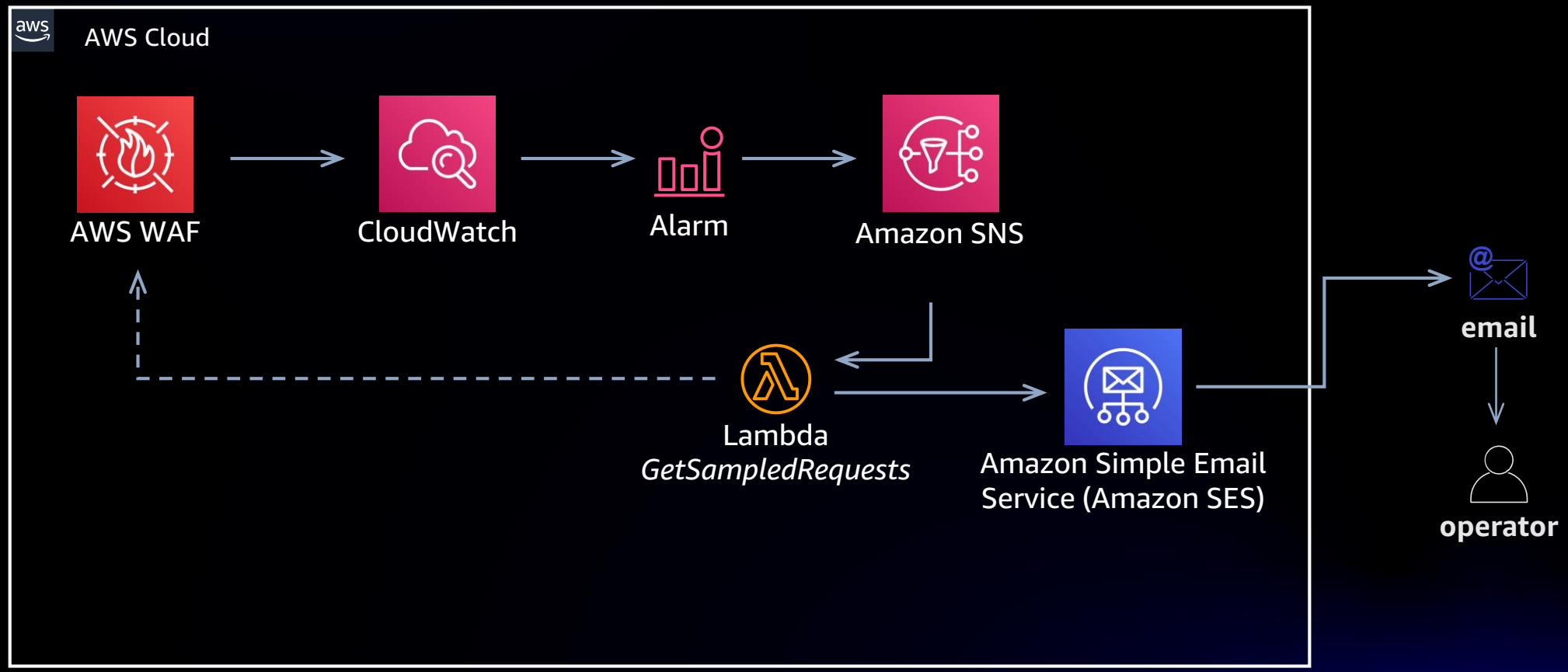
- Viewer requests varying beyond threshold
- Error rates spikes



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitor malicious traffic

- BlockedRequests over threshold

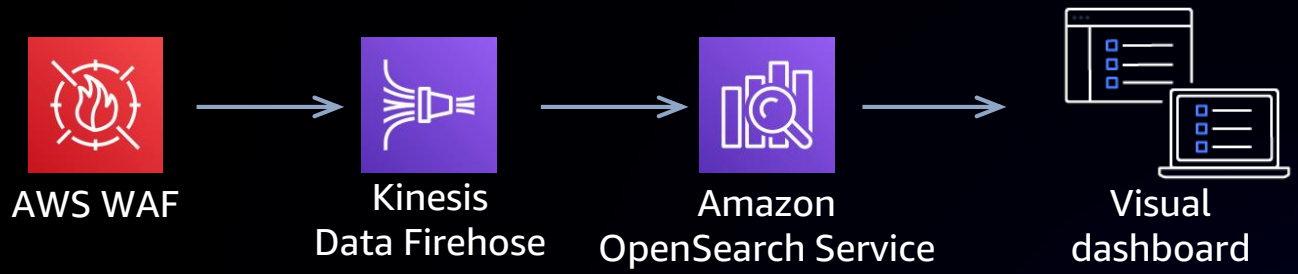


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Create real-time granular dashboard

- Review request, latency, result type for different geographies
- Use real-time log delivery to minimize latency





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Upcoming sessions

- NET308-R2: Protect your web applications across multiple AWS accounts
- NET321: Accelerating access to compute endpoints
- NET318: Building resilient and low-latency gaming architecture on AWS
- NET212: Securing non-cacheable end-user workloads at the edge

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.