AWS re:Invent

SRV314

Workshop: Securing Serverless Applications and AWS Lambda

Angela Wang
Solutions Architect
AWS

Nacho Garcia Alonso
Solutions Architect
AWS

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

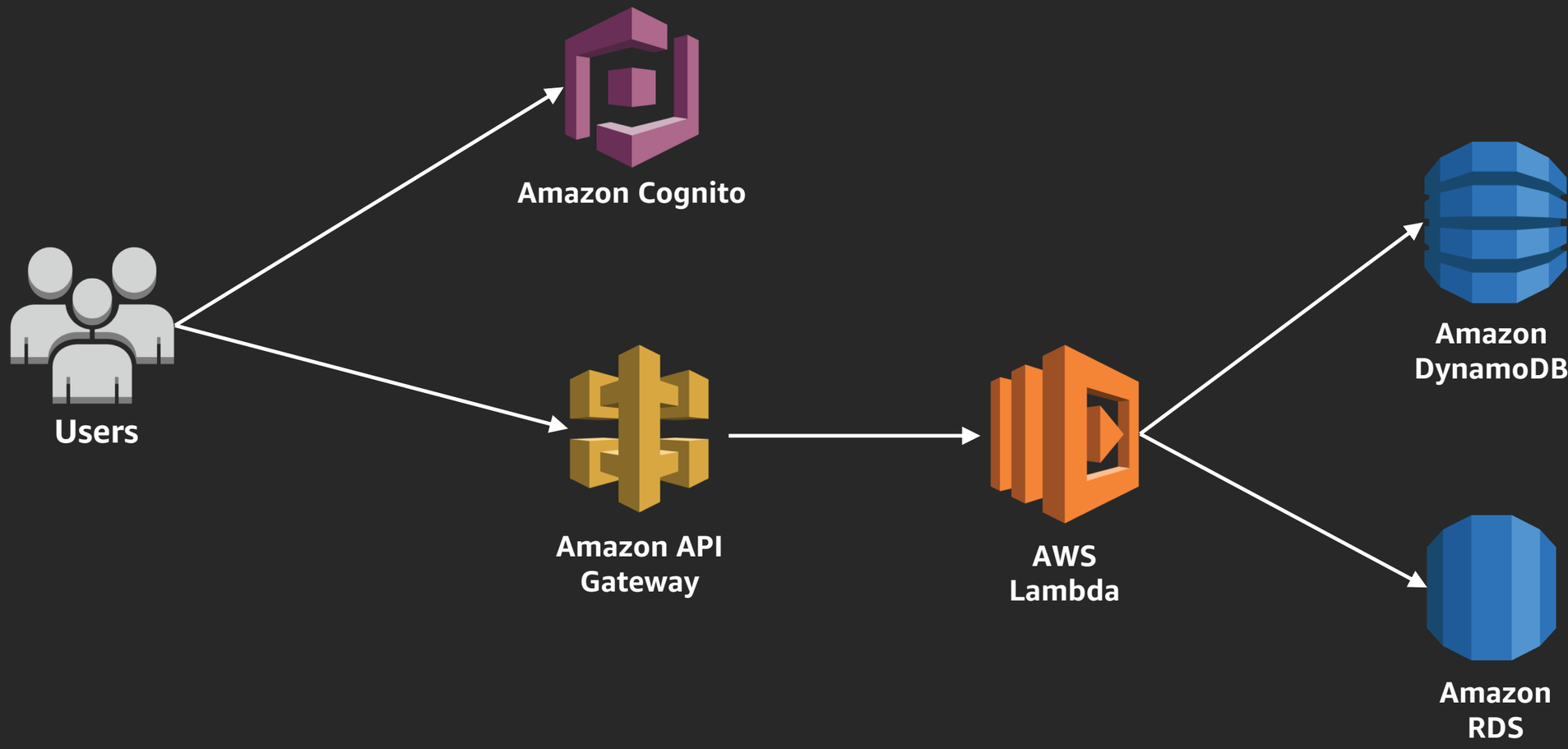
aws

Agenda

- Serverless security – is it different?
- Security domains for serverless applications
- Workshop scenario
- How to secure serverless applications
- Hands-on

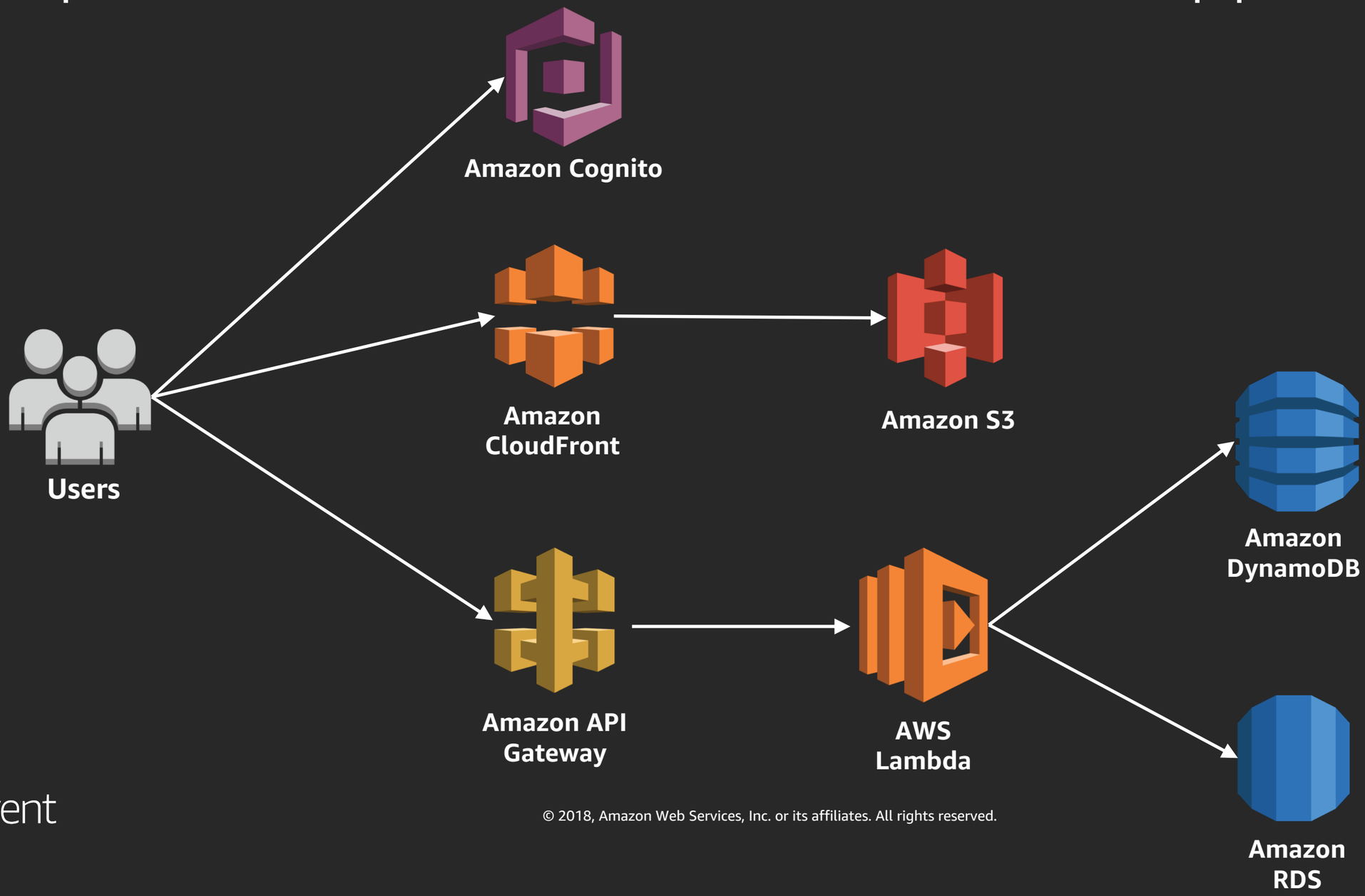
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample architecture for serverless API endpoint



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample architecture for serverless web app



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How is serverless security different?

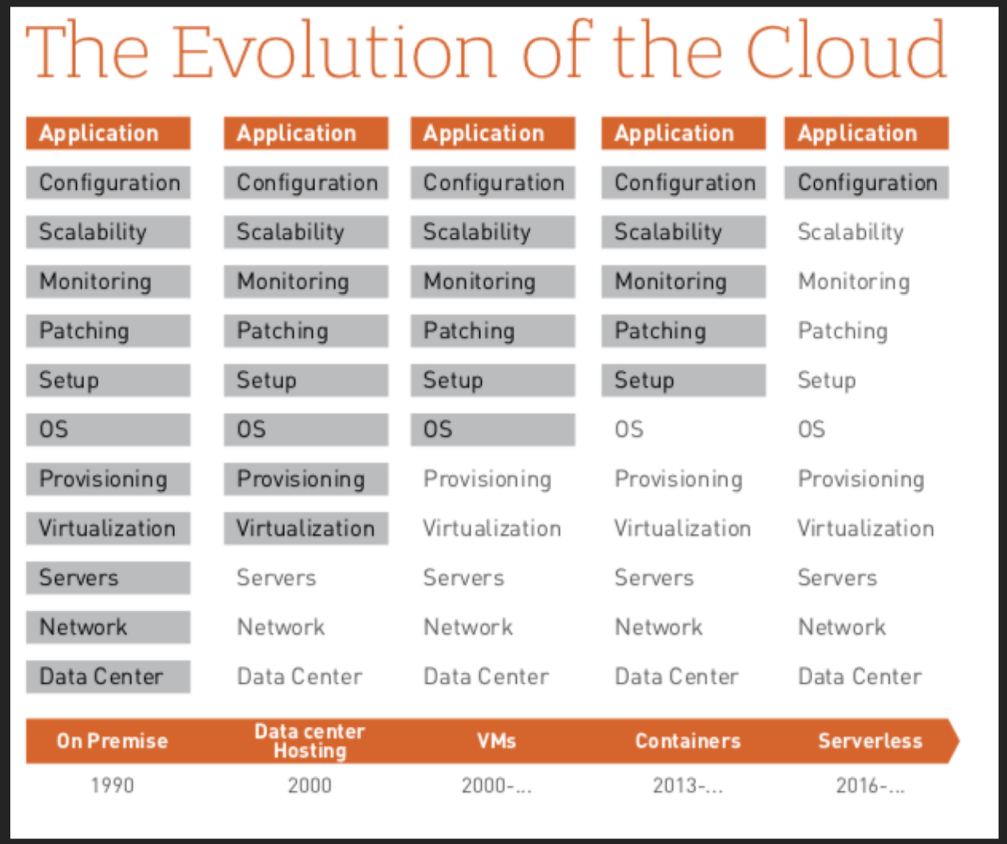


Image credit: Protego Serverless Security Primer eBook
https://www.protego.io/ebook/

Different:

- Reduced scope
- Ephemeral environment
- More events can trigger your lambda
- Old techniques might not be relevant

But still...

- Need to secure databases, s3 buckets, etc.
- Need to secure your code.
- Need to use minimum privilege access.
- Need to monitor usage and data flow.

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

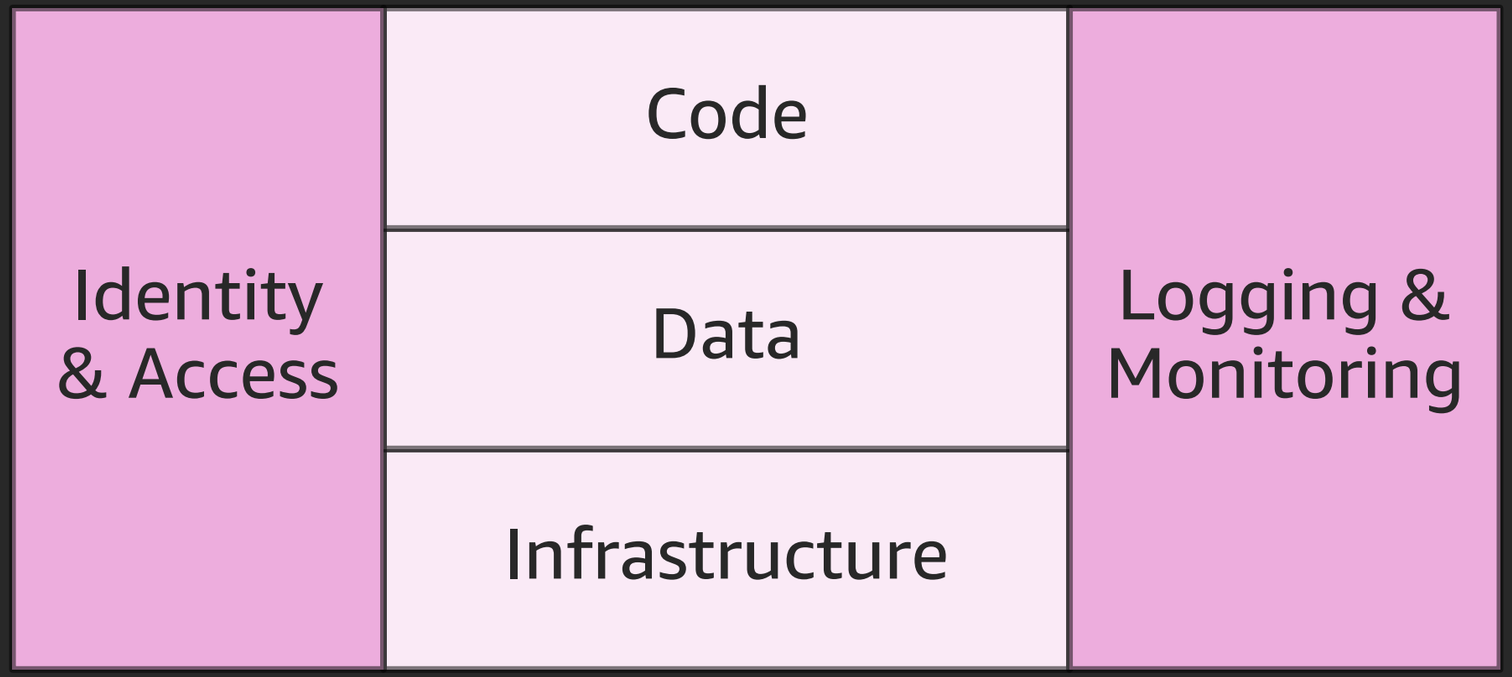
Security domains for serverless applications

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Domains of security for (serverless) applications



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OWASP 2017- Top 10 Web Application Security Risks

- **Exploitability**
- **Prevalence**
- **Detectability**
- **Technical impact**

Rank	Security risks
1	Injection
2	Broken Authentication
3	Sensitive Data Exposure
4	XML External Entities (XXE)
5	Broken Access Control
6	Security Misconfiguration
7	Cross-Site Scripting (XSS)
8	Insecure Deserialization
9	Using Components with Known Vulnerabilities
10	Insufficient Logging & Monitoring

https://www.owasp.org

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OWASP Top 10 mapped to security domains

Identity & Access

- Broken Authentication(#2)
- Broken Access Control (#5)

Code

- Injection (#1)
- XXE (#4)
- XSS (#7)
- Insecure Deserialization (#8)
- Using Components with Known Vulnerabilities (#9)

Data

- Sensitive Data Exposure (#3)

Infrastructure

- Using Components with Known Vulnerabilities (#9)

Logging & Monitoring

- Security Misconfiguration (#6)
- Insufficient Logging & Monitoring (#10)

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop scenario

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario: Wild Rydes (www.wildrydes.com)

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

3rd party functionality– unicorn customization

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sock image Credit: Freepik from www.flaticon.com

3rd party API: Unicorn customization

List customization options and prices:

GET /capes

GET /glasses

GET /horns

GET /socks

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Image Credit:
Smashicons, Freepik, from www.flaticon.com
johnny_automatic from www.openclipart.org

3rd party API: Unicorn customization

Create and manage customizations

POST /customizations

GET /customizations

GET /customizations/{id}

DELETE /customizations/{id}

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Admin API: register 3rd party partners

Register new partners

POST /partners

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop architecture – starting point

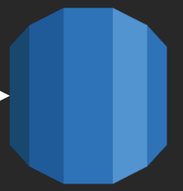
Deployed using SAM

(Serverless Application Model)

3rd party

Amazon API Gateway

AWS Lambda

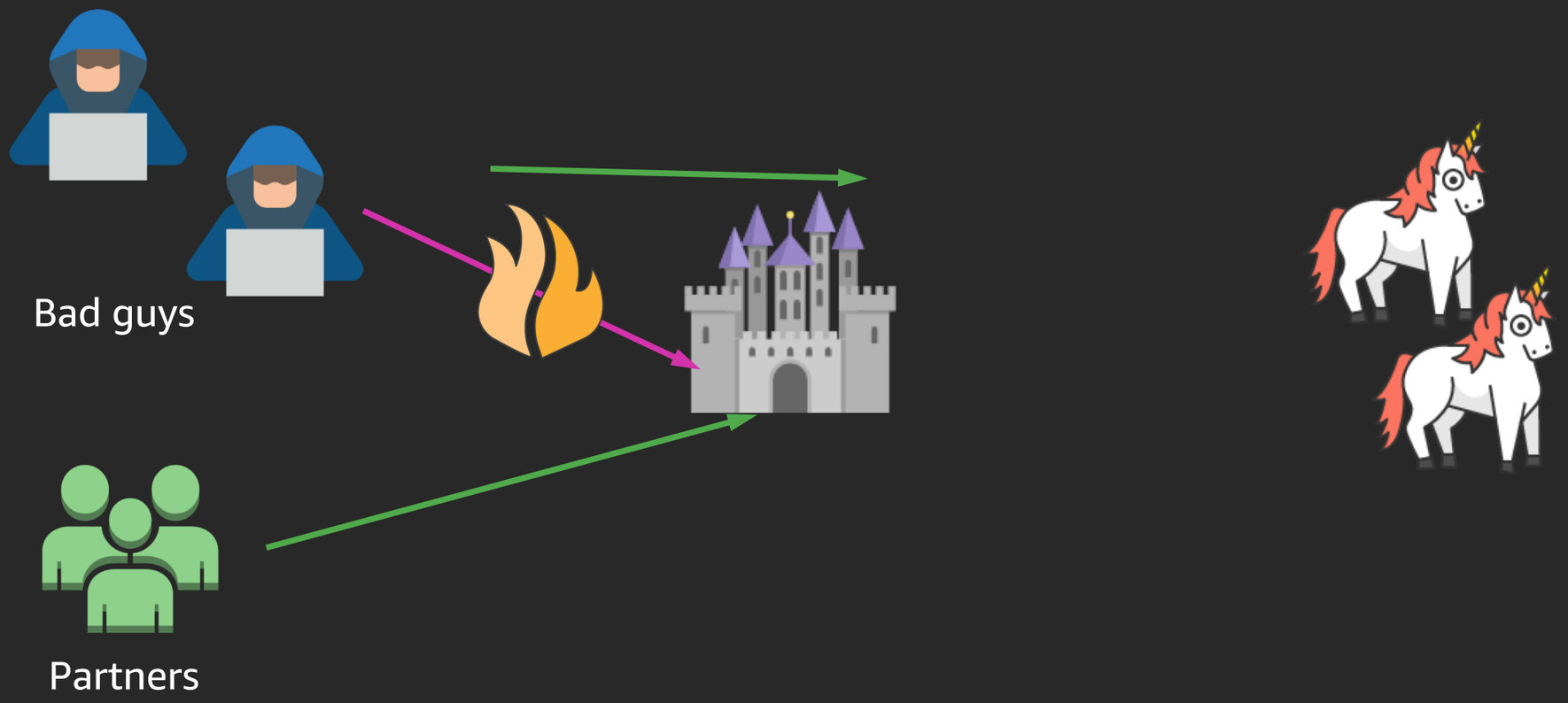


Amazon RDS

Not secure!

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Your task: secure the application against attackers!



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Image Credit:
pongsakornred, Freepik from www.flaticon.com

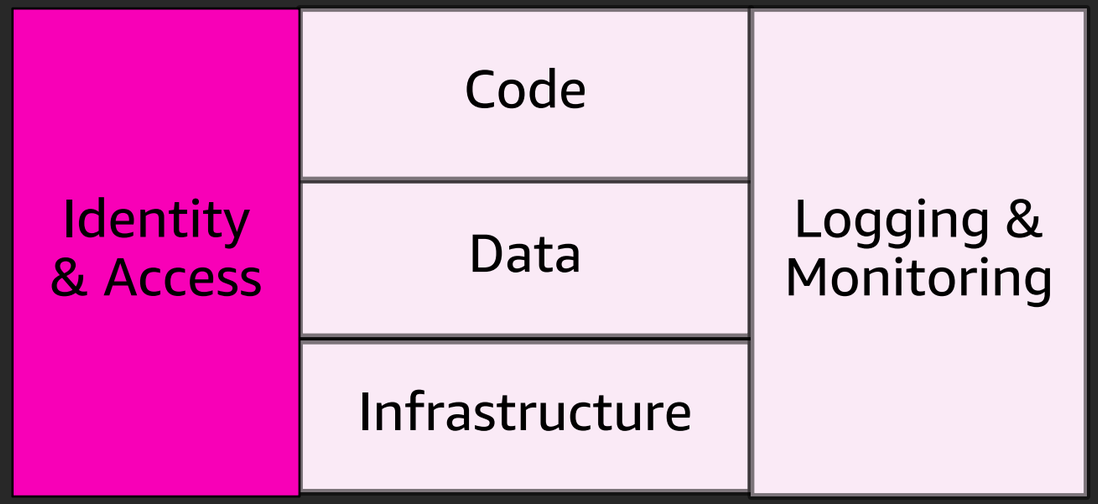
How to secure serverless applications

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Identity and access management for serverless applications



- Authenticate and authorize end-users/clients
- Access between backend services (e.g. AWS Lambda to DynamoDB tables)

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity and access management for serverless applications

Authenticate & authorize end-users/clients

API Gateway

3 ways for AuthN & AuthZ:

- AWS IAM
- Lambda Custom authorizer
- Cognito User Pool authorizer

Cognito

- Managed user directory or federation with other Idps
- Standard JWT tokens or AWS credentials

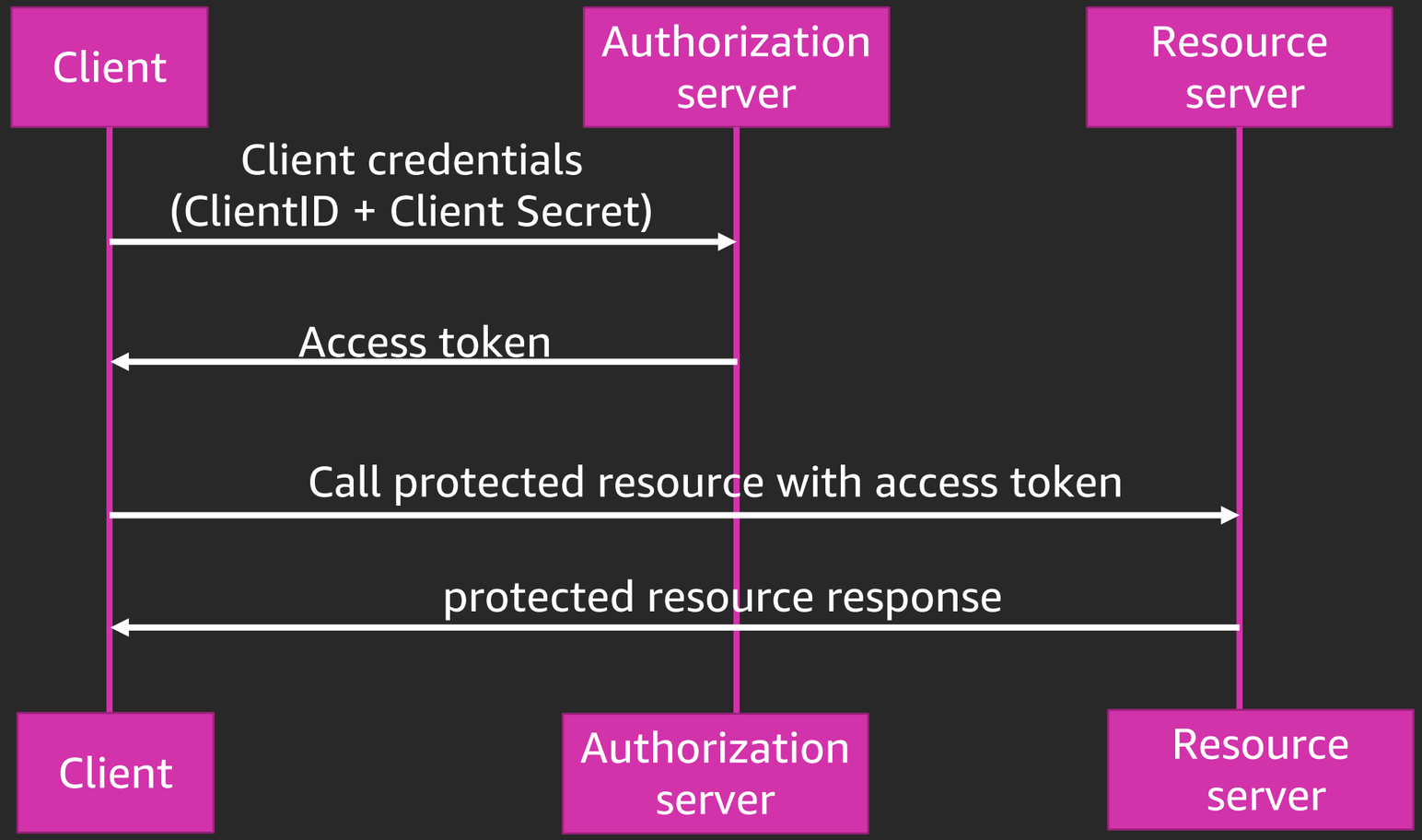
Access control between services

AWS Lambda:

- Invocation permissions
- Execution permissions

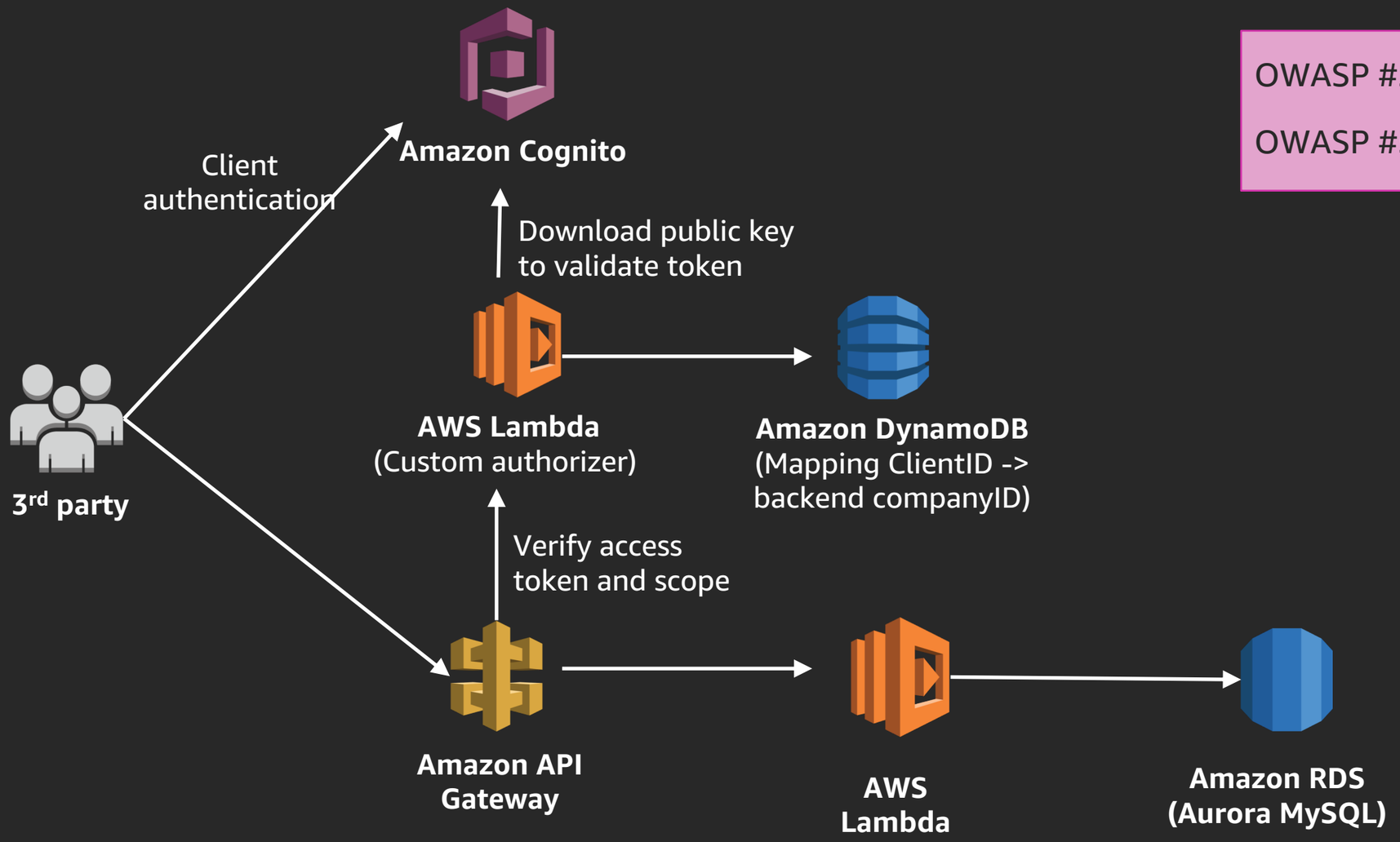
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop module 1: OAuth Client Credentials Flow



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop module 1: add authentication



OWASP #2: Broken Authentication

OWASP #5: Broken Access Control

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop module 1: add authentication

Amazon Cognito

Admin App client:
- Client ID: ZZZ
- Client Secret

Company foo app client:
- Client ID: XXX
- Client Secret

Company bar app client:
- Client ID: YYY
- Client Secret

...

Amazon DynamoDB

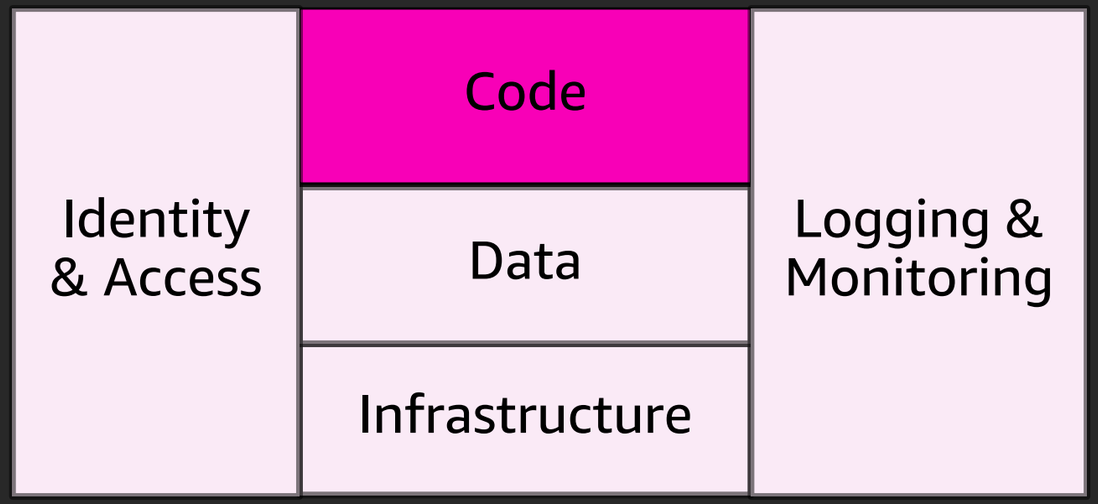
Mapping table	
ClientID	BackendID
XXX	1
YYY	2

Amazon Aurora

Company table	
ID	Name
1	Foo
2	Bar

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing code for serverless applications



- Input validation
- Dependency vulnerabilities
- Secrets in source code

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing code for serverless applications

Input validation

AWS WAF:

- *XSS Rules*
- *SQL injection rules*

API Gateway:

- Request Validation

AWS Lambda:

- Sanitize input in code

Dependency vulnerabilities

AWS Lambda:

- Minimize dependencies
- Vulnerability Dependency Check tools:
  - OWASP
  - Snyk
  - Twistlock
  - …

Storing secrets

AWS Secrets Manager

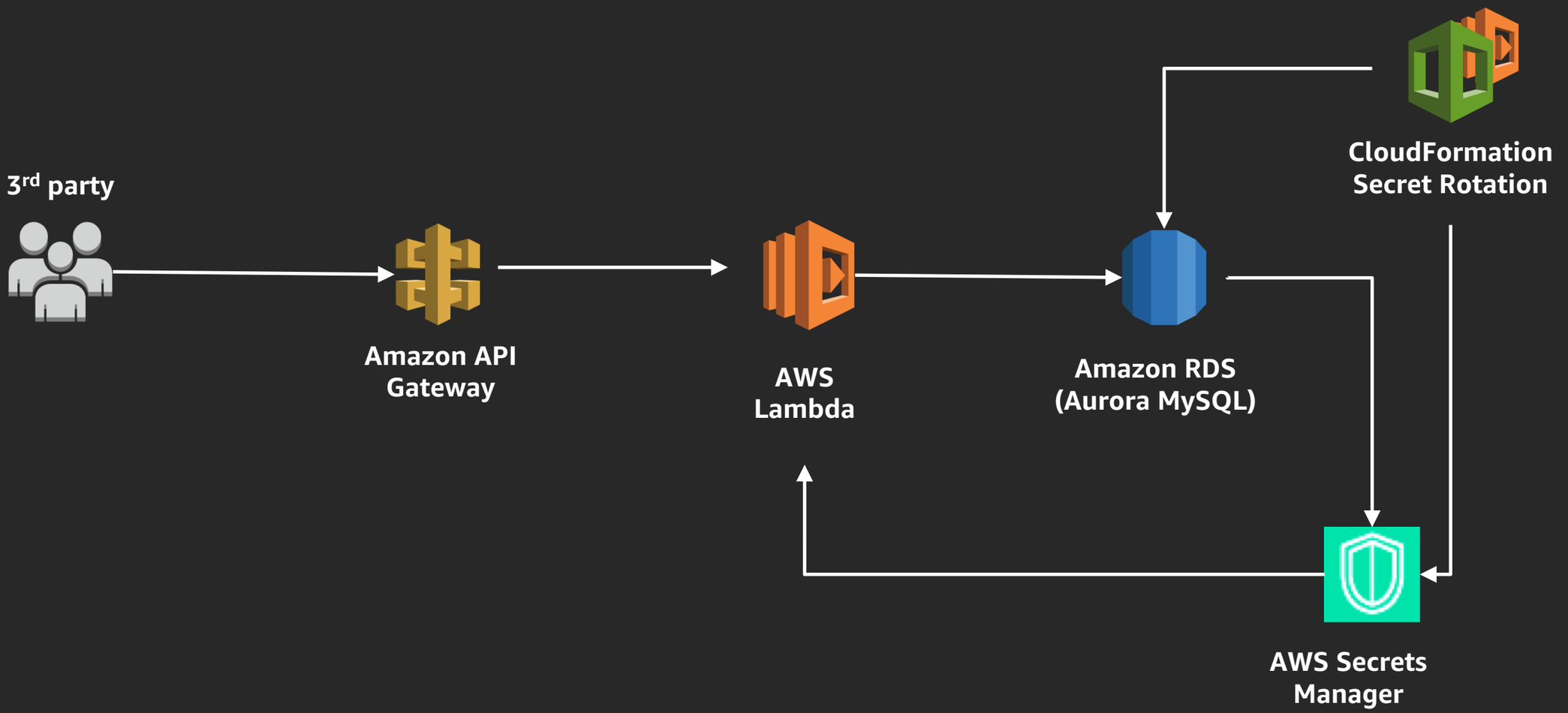
Systems Manager Parameter Store

AWS Lambda encrypted environment variables

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 2: Secret Manager

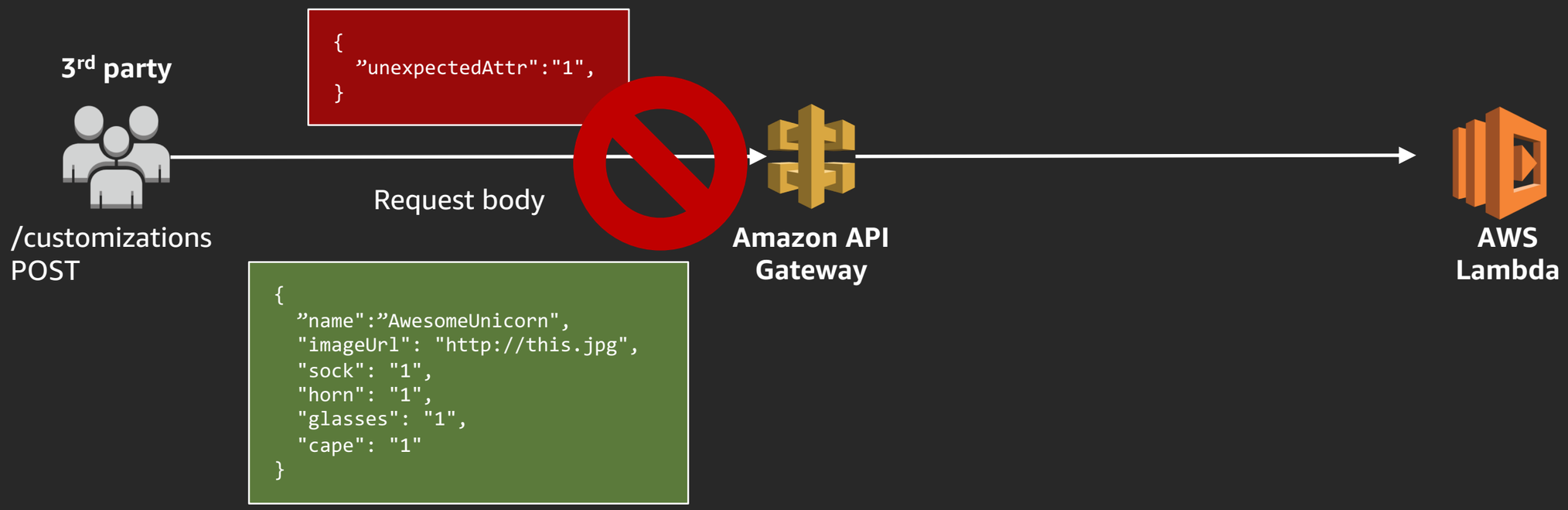
OWASP #3: Sensitive Data Exposure



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 3: Input Validation

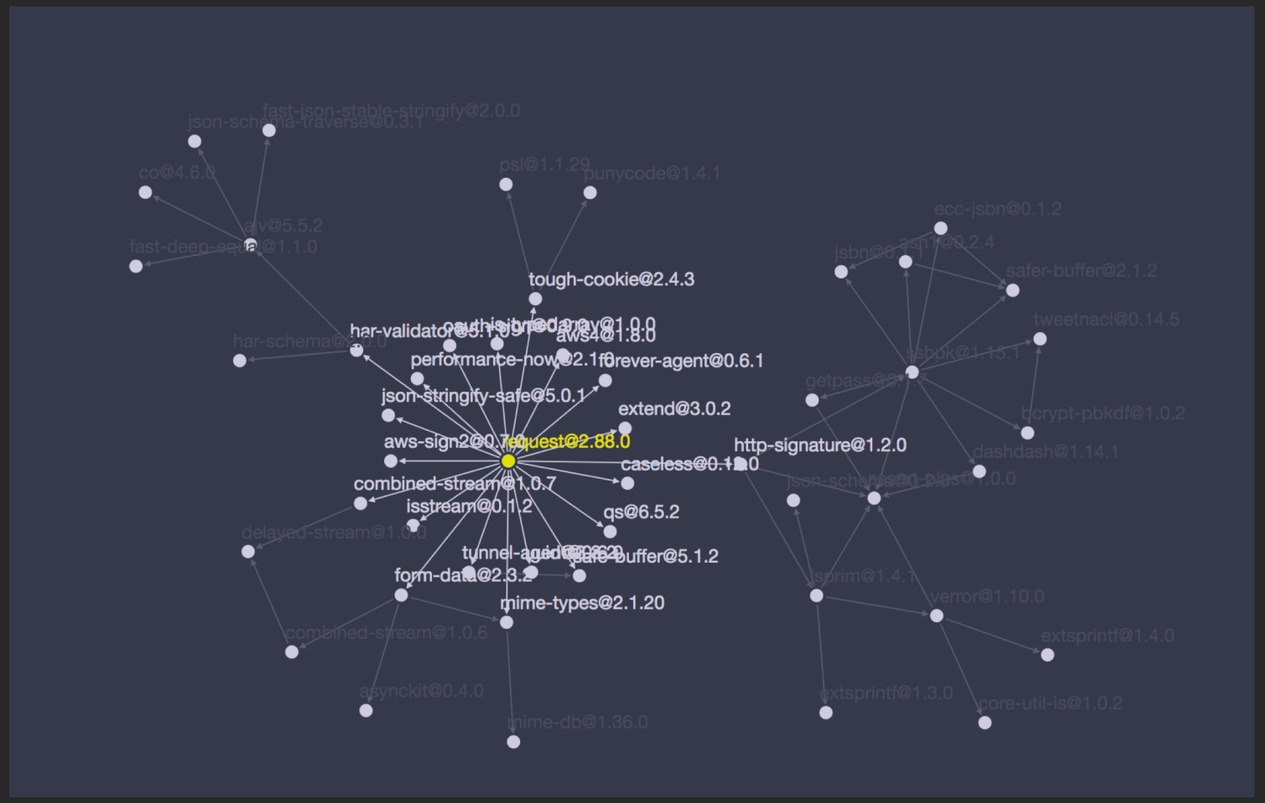
- OWASP #1: Injection
- OWASP #8: Insecure Deserialization



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 7: Dependency Vulnerability

- OWASP #9: Using Components with Known Vulnerabilities

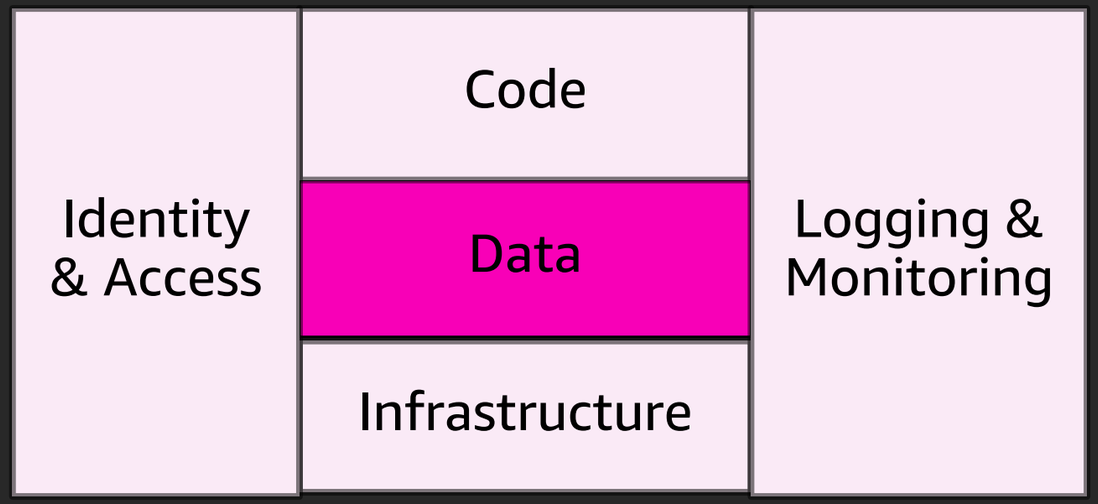


http://npm.anvaka.com/#/view/2d/request

- Check for vulnerabilities on our dependencies
  - OWASP Dependency Check: https://www.owasp.org/index.php/OWASP_Dependency_Check
  - Third party tools
- Remove unused dependencies
  - depcheck: https://www.npmjs.com/package/depcheck

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing data for serverless applications



Your responsibility:

- Data Classification and Data Flow
- Tokenization
- Encryption at rest
- Encryption in transit
- Data Backup/Replication/Recovery

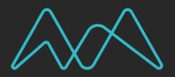
AWS platform takes care of:

- Automatic replication of data across availability zones for high durability
- Managed backups/ encryption

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing data for serverless applications

Data Classification



Amazon Macie

Data Flow

AWS X-Ray

Data Tokenization

- DIY
- AWS Marketplace

Data Encryption at rest

AWS KMS:

- Server-side encryption
  - S3, DynamoDB, RDS
  - …
- Client-side encryption

Data Encryption in transit

API Gateway : HTTPS only

Amazon Certificate Manager:

- Manage SSL certs for custom domains

Data backup/Replication

S3

- Versioning
- MFA delete
- Cross-region replication

DynamoDB

- On-demand backup
- Point-in-time restore
- Change streams

RDS

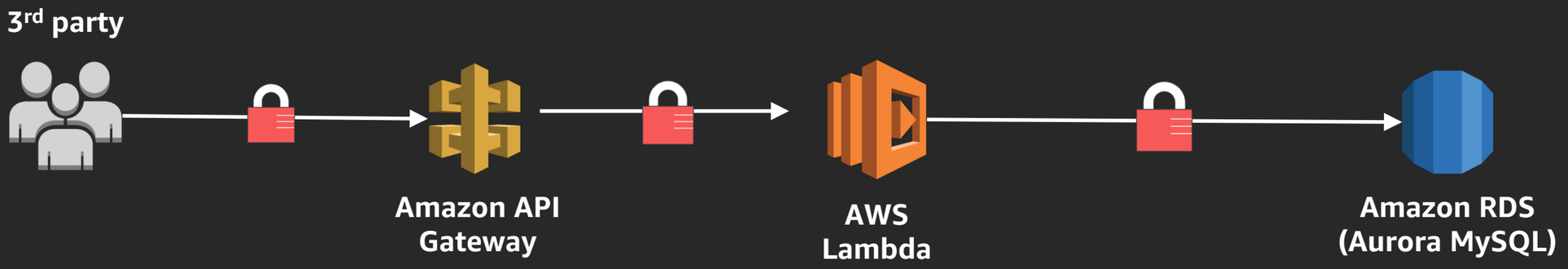
- Automated backups

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 4: encryption in transit

OWASP #3: Sensitive Data Exposure

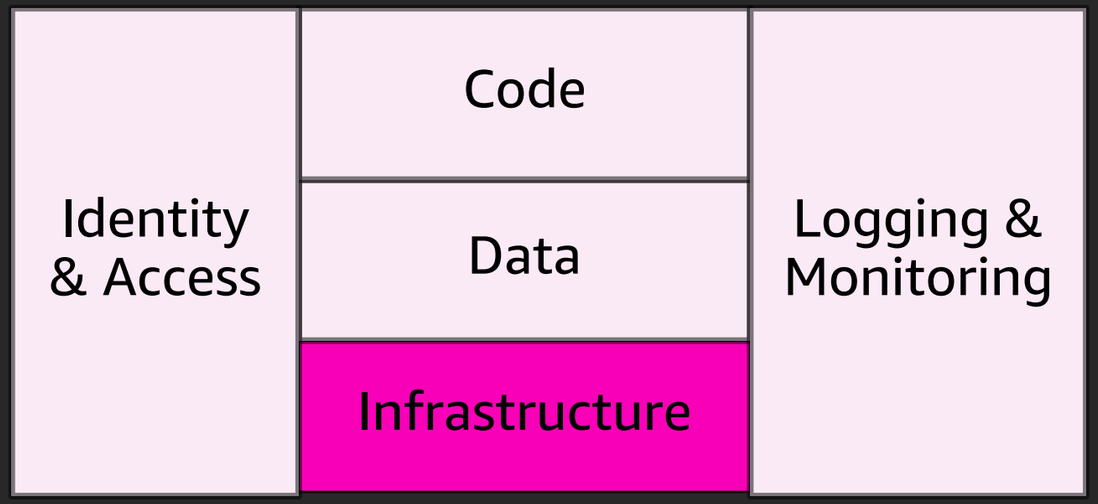
```
{
      host: ”database.host.com",
      user: "admin",
      password: ”xxxxxxxxx",
      database: "unicorn_customization"
}
```




```
{
      host: ”database.host.com",
      user: "admin",
      password: ”xxxxxxx",
      database: "unicorn_customization",
      ssl: "Amazon RDS"
}
```


© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing infrastructure for serverless applications



Your responsibility:

- DDOS protection
- Throttling/ Rate limiting
- Network boundaries

Serverless platform takes care of:

- Physical security
- Virtualization
- OS security & patching
- Scaling & HA

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing infrastructure for serverless applications

DDOS protection + Throttling/ Rate limiting

AWS Shield Standard

AWS Shield Advanced

AWS WAF:

- *Geoblocking*
- *IP reputation lists*
- Rate-based rules
- Size constraint
- …

API Gateway:

- Account level throttling
- API Stage level throttling
- Usage Plan
  - Method level throttling
  - Metered by API key
  - Request rate and Quota limits

AWS Lambda :

- concurrency Limits

Network boundaries

API Gateway:

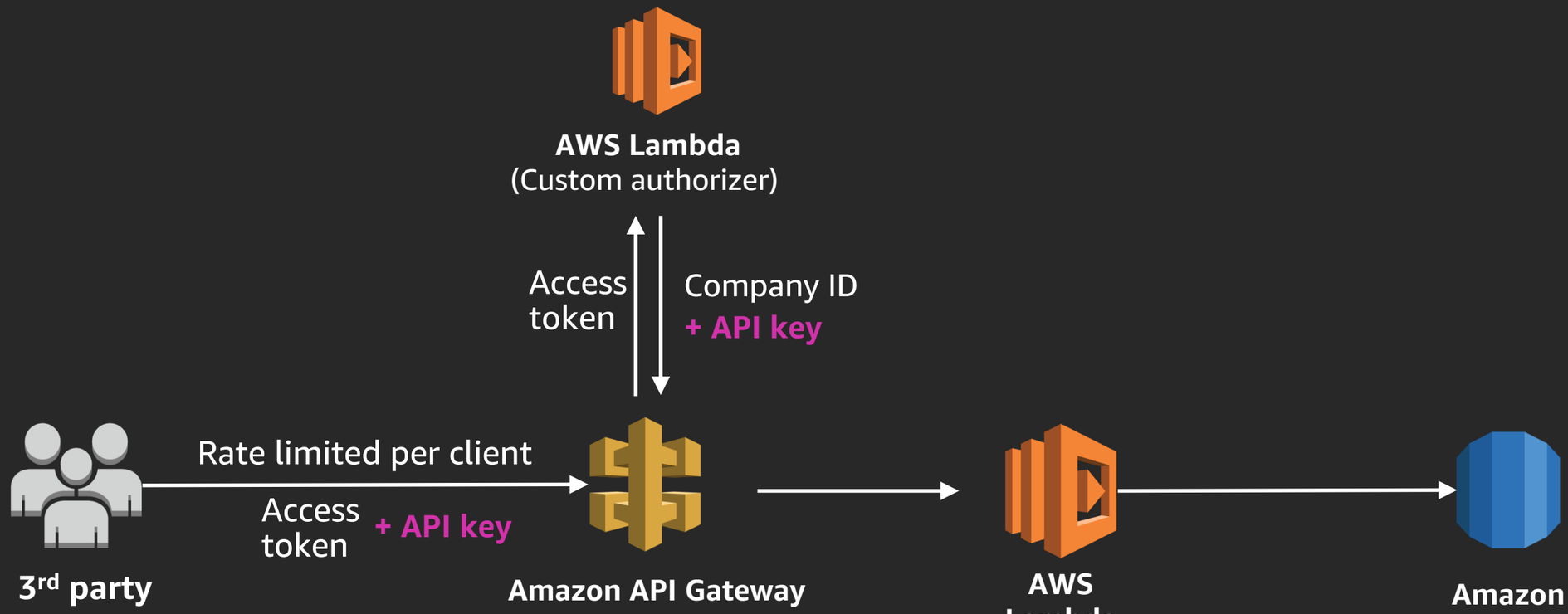
- Private VPC endpoints
- Resource policy

AWS Lambda:

- Access resources in VPC
- Security groups
- NACLs
- Proxy-based egress filtering

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 5: Usage Plans



Basic usage plan

- 5 requests/s
- 1000 requests/month

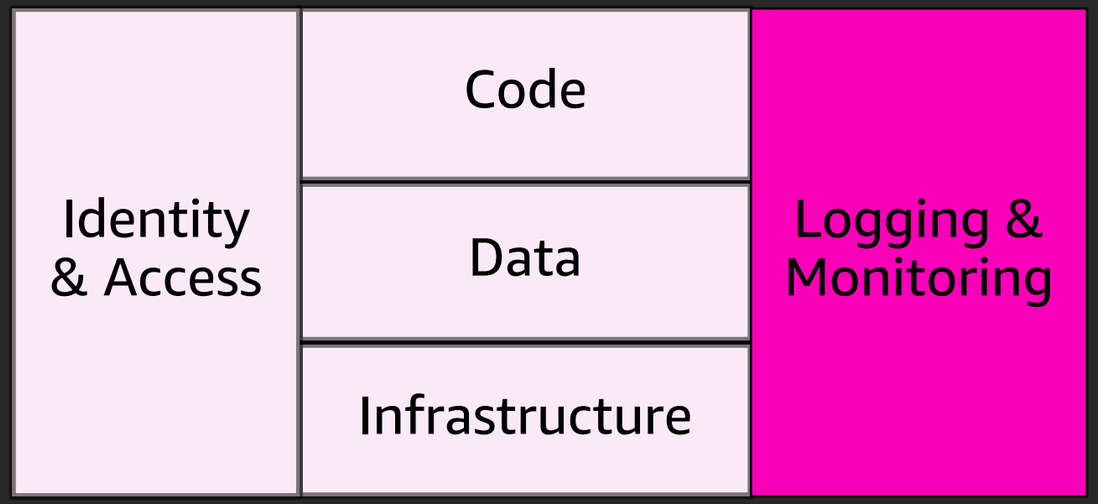
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 6: WAF

- IP reputation lists
- Size restrictions
- SQL injection
- XSS
- …

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logging & monitoring for serverless applications



- Application logs
- Access logs
- Control plane audit logs
- Metrics
- Alarms
- Compliance validation

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logging & monitoring for serverless applications

Logging and tracing

API Gateway :

- Access logs
- Execution logs

AWS Lambda :

- CloudWatch Logs

X-Ray

Metrics

API Gateway :

- Built-in CloudWatch metrics
- Detailed CloudWatch metrics

AWS Lambda :

- Built-in CloudWatch metrics
- Custom CloudWatch metrics
- Metrics from CloudWatch logs
- Third party tools:
  - IOPipe, Datadog, …

Compliance validation

AWS Config

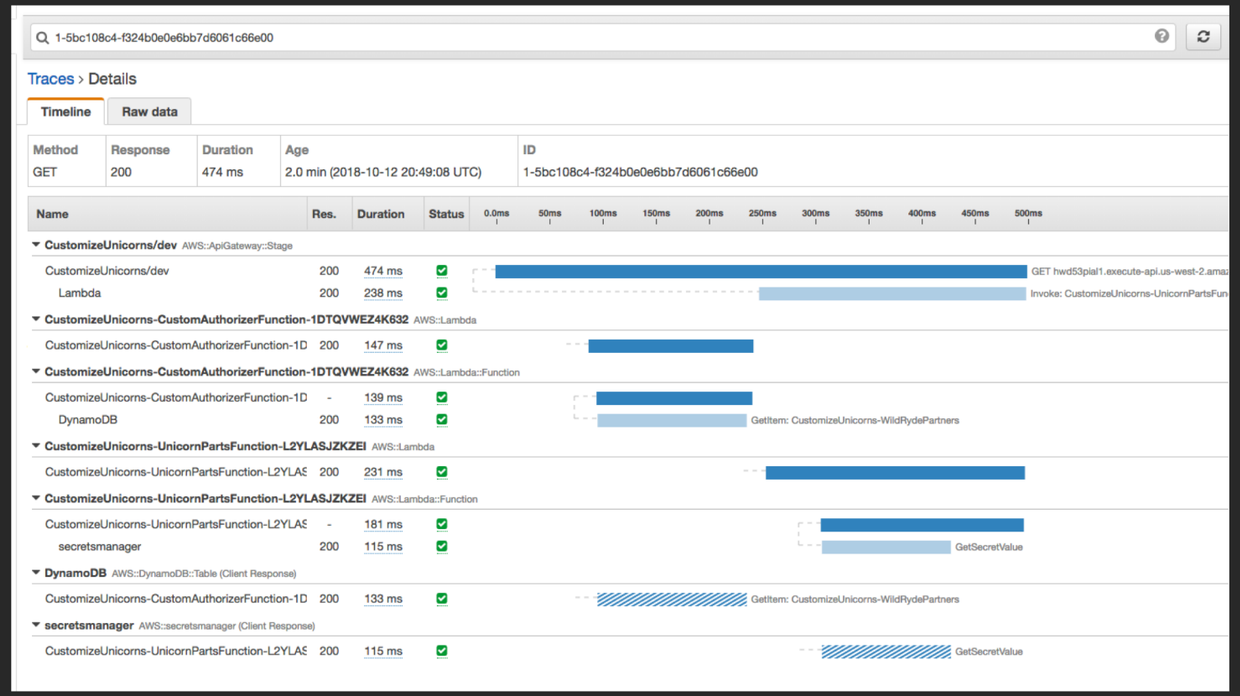
CloudWatch Events

AWS Budgets

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 8: XRay

OWASP #10: Insufficient Logging & Monitoring



AWS re:Invent

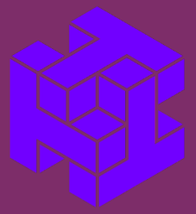
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Serverless Security Partners

PURESEC

snyk



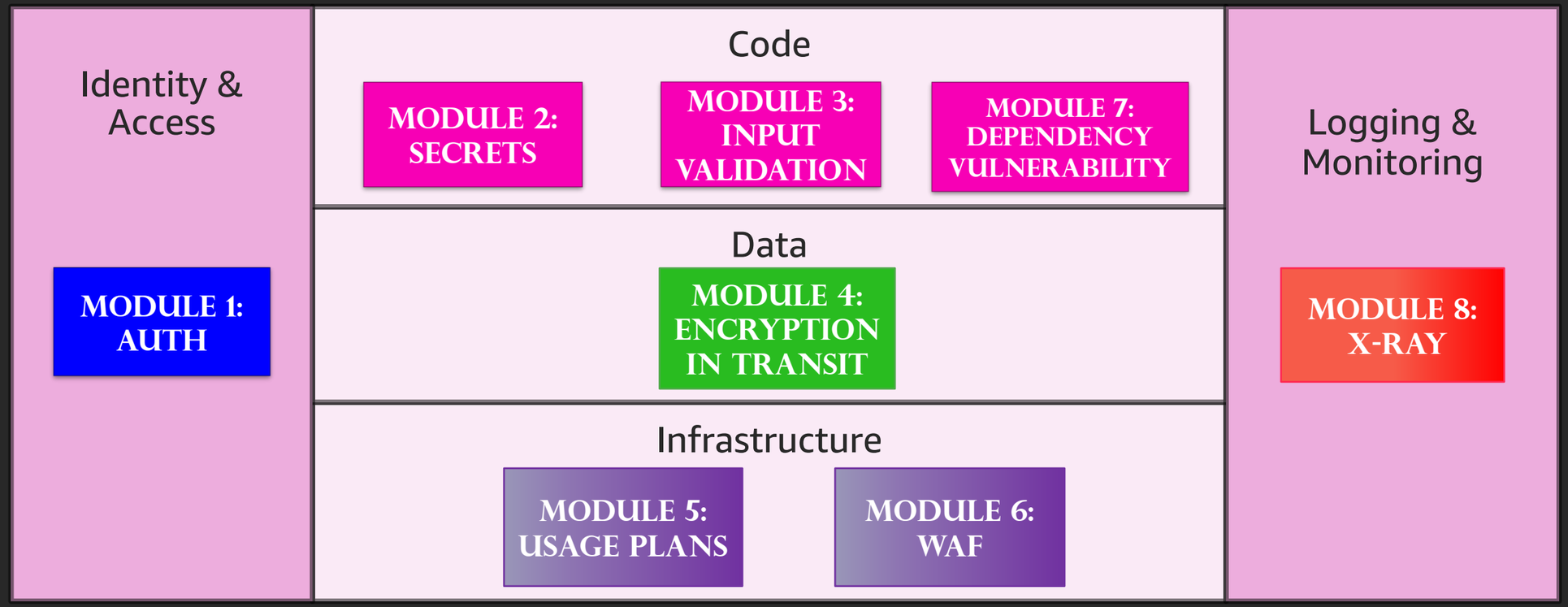
Twistlock™

Protego

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop

Link to the workshop: https://amzn.to/serverless-security
Module 0 mandatory
Module 1-8: Pick your own battle!



Thank you!

Angela Wang
Nacho Garcia Alonso

Please remember to complete your session evaluation for **SRV314** in the app

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Please complete the session survey in the mobile app.

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws