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

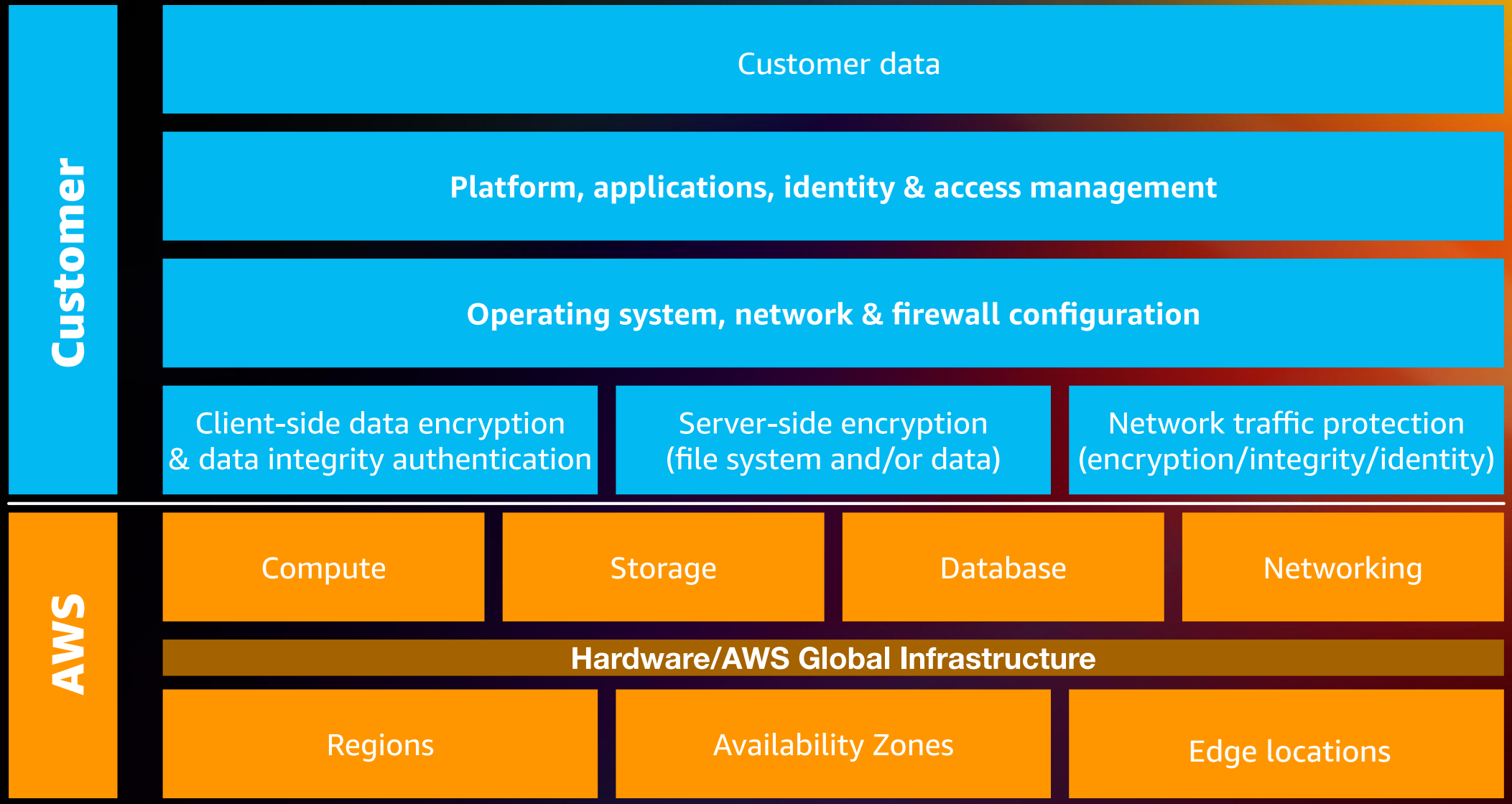
SVS309-R

Securing serverless applications

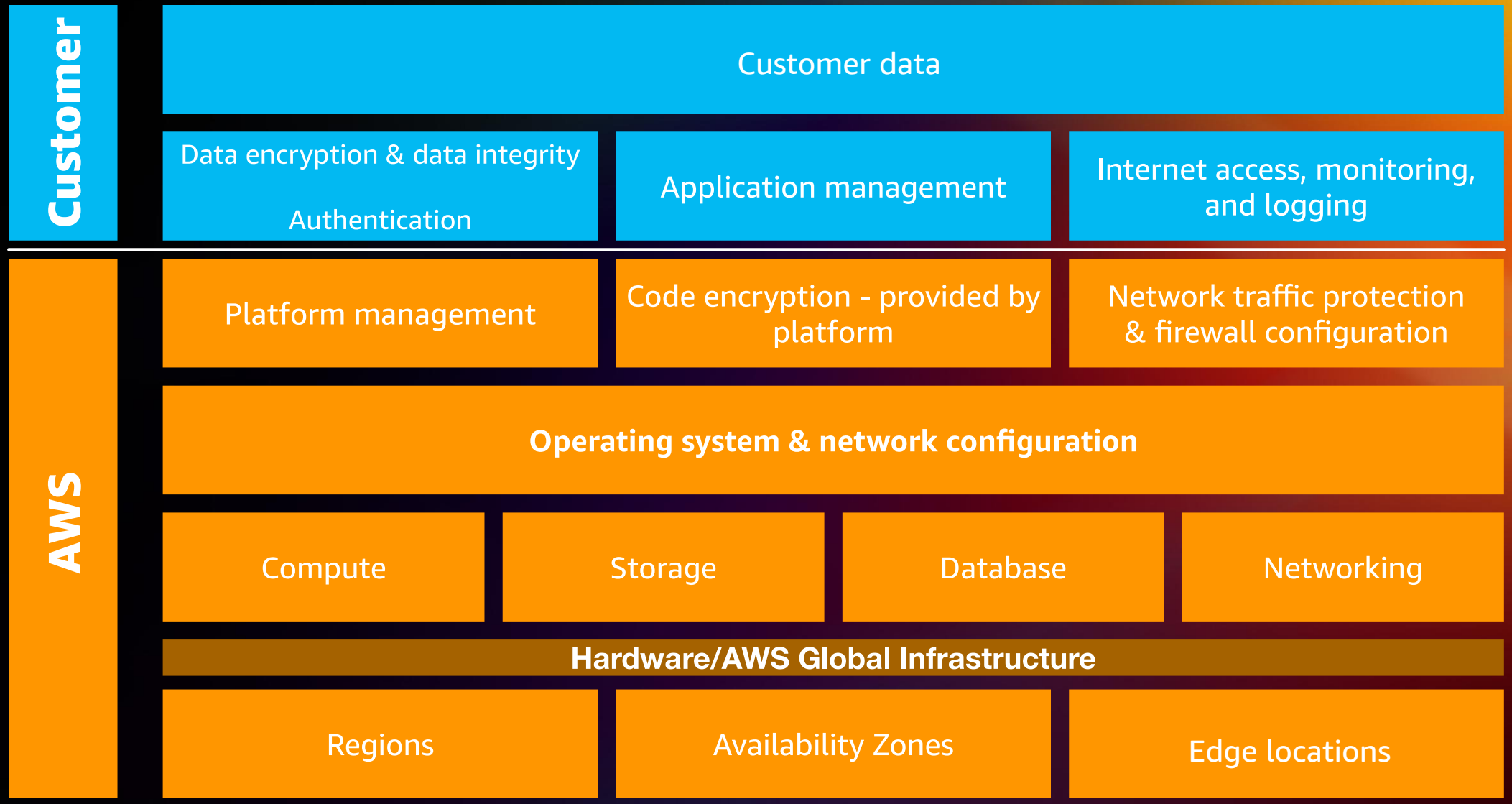
Chris McPeek

Principal Solutions Architect
Amazon Web Services

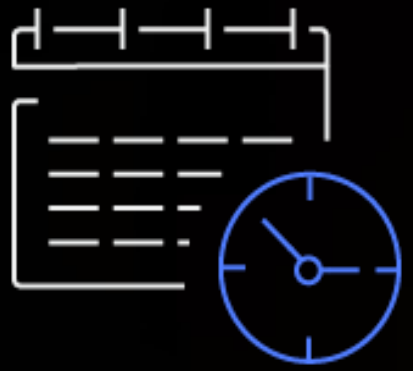
Shared responsibility model: “Serverful"



Shared responsibility model: Serverless



What else is different?



Ephemerality

Diffused perimeter

Fine-grained control

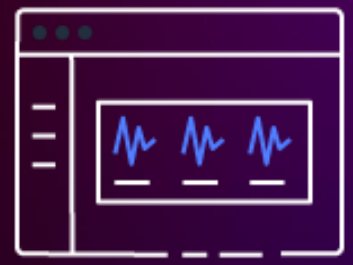
Tooling

What stays the same?

Securing data

Quality code

Least privilege



Monitoring

Security domains for serverless applications

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6 ↑	Vulnerable and outdated components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

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- Vulnerable and outdated components (#6)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)

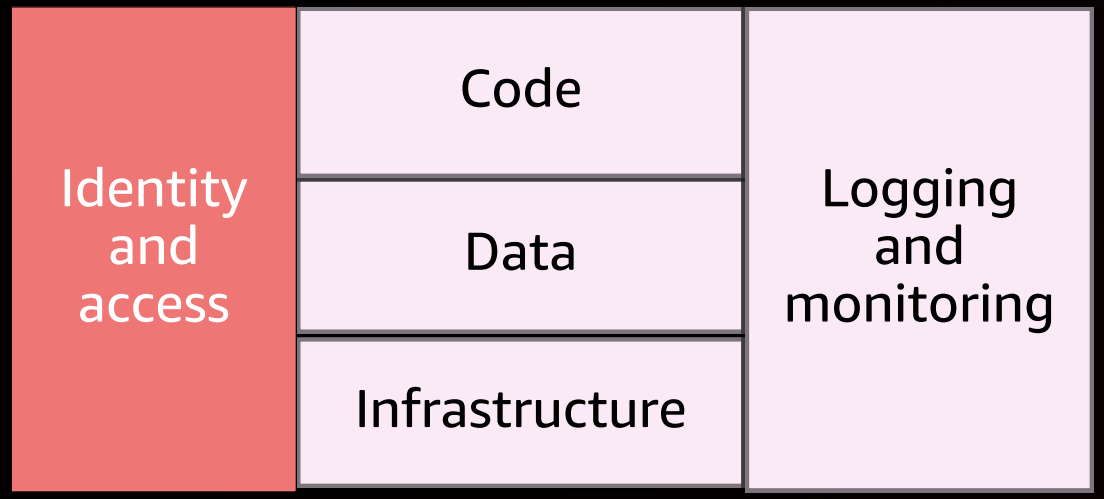
Logging and monitoring

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

Workshop scenario

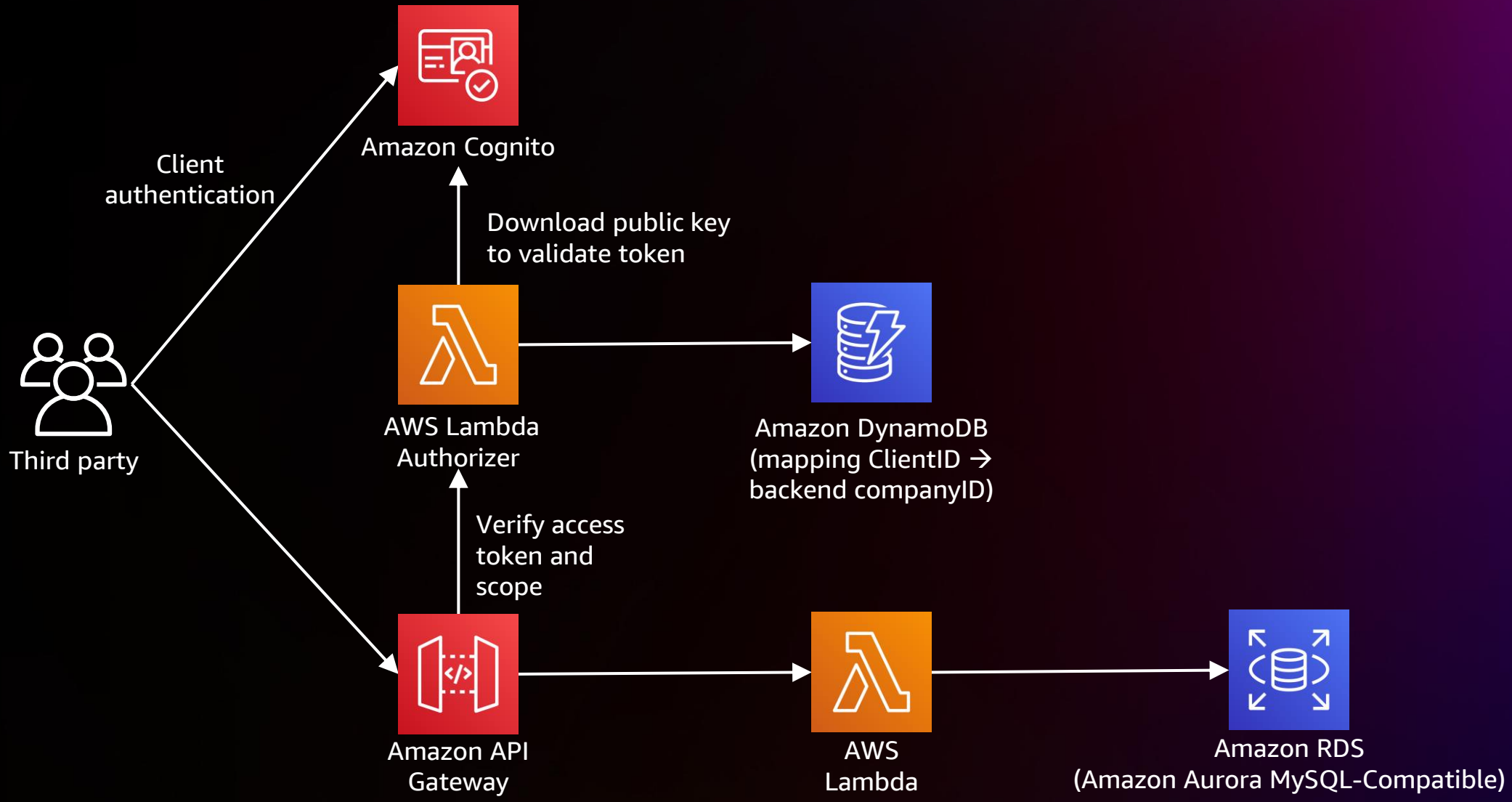
Scenario: Wild Rydes (www.wildrydes.com)

Identity and access management for serverless applications

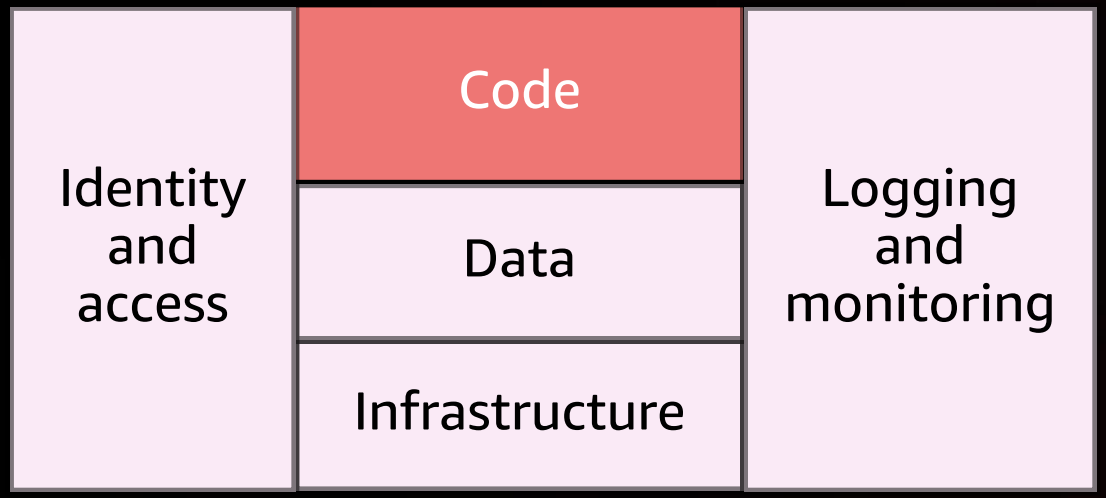


- Authenticate and authorize users or clients
- Access between backend services (e.g., AWS Lambda to Amazon DynamoDB tables)

Workshop module 1: Add authentication

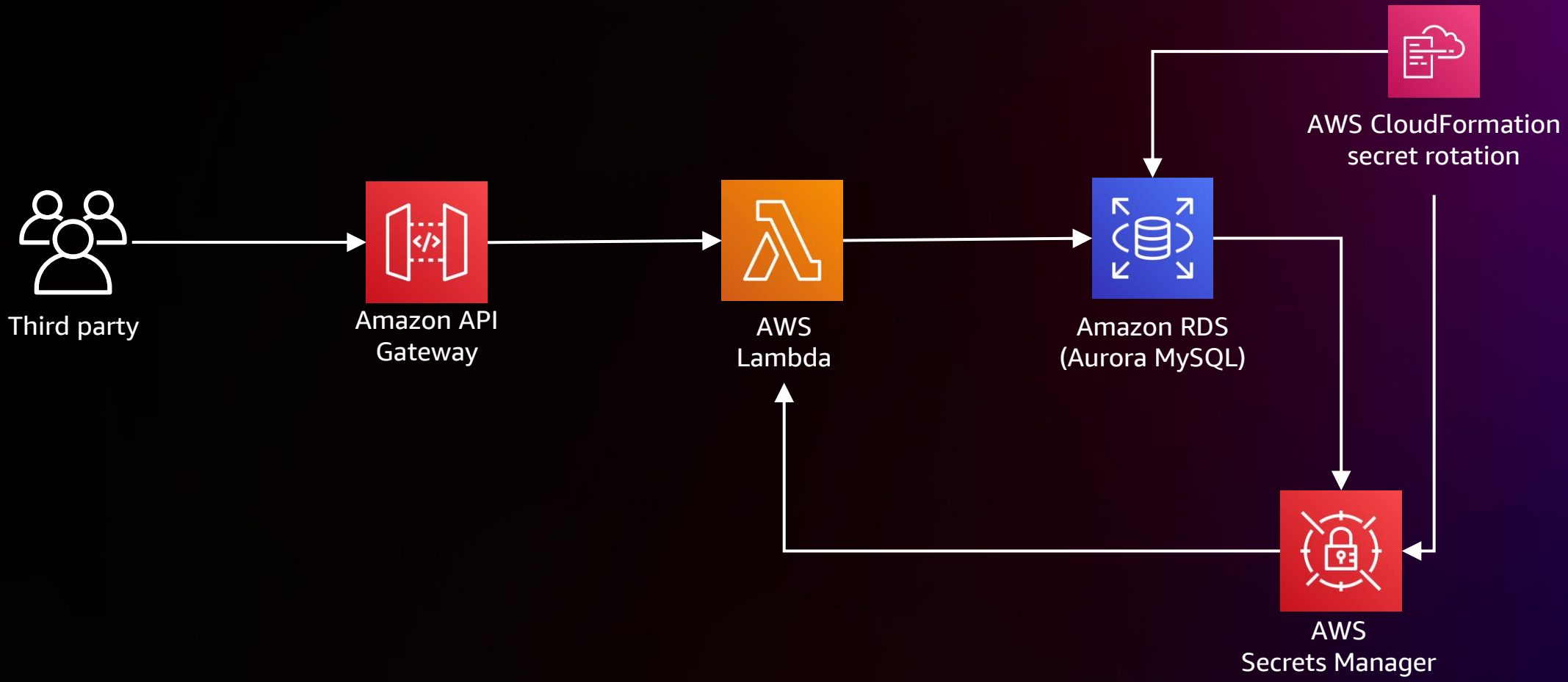


Securing code for serverless applications

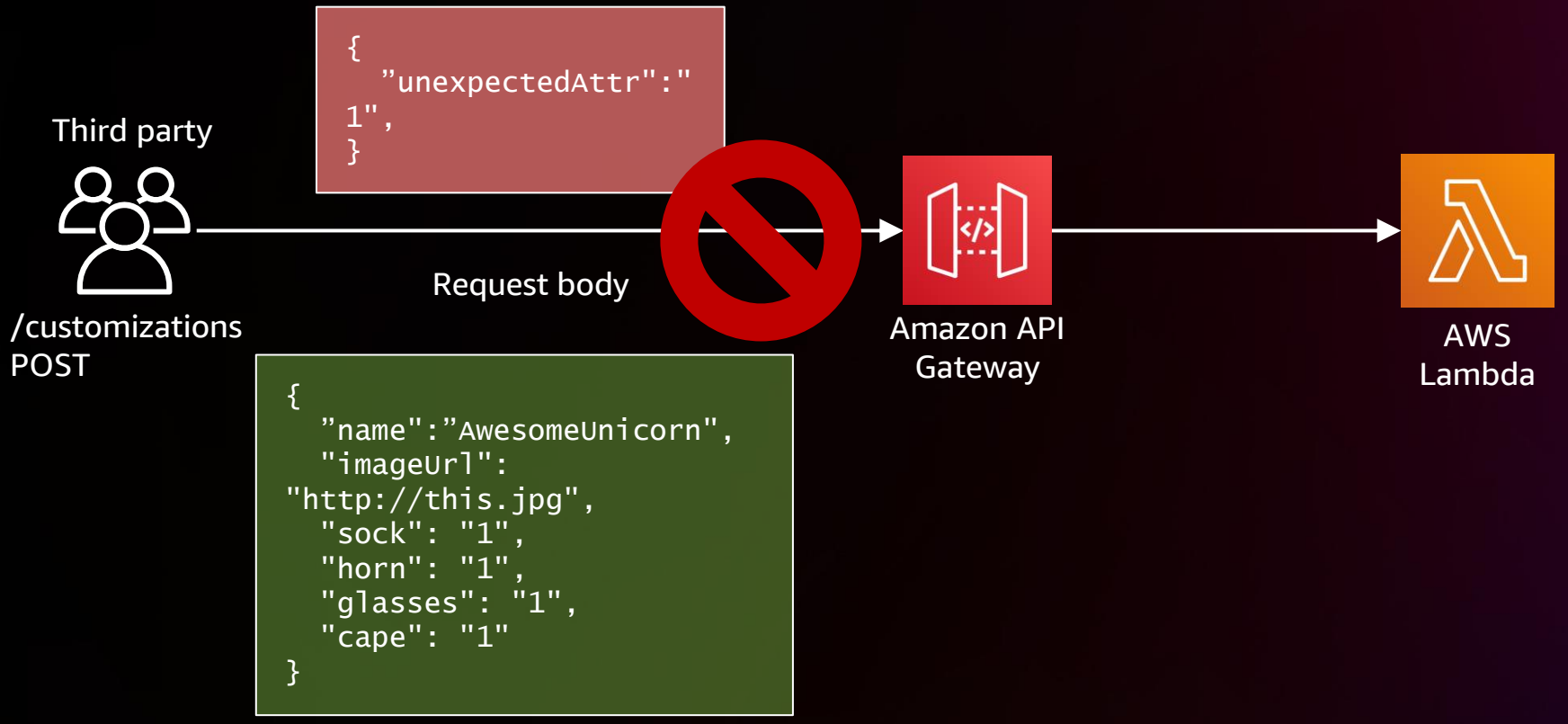


- Input validation
- Dependency vulnerabilities
- Code signing
- Secrets in source code

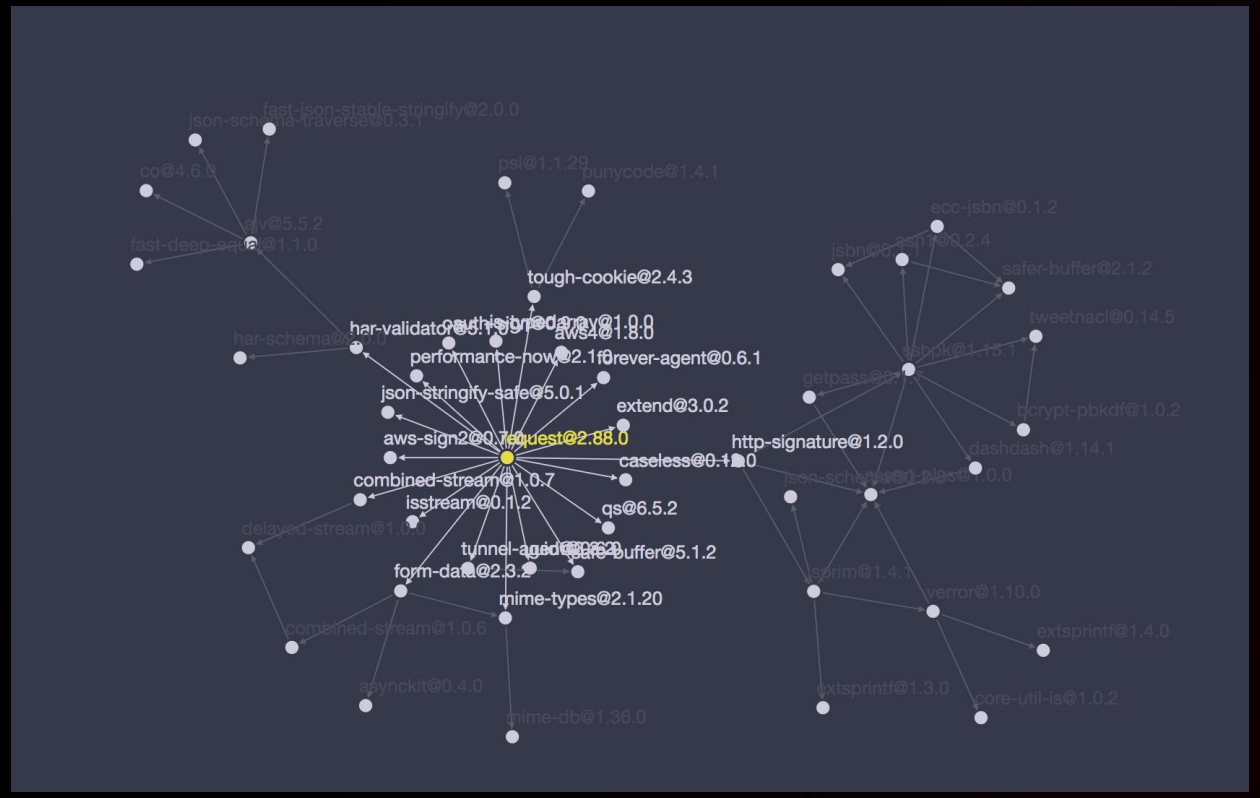
Module 2: Managing secrets



Module 3: Input validation



Module 7: Dependency vulnerability



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

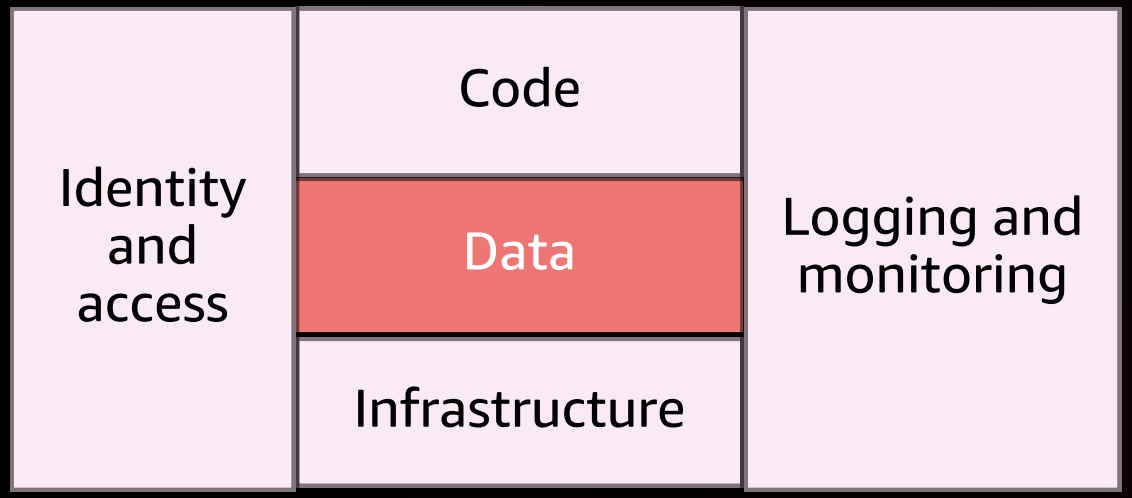
Check for vulnerabilities on our dependencies

- 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

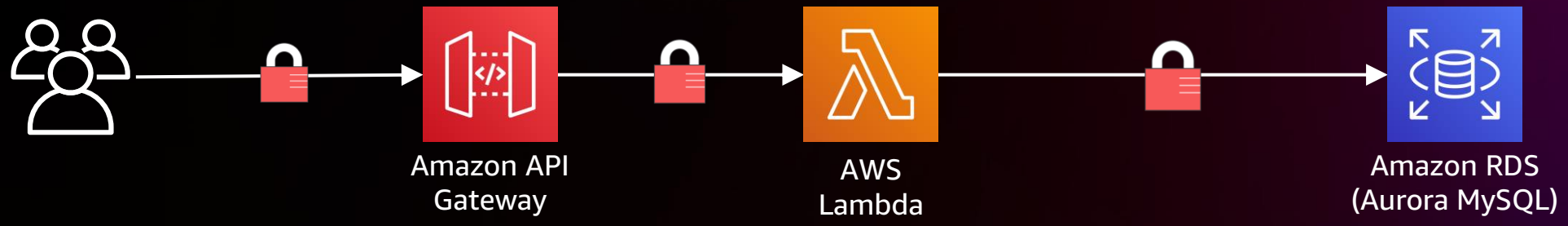
Securing data for serverless applications



- Data classification and data flow
- Tokenization
- Encryption at rest
- Encryption in transit
- Data backup, replication, and recovery

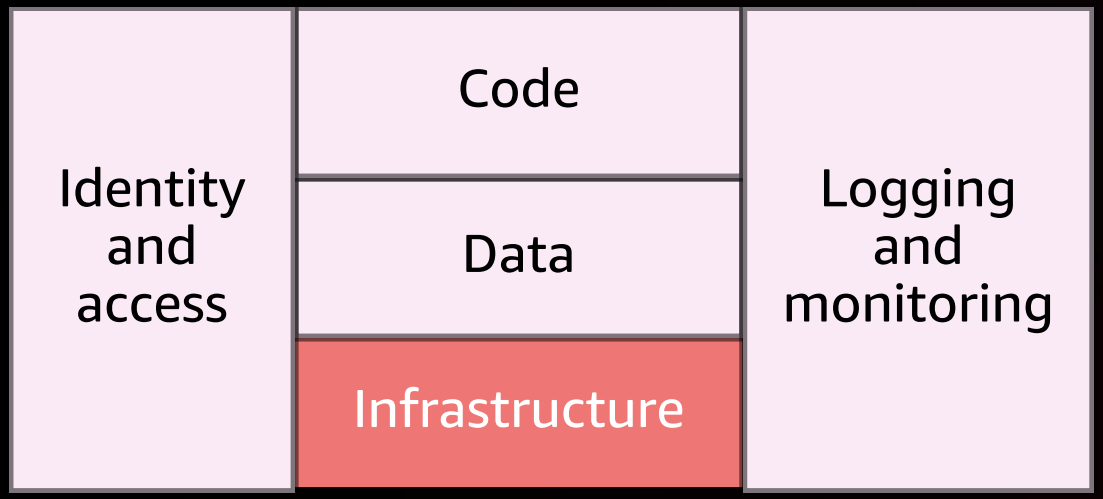
Module 4: Encryption in transit

```
{
     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"
}
```

Securing infrastructure for serverless applications



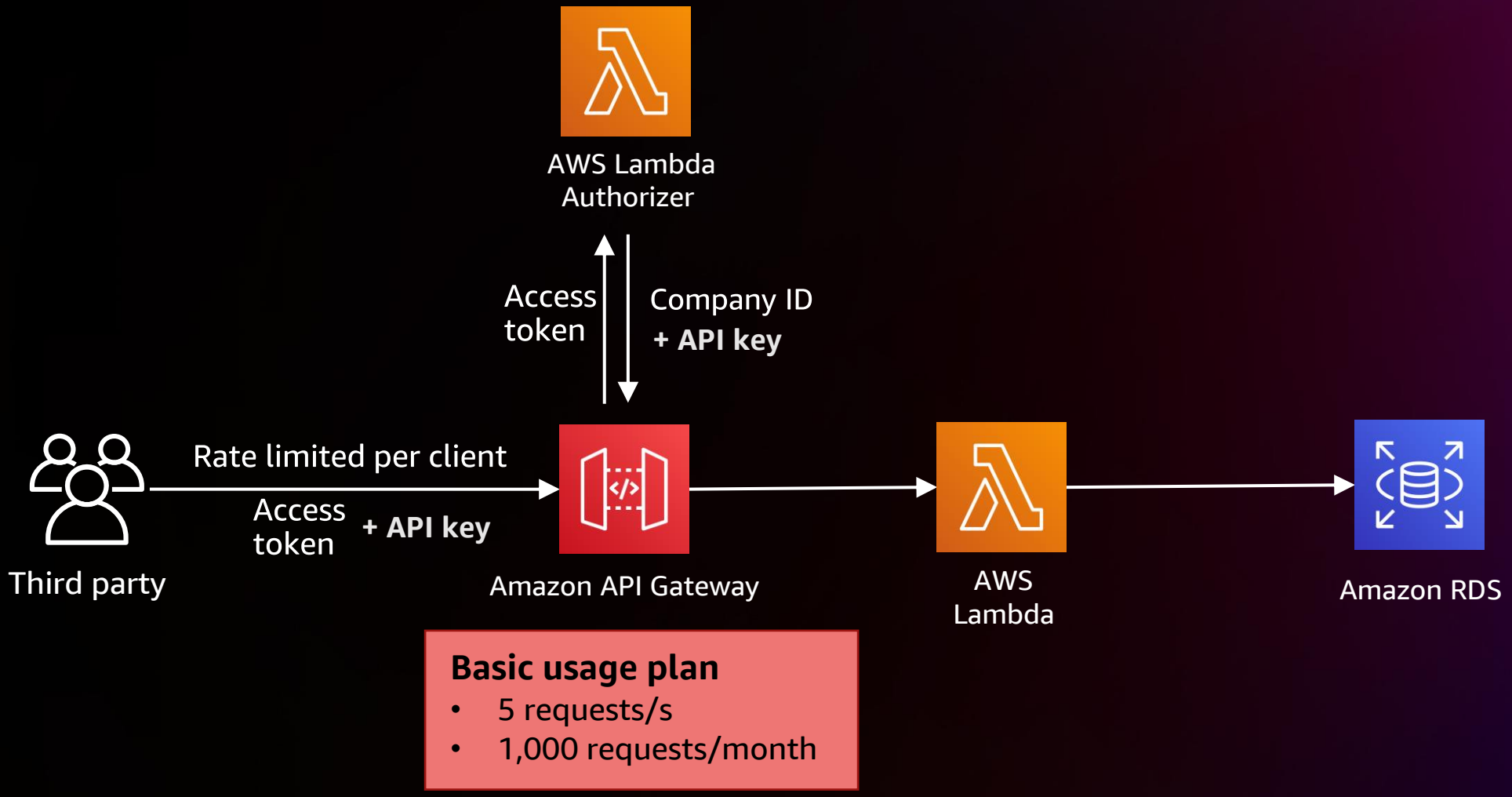
Your responsibility:

- DDoS protection
- Throttling/rate limiting
- Network boundaries

AWS Serverless takes care of:

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

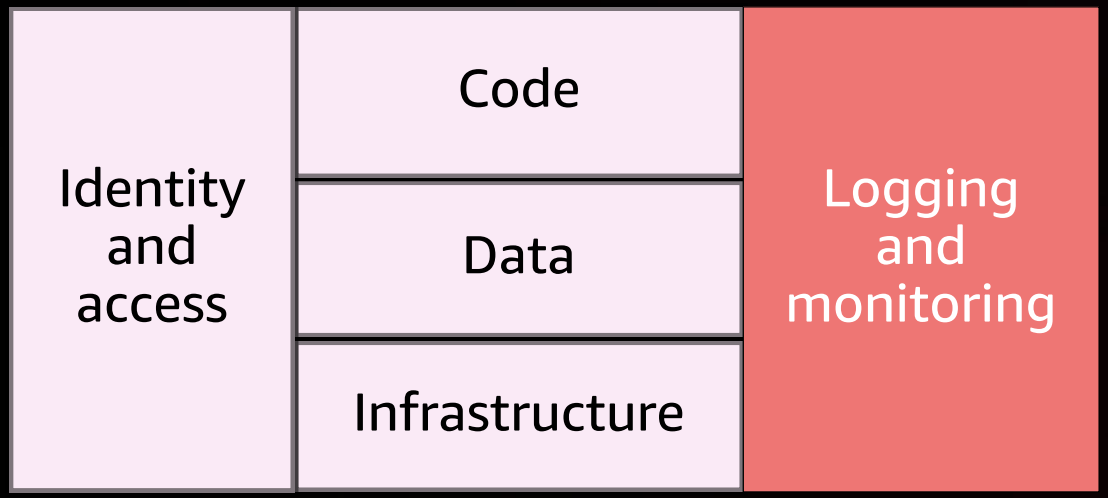
Module 5: Usage plans



Module 6: AWS WAF

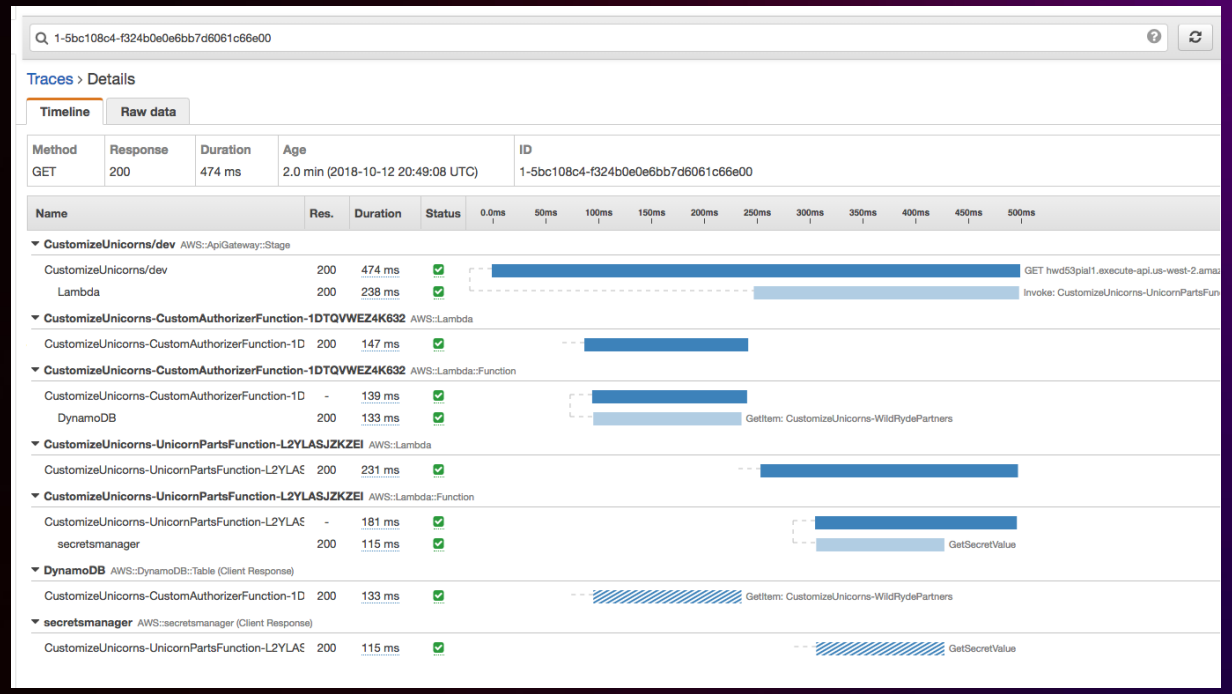
- IP reputation lists
- Size restrictions
- SQL injection
- XSS
- …

Logging and monitoring for serverless applications



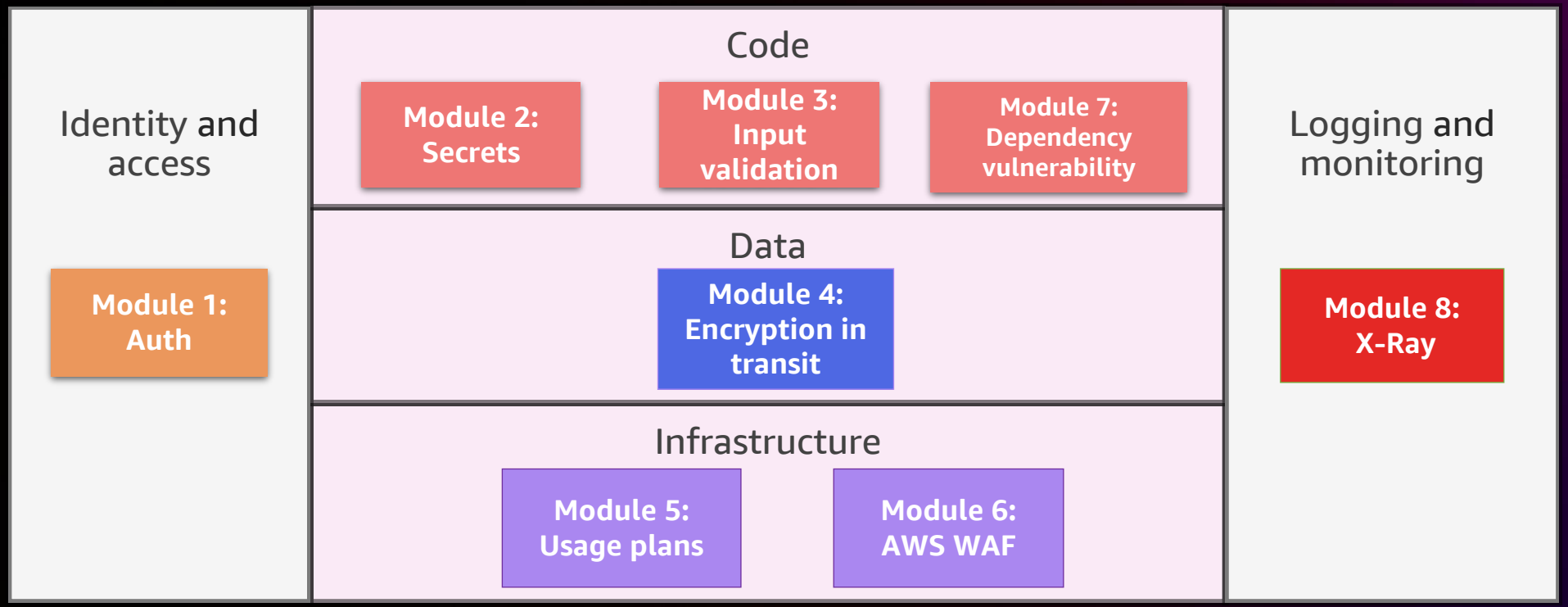
- Application logs
- Access logs
- Control plane audit logs
- Metrics
- Alarms
- Compliance validation

Module 8: AWS X-Ray



Workshop

- Link to the workshop: https://s12d.com/SVS309
- **Module 0: Mandatory**
- Modules 1–8: Pick your own adventure



Check out these other sessions…

SVS404: A closer look at AWS Lambda

Wednesday (Nov 30) at 10:00 AM – Mandalay Bay South Pacific F

SVS306: Serverlesspresso: Building an event-driven application from the ground up

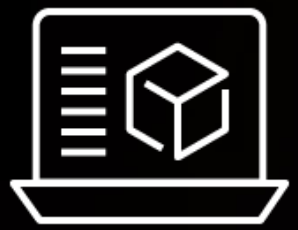
Wednesday (Nov 30) at 2:30 PM – Wynn Cristal 3

SVS314: AWS Lambda performance tuning: Best practices and guidance

Thursday (Dec 1) at 4:15 PM – MGM Grand Boulevard 169

Continue your AWS serverless learning

Learn at your own pace



Expand your serverless skills with our Learning Plan on **AWS Skill Builder**

Increase your knowledge

Use our **Ramp-Up Guides** to build your serverless knowledge

Earn AWS Serverless badge

Demonstrate your knowledge by achieving **digital badges**

https://s12d.com/serverless-learning

Thank you!

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