



AWS Security, Identity, and Compliance

Infrastructure and services to elevate your security in the cloud

Jason Cahill, WWPS VC & Startups

April 1, 2021

Why is on-premises security traditionally challenging?




Lack of
visibility



Low degree
of automation

Before...

Move fast  OR Stay secure

Now...

Move fast **AND** Stay secure

The most sensitive workloads run on AWS



"We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance."

—John Brady, CISO, FINRA (Financial Industry Regulatory Authority)



"AWS allowed us to scale our business to handle 6 million patients a month and elevate our security—all while maintaining HIPAA compliance—as we migrated 100% to cloud in less than 12 months"

—Brian Lozada, CISO, Zocdoc.



"Amazon Web Services was the clear choice in terms of security and PCI DSS Level 1 compliance compared to an on-premises or co-location data center solution."

—Stefano Harak, online senior product manager for Vodafone Italy

Infrastructure and services to elevate your security in the cloud



Inherit global
security &
compliance
controls



Scale with
superior visibility
& control



Highest
standards
for privacy & data
security



Automate & reduce
risk with deeply
integrated services

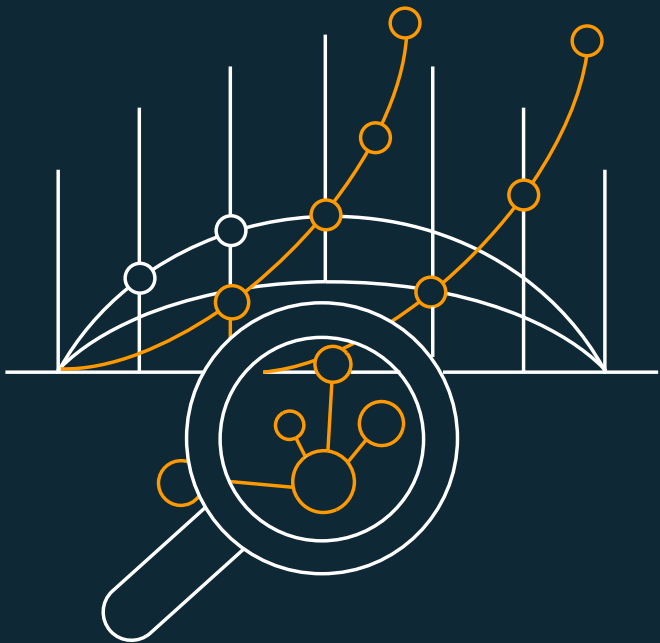


Largest
ecosystem
of security
partners & solutions

Inherit global security and compliance controls



Scale with superior visibility and control



Control where your data is stored
and who can access it

Fine-grain identity & access controls so users
and groups have the right access to resources

Reduce risk via security automation and
continuous monitoring

Integrate AWS services with your solutions
to support existing workflows, streamline ops,
and simplify compliance reporting

Highest standards for privacy and data security



Meet data residency requirements

Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so



Encryption at scale

with keys managed by our AWS Key Management Service (KMS) or managing your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs



Comply with local data privacy laws

by controlling who can access content, its lifecycle, and disposal



Access services and tools that enable you to **build compliant infrastructure** on top of AWS

Automate and reduce risk with integrated 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

AWS security, identity, and compliance solutions

 Identity & access management	 Detection	 Infrastructure protection	 Data protection	 Incident response	 Compliance
<ul style="list-style-type: none">AWS Identity & Access Management (IAM)AWS Single Sign-OnAWS OrganizationsAWS Directory ServiceAmazon CognitoAWS Resource Access Manager	<ul style="list-style-type: none">AWS Security HubAmazon GuardDutyAmazon InspectorAmazon CloudWatchAWS ConfigAWS CloudTrailVPC Flow LogsAWS IoT Device Defender	<ul style="list-style-type: none">AWS Firewall ManagerAWS Network FirewallAWS ShieldAWS WAF – Web application firewallAmazon Virtual Private Cloud (VPC)AWS PrivateLinkAWS Systems Manager	<ul style="list-style-type: none">Amazon MacieAWS Key Management Service (KMS)AWS CloudHSMAWS Certificate ManagerAWS Secrets ManagerAWS VPNServer-Side Encryption	<ul style="list-style-type: none">Amazon DetectiveCloudEndure DRAWS Config RulesAWS Lambda	<ul style="list-style-type: none">AWS ArtifactAWS Audit Manager

Largest ecosystem of security partners and solutions

Network & infrastructure security



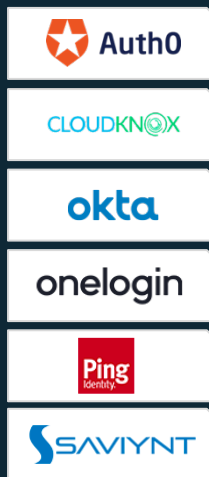
Host & endpoint security



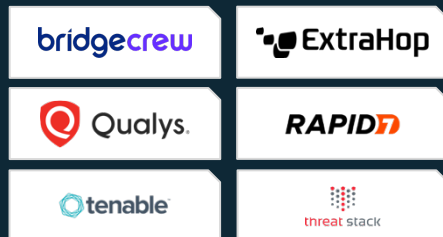
Application security



Identity & access control



Vulnerability & configuration analysis



Data protection & encryption



Logging, monitoring, SIEM, threat detection, & analytics



Consulting and technology competency partners

Security engineering

Governance, risk, & compliance

Security operations & automation

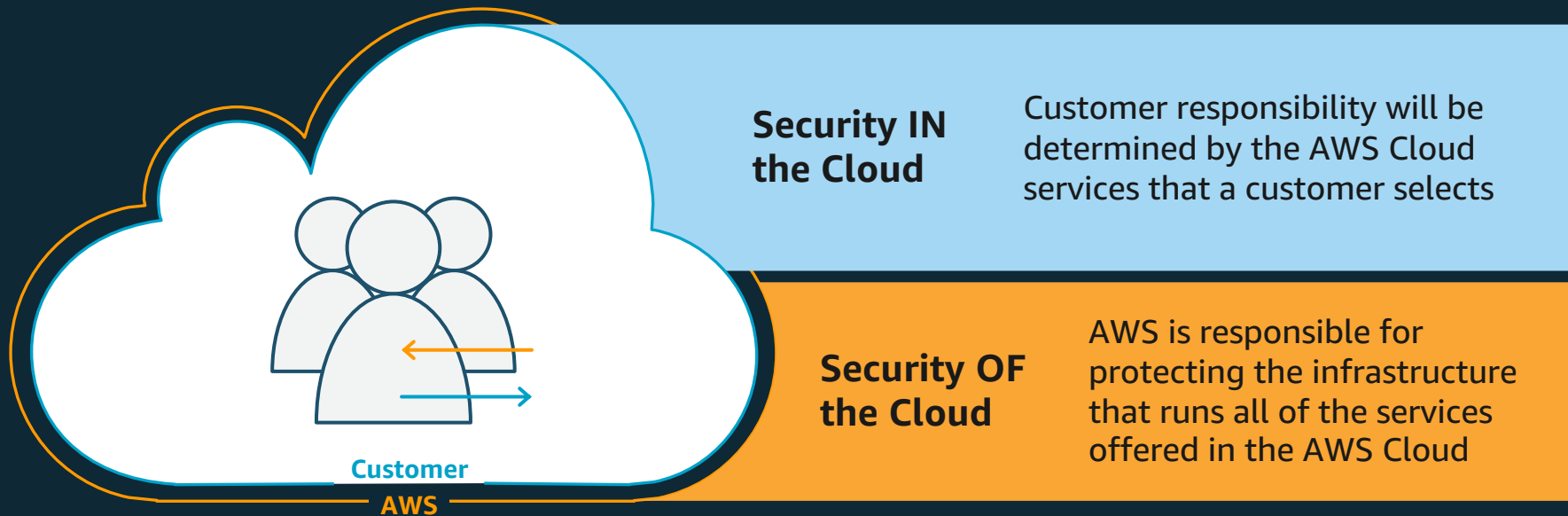




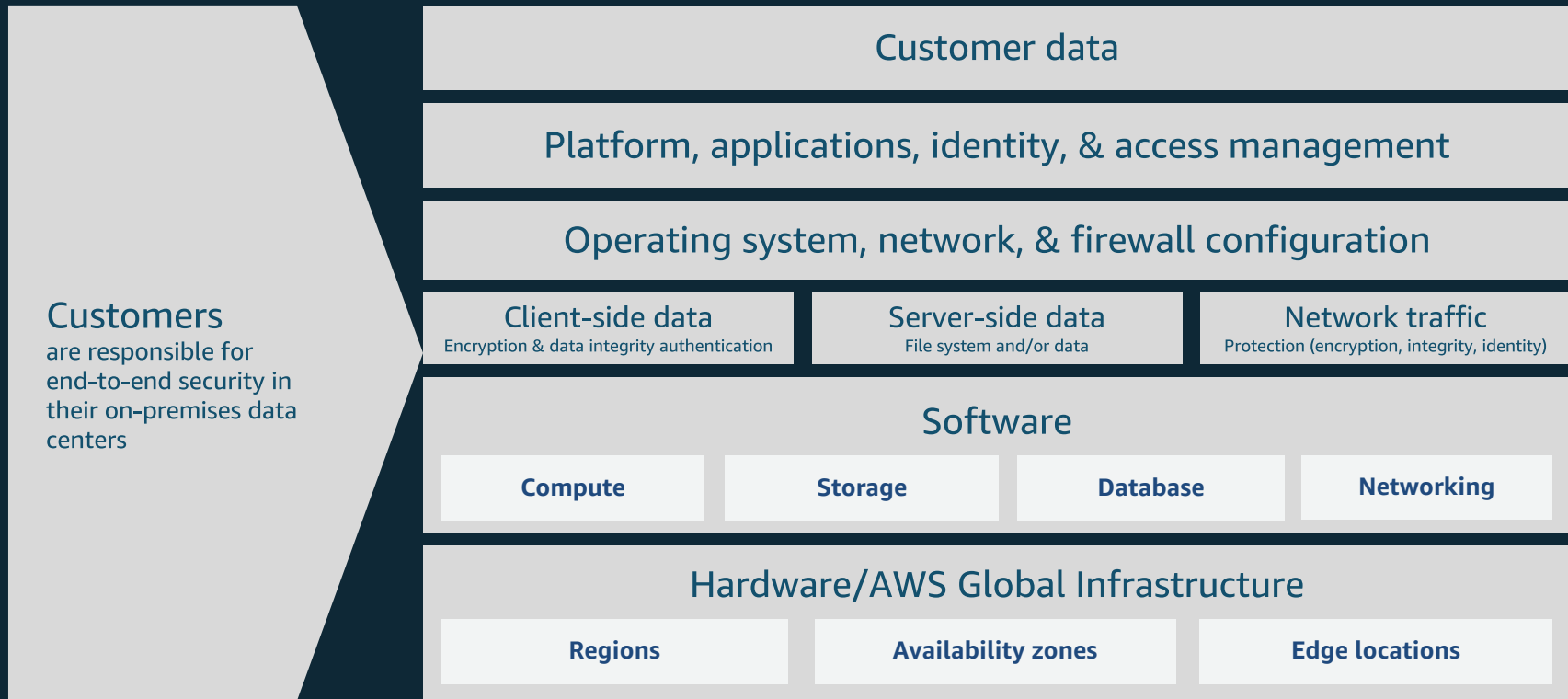




Shared responsibility model



Traditional on-premises security model



Financial industry regulatory authority

- Looks for fraud, abuse, and insider trading over nearly 6 billion shares traded in U.S. equities markets every day
- Processes approximately 6 terabytes of data and 37 billion records on an average day
- Went from 3–4 weeks for server hardening to 3–4 minutes
- DevOps teams focus on automation and tools to raise the compliance bar and simplify controls
- Achieved incredible levels of assurance for consistencies of builds and patching via rebooting with automated deployment scripts



"I have come to realize that as a relatively small organization, we can be far more secure in the cloud and achieve a higher level of assurance at a much lower cost, in terms of effort and dollars invested. We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance."

—John Brady, CISO FINRA



Online medical care scheduling

- Migrated all-in on AWS in under 12 months, becoming a HIPAA compliant cloud-first organization
- New York based startup leveraged infrastructure as code to securely scale to 6 million patients per month
- Data liberation—use data to innovate and drive more solutions for patients, reducing patient wait times from 24 days to 24 hours
- Maintain end to end visibility of patient data using AWS



"Previously all our servers were configured and updated by hand or through limited automation, we didn't take full advantage of a configuration management...All our new services are built as stateless docker containers, allowing us to deploy and scale them easily using Amazon's ECS."

"AWS allowed us to scale our business to handle 6 million patients a month and elevate our security—all while maintaining HIPAA compliance—as we migrated 100% to cloud in less than 12 months"

—Brian Lozada, chief information security officer



Mobile top-up service



- Vodafone Italy is a prominent player in the Italian mobile phone market with over 30 million users.
- With a rise in SIM transactions, the company wanted to find a way to make it easier for customers to top up using a credit or debit card—and since each SIM card contains valuable personal information, that solution needed to be not only flexible, but also secure.
- With AWS Cloud, Vodafone Italy was able to users to purchase credits online with strong security and be compliant with the Payment Card Industry Data Security Standard (PCI DSS).
- With the muscle of the AWS cloud behind it, Vodafone easily managed top-up requests through the new service as it grew to several thousand daily and spread to multiple online channels, including social media platforms.

“Amazon Web Services was the clear choice in terms of security and PCI DSS Level 1 compliance compared to an on-premises or co-location data center solution.”

“Using AWS, we were able to design and launch a security-compliant solution in three months while reducing our capital expenses by 30 percent.”

—Stefano Harak, online senior product manager



Thank you

<https://aws.amazon.com/security/>
<https://aws.amazon.com/compliance/>
<https://aws.amazon.com/products/security>

 @AWSSecurityInfo
@AWSIdentity



Identity & access management

Define, enforce, and audit user permissions across AWS services, actions, and resources



AWS Identity and Access Management (IAM)

Securely manage access to AWS services and resources



AWS Single Sign-On (SSO)

Centrally manage SSO access to multiple AWS accounts & business apps



AWS Directory Service

Managed Microsoft Active Directory in AWS



Amazon Cognito

Add user sign-up, sign-in, and access control to your web/mobile apps



AWS Organizations

Policy-based management for multiple AWS accounts



AWS Resource Access Manager

Simple, secure service to share AWS resources



Detective controls

Gain the visibility you need to spot issues before they impact the business, improve your security posture, and reduce the risk profile of your environment



AWS Security Hub

Centrally view & manage security alerts & automate compliance checks



Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads



Amazon Inspector

Automates security assessments to help improve the security and compliance of applications deployed on AWS



Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically [react to changes](#)



AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, & security analysis



AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational/risk auditing of your AWS account



VPC Flow Logs

Capture info about the IP traffic going to and from network interfaces [in your VPC](#). Flow log data is stored using [Amazon CloudWatch Logs](#)



Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS



AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications



AWS Network Firewall

Deploy network security across your Amazon VPCs with just a few clicks



AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS



AWS WAF—Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security



Amazon Virtual Private Cloud (VPC)

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define



AWS PrivateLink

Access services hosted on AWS easily and securely by keeping your network traffic within the AWS network



AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure OSs



Data protection

In addition to our automatic data encryption and management services, employ more features for data protection

(including data management, data security, and encryption key storage)



Amazon Macie

Discover and protect your sensitive data at scale



AWS Key Management Service (KMS)

Easily create and control the keys used to encrypt your data



AWS CloudHSM

Managed hardware security module (HSM) on the AWS Cloud



AWS Certificate Manager

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services



AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle



AWS VPN

Extend your on-premises networks to the cloud and securely access them from anywhere



Server-Side Encryption

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



Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice



Amazon Detective

Analyze and visualize security data to rapidly get to the root cause of potential security issues



CloudEndure
An AWS Company

CloudEndure Disaster Recovery

Fast, automated, cost-effective disaster recovery



AWS Config Rules

Create rules that automatically take action in response to changes in your environment, such as isolating resources, enriching events with additional data, or restoring configuration to a known-good state



AWS Lambda

Use our serverless compute service to run code without provisioning or managing servers so you can scale your programmed, automated response to incidents



Compliance

AWS supports security standards and compliance certifications to help customers satisfy compliance requirements for virtually every regulatory agency around the globe.



AWS Artifact

No cost, self-service portal for on-demand access to AWS' compliance reports



AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance