CSA cloud security alliance®

The future of cloud security

PRESENTED BY

Alejandra Artiguez

Principal Security Solutions Architect

The importance of security

Organizations are moving to the cloud

In their shift to the cloud, organizations are confronting a range of familiar and emerging challenges:

- Evolving requirements that vary across regions
- Highly dynamic security threat landscape
- Stringent reporting requirements
- High standards for privacy and data security
- Limited cloud security & compliance specialists

AWS Global infrastructure

Designed to support operational resilience

31 Launched Regions

99 Availability Zones (AZs)

Announced plans for15 more AZ and 5 more Regions in Canada, Israel, Malaysia, New Zealand, and Thailand.

https://aws.amazon.com/about-aws/global-infrastructure/

AWS Security, identity, & compliance services

Identity and access management

AWS Identity and Access Management (IAM)

AWS IAM Identity Center

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Amazon Verified Permissions

Detective controls

AWS Security Hub

Amazon GuardDuty

Amazon Security Lake

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender

Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager

AWS Verified Access

Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Private CA

AWS Secrets Manager

AWS VPN

Server-Side Encryption

Incident response

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery

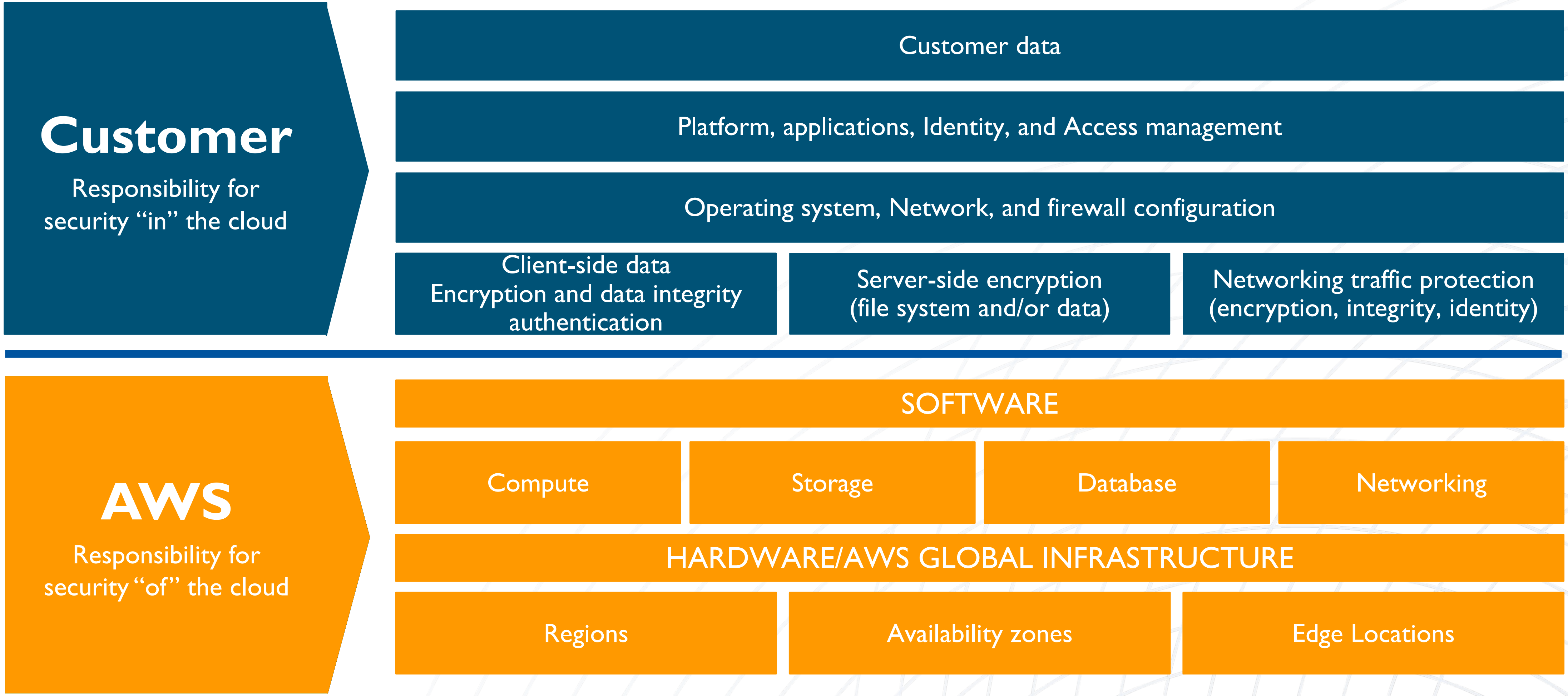
Compliance

AWS Artifact

AWS Audit Manager

https://aws.amazon.com/products/security/

Security and compliance is a shared responsibility



Customer

Responsibility for security “in” the cloud

Customer data

Platform, applications, Identity, and Access management

Operating system, Network, and firewall configuration

Client-side data Encryption and data integrity authentication

Server-side encryption (file system and/or data)

Networking traffic protection (encryption, integrity, identity)

AWS

Responsibility for security “of” the cloud

SOFTWARE

Compute

Storage

Database

Networking

HARDWARE/AWS GLOBAL INFRASTRUCTURE

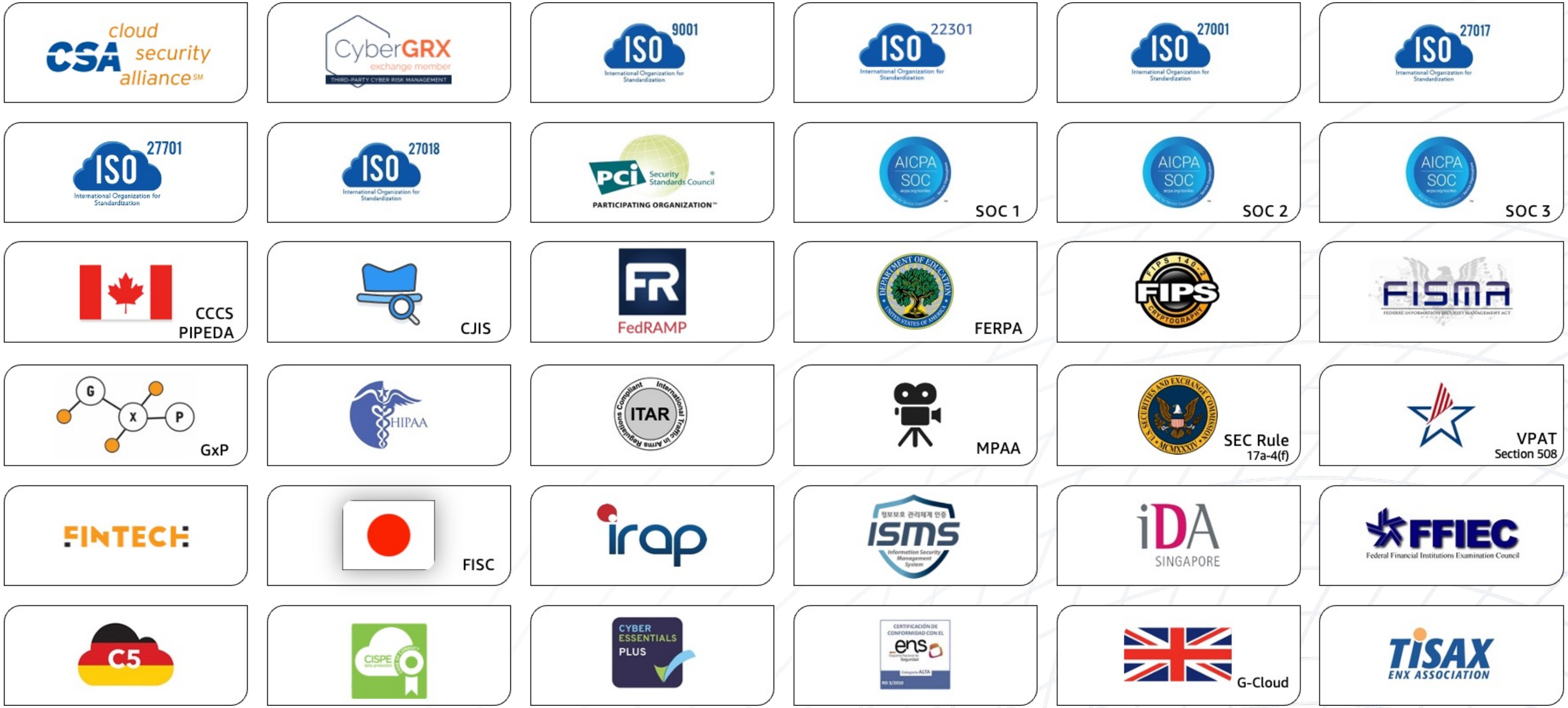
Regions

Availability zones

Edge Locations

https://aws.amazon.com/compliance/shared-responsibility-model/

Customers inherit global security and compliance controls


CSA cloud security alliance SM
CyberGRX exchange member
THIRD-PARTY CYBER RISK MANAGEMENT
ISO 9001
International Organization for Standardization
ISO 22301
International Organization for Standardization
ISO 27001
International Organization for Standardization
ISO 27017
International Organization for Standardization
ISO 27701
International Organization for Standardization
ISO 27018
International Organization for Standardization
PCI Security Standards Council
PARTICIPATING ORGANIZATION
AICPA SOC
SOC 1
AICPA SOC
SOC 2
AICPA SOC
SOC 3
CCCS
PIPEDA
CJIS
FR
FedRAMP
DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA
FERPA
FIPS 140-2
CRYPTOGRAPHY
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
G
X
P
GxP
HIPAA
ITAR
International Traffic in Arms Regulations Compliant
MPAA
U.S. SECURITIES AND EXCHANGE COMMISSION
SEC Rule
17a-4(f)
VPAT
Section 508
FINTECH
FISC
irap
정보보호 관리체계 인증
ISMS
Information Security Management System
iDA
SINGAPORE
FFIEC
Federal Financial Institutions Examination Council
C5
CISPE
CYBER ESSENTIALS PLUS
CERTIFICACIÓN DE CONFORMIDAD CON EL
ens
G-Cloud
TISAX
ENX ASSOCIATION

https://aws.amazon.com/compliance/programs/

5 Security predictions

1. Organizations will infuse security into everything they do

Automate and reduce risk with integrated cloud services

Comprehensive set of APIs and security tools

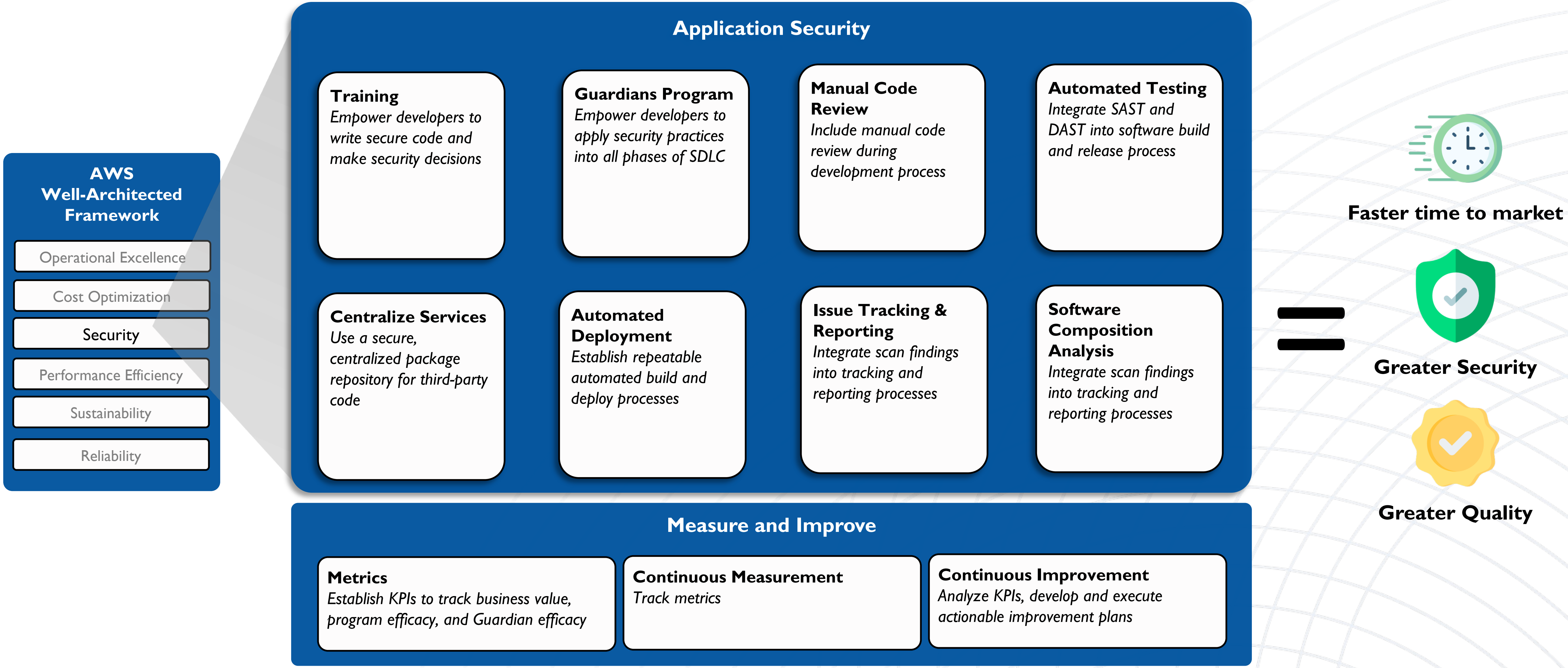
Continuous monitoring and protection

Threat remediation and response

Operational efficiencies to focus on critical issues

Securely deploy business critical applications

Application security



AWS Well-Architected Framework

- Operational Excellence
- Cost Optimization
- Security
- Performance Efficiency
- Sustainability
- Reliability

Application Security

Training
Empower developers to write secure code and make security decisions

Guardians Program
Empower developers to apply security practices into all phases of SDLC

Manual Code Review
Include manual code review during development process

Automated Testing
Integrate SAST and DAST into software build and release process

Centralize Services
Use a secure, centralized package repository for third-party code

Automated Deployment
Establish repeatable automated build and deploy processes

Issue Tracking & Reporting
Integrate scan findings into tracking and reporting processes

Software Composition Analysis
Integrate scan findings into tracking and reporting processes

=

Faster time to market

Greater Security

Greater Quality

Measure and Improve

Metrics
Establish KPIs to track business value, program efficacy, and Guardian efficacy

Continuous Measurement
Track metrics

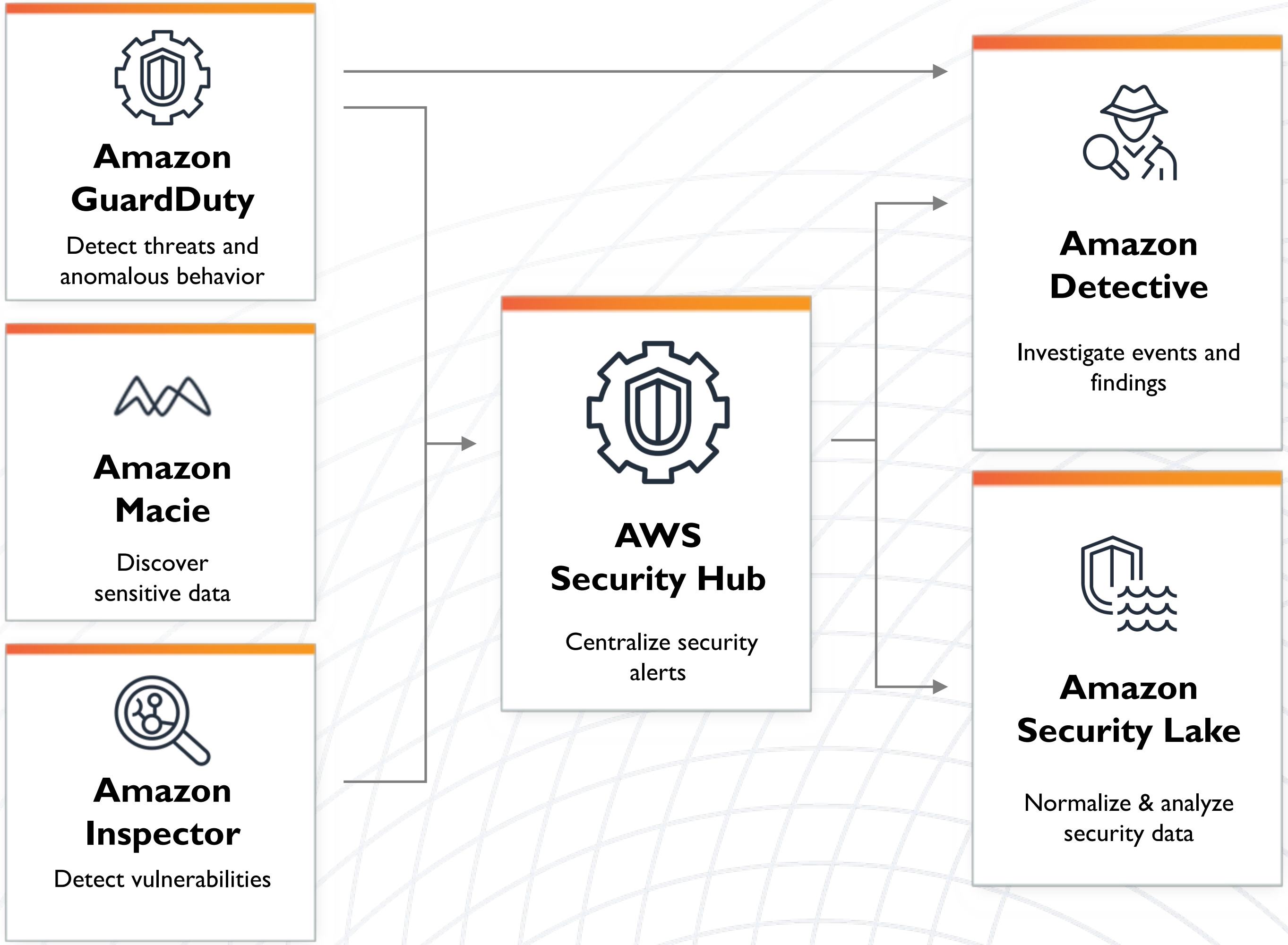
Continuous Improvement
Analyze KPIs, develop and execute actionable improvement plans

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/application-security.html

2. AI/ML will enable stronger security

Detection, monitoring and response

Security monitoring and threat detection



Amazon GuardDuty

Detect threats and anomalous behavior

Amazon Macie

Discover sensitive data

Amazon Inspector

Detect vulnerabilities

AWS Security Hub

Centralize security alerts

Amazon Detective

Investigate events and findings

Amazon Security Lake

Normalize & analyze security data

3. The need for security professionals will only continue to increase

Diversity will help address the continued security talent gap

As the scale of the cloud grows, the need for security professionals will grow along with it.

Diversity is part of the solution to this problem.

Education is key to improve organizations security posture

AWS helps to upskill/re-skill technology and non-technology employees

I am...new to the cloud or want to learn more as a technologist or business associate…

I am… a technologist looking to get certified in cloud or plan to use cloud in my daily work…

I am...a risk management professional and want to learn about assessing regulated workloads in the cloud…

I am...an internal IT auditor and want to learn about cloud-specific considerations and AWS best practices for security auditing…

- AWS Jams
- Cloud Audit Academy
- Risk and Compliance Immersion Days
- Instructor-led courses
- Self-paced courses
- Customized workshops hosted at customer location or at AWS
- Videos, whitepapers, and other resources

AWS can help you customize a learning path with your organization's needs in mind

https://learnsecurity.amazon.com/en/index.html
https://aws.amazon.com/training/learn-about/security/

4. Organizations will continue to invest in data protection and privacy

Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.

Amazon Macie

Discover and protect your sensitive data at scale.

AWS Key Management Service (AWS KMS)

Create and control keys used to encrypt or digitally sign your data.

AWS CloudHSM

Manage single-tenant hardware security modules (HSMs) on AWS.

AWS Certificate Manager

Provision and manage SSL/TLS certificates with AWS services and connected resources.

AWS Secrets Manager

Centrally manage the lifecycle of secrets.

AWS VPN

Connect your on-premises networks and remote workers to the cloud.

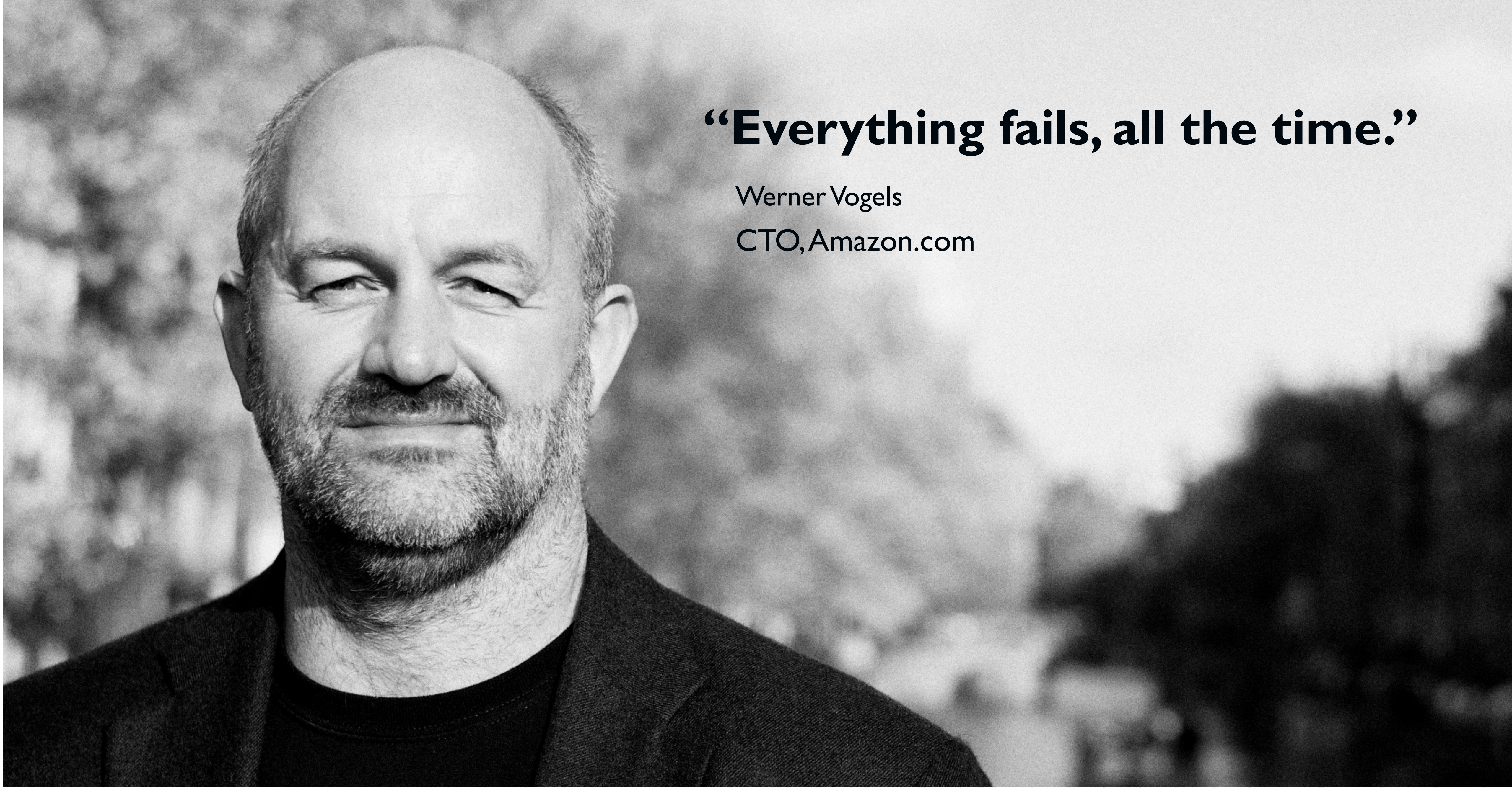
Server-Side Encryption

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

AWS Private CA

Create private certificates to identify resources and protect data.

https://aws.amazon.com/compliance/data-protection/



“Everything fails, all the time.”

Werner Vogels

CTO, Amazon.com

Data storage and resilience

AWS Backup

AWS Elastic Disaster Recovery

AWS Resilience Hub

AWS storage portfolio

BLOCK

Amazon EBS

OBJECT

Amazon S3 and Amazon S3 Glacier

FILE

Amazon FSx

Amazon EFS

AWS Transfer Family

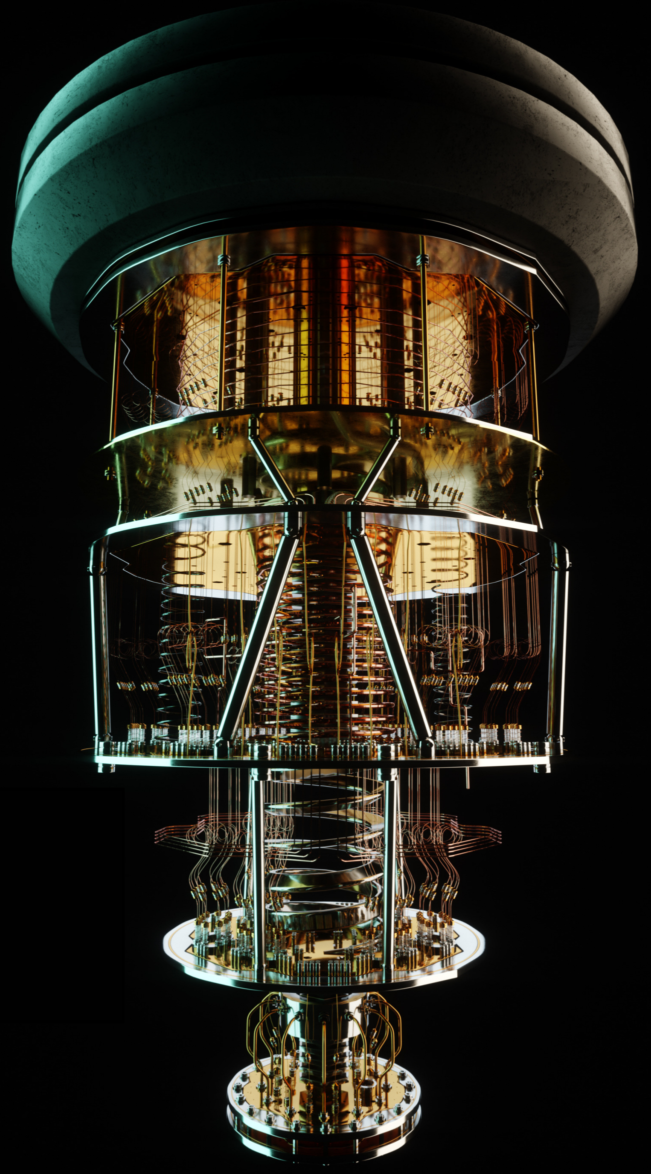
AWS Snow Family

AWS Storage Gateway

AWS DataSync

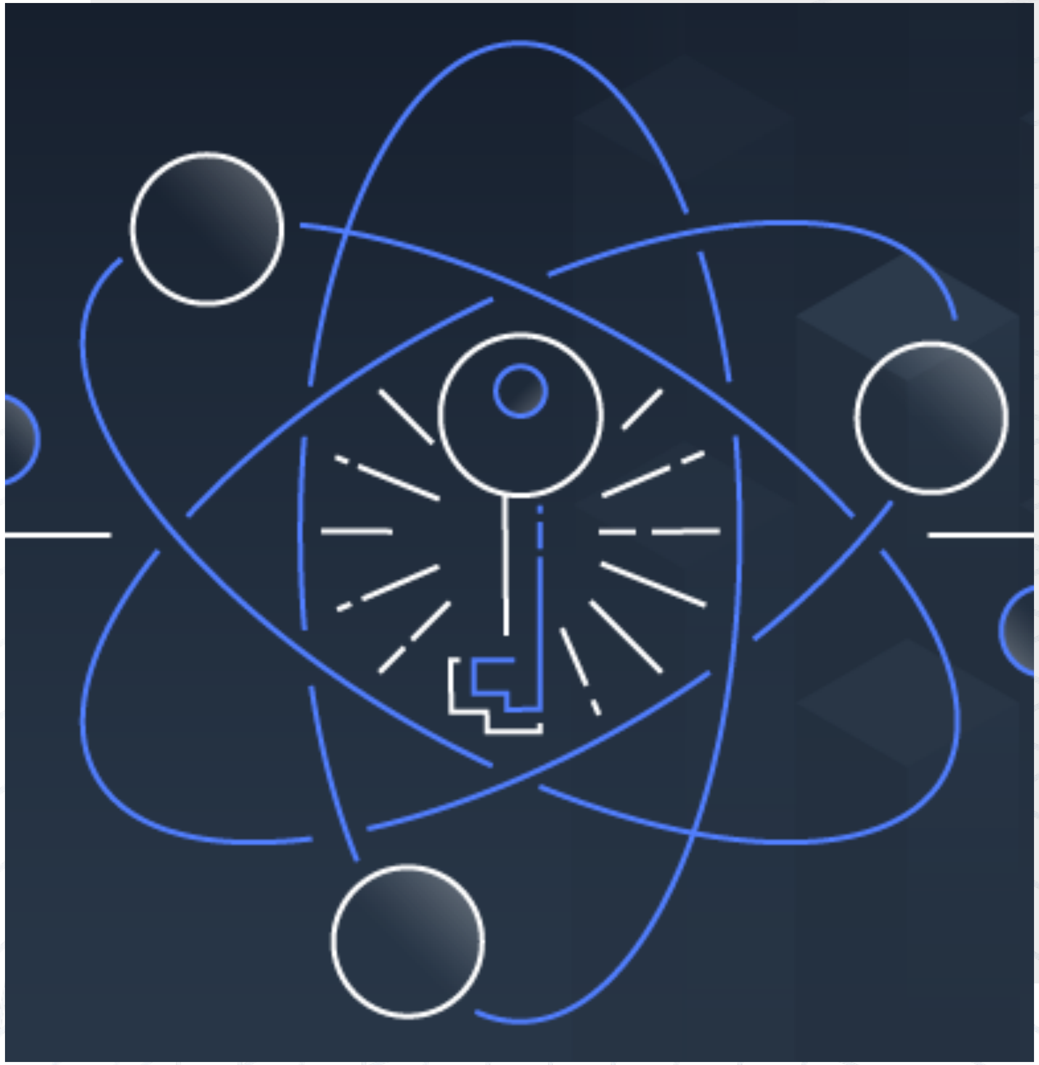
https://aws.amazon.com/products/storage/

5. Quantum computing will benefit security



AWS is preparing for a post-quantum world

AWS research and engineering efforts focus on the continuation of providing cryptographic security for our customers, while developing and testing new cryptographic systems that exceed current customers' demands and protect against projected future adversaries.



https://aws.amazon.com/security/post-quantum-cryptography/

Final thoughts
&
Call to actions

- Create a culture of security.
- Review the shared responsibility model and perform due diligence.
- Automate security as much as possible.
- Include security in your application development.
- Embrace AI/ML in security.
- Revisit your hiring standards, focus on development and retention.
- Monitor privacy regulatory and legislative landscape.
- Classify and secure your data.
- Build a strong resilience strategy that includes data.
- Keep an eye on quantum computing.

CALL TO ACTION

Position security as a business enabler and a driver to future innovation.

CSA cloud security alliance®

Thank you

PRESENTED BY

Alejandra Artiguez

Principal Security Solutions Architect