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

SEC210

AWS and privacy engineering: Explore the possibilities

Jessie Skibbe (she/her)

Principal Practice Leader,
AWS Security Assurance Services, LLC
AWS

Carl Mathis(he/him)

Senior Privacy Architect,
AWS Security Assurance Services, LLC
AWS

This presentation is provided for the purposes of information only; it is not legal advice, and should not be relied on as legal advice. AWS encourages its customers to obtain appropriate advice on their implementation of privacy and data protection environments, and more generally, applicable laws relevant to their business.

Agenda

Building privacy compliance on AWS

- Privacy risks and challenges
- Shared responsibility model
- Security and privacy
- Services and feature
- Privacy engineering adoption
- Customer challenges – sample architectures

Organizations face unique data privacy risks and challenges

In their shift to the cloud, companies across all industries and sectors are confronting a range of familiar and emerging data privacy issues

Evolving and expanding regulatory requirements

Requirements that vary significantly across geographies and industries

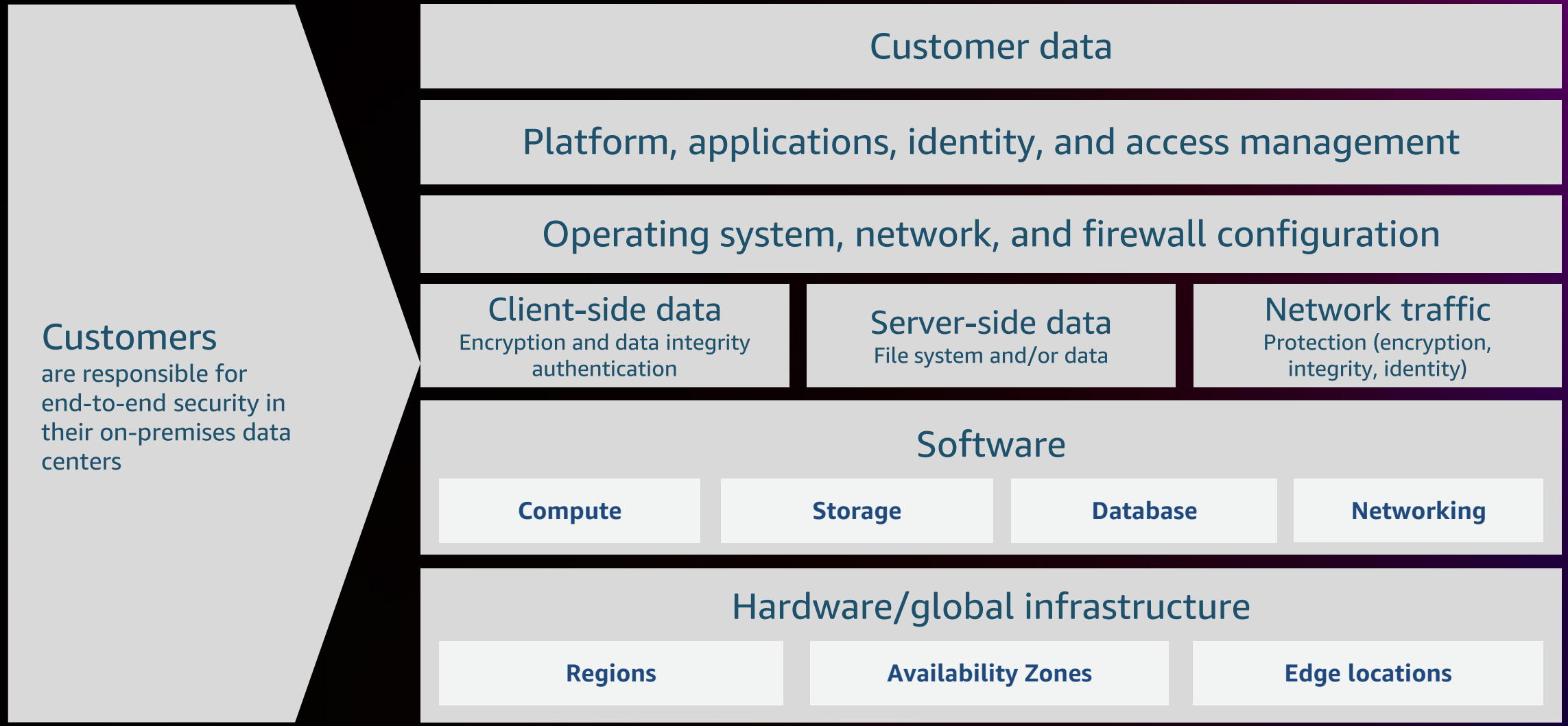
Highly dynamic security and privacy threat landscape

A mix of precise and vague requirements

Legal, privacy, and engineering silos

Shared responsibility model

Traditional on-premises security/privacy model



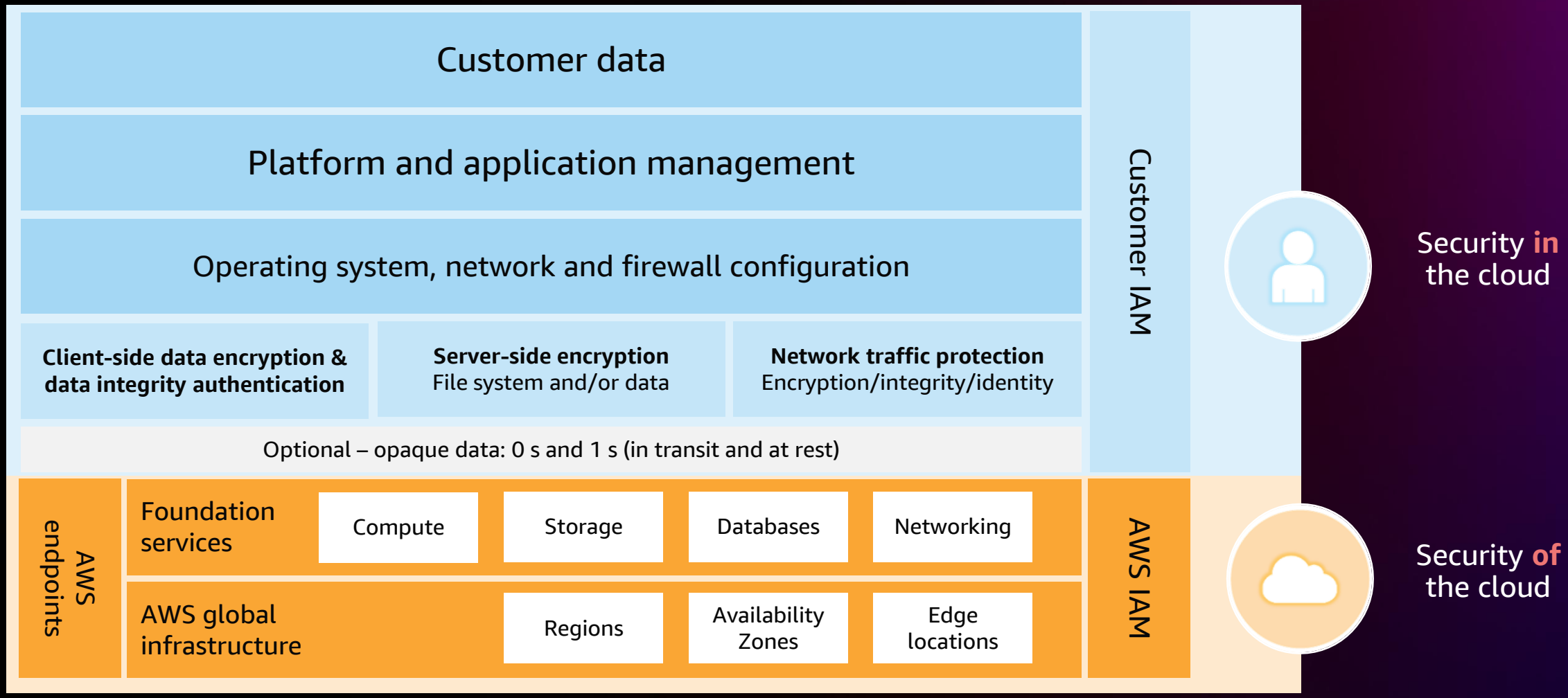
What is the AWS shared responsibility model?

When evaluating a security-of-the-cloud solution, it is important for customers to understand and distinguish between

- Security measures that the cloud service provider (AWS) implements and operates – **security of the cloud**
- Security measures that the customer implements and operates related to the security of customer content and applications that make use of AWS services – **security in the cloud**

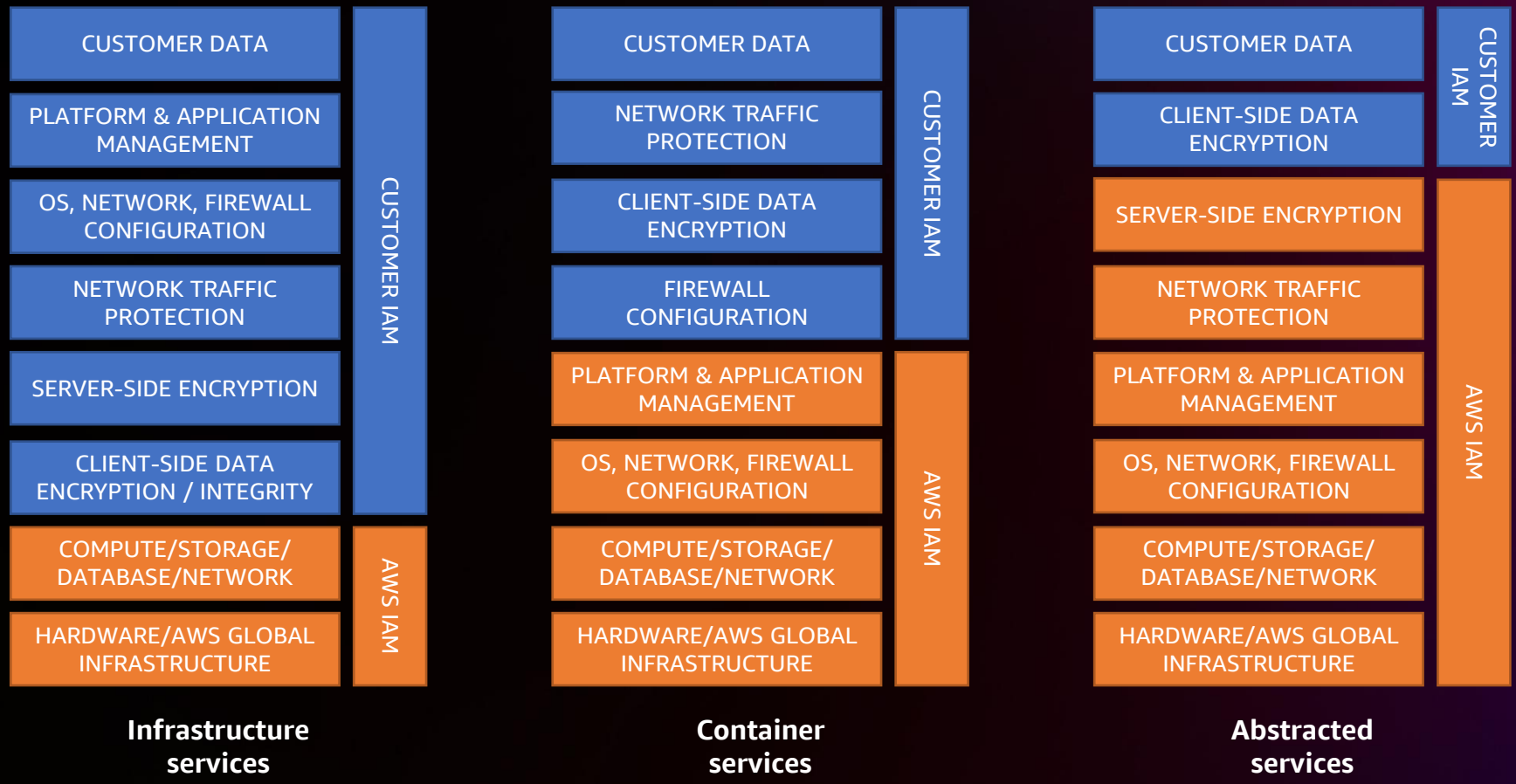
Working together

SECURITY IN THE CLOUD IS A SHARED RESPONSIBILITY



The line varies

More customizable
+
More customer responsibility

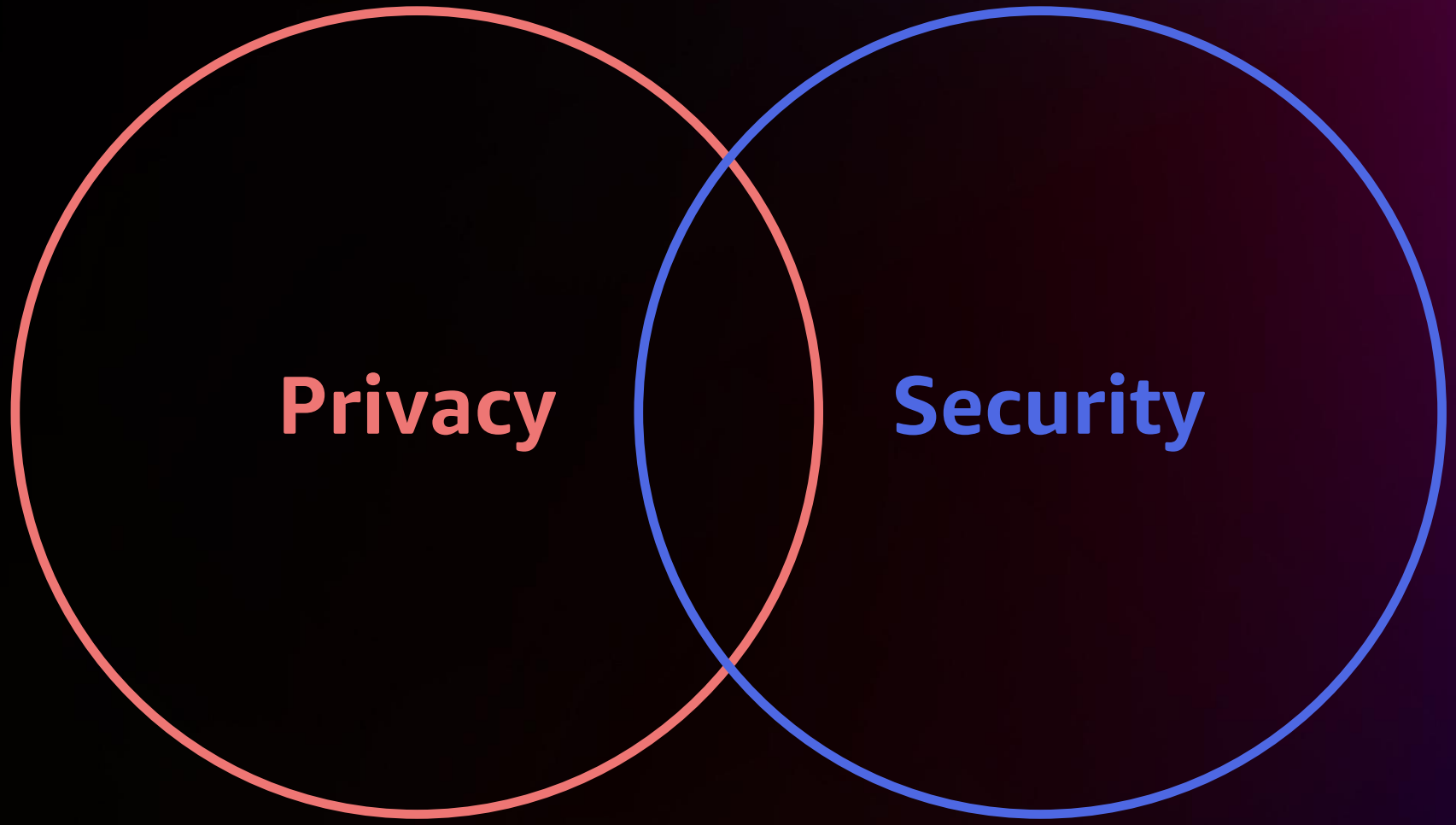


Less customizable
+
Less customer responsibility
+
More best practices built in

https://aws.amazon.com/whitepapers/aws-security-best-practices/

Security and privacy

Is security sufficient for privacy?



Services and features

AWS services to help enhance your privacy

Data minimization

- Amazon Comprehend
- AWS KMS
- AWS Backup
- Amazon API Gateway
- Amazon Macie
- Amazon Data Lifecycle Manager
- Amazon S3

Data-centric design

- AWS Control Tower
- Amazon VPC
- AWS PrivateLink
- AWS Identity and Access Management (IAM)
- Amazon WorkSpaces
- AWS Nitro Enclaves
- AWS RAM
- Amazon CloudFront
- Amazon Route 53

Disclosure control

- IAM
- AWS Organizations
- AWS Firewall Manager
- AWS Signer
- Amazon CodeGuru
- AWS WAF
- Amazon Inspector
- AWS Systems Manager
- AWS Identity and Access Management Access Analyzer

Continuous oversight

- AWS Security Hub
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- Amazon VPC Flow Logs
- Amazon Detective
- AWS Audit Manager
- Amazon GuardDuty
- Amazon OpenSearch Service

Individual autonomy

- AWS Glue
- Amazon SageMaker
- Amazon Kendra
- Amazon Cognito
- Amazon Lex
- Amazon Polly
- Amazon DynamoDB
- AWS Lambda

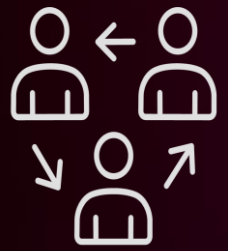
Why adopt privacy engineering?

Realized benefits

Innovation

Agility

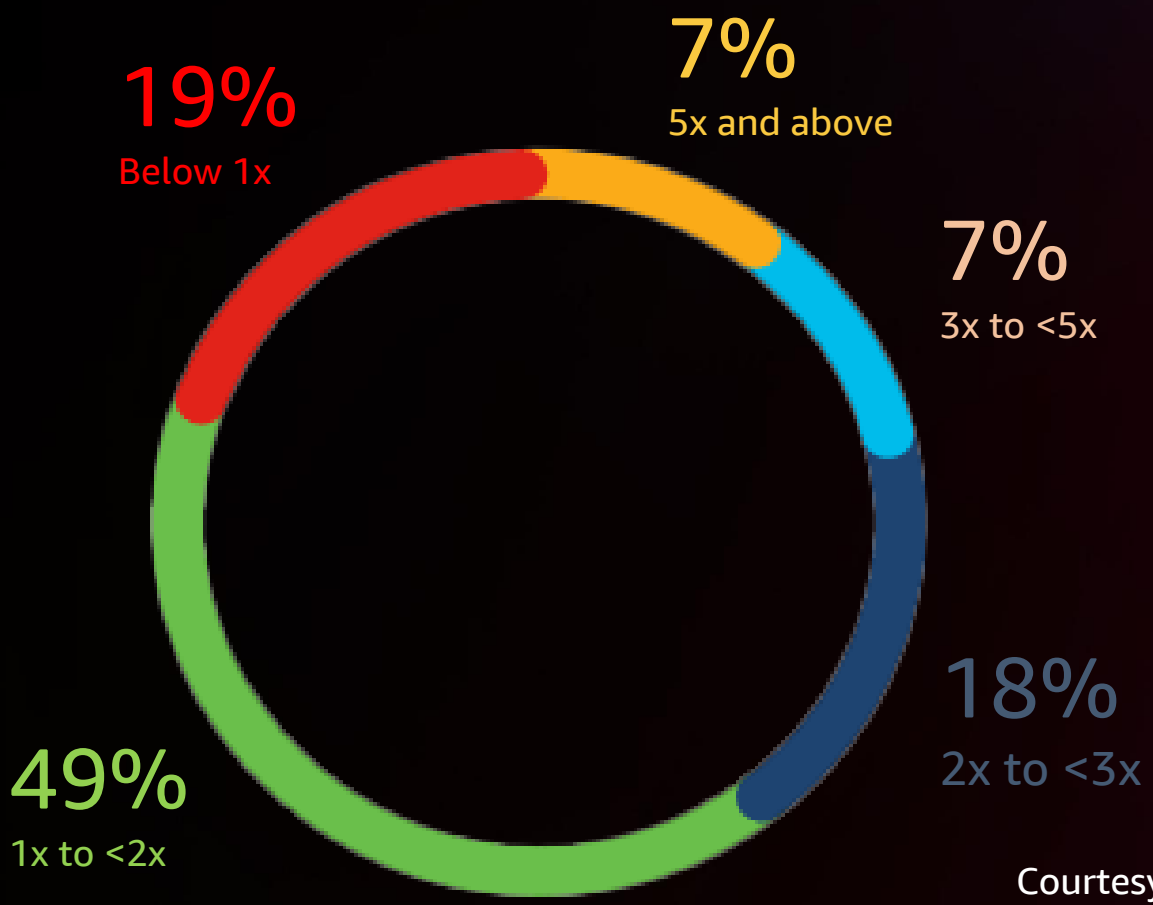
Shorter sales cycles



Fewer silos, more collaboration

Faster expansion

81% positive return on privacy investments



Courtesy of Cisco Systems, Inc. Unauthorized use not permitted
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-infographic-2022.pdf?CCID=cc000742&DTID=odicdc000016
10/28/2022

Customer challenges

Continuous oversight

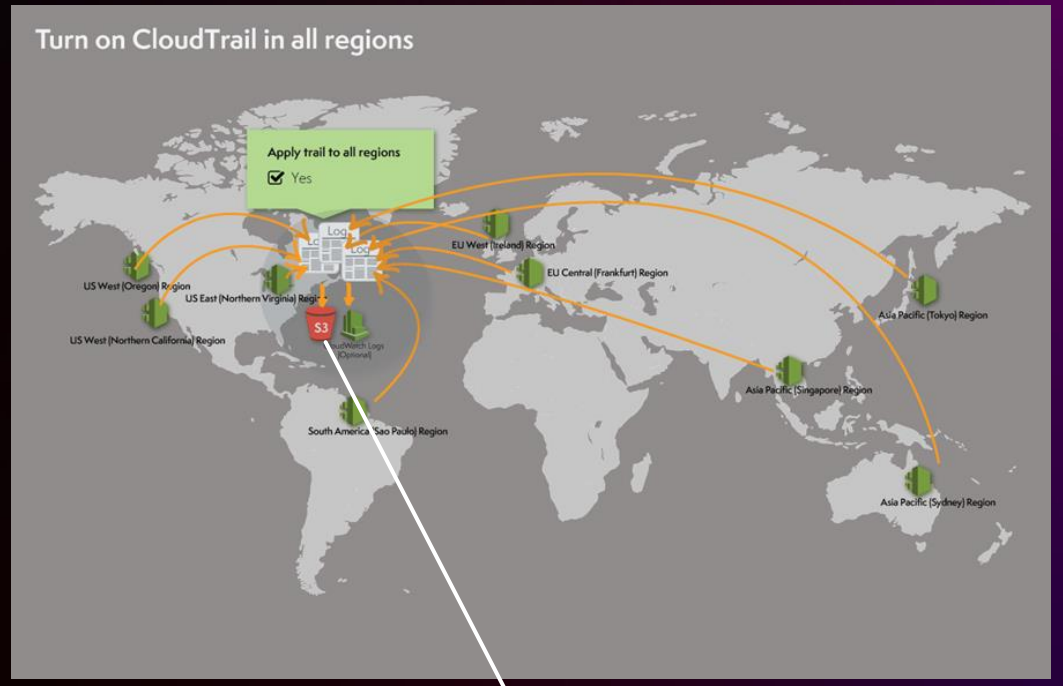
Centralizing CloudTrail logs

You can create two types of CloudTrail “trails”

- A trail that applies to **all Regions**
- A trail that applies to **one Region**

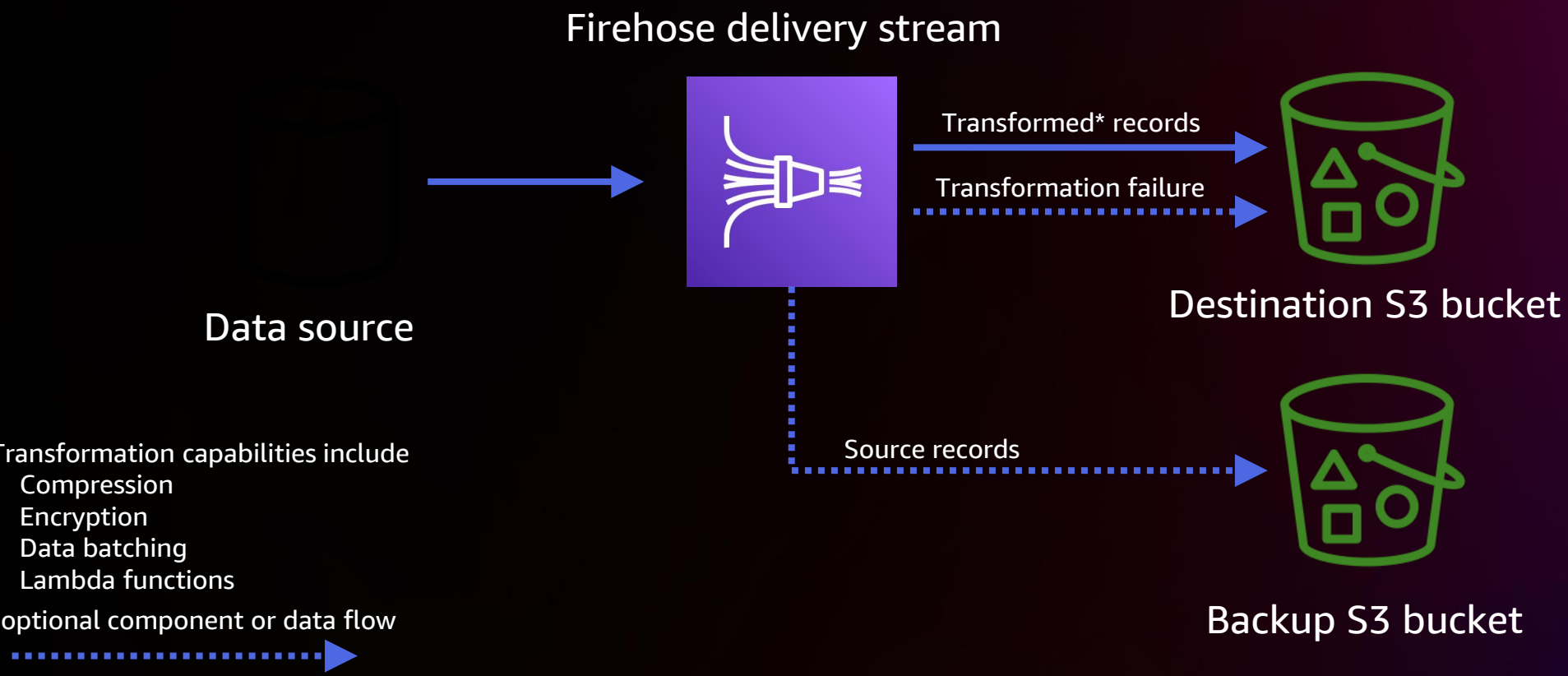
Many-to-one centralization

- From **multiple Regions** into one S3 bucket
- From **multiple accounts** into one account’s S3 bucket



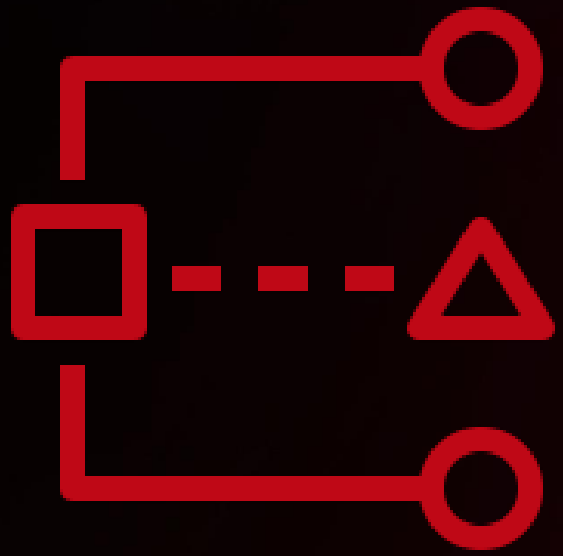
`userAgent? sourceIPAddress? userName?`

Ingestion and transformation with Amazon Kinesis Data Firehose



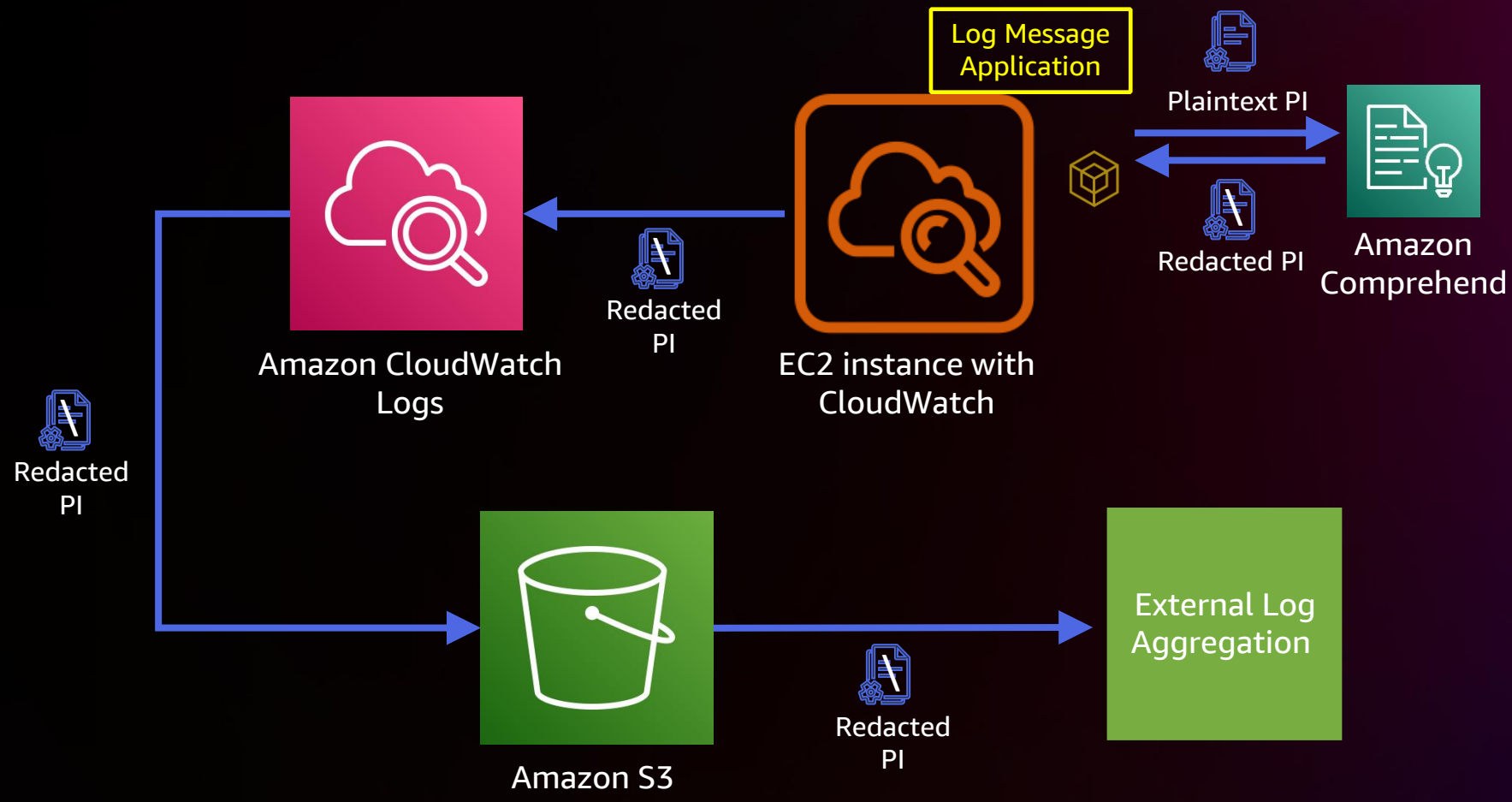
Zones of trust with IAM Access Analyzer

Makes it simple for security teams and administrators to check that their policies provide only the intended access to resources

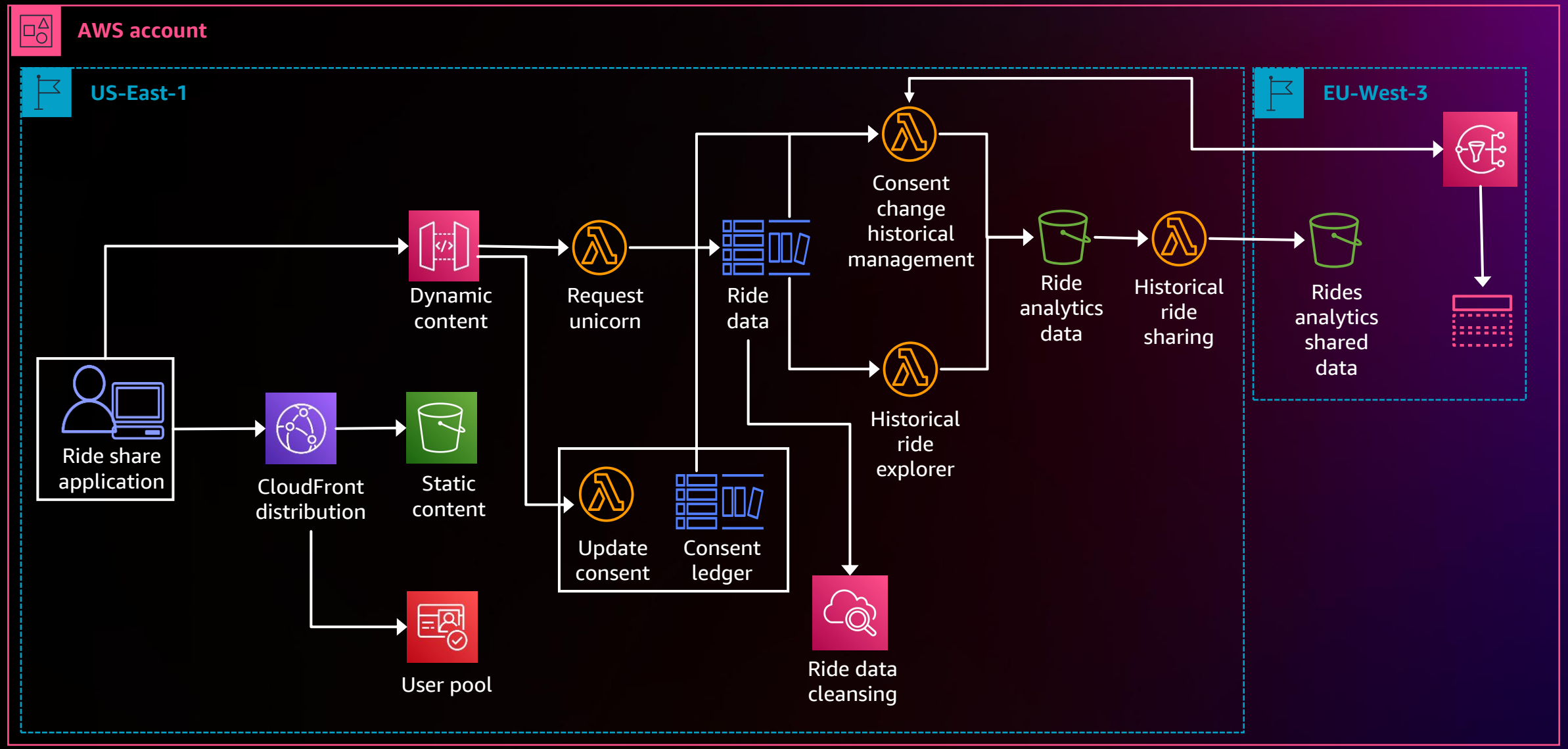


Data minimization

PI redaction from application logs with Amazon Comprehend

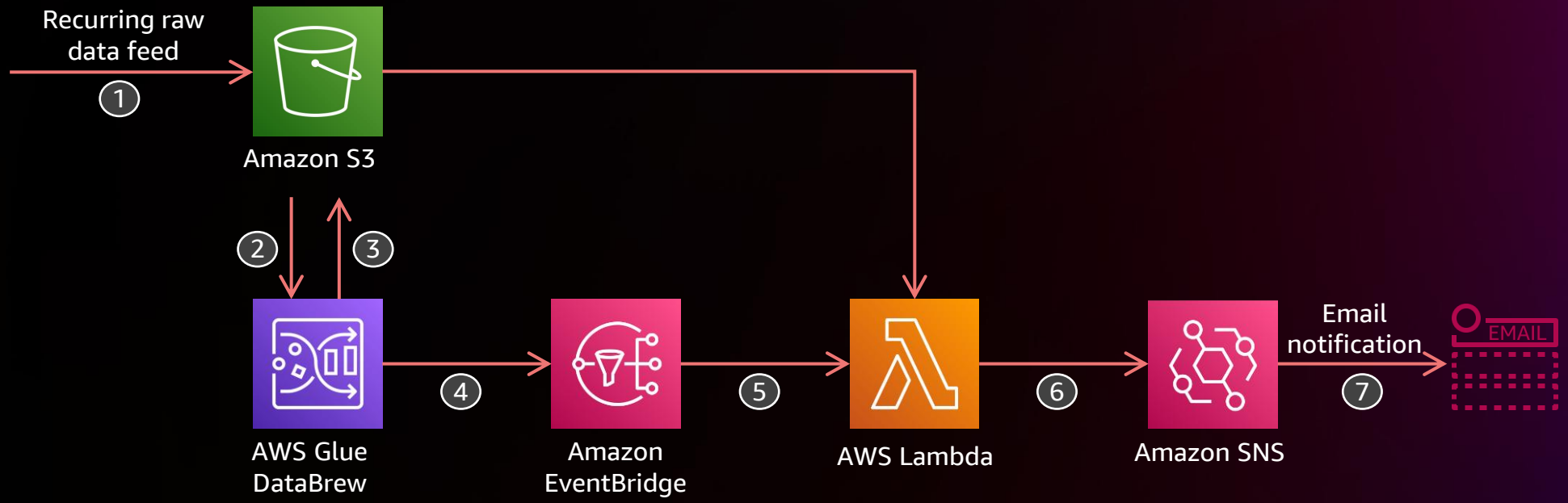


Consent tracking

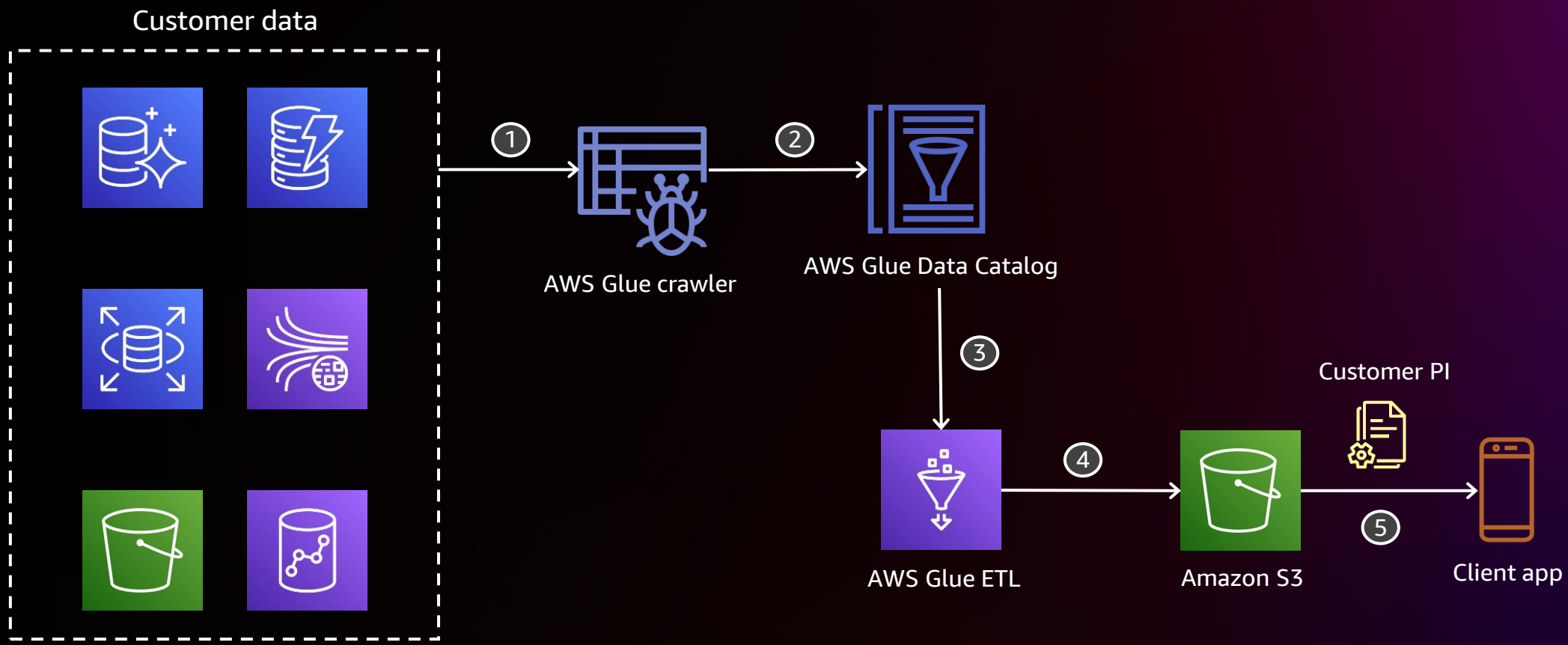


Individual autonomy

AWS Glue DataBrew and Lambda for quality automation



Making data portable with AWS Glue

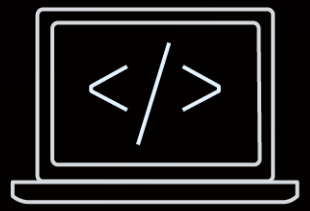


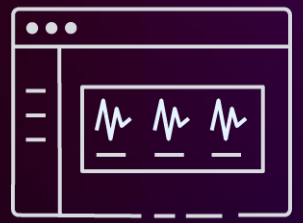
Disclosure control

Data leakage code review with Amazon CodeGuru

CodeGuru Reviewer

CodeGuru Profiler





Coding

Built-in code reviews with actionable recommendations

Build and test

Detect and optimize the problematic lines of code pre-production

Deploy

Measure

Easily identify privacy and security improvements in production environment

Example: Detecting sensitive information leaks

Code

```
try {
    updateJobStatus(context.getAwsRequestId(),
                    request.getAwsAccountId(),
                    request.getPredictorName(),
                    request.getInternalStatus());
} catch (validationException e) {
    log.error(NON_RETRIABLE_LIST_ERROR_MESSAGE, e);
    throw e;
} catch (internalServerException e) {
    log.warn(RETRIABLE_LIST_ERROR_MESSAGE, e);
    retries++;
    continue;
}
```

Fix

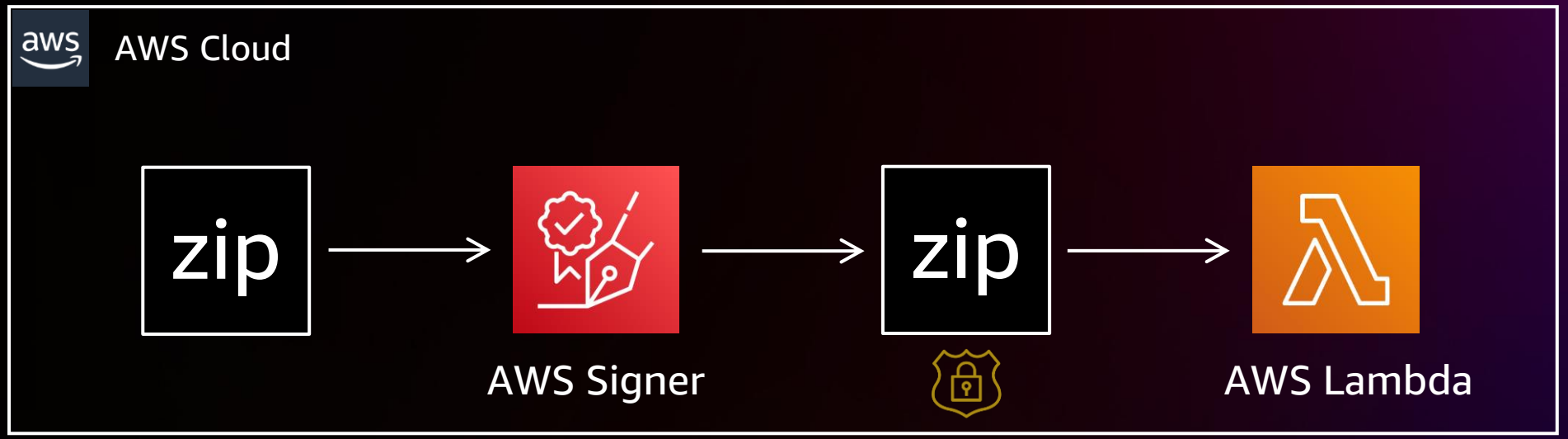
```
try {
    updateJobStatus(context.getAwsRequestId(),
                    request.getAwsAccountId(),
                    request.getPredictorName(),
                    request.getInternalStatus());
} catch (validationException e) {
    log.error(NON_RETRIABLE_LIST_ERROR_MESSAGE, redact(e));
    throw readact(e);
} catch (internalServerException e) {
    log.warn(RETRIABLE_LIST_ERROR_MESSAGE, redact(e));
    retries++;
    continue;
}
```

Recommendation

This code contains potential unintended disclosure of information in the error handling for the following call: '**getAwsAccountId()**'. You are handling the error with catch classes. There are methods available that could be added to handle sensitive data, **like masking and redaction**.

Code signing with AWS Signer

Validate code against a digital signature to confirm that the code is unaltered and from a trusted publisher



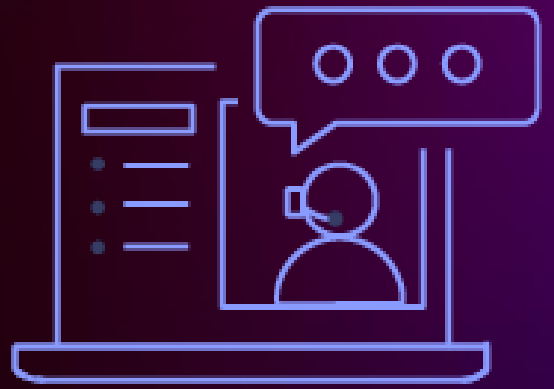
Call to action

Privacy is a positive–sum game!

Integrate privacy engineering principles into your entire data lifecycle management

Proactively define privacy requirement within regulated workloads

Codify and automate privacy as code using AWS services such Amazon Comprehend and AWS Glue



Reach out to AWS Security Assurance Services

Resources

Online resources

AWS Artifact A globally available, no-cost portal that provides on-demand access to the most recent external security and compliance certifications from AWS

CISPE certification 52 AWS services have been declared compliant

ISO 27001 Security management controls

ISO 27017 Cloud-specific controls

ISO 27701 Privacy information management

ISO 27018 Personal data protection

New and updated resources

Data Privacy Center

Data Privacy FAQ

General Data Protection Regulation (GDPR) Center

Privacy Features of AWS Services

AWS Sub-processors

Data Protection at AWS

EU data protection

How AWS is helping EU customers navigate the new normal for data protection

Thank you!

Jessie Skibbe
Skibbe@amazon.com
LinkedIn: @JessieSkibbe

Carl Mathis
Carmathi@amazon.com
LinkedIn: @CarlMathis

AWS Security Assurance Services
https://aws.amazon.com/professional-services/security-assurance-services/

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