
AWS
re:Invent

SEC322

Network security for serverless workloads

Alex Tomic

Solutions Architect

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Serverless architecture security

Improving perimeter protection

Gaining greater networking control

Improving observability

Summary



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

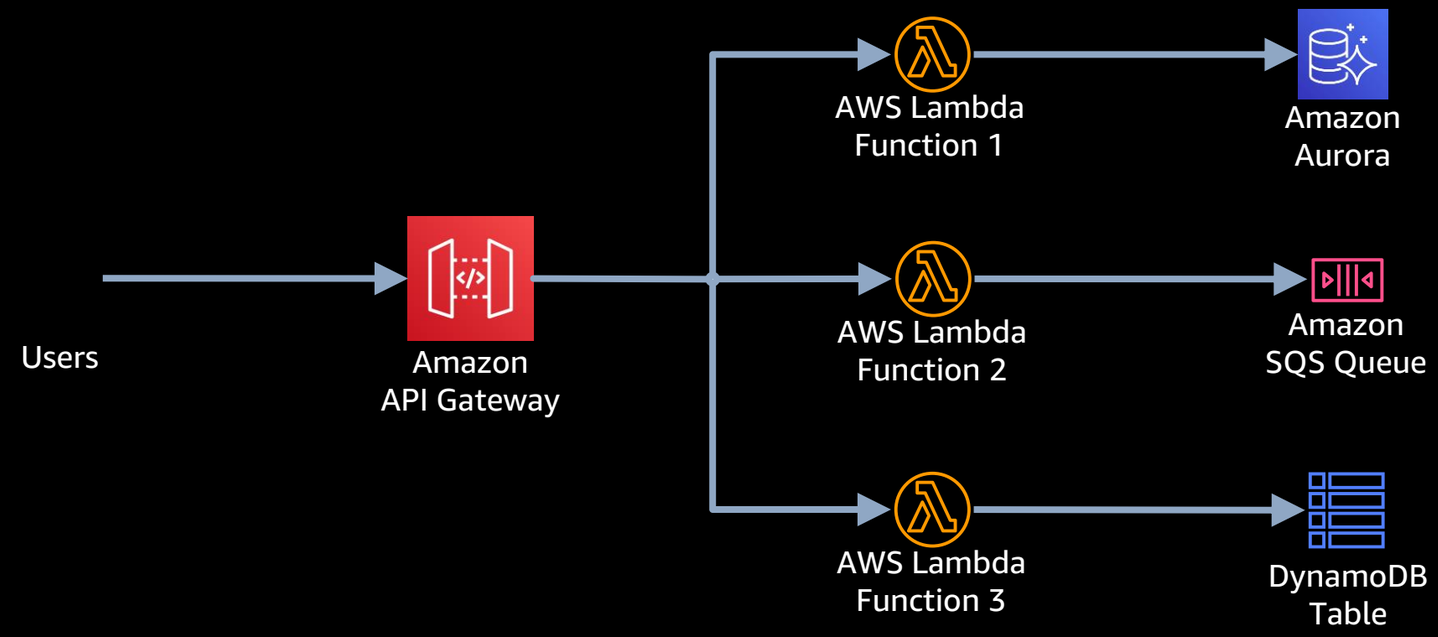
Serverless architecture security



AWS re:Invent

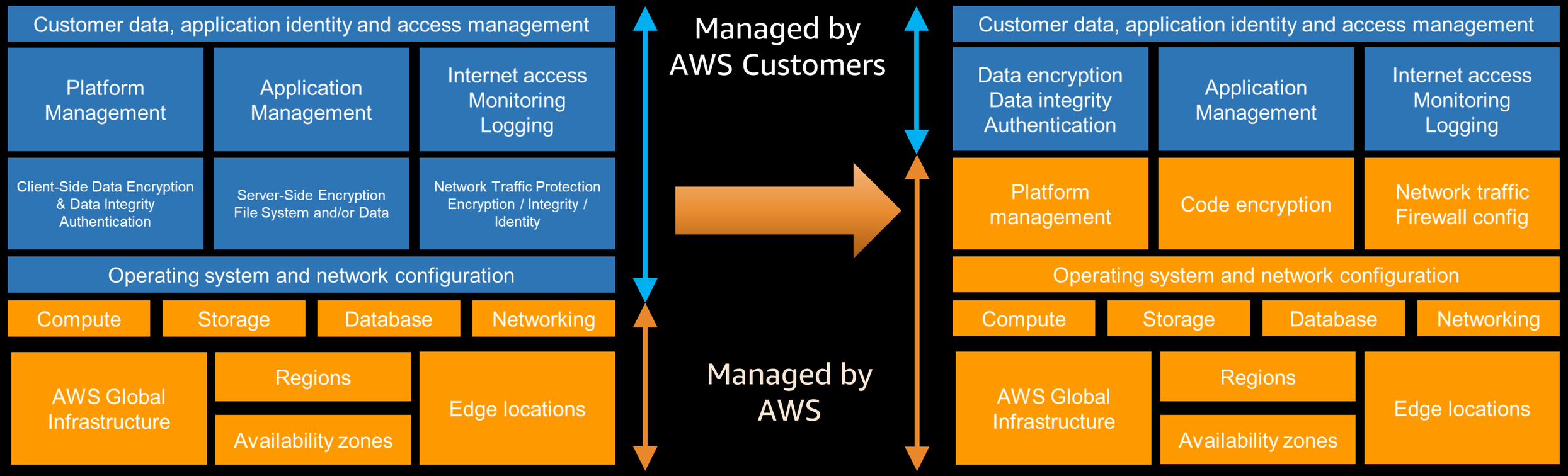
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A typical serverless architecture



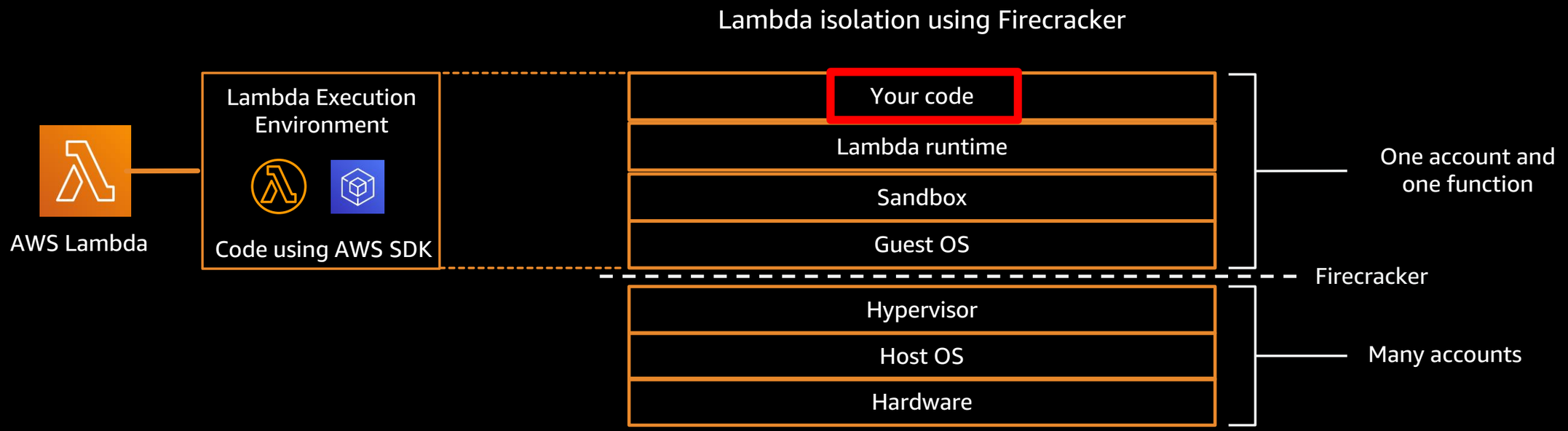
How serverless can improve security

- Serverless emphasizes use of managed and abstracted services

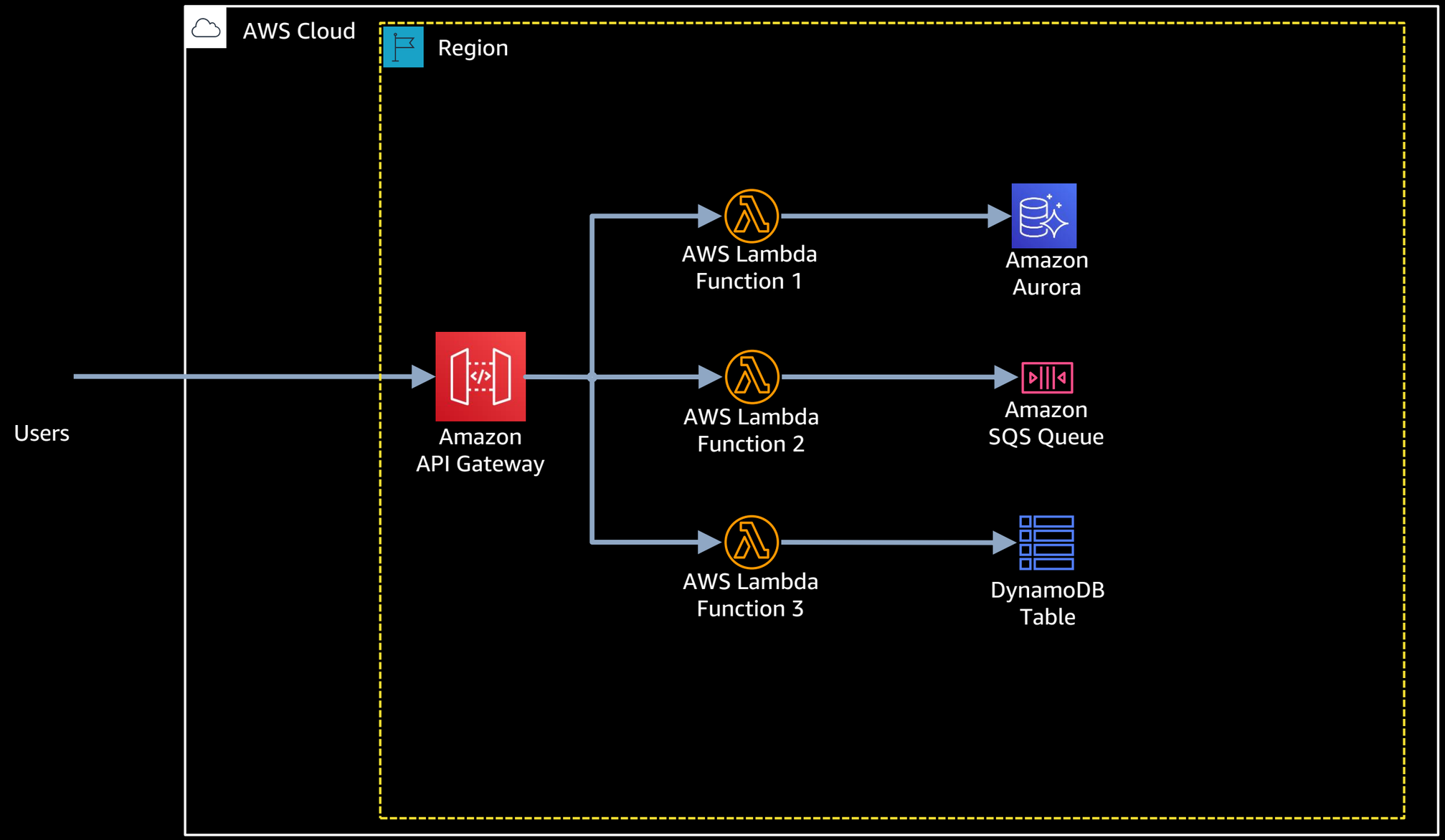


Reducing the attack surface

- AWS Lambda execution environment is short-lived (minutes)
- No inbound network traffic to AWS Lambda functions
- AWS Lambda provides strong isolation boundaries



Operating within secure AWS network



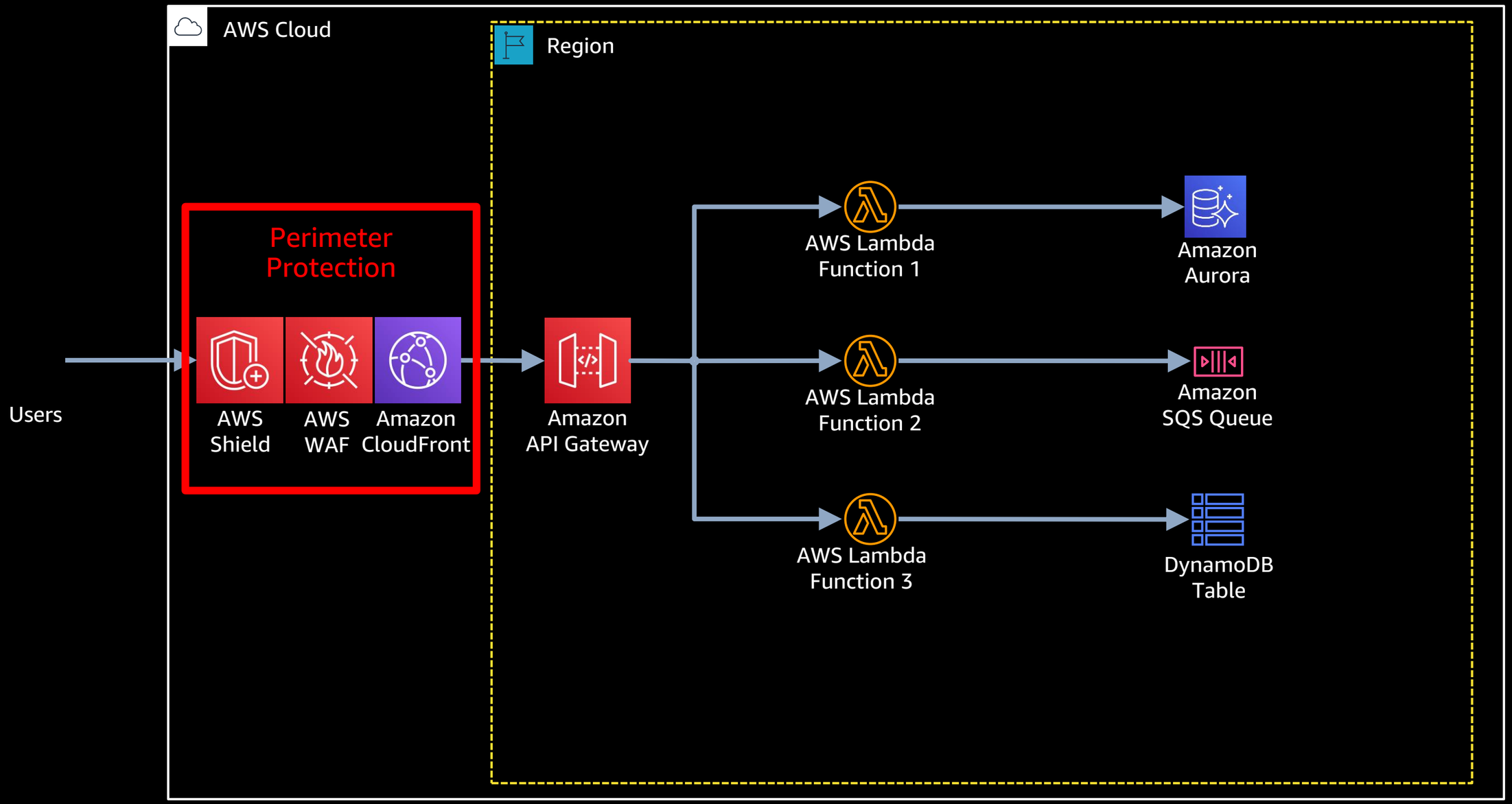
Improving perimeter protection



AWS re:Invent

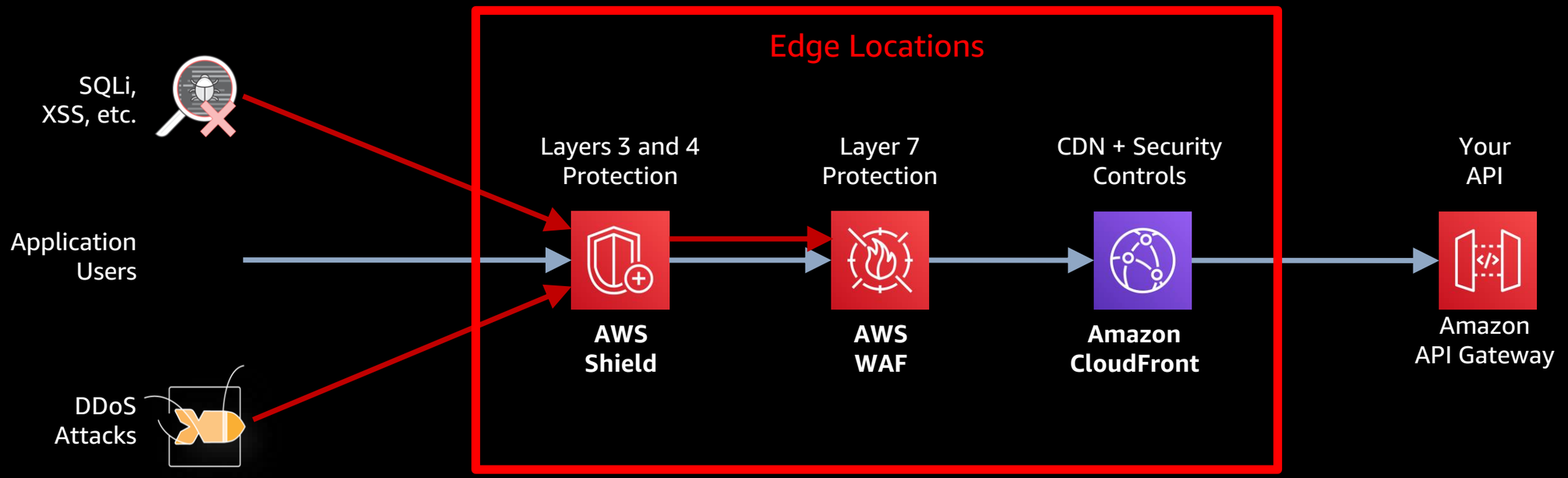
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Perimeter protection (security at the edge)



How to improve security at the edge

- Filter out unwanted requests at the edge of network
- Increase your capacity against distributed denial of service (DDoS) threats with 200+ edge locations



Building custom AWS WAF rules

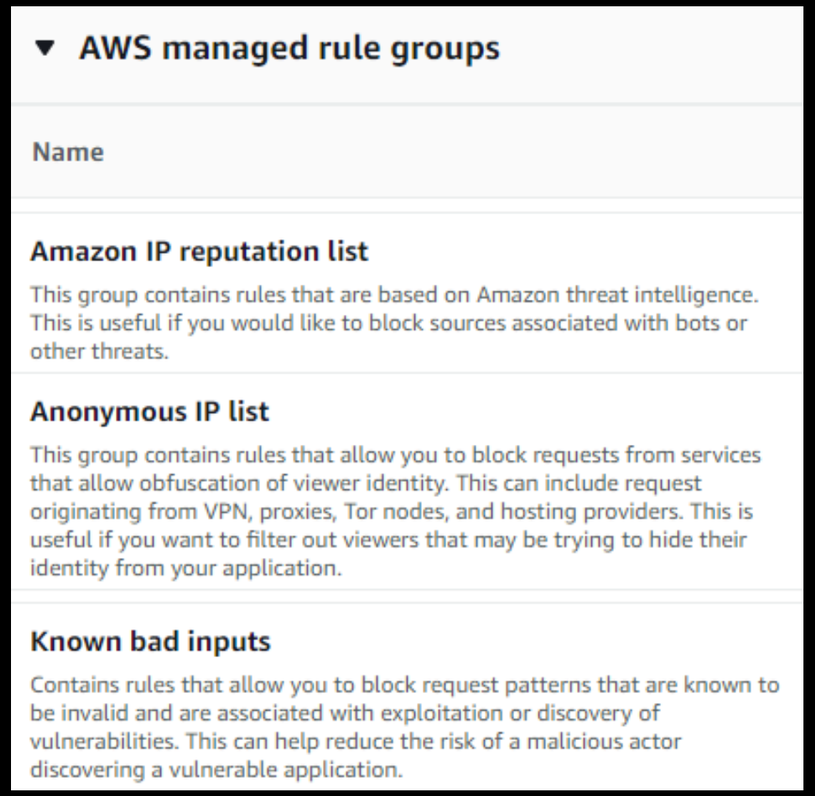
- Build rules using a visual builder in the console
- Or declare rules in JSON documents



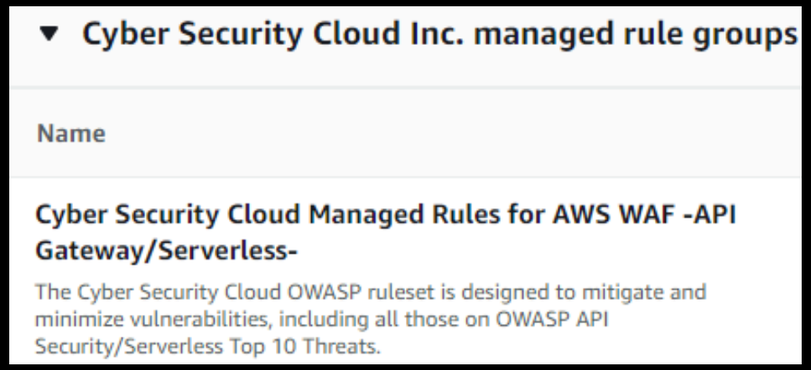


Managed rules for AWS WAF

- Use AWS-managed rules provided at no additional cost
- Or subscribe to rule groups in AWS Marketplace

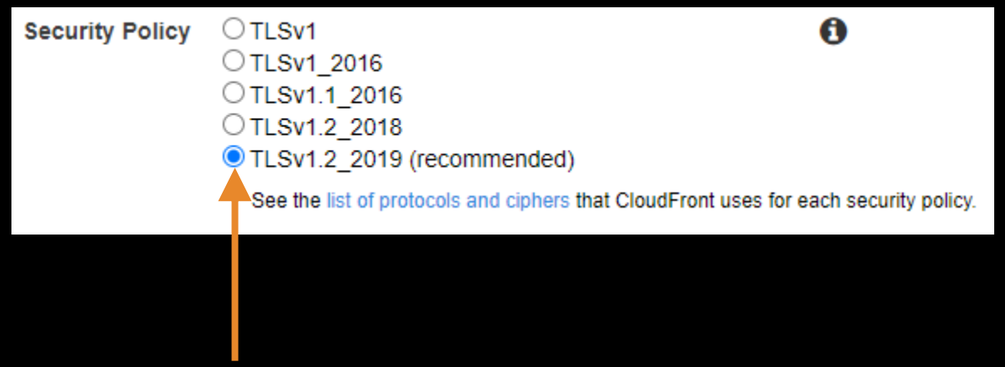






Why Amazon CloudFront for APIs?

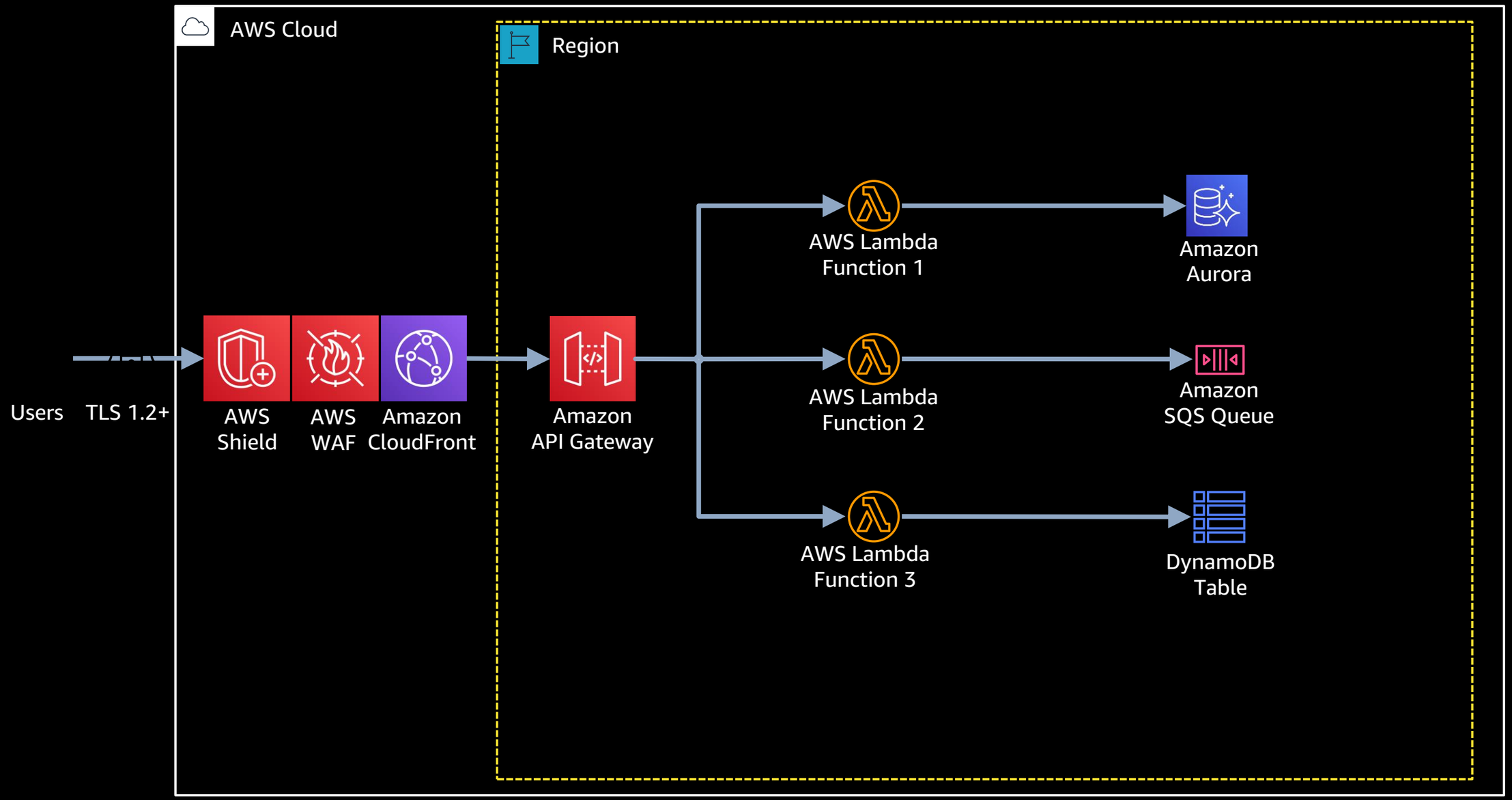
- Security features such as OCSP stapling and field-level encryption
- API Gateway's Regional API endpoints + CloudFront for added control



Enforce TLS 1.2+ connections to edge locations

	TLSv1.1_2016	TLSv1.2_2018	TLSv1.2_2019
SSL/TLS protocols supported			
TLSv1.3[1]	♦	♦	♦
TLSv1.2	♦	♦	♦
TLSv1.1	♦		
TLSv1			
SSLv3			
Ciphers supported			
TLS_AES_128_GCM_SHA256	♦	♦	♦
TLS_AES_256_GCM_SHA384	♦	♦	♦
TLS_CHACHA20_POLY1305_SHA256	♦	♦	♦

Integrating perimeter protection



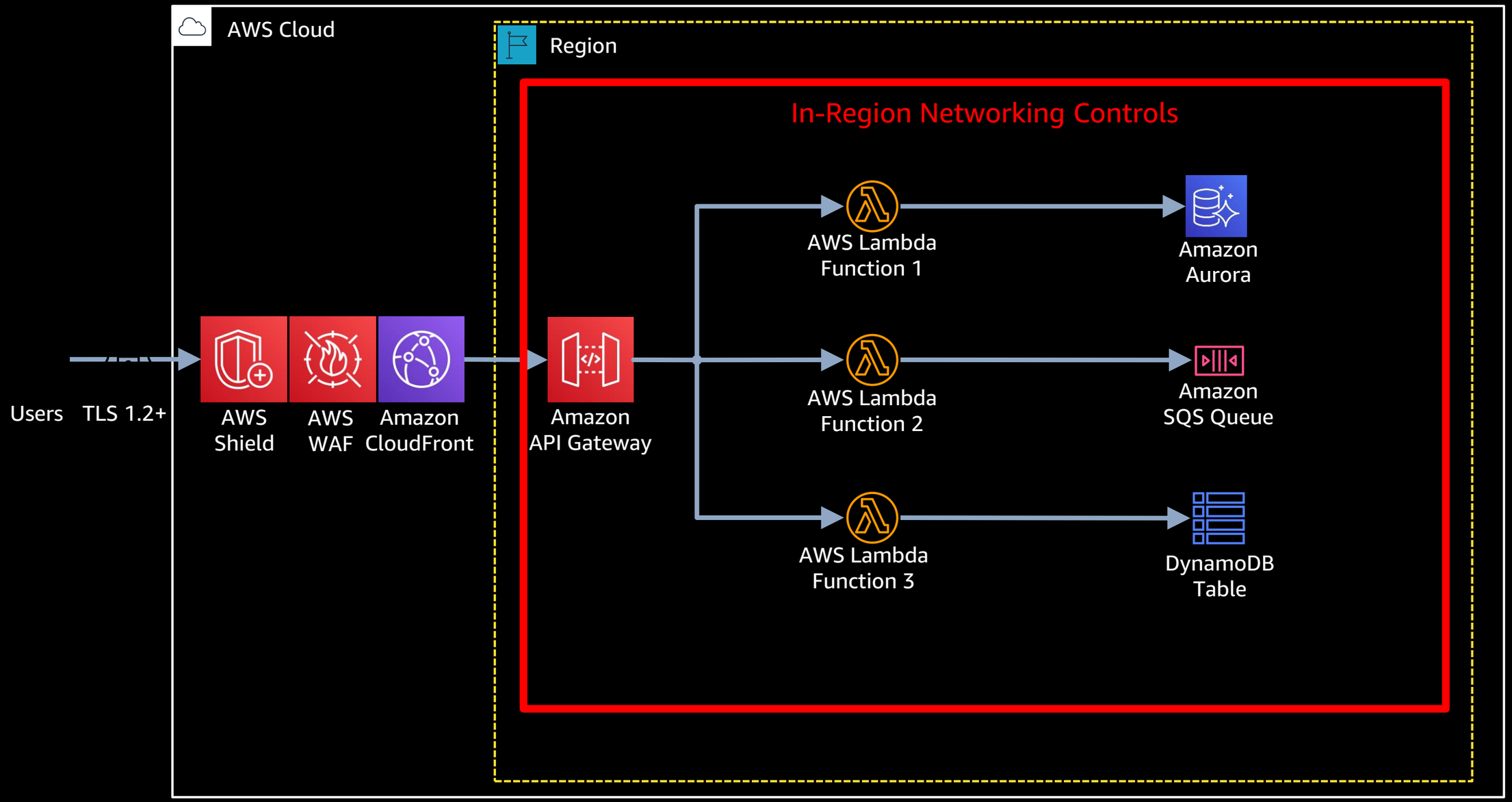
Gaining greater control of networking



AWS re:Invent

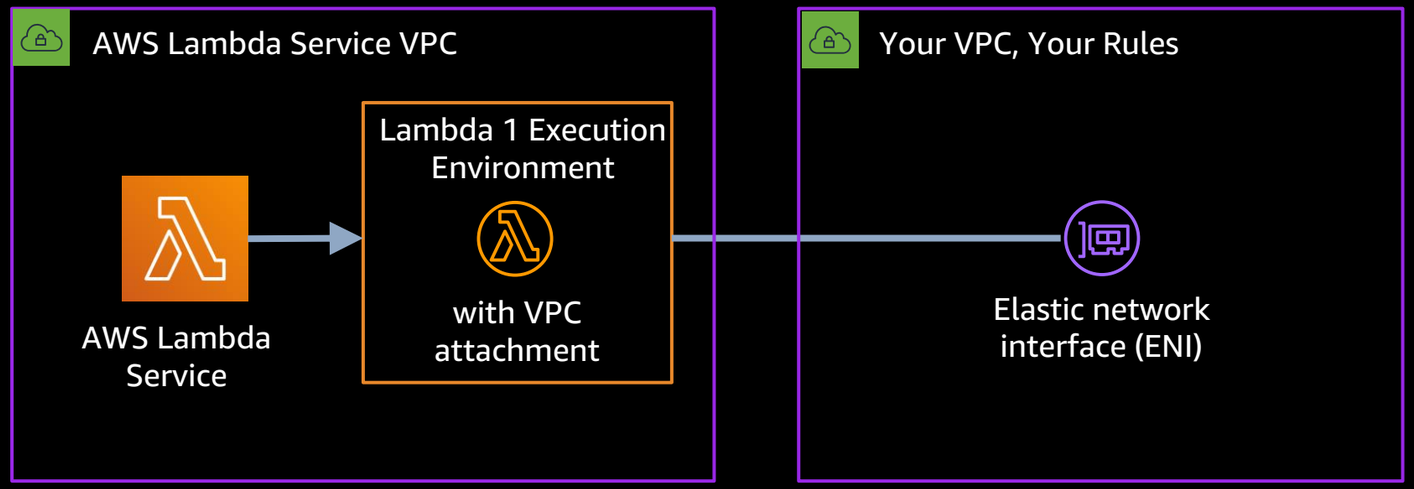
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Gaining greater control of networking

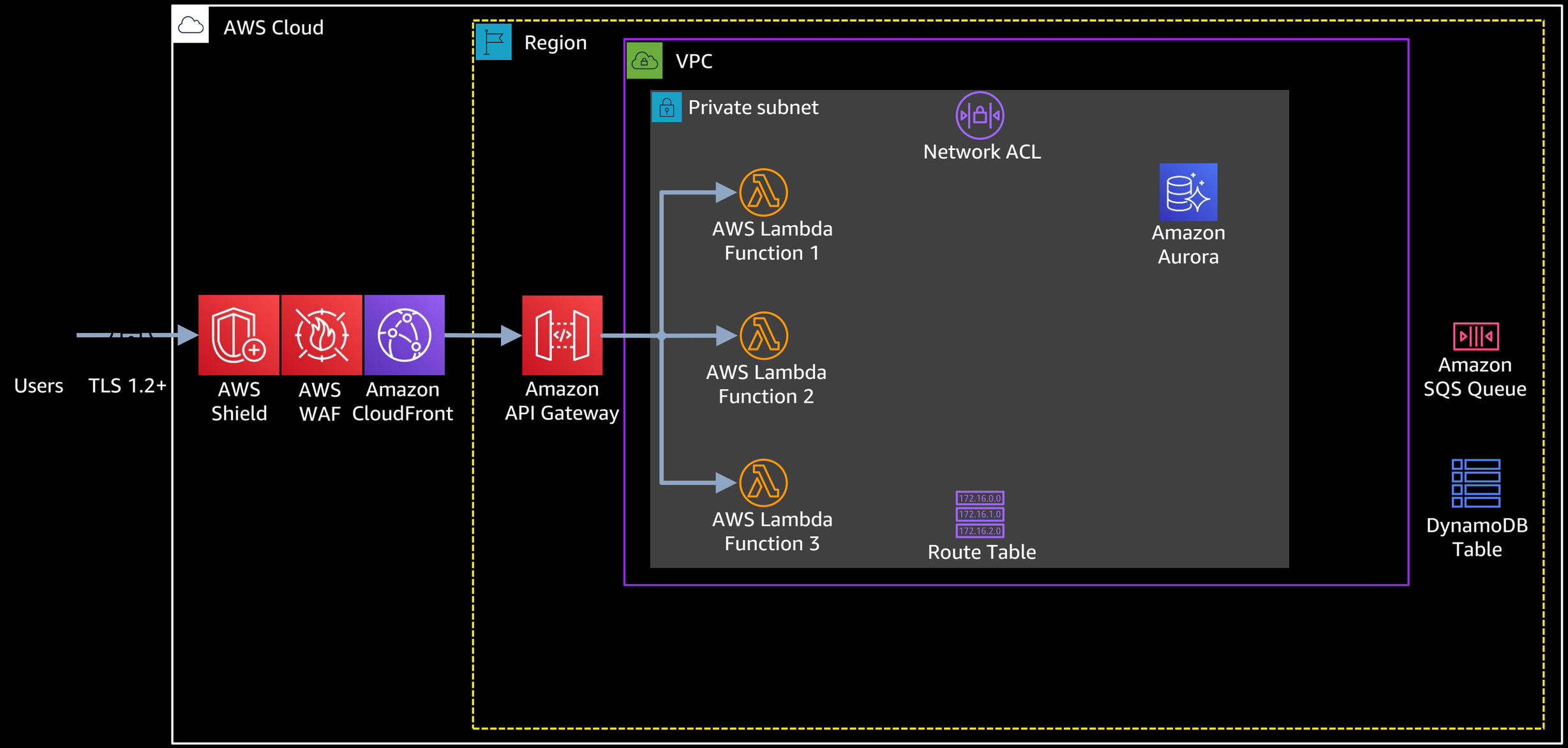


Why attach Lambda functions to your VPC?

- Apply least-privilege networking rules to your Lambda functions
- You can apply your custom routing, network access control lists (ACLs), security groups, etc.

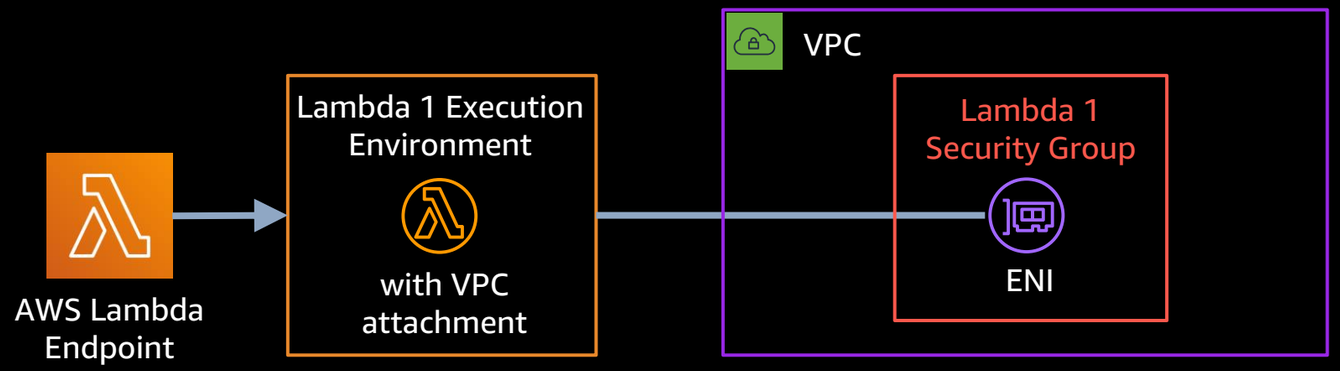


Attaching Lambda functions to VPCs



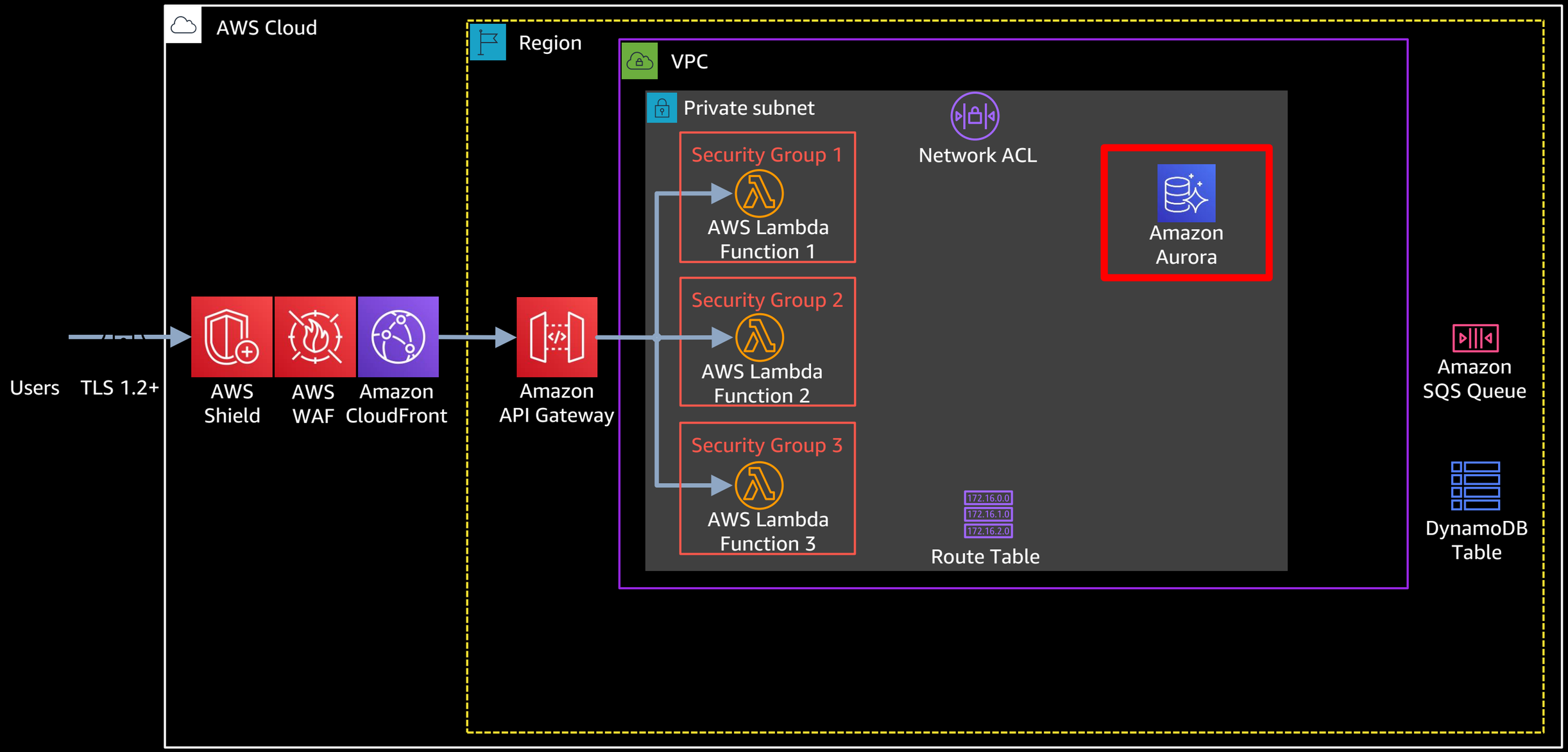
How to control Lambda function traffic

- Lambda functions cannot accept inbound network traffic
- Lambda security groups do NOT need inbound rules



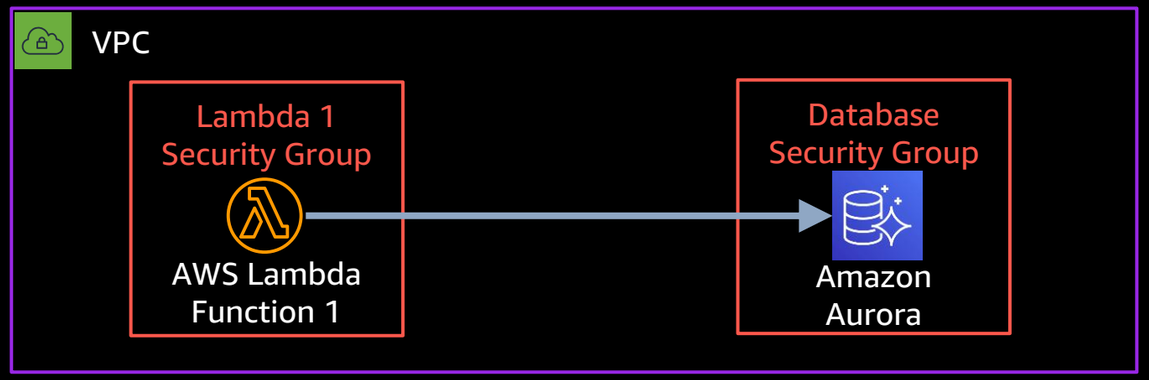
Lambda 1 Security Group (SG)	
Inbound	
From:	(None)
Outbound	
To:	Some other SG or IP

Attaching security groups to Lambda functions



How functions access resources in VPCs

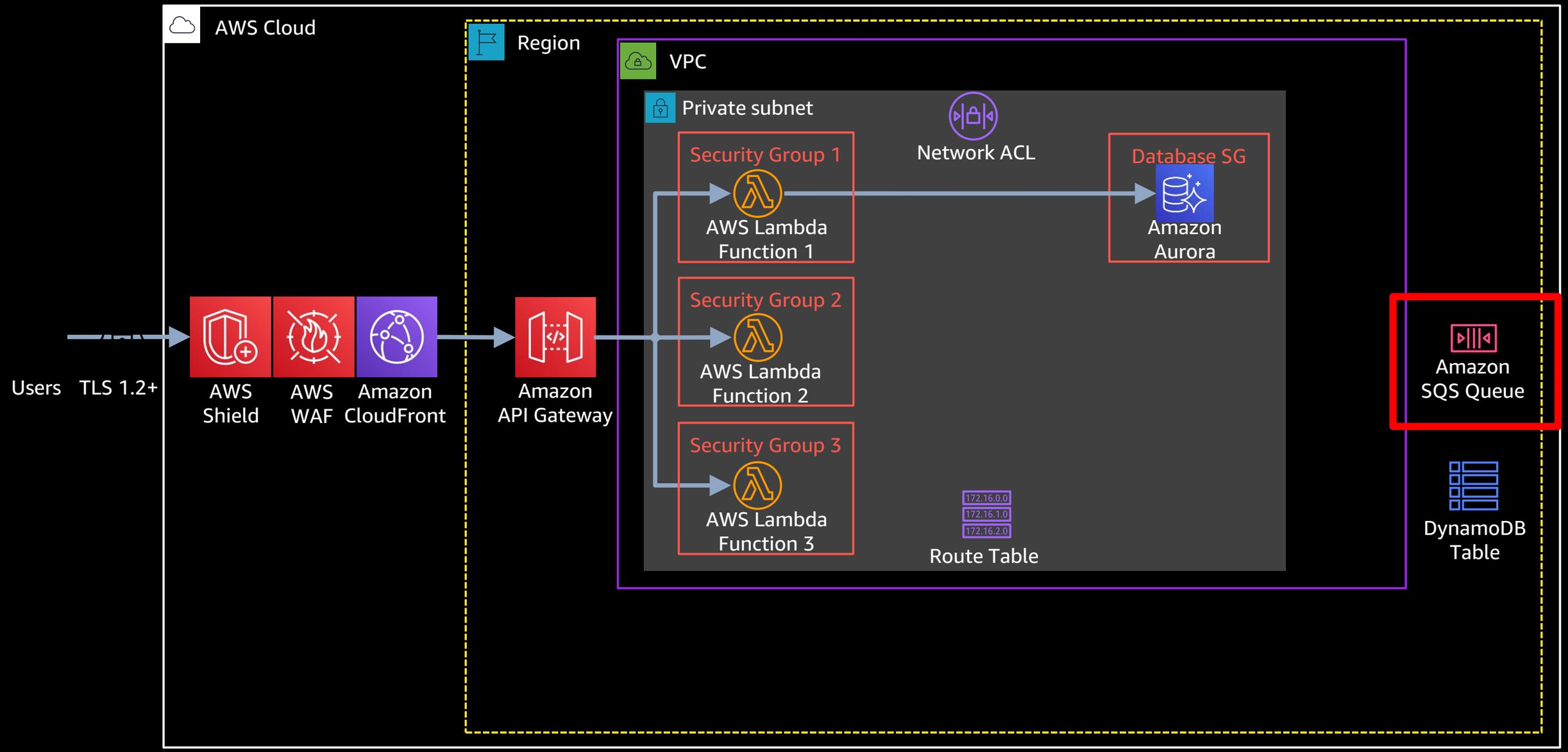
- Lambda functions outbound traffic governed by security groups
- Resources need to allow incoming traffic from Lambda SGs



Lambda 1 Security Group Rules	
Inbound Rules	
From:	(None)
Outbound Rules	
To:	Database SG (3306)

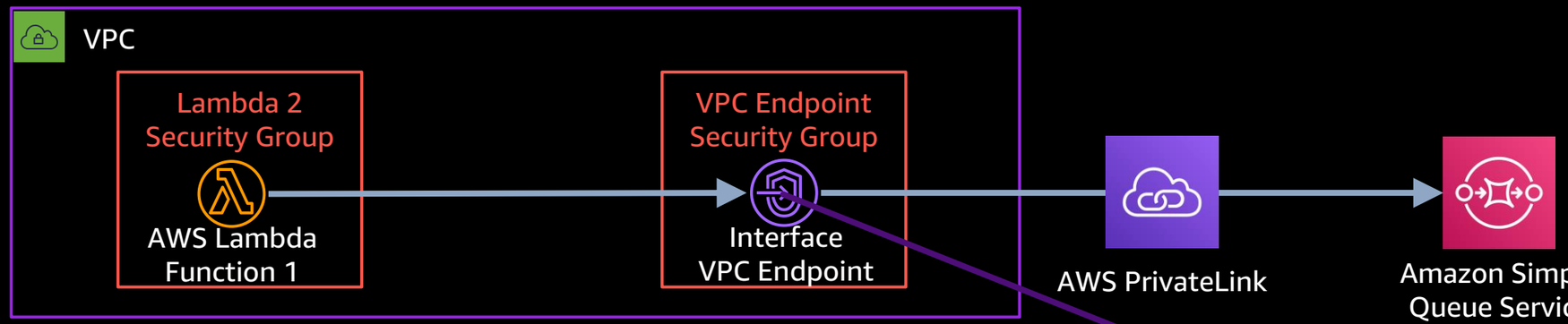
Database Security Group Rules	
Inbound Rules	
From:	Lambda 1 SG (3306)
Outbound Rules	
To:	(None)

Accessing resources inside VPCs



Accessing services via VPC interface endpoints

- VPC endpoints enable private connections to supported services
- AWS PrivateLink creates a connection to a service outside of VPC



Lambda 2 Security Group Rules	
Inbound Rules	
From:	(None)
Outbound Rules	
To:	VPC Endpoint Security Group (https)

VPC Endpoint Security Group Rules	
Inbound Rules	
From:	Lambda 1 Security Group (https)
Outbound Rules	
To:	(None)

VPC Endpoint Policy

```
…
"Action": [
      “sqs:SendMessage",
      “sqs:ReceiveMessage"
],
"Resource": "arn:aws:sqs:…:MYQUEUE“
…
```

Policies to control traffic

- VPC endpoint policies control calls to resources outside of VPC
- Combine with resource policies to ensure the use of your VPC

VPC Endpoint Policy

```
{
"Statement": [{
  "Action":  [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage“
   ],
  "Effect": "Allow",
  "Resource": “arn:aws:sqs:us-east-1:MYACCTID:QUEUE1",
  "Principal": { "AWS": “MYACCTID" }
}]
}
```

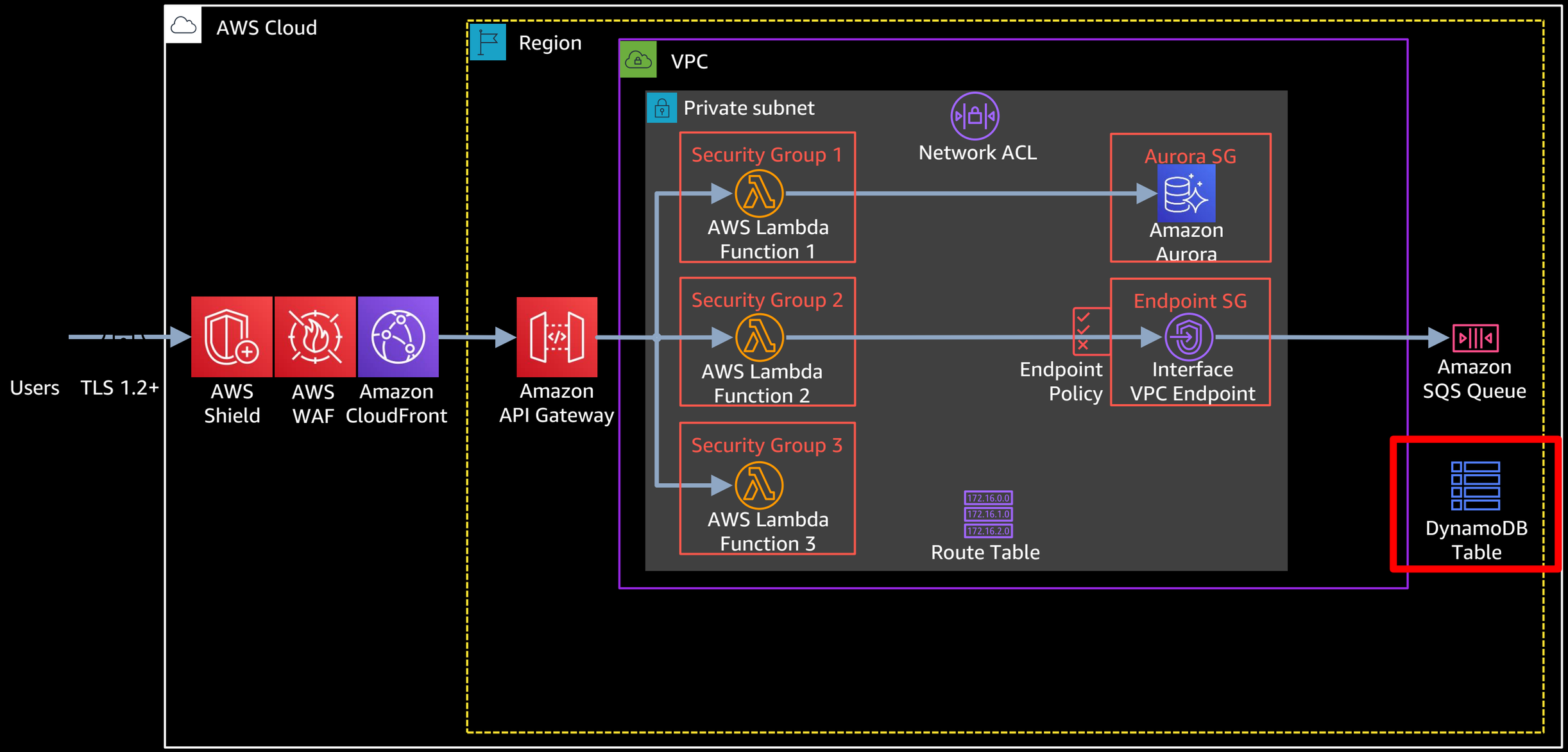
English: resources in this VPC can only interact with queue1 in my account; principals must be from my account

SQS Queue Resource Policy

```
{
"Statement": [{
  "Action":  [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage“
   ],
  "Effect“ : “Deny",
  “Condition": {
      “StringNotEquals": {
            “aws:sourceVpce“: “vpce-a2b3c4d“
      },
  }] }}
```

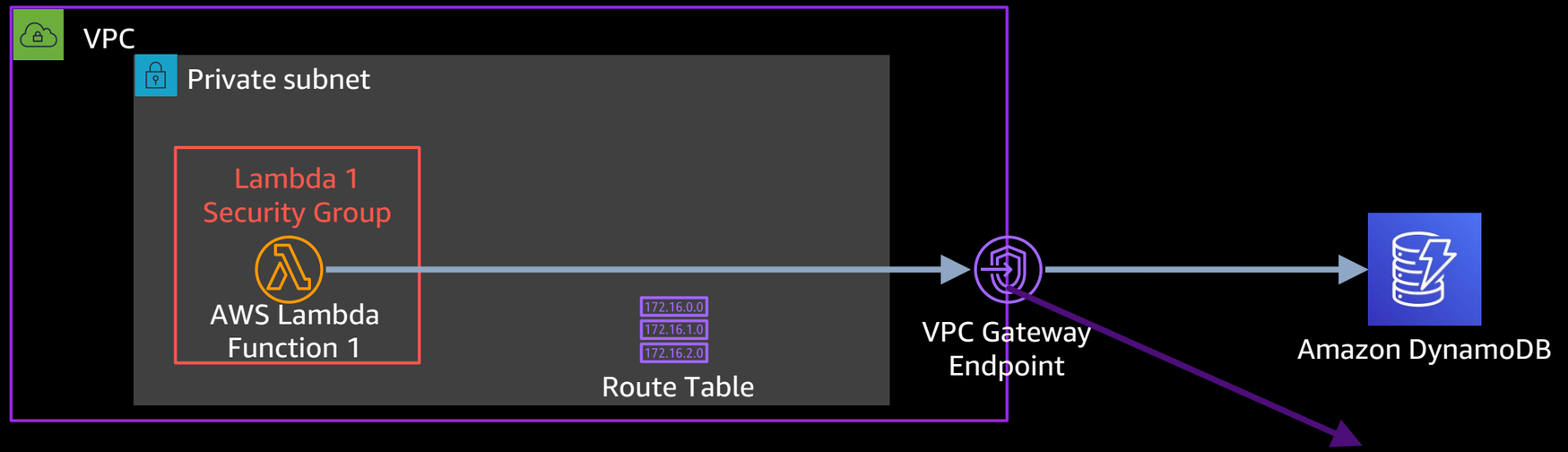
English: deny API calls not coming through a specific VPC endpoint

Accessing services via interface VPC endpoints



Accessing services via VPC gateway endpoints

- Amazon S3 and Amazon DynamoDB require VPC gateway endpoints
- VPC gateway endpoints use routing tables and prefix lists



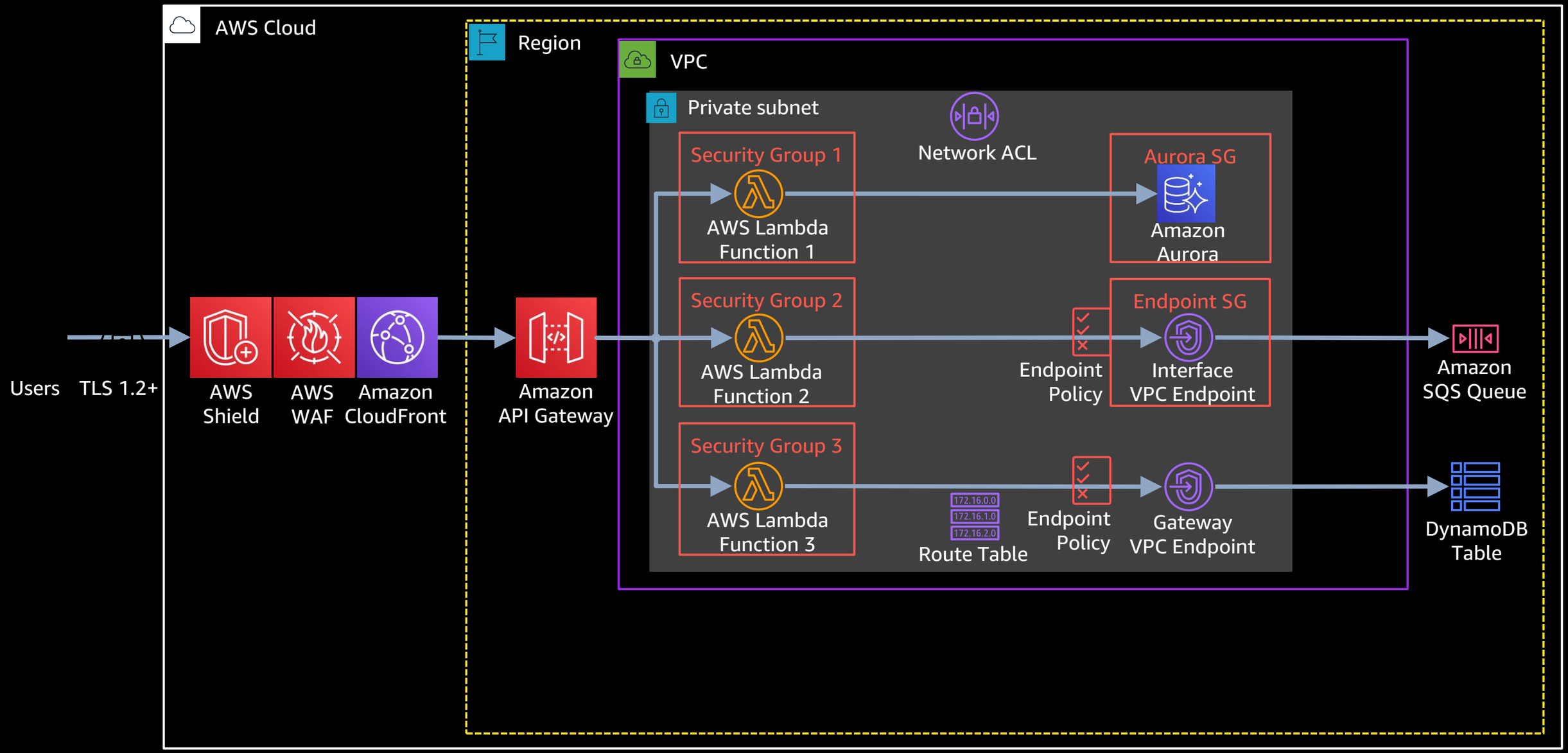
Lambda 1 Security Group Rules	
Inbound Rules	
From:	(None)
Outbound Rules	
To:	**Prefix list ID for DynamoDB** (https)

Route Table	
Routing Destination	Target
10.0.0.0/16	local
Prefix List ID for Amazon DynamoDB	**VPC Endpoint ID**

VPC Endpoint Policy

```
…
"Action": [
          "dynamodb:GetItem",
          "dynamodb:PutItem"
],
"Resource":
"arn:aws:dynamodb:…:table/MYTABLE“
…
```

Serverless with your VPC networking controls



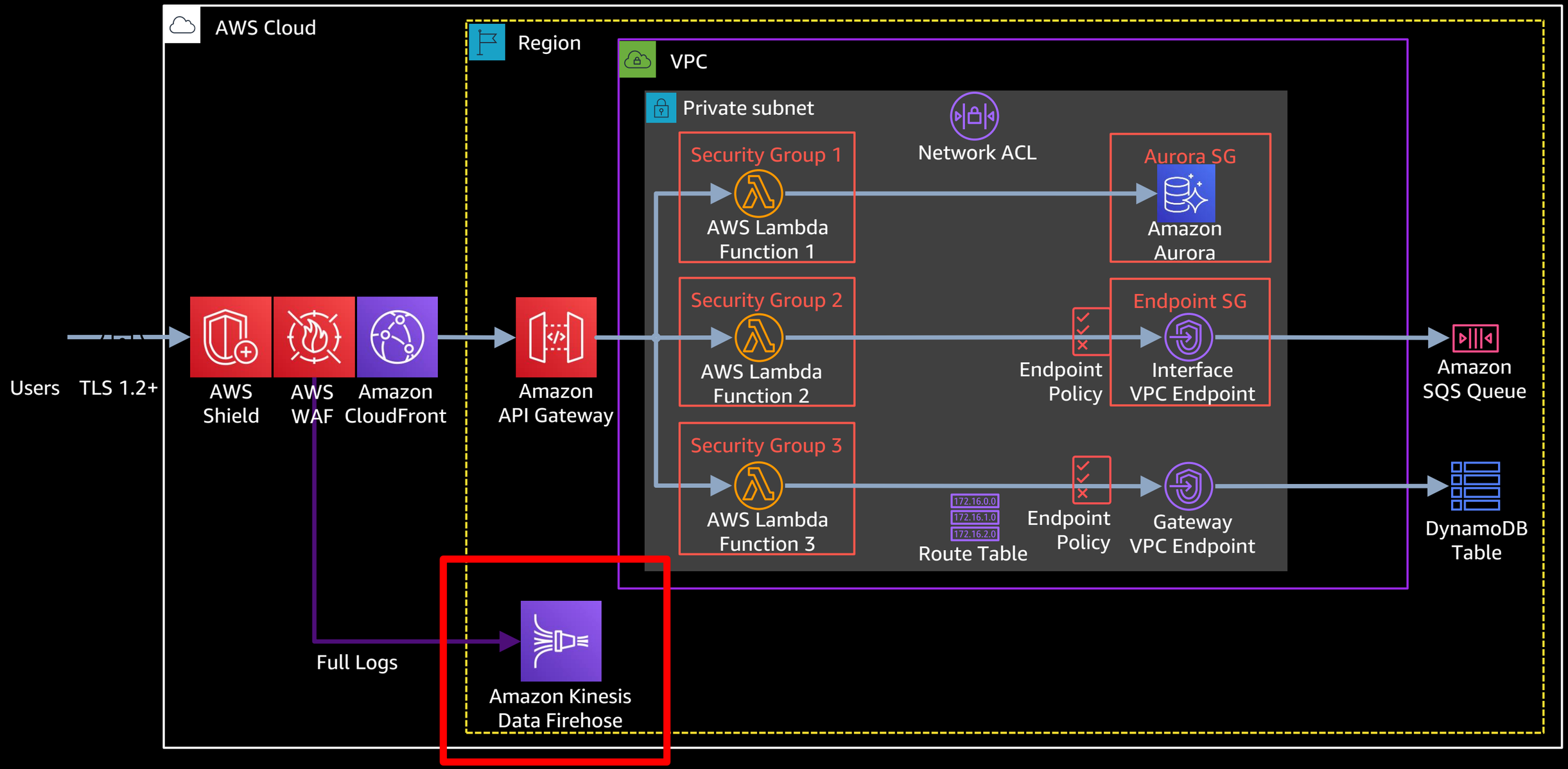
Improving observability



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Observability for perimeter protection



What data is in AWS WAF logs?



Blocked requests generate 403 error message



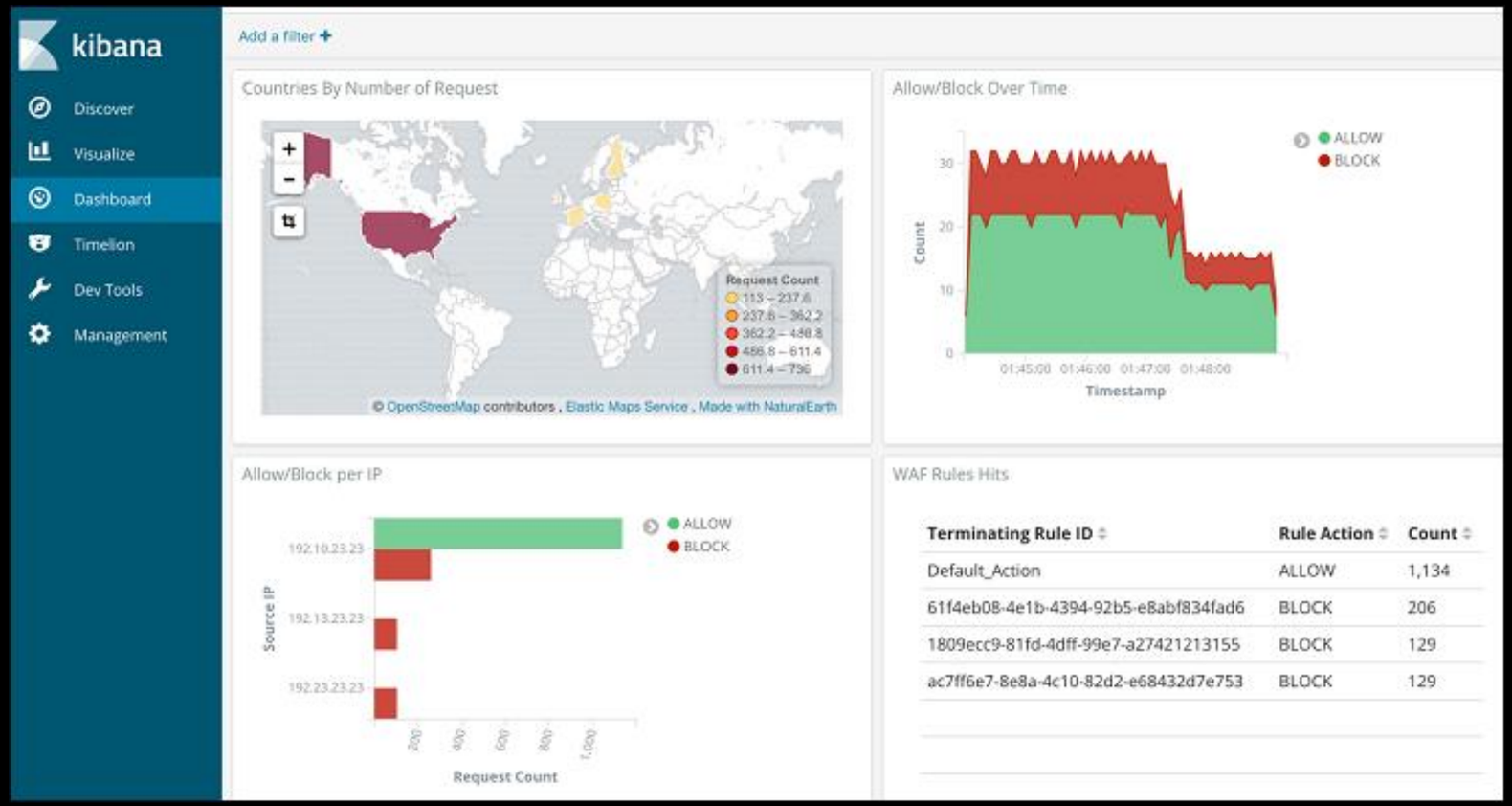
Logs provide details about requests, callers, and WAF action

SQLi and XSS rules log matched data for easier diagnostics

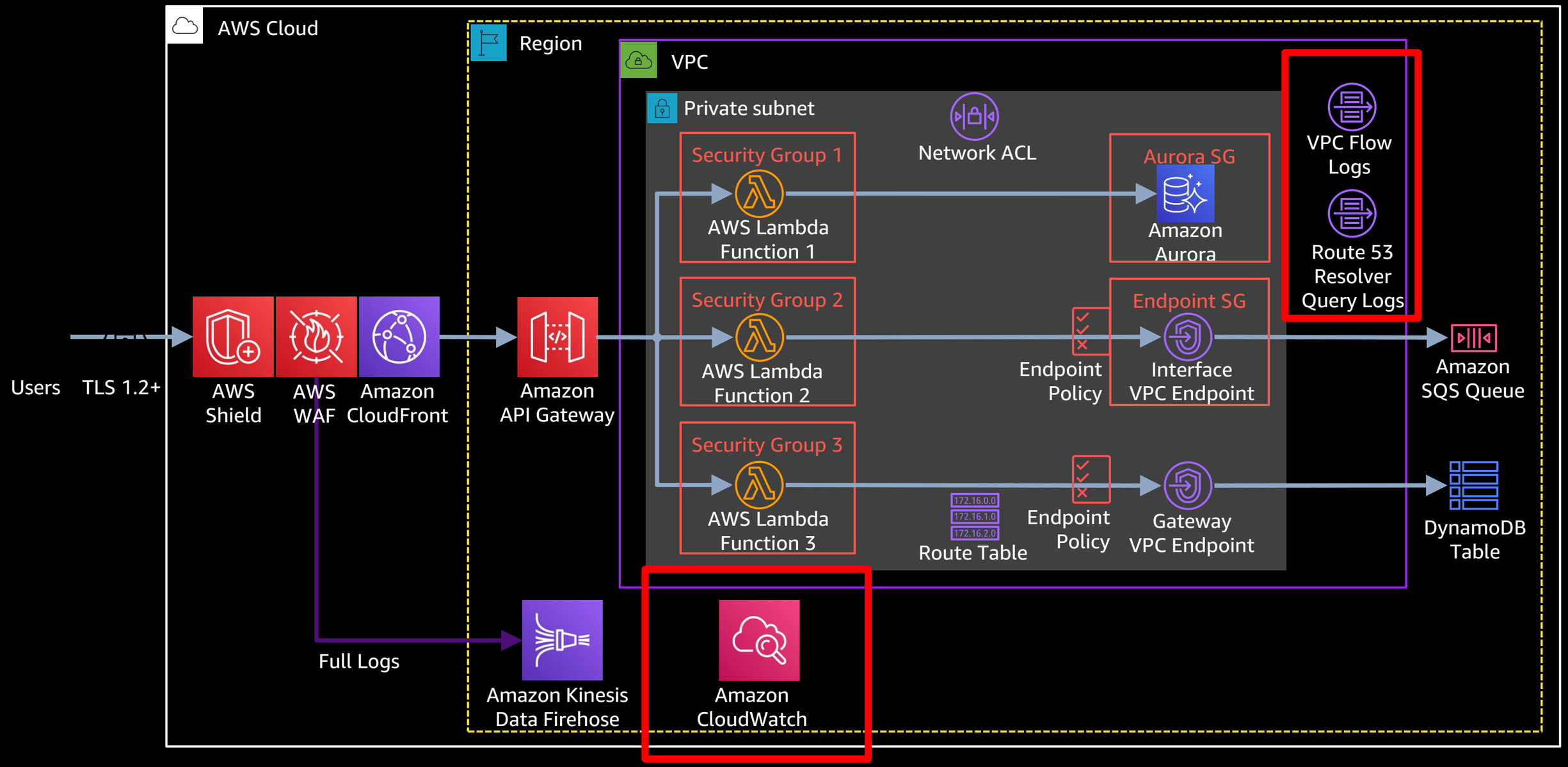

```
"webaclId": "arn:aws:wafv2:us-east-2:012345678901:regi
"terminatingRuleId": "AWS-AWSManagedRulesSQLiRuleSet",
"terminatingRuleType": "MANAGED_RULE_GROUP",
"action": "BLOCK",
"terminatingRuleMatchDetails": [
    {
        "conditionType": "SQL_INJECTION",
        "location": "URI",
        "matchedData": [
            "/robert",
            ";",
            "drop",
            "table",
            "students"
        ]
    }
],
```

How to analyze AWS WAF full logs

- AWS WAF logs can be delivered to Amazon Elasticsearch Service
- “How to analyze AWS WAF logs using Amazon Elasticsearch Service” blog: https://amzn.to/2Ue0QMk

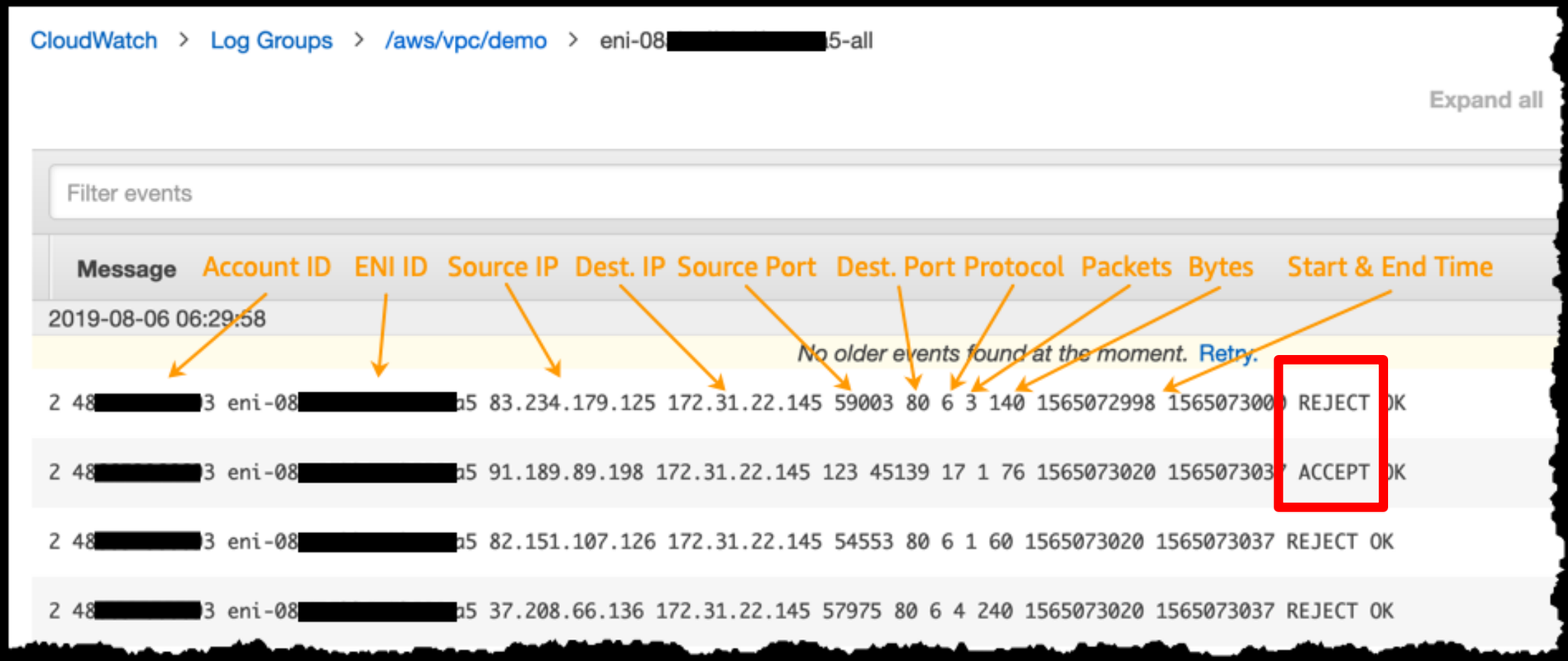


Adding observability of network traffic



How to analyze network flows

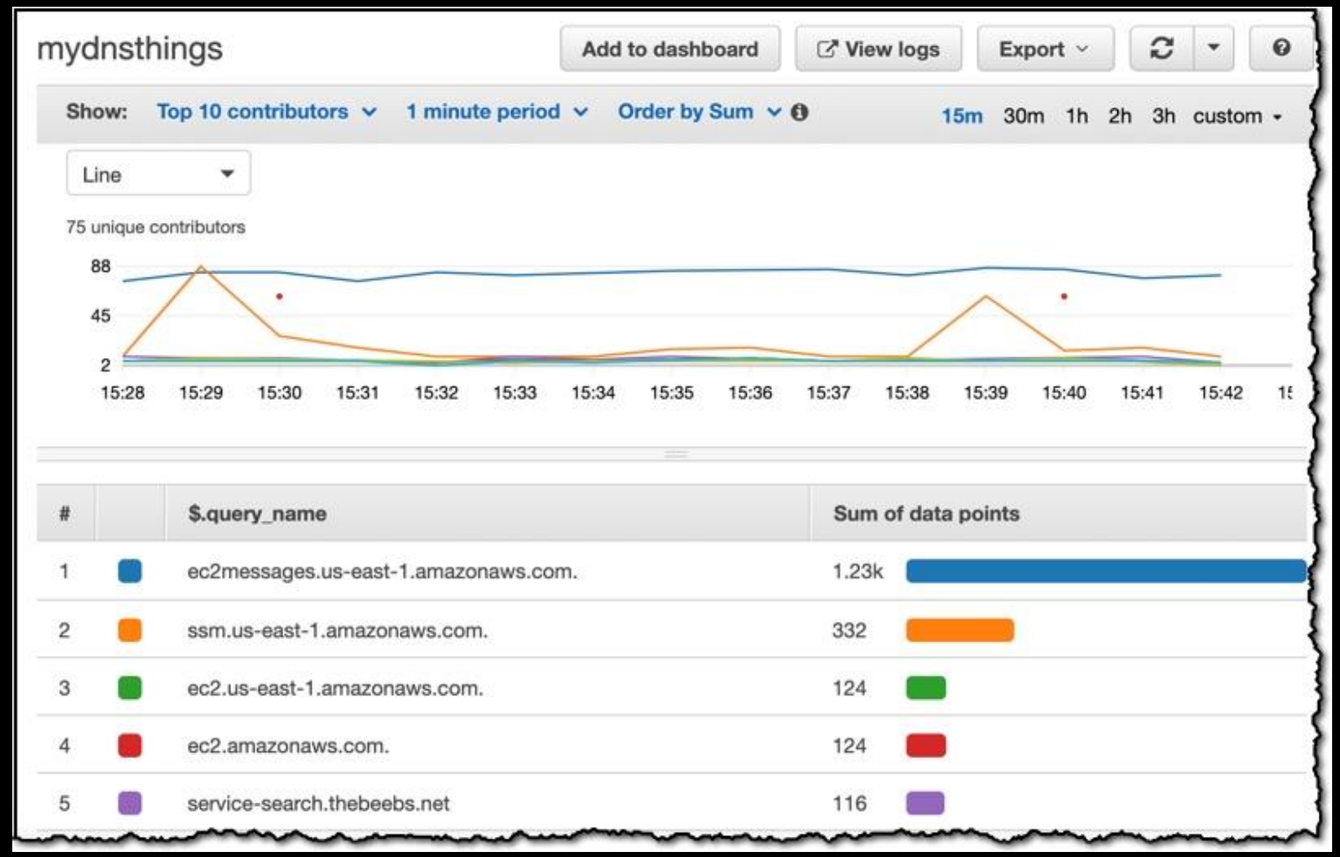
- VPC flow logs provide details of network flows in your VPC
- Data is aggregated in Amazon CloudWatch logs



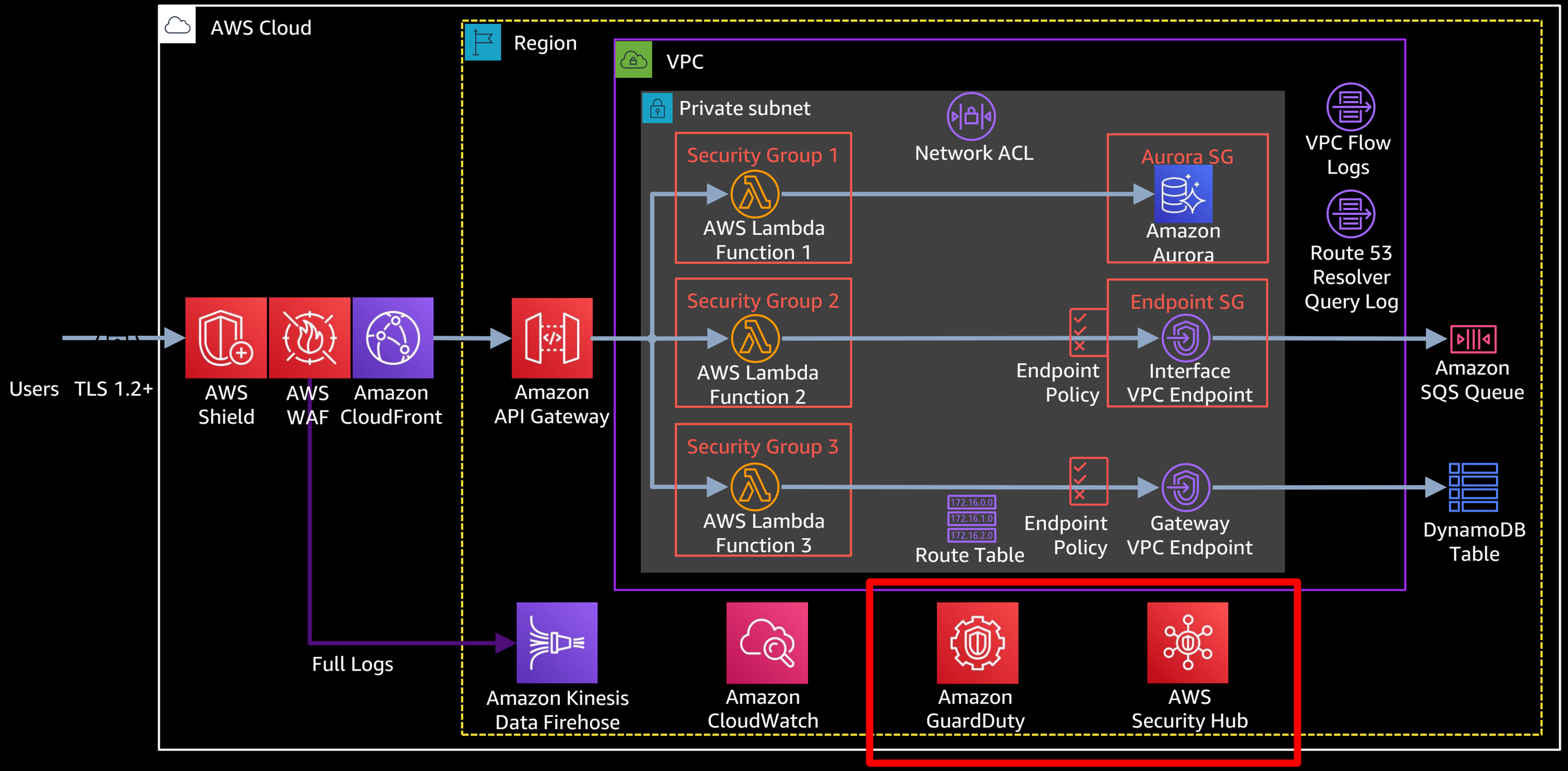
How to analyze DNS logs

NEW!

- Log your VPC DNS queries with Route 53 Resolver Query Logs
- CloudWatch log insights can help analyze and visualize logs

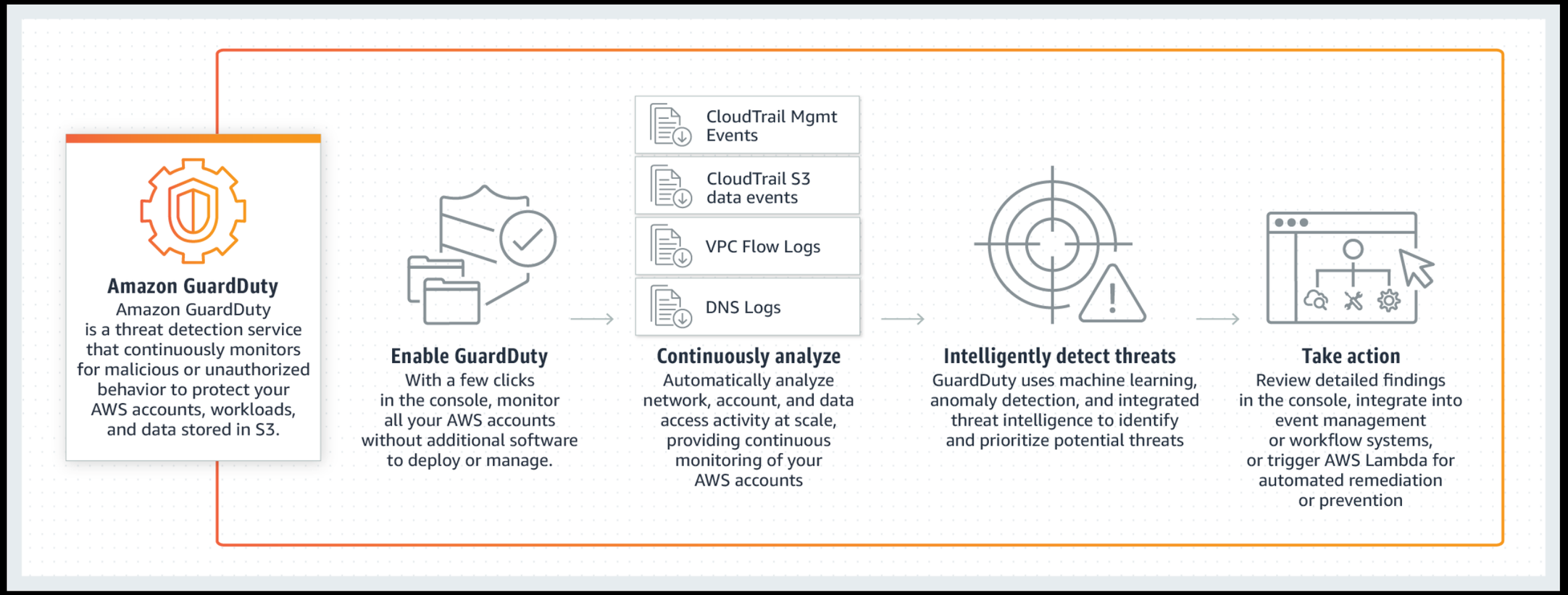


Threat detection and incident investigation



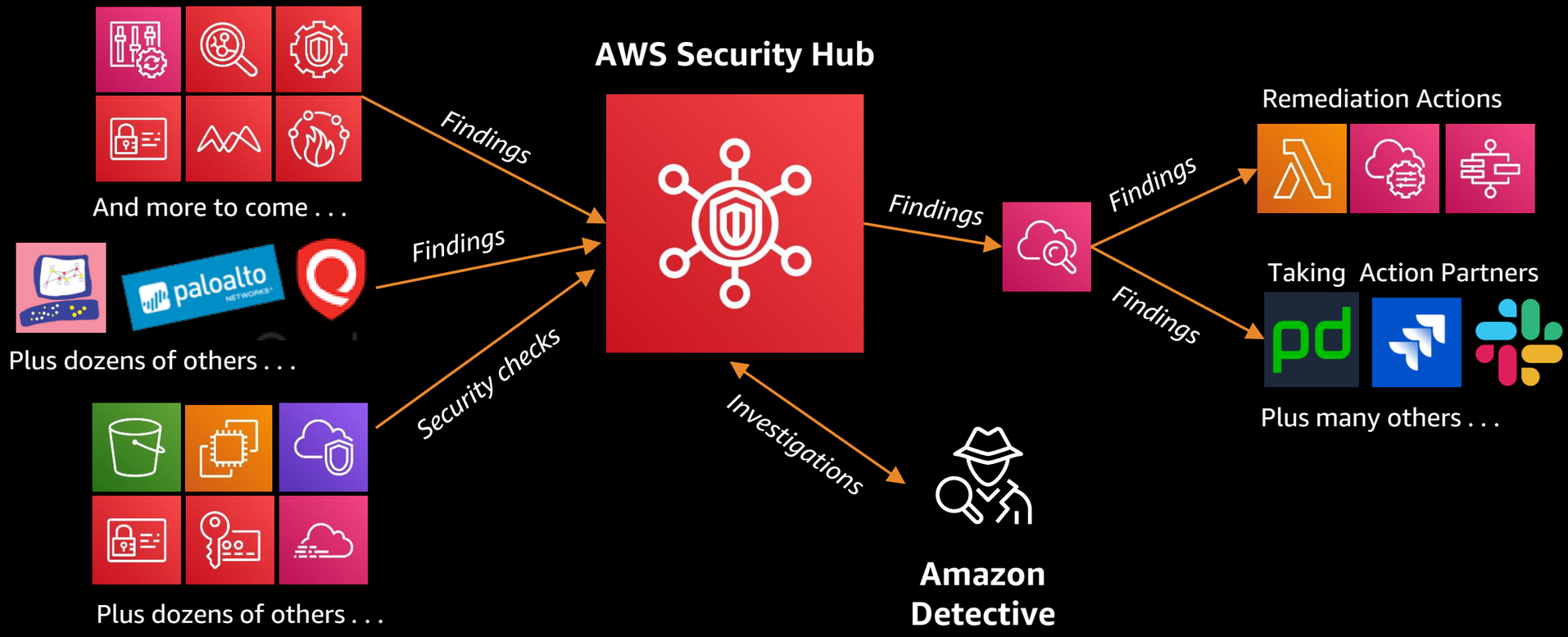
How to detect threats to your application

- Amazon GuardDuty uses threat intelligence and machine learning
- Continuously monitors VPC flow logs and DNS logs in your VPCs

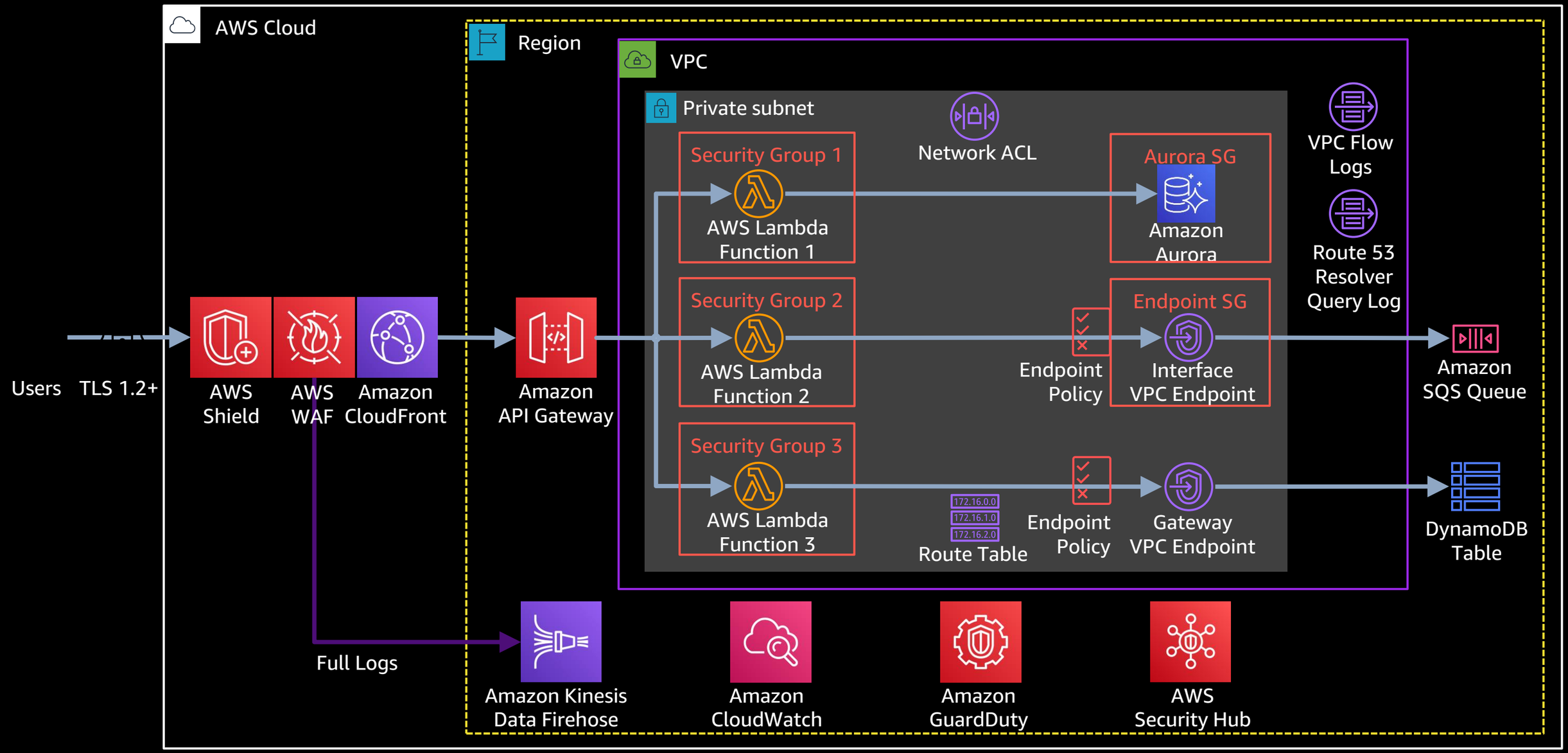


How to centralize security information

- AWS Security Hub provides automated compliance checks and security alert prioritization



Improved observability

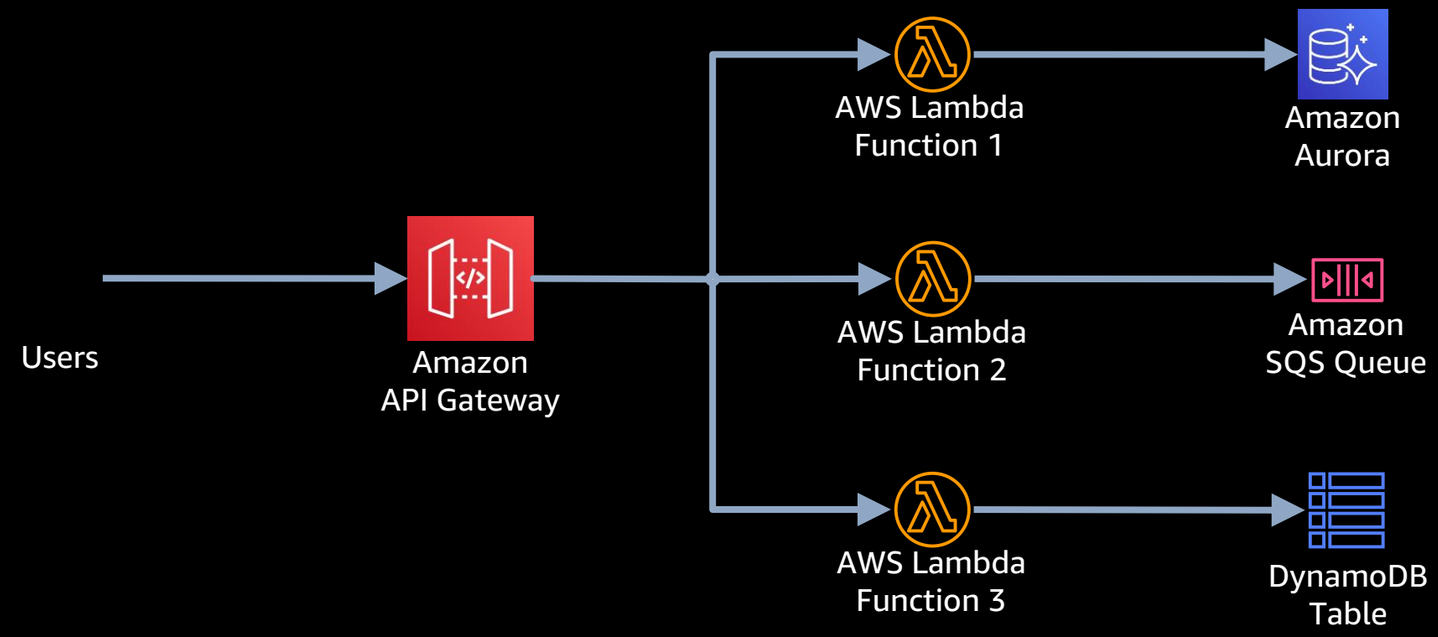


Summary

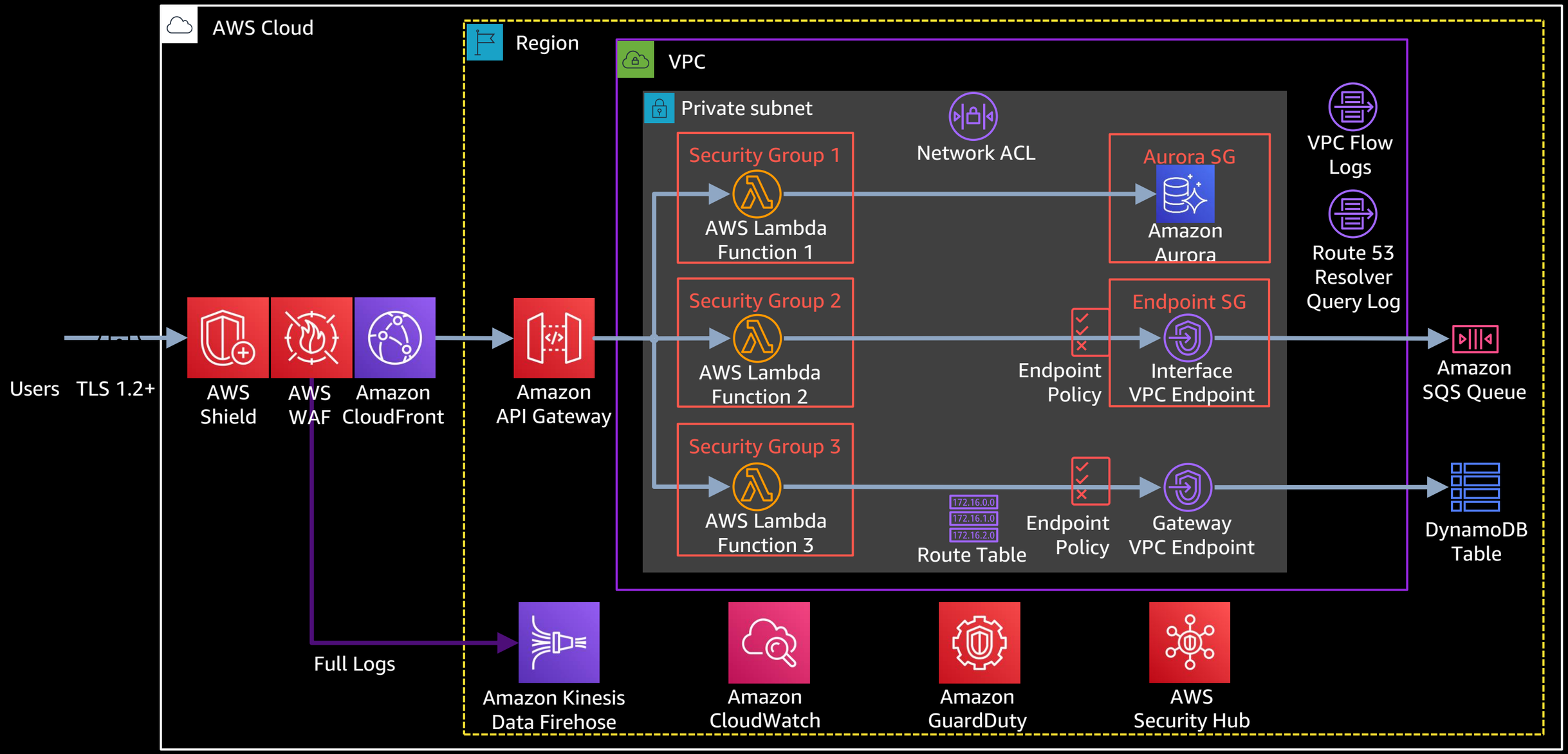


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Serverless architecture with secure defaults



More protection, control, and observability



Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.