
AWS
re:Invent

WPS201

Securing student data in the age of virtual learning

Larry Kiger

Sr. Industry Specialist

Security and Compliance

AWS

AWS re:Invent

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

Agenda

- What student data are and who is responsible
- Seven fundamental principles of privacy by design
- Some industry challenges
- Getting started
- Designing it right
- Show me
- How are others in the industry doing it



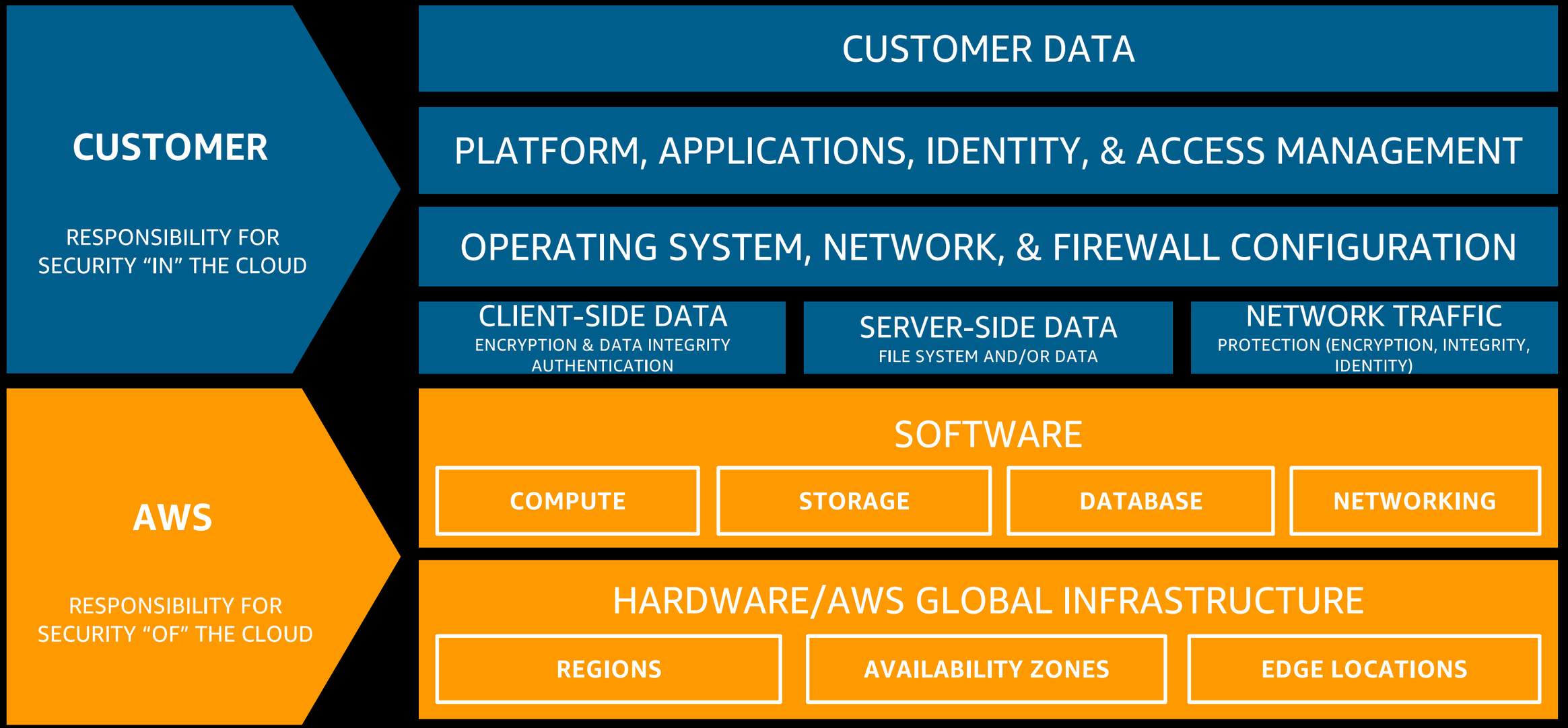
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are student data?

In education, ***student data*** refers to any information that educators, schools, districts, and state agencies collect on individual students, including:

- **Personally identifiable information** (PII) (e.g., a student's age, gender, race, place of residence)
- **Enrollment information** (e.g., the school a student attends, a student's current grade level and years of attendance, the number of days a student was absent)
- **Academic information** (e.g., the courses a student completed, the test scores and grades a student earned, the academic requirements a student has fulfilled)
- Various other forms of data collected and used by educators and educational institutions (e.g., information related to disciplinary problems, learning disabilities, medical and health issues, etc.)

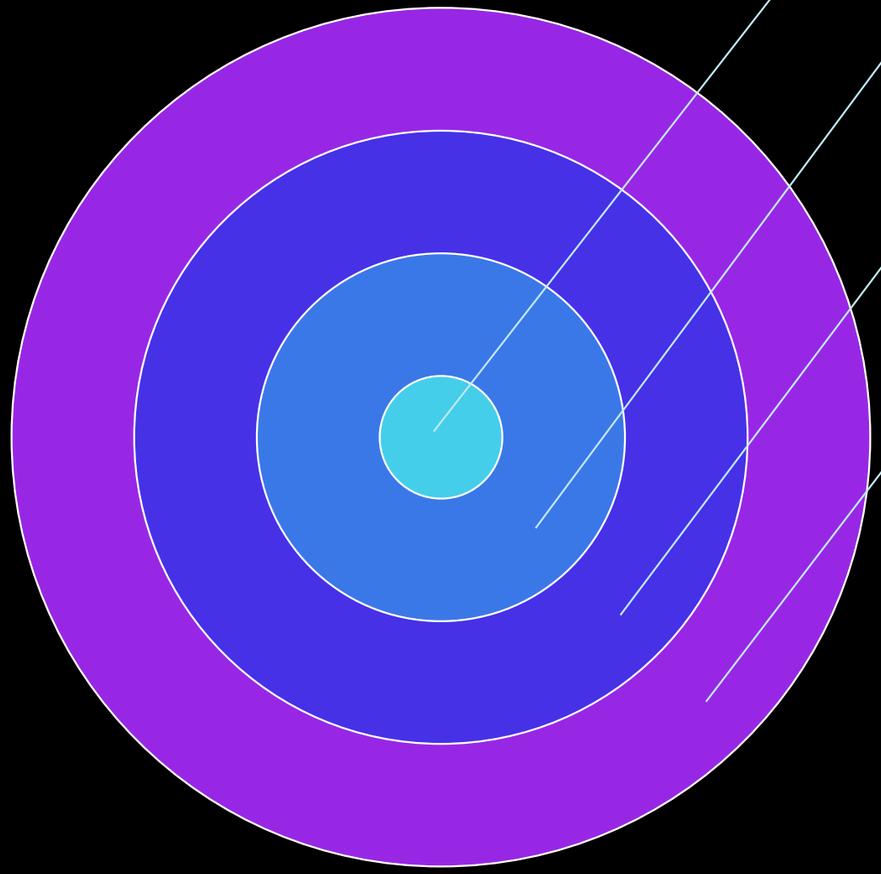
AWS Shared Responsibility Model



Seven fundamental principles of privacy by design

1. Proactive not reactive; preventive not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Full functionality — positive sum, not zero sum
5. End-to-end security — protection over the life cycle
6. Visibility and transparency
7. Respect for user privacy

Jim, I’m a teacher not a technologist!



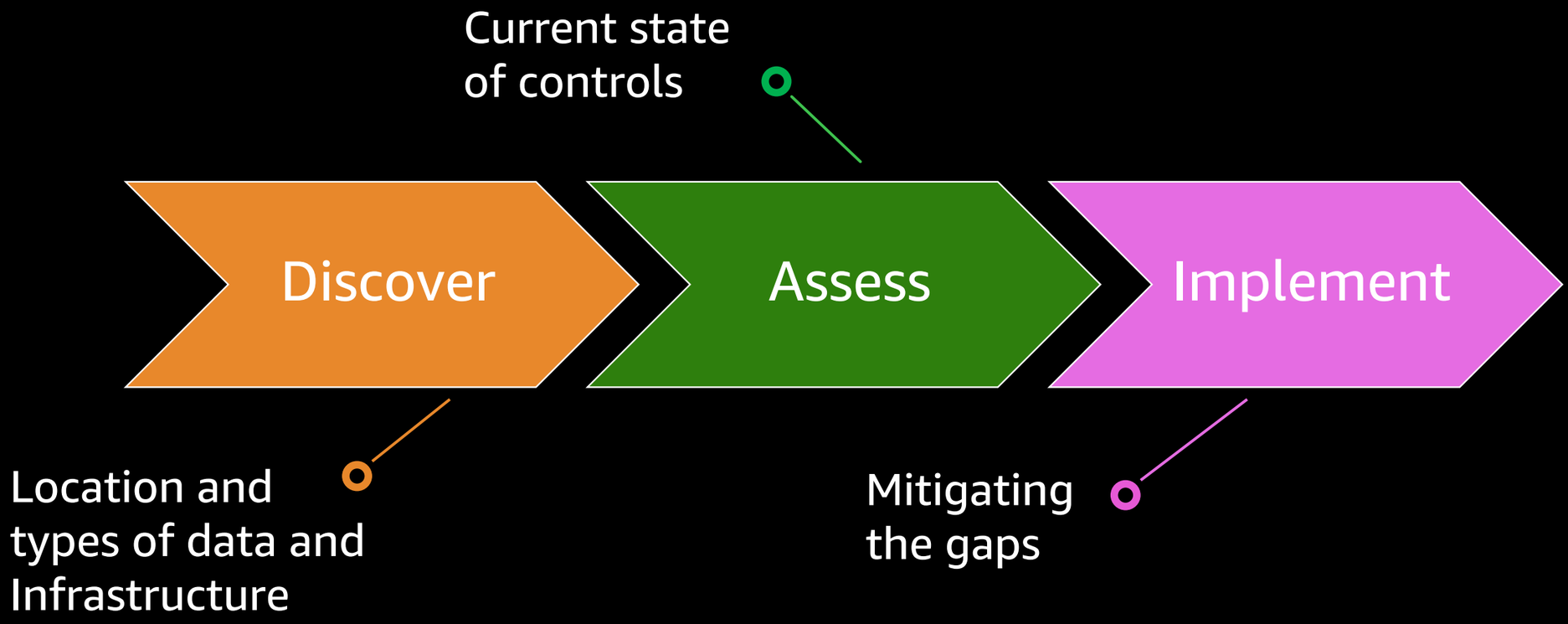
Do more for less money

Accelerated adoption of distance learning platforms

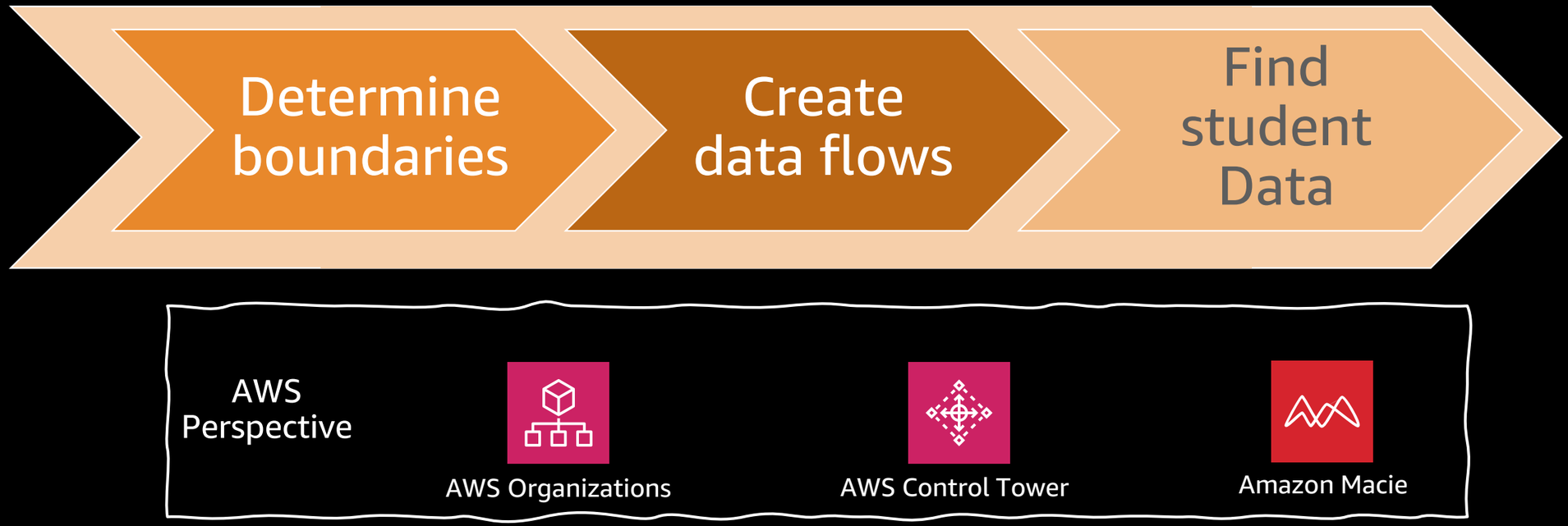
More devices, more problems

Higher demand

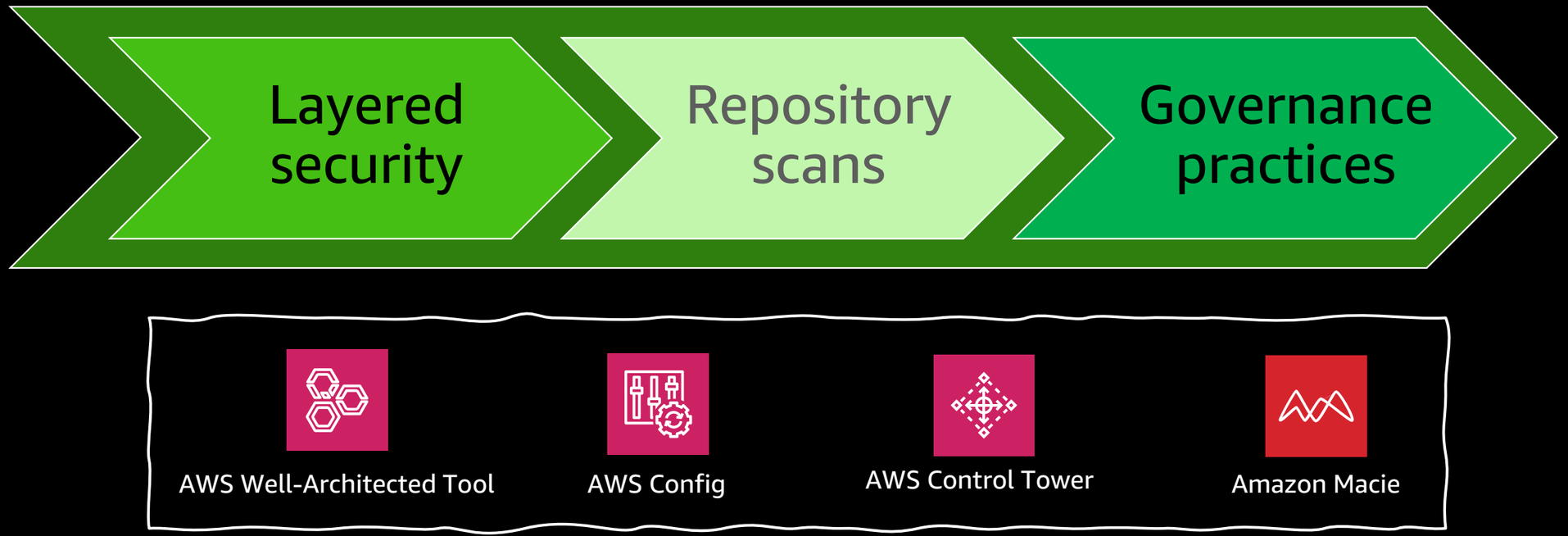
You have to start somewhere



Discover student data



Assess against best practices

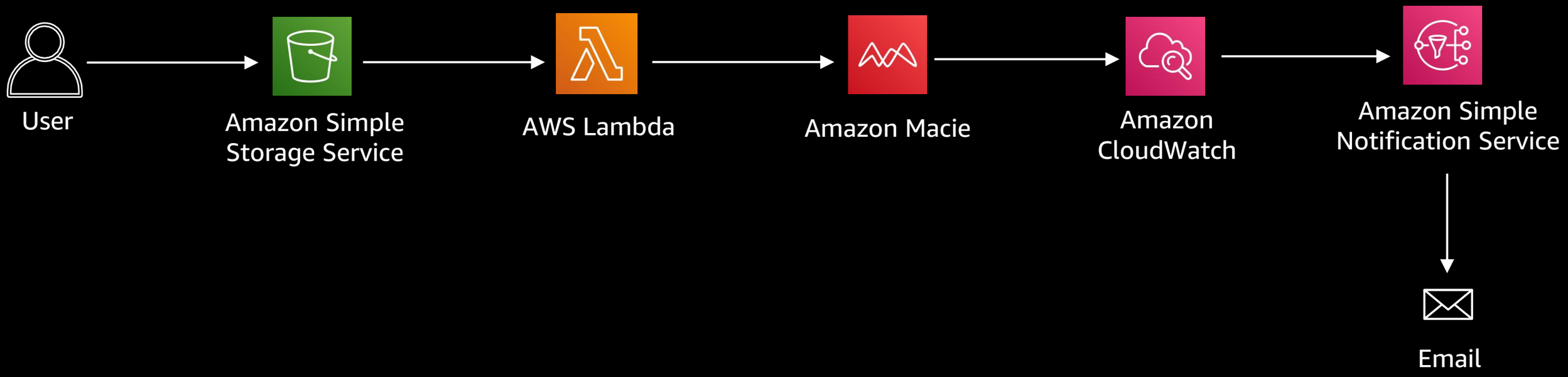


Security design principles

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events



Demo architectural flow



Implement: Best-in-class security controls



Identity and access management

AWS Identity and Access Management

AWS Single Sign-On

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager



Detection

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC flow logs



Infrastructure protection

AWS Firewall Manager

AWS Shield

AWS WAF

Amazon Virtual Private Cloud (Amazon VPC)

AWS PrivateLink

AWS Systems Manager



Data protection

Amazon Macie

AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS Client VPN

Server-side encryption



Incident response

Amazon Detective

AWS CloudEndure DR

AWS Config rules

AWS Lambda

Desire2Learn

TRANSFORMING THE WAY PEOPLE LEARN ONLINE, IMPLEMENTS BEST PRACTICES TO DETECT AND ADDRESS MISCONFIGURATIONS

Challenge

Detecting and remediating AWS misconfigurations across all regions and D2L's 225+ accounts.

Solution

AWS Config and, AWS Security Hub using managed and custom insights, a 3rd party ticket system and a slackbot integration for notification and tracking.

Benefits

An accurate and automated solution from detection to ownership assignment to remediation. This allows D2L security analysts to focus on impactful work versus mundane, repeatable tasks.

D2L believes learning is the foundation upon which all progress and achievement rests. Working closely with organizations globally, D2L has transformed the way millions of people learn online and in the classroom.

D2L
DESIRE2LEARN

Industry: Education

Country: Canada

Employees: 900

Website: http://www.d2l.com/

Athabasca University

FIRST “ALL-IN” AWS MIGRATION BY A UNIVERSITY IN CANADA, WHICH IMPLEMENTS BEST PRACTICES TO SECURE DATA

Challenge

As part of the university’s all-in migration to the cloud, Athabasca University (AU) was looking to modernize its approach to security

Solution

Customized centralized logging including Amazon SQS, Amazon SNS, and Slack integration; Simple Incident Response System; Security Hub Findings Exporter; and automatic EC2 forensic isolation process

Benefits

Modern cloud-based approach to cyber security threats, providing detective controls, incident management, and automation approaches to protect AU’s digital information and technology assets

AU Canada’s Online University

Industry: Education

Country: Canada

Students: 43,000

Website: https://www.athabascau.ca/

Athabasca University provides learning for life. Through the achievements of its students, faculty, and staff, AU stands out as a provider of high-quality post-secondary education

Before you go, remember

- Start with your fundamentals
  https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
- Always consider the AWS security design principles
  https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf
- Don’t forget about the Quick Starts and associated white papers
  https://aws.amazon.com/quickstart/architecture/compliance-hipaa/
  https://aws.amazon.com/compliance/iso-27018-faqs/
- Save time and effort with automation

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.