AWS re:Invent

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

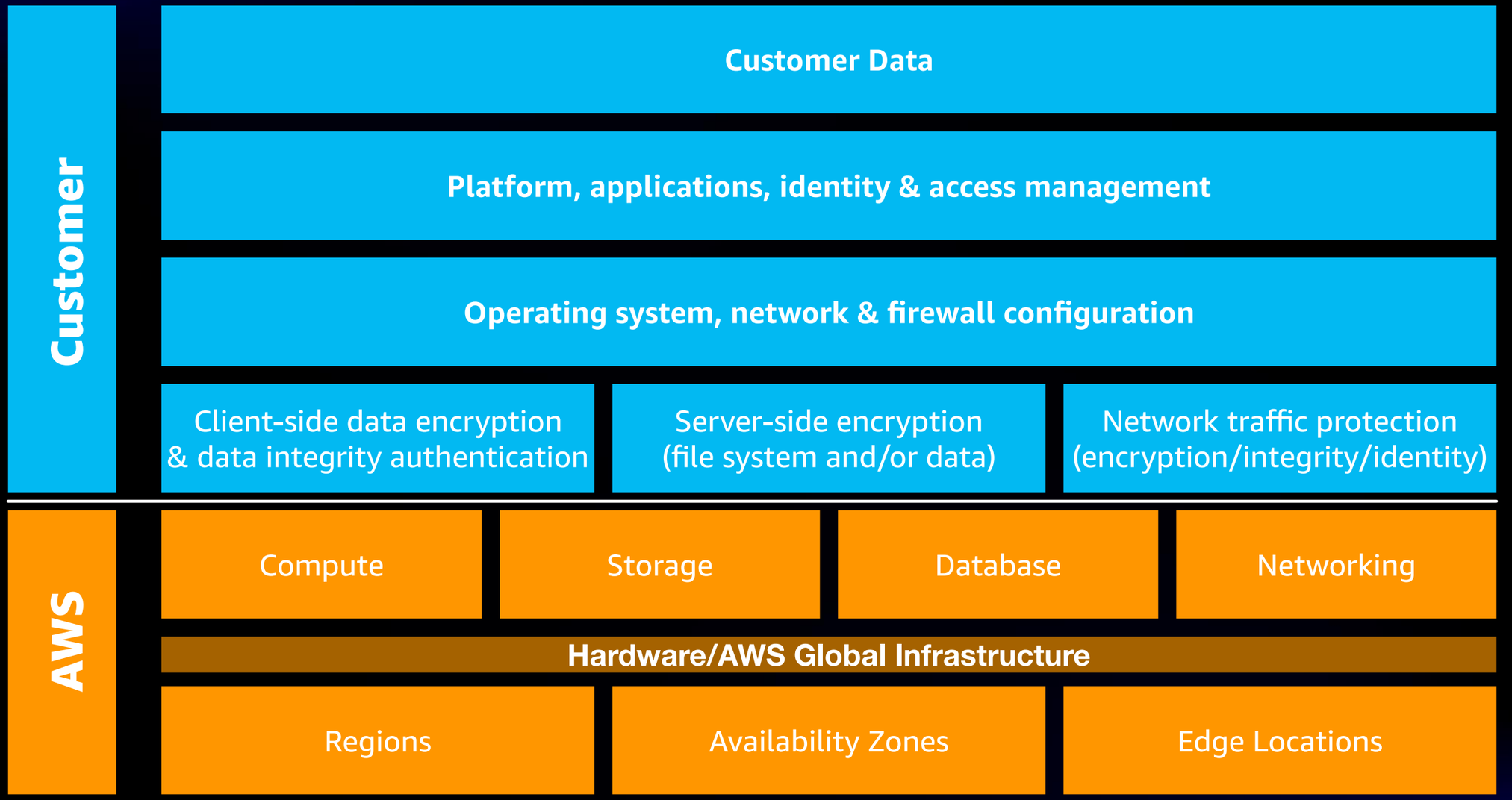
SVS303

Serverless security

Chris McPeek
Principal Solutions Architect
Amazon Web Services

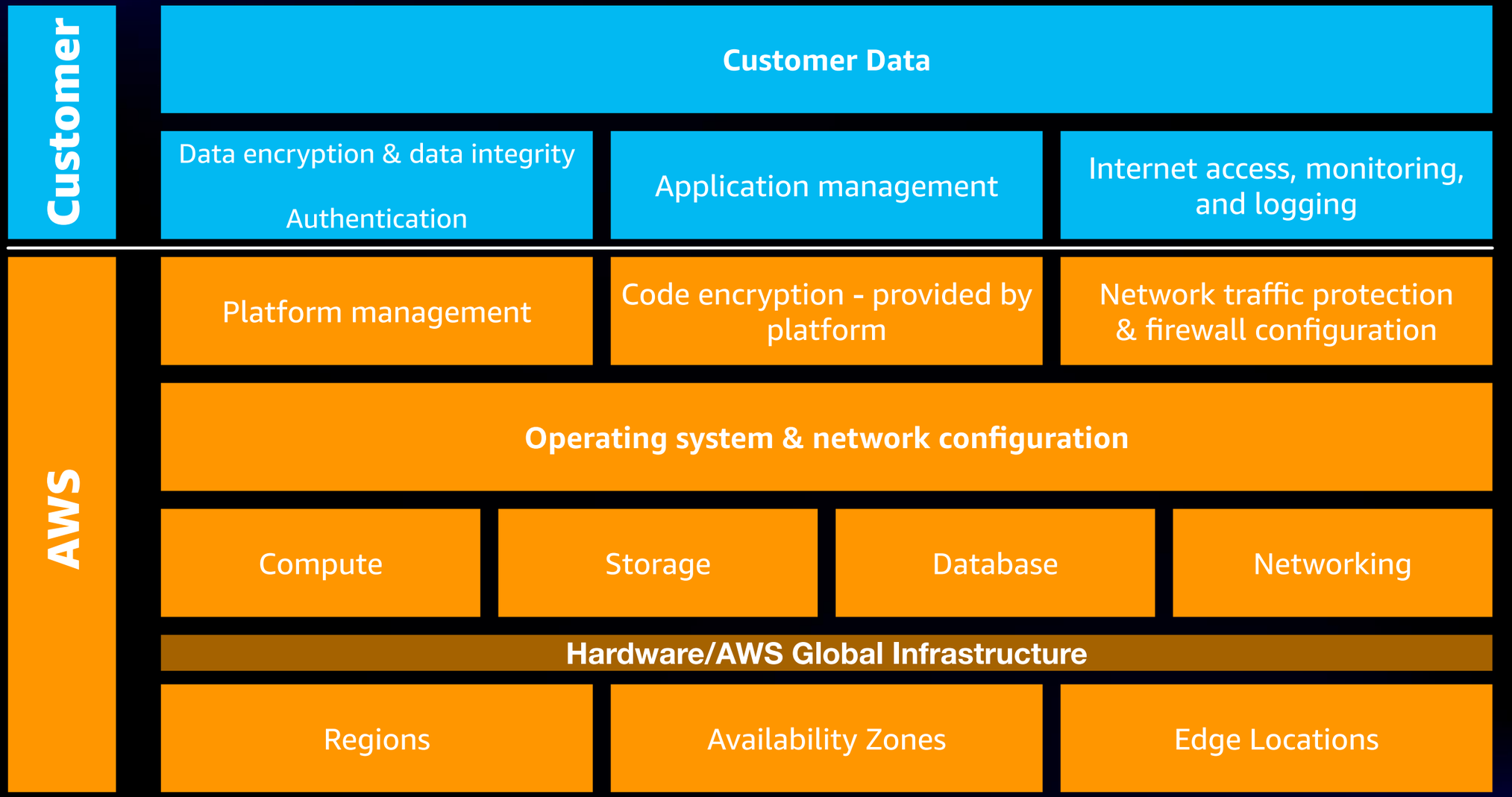
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model: “Serverful"



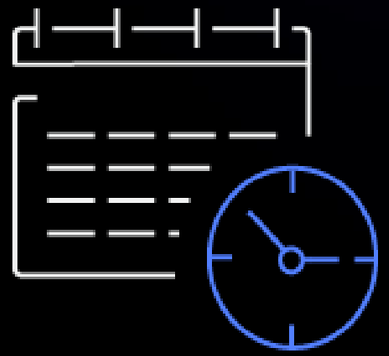
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model: Serverless

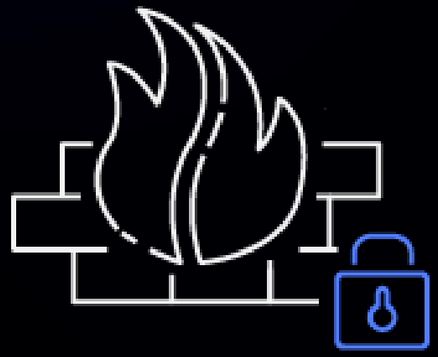


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What else is different?



Ephemerality



Diffused perimeter



Fine-grained control



Tooling

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

What stays the same?



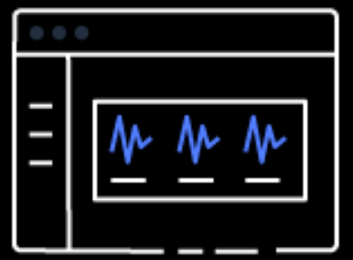
Securing data



Quality code



Least privilege



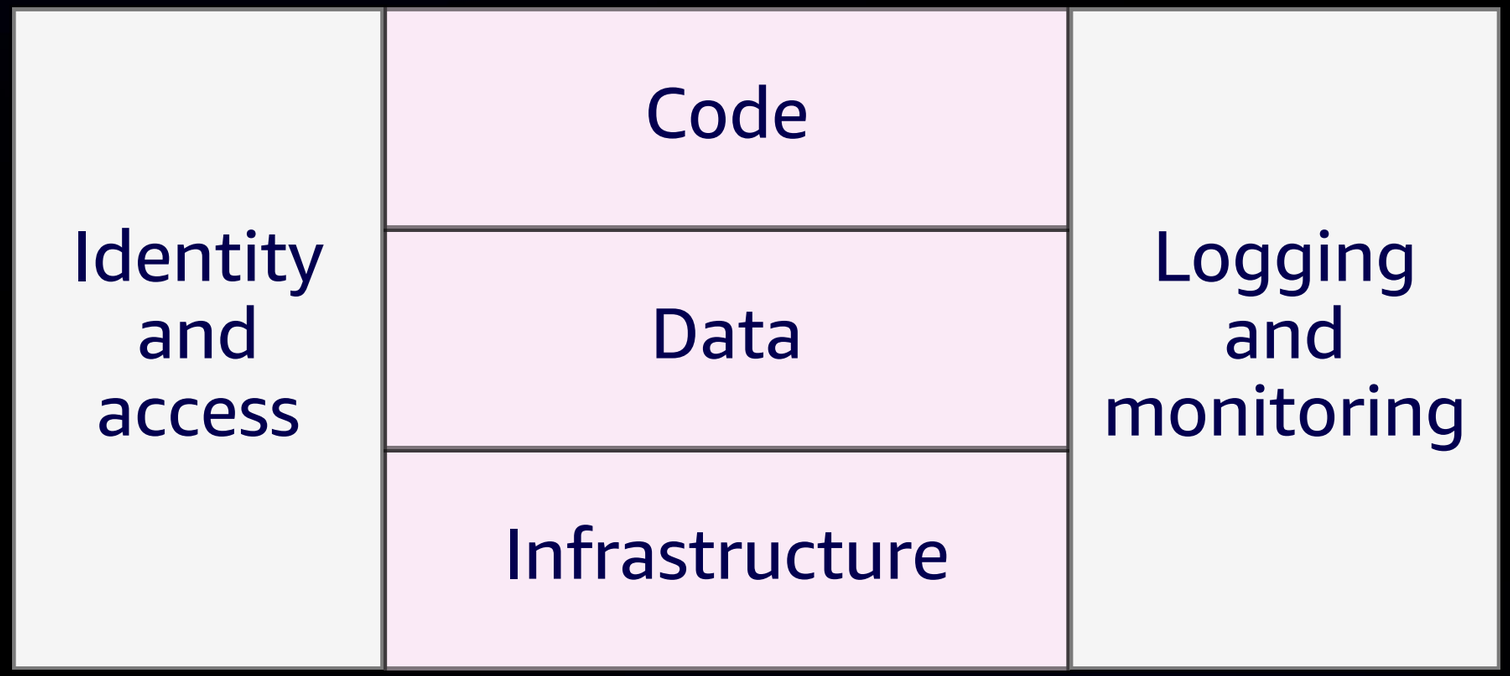
Monitoring

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

Security domains for serverless applications

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

Domains of security for (serverless) applications



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

OWASP top 10 web application security risks

2017

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

2021

Rank		Security risks
1	↑	Broken access control
2	↑	Cryptographic failures
3	↓	Injection
4	(new)	Insecure design
5	↑	Security misconfiguration
6	↑	Vulnerable and outdated components
7	↓	Identification and authentication failures
8	(new)	Software and data integrity failures
9	↑	Security logging and monitoring failures
10	(new)	Server-side request forgery

https://www.owasp.org

aws

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

OWASP top 10 mapped to security domains

Identity and access

- Broken access control (#1)
- Identification and authentication failures (#7)

Code

- Injection (#3)
- Insecure design (#4)
- Vulnerable and outdated components (#6)
- Software and data integrity errors (#8)
- Server-side request forgery (#10)

Data

- Cryptographic failures (#2)
- Software and data integrity failures (#8)

Infrastructure

- Insecure design (#4)
- Vulnerable and outdated components (#6)
- Server-side request forgery (#10)

Logging and monitoring

- Security misconfiguration (#5)
- Security logging and monitoring failures (#9)

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

Workshop scenario

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

Scenario: Wild Rydes (www.wildrydes.com)

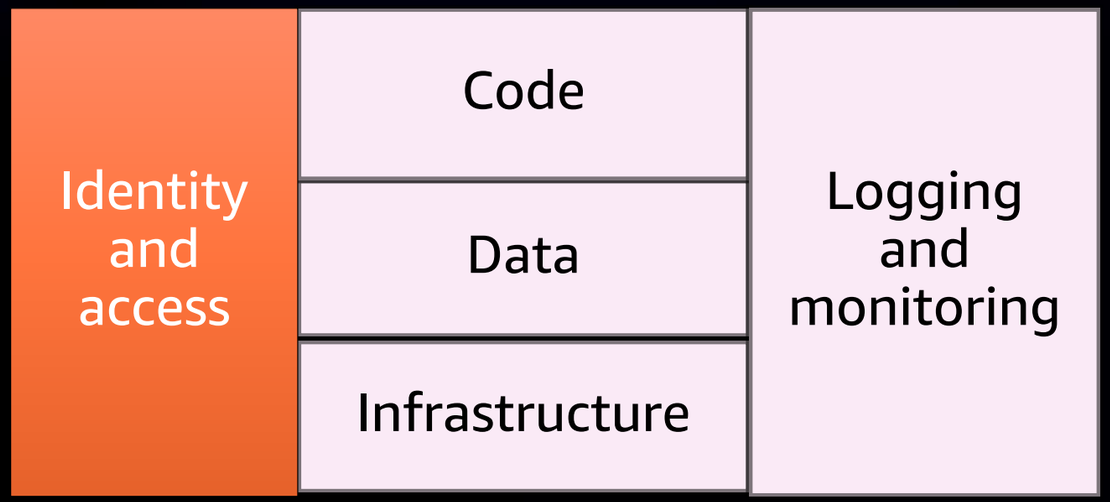


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How to secure serverless applications

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

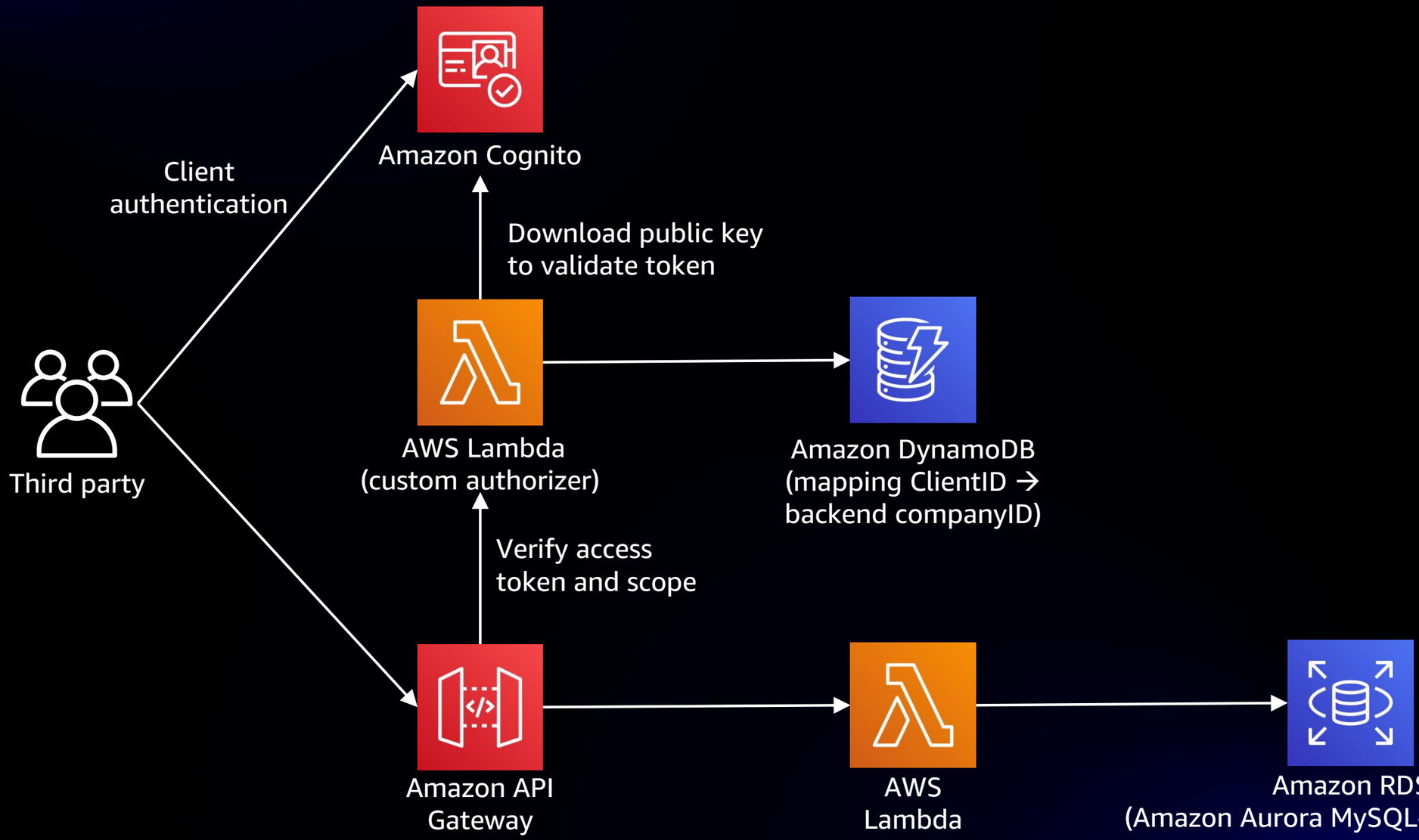
Identity and access management for serverless applications



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

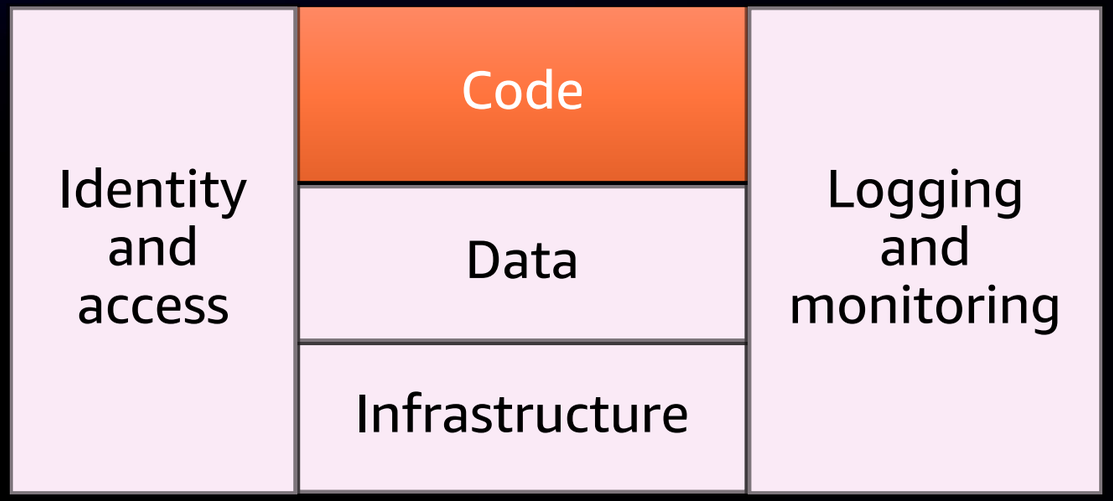
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop module 1: Add authentication



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

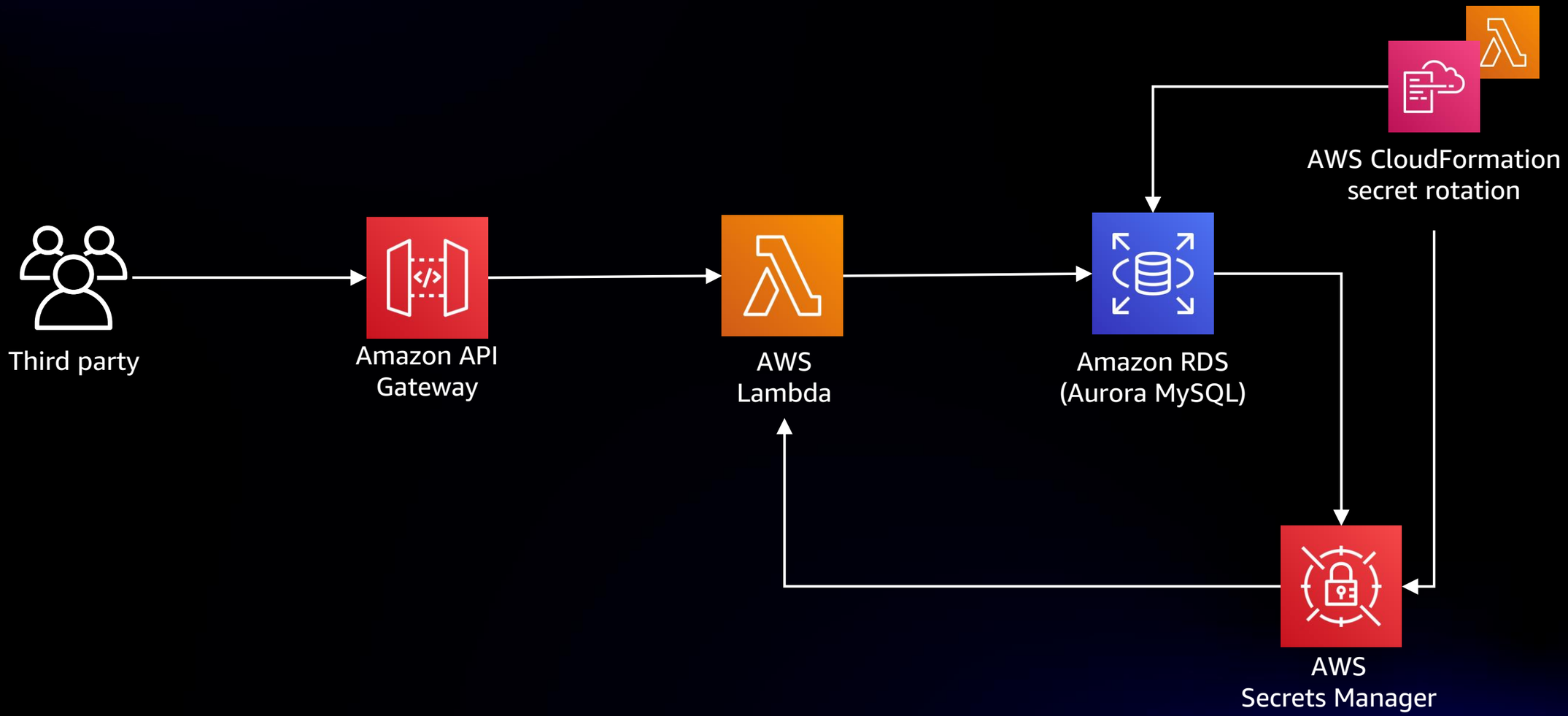
Securing code for serverless applications



- Input validation
- Dependency vulnerabilities
- Secrets in source code

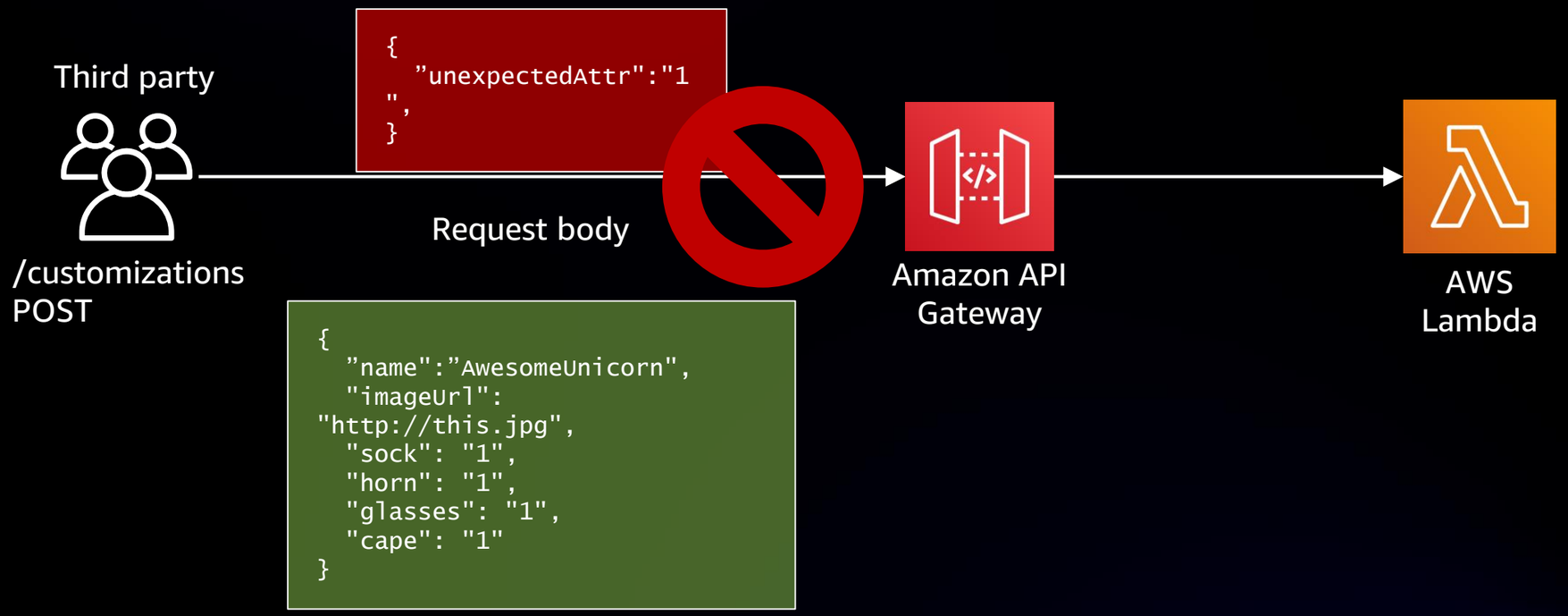
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 2: Managing secrets



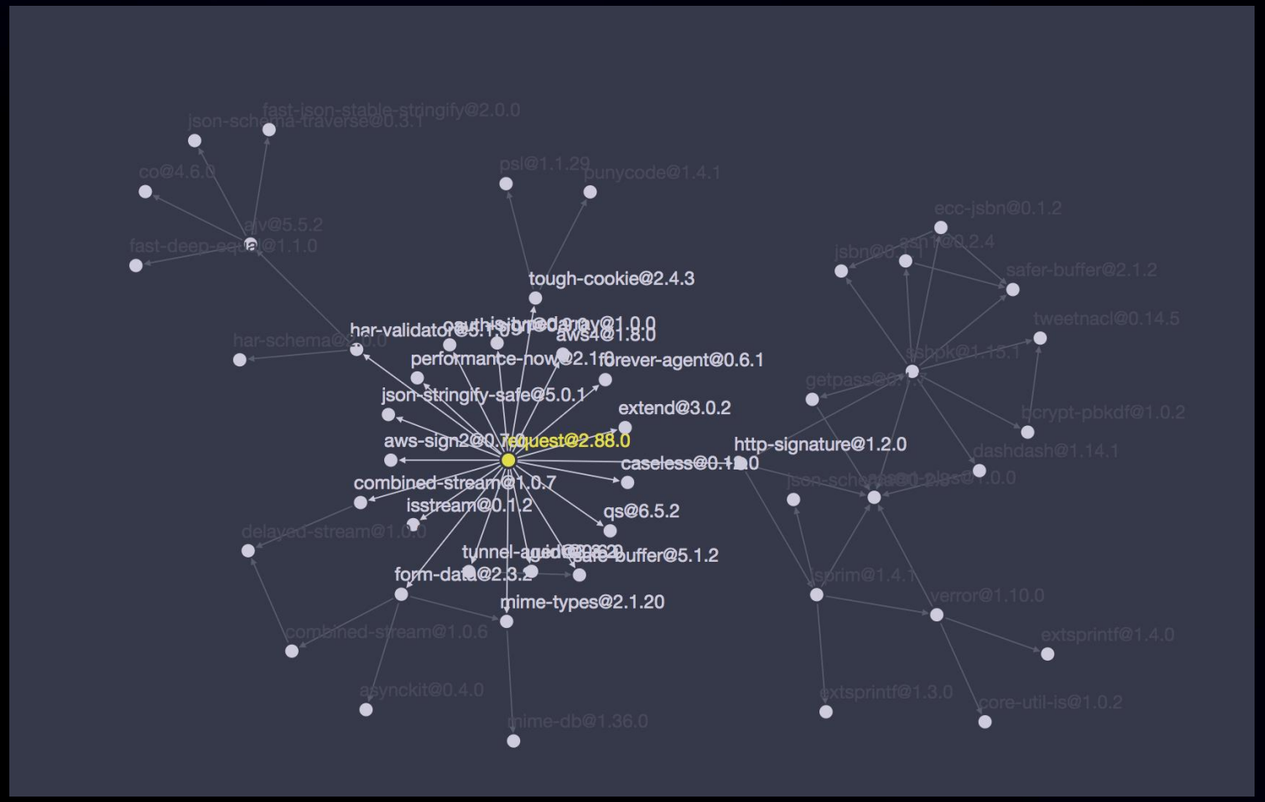
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module 3: Input validation



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

Module 7: Dependency vulnerability



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

Check for vulnerabilities on our dependencies

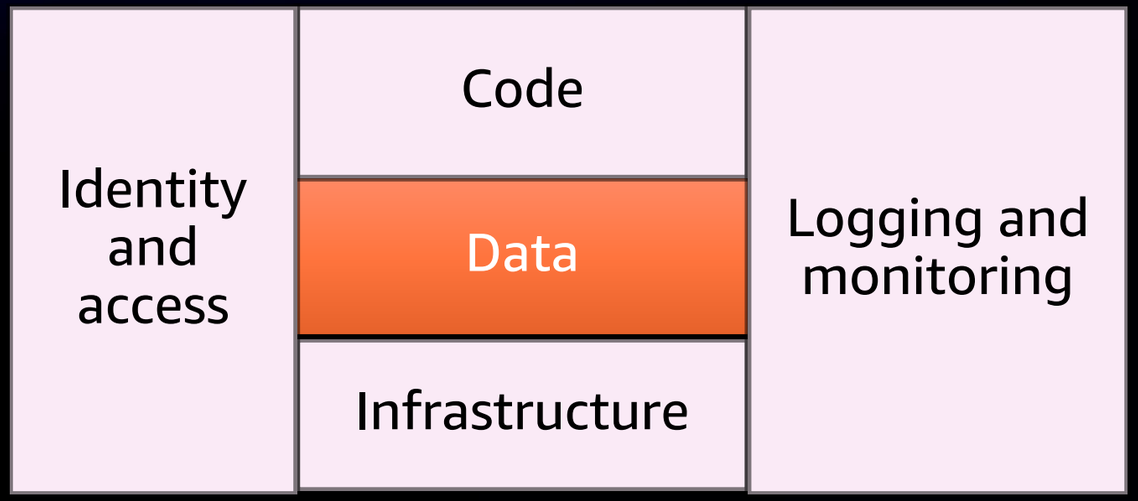
- OWASP Dependency-Check: https://www.owasp.org/index.php/OWASP_Dependency_Check
- Third-party tools

Remove unused dependencies

- Depcheck: https://www.npmjs.com/package/depcheck

© 2021, 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, and recovery

AWS takes care of:

- Automatic replication of data across Availability Zones for high durability
- Managed backups and encryption

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

Module 4: Encryption in transit

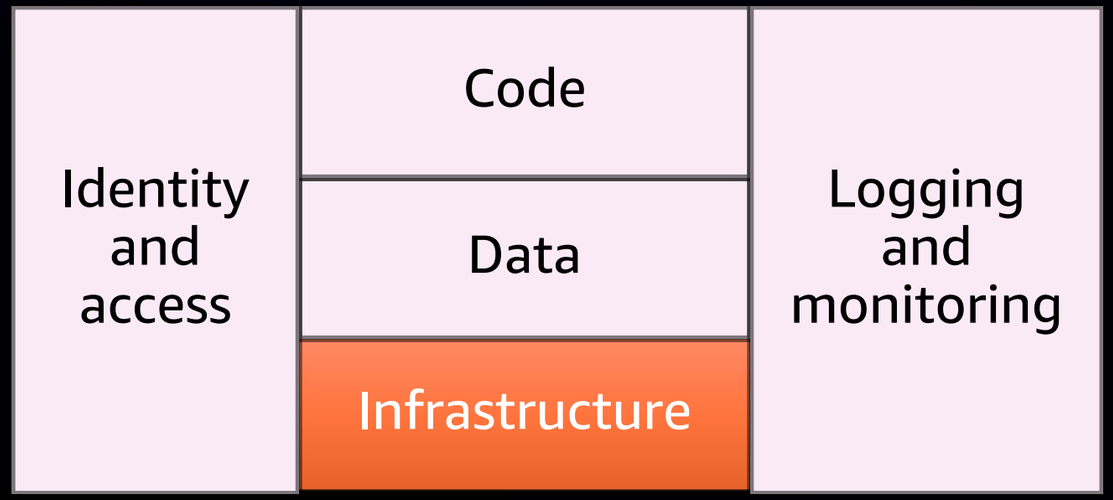
```
{
      host: ”database.host.com",
      user: "admin",
      password: ”xxxxxxxxx",
      database: "unicorn_customization"
}
```




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

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

Securing infrastructure for serverless applications



Your responsibility

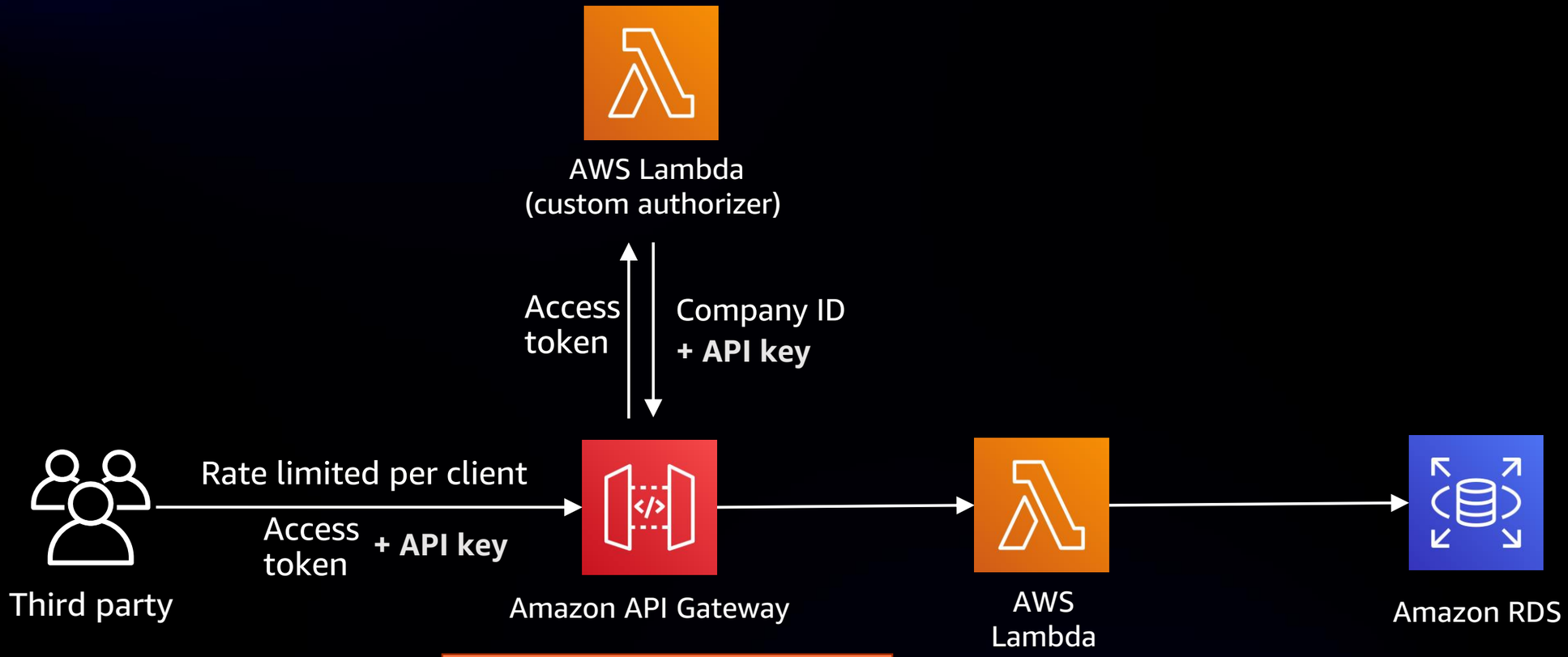
- DDoS protection
- Throttling/rate limiting
- Network boundaries

Serverless platform takes care of:

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

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

Module 5: Usage plans



Basic usage plan

- 5 requests/s
- 1,000 requests/month

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

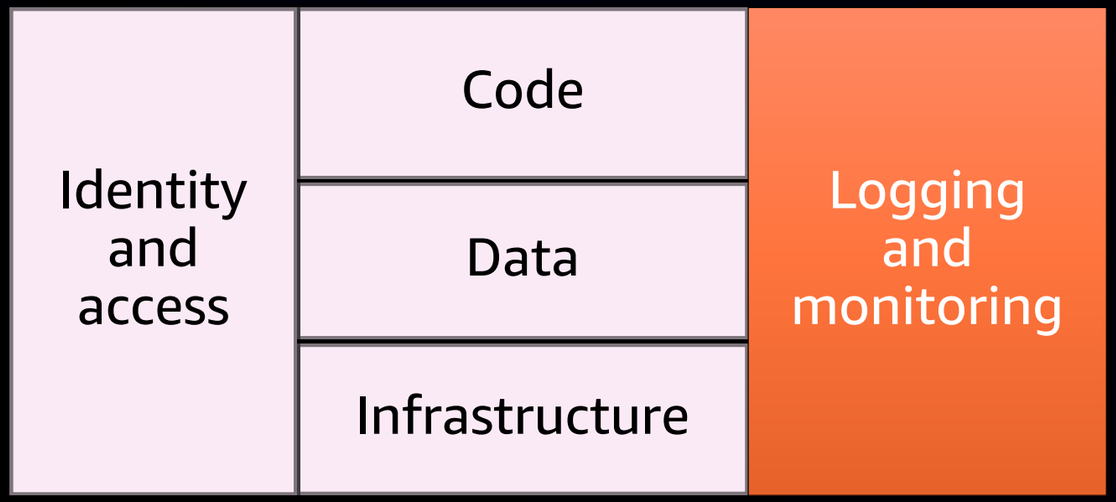
Module 6: AWS WAF

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



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

Logging and monitoring for serverless applications

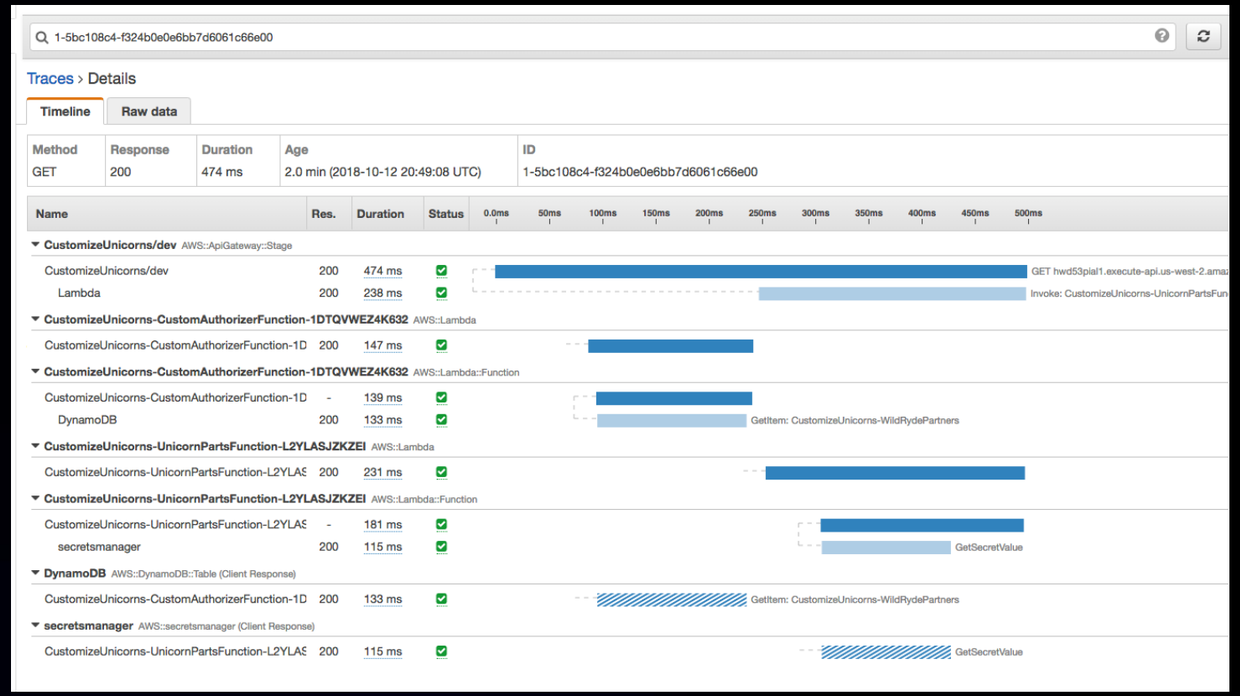


- Application logs
- Access logs
- Control plane audit logs
- Metrics
- Alarms
- Compliance validation

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

Module 8: AWS X-Ray

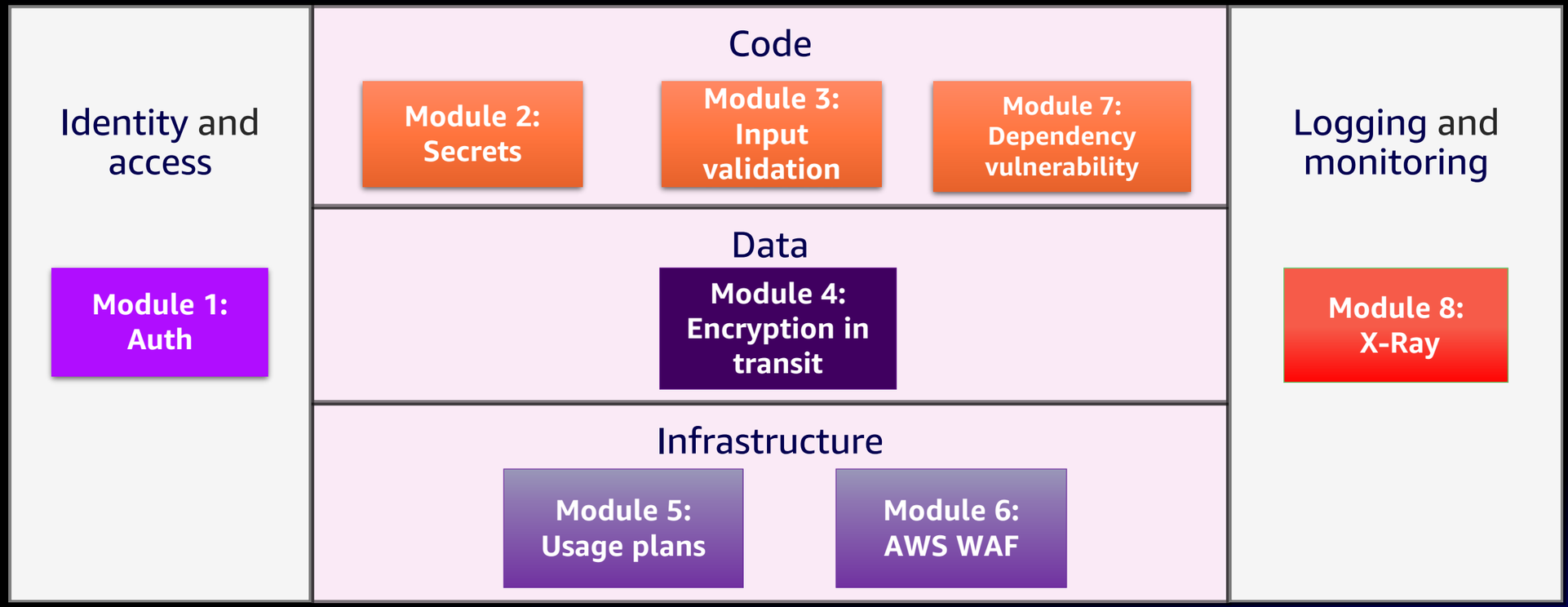




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop

- Link to the workshop: https://s12d.com/SVS303-R21
- Event Engine login: https://s12d.com/SVS303-R21-Lab
- **Module 0: Mandatory**
- Modules 1–8: Pick your own adventure



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

Thank you!

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