THE EXECUTIVES GUIDE TO

Cloud Security and Compliance

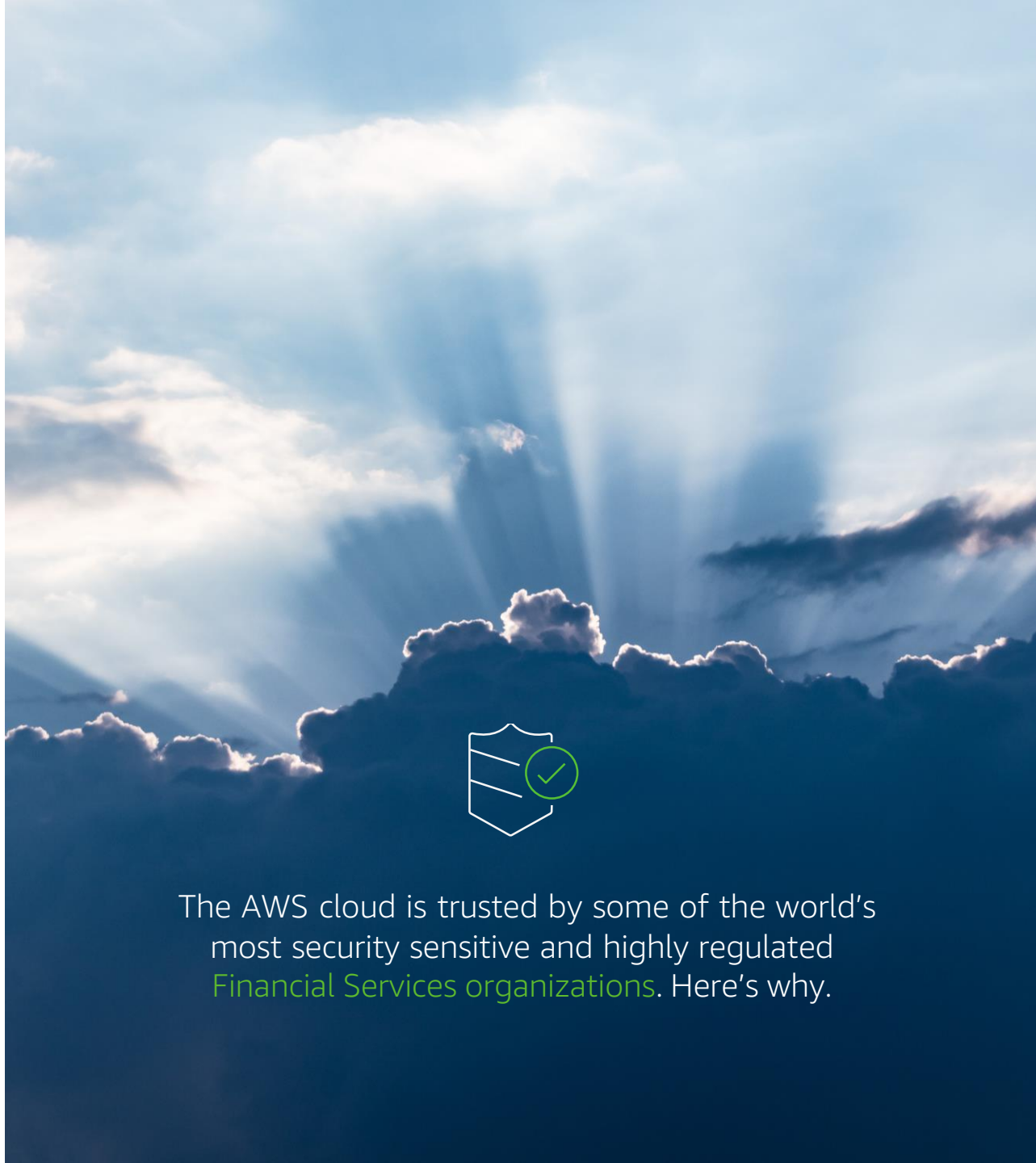
aws financial services

Table of Contents

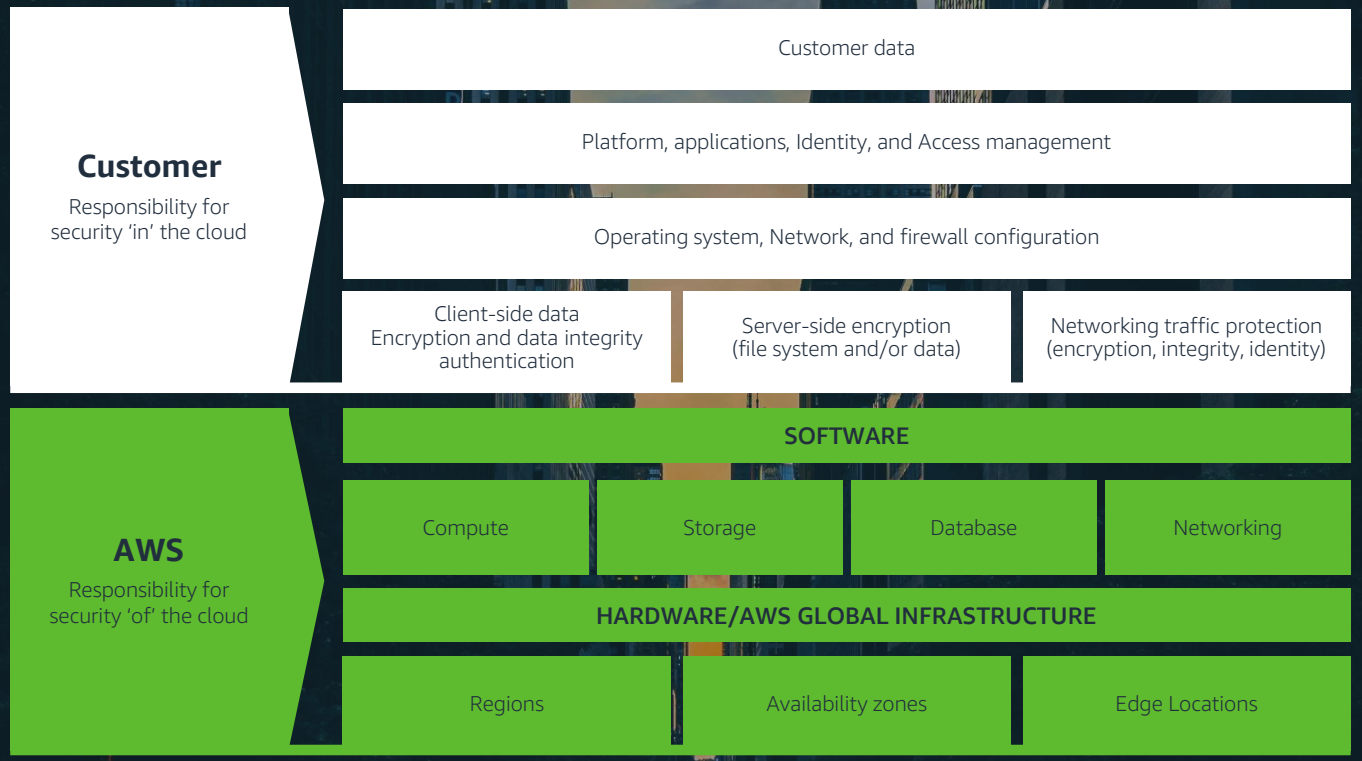
The cloud you can bank on (and trade, invest, and insure)

The Financial Services industry is one of the most regulated industries in the world. Yet in order to stay competitive, Financial Services companies need to push the boundaries of innovation while complying with strict security requirements. AWS understands the security, regulatory, and compliance obligations financial institutions face and has worked with the industry's most complex organizations to meet their requirements at every stage of their cloud journeys.

aws financial services



The AWS cloud is trusted by some of the world's most security sensitive and highly regulated Financial Services organizations. Here's why.



aws financial services

AWS enhances your specific protections

AWS operates on a Shared Responsibility Model. While AWS manages the security of the cloud, customers are responsible for security in the cloud. This shared model reduces your operational burden, because AWS operates, manages, and controls the layers of IT components from the host operating system and virtualization layer down to the physical security of the facilities. You can then use AWS control and compliance documentation to perform your own control evaluation and verification procedures. Although you retain control of your security protocols, AWS controls strengthen your compliance and certification programs by providing access to guidance materials and industry-leading security teams while maintaining your specific security assurance requirements.

Built to the highest standards for security, compliance, and privacy

Nothing is more important to us than protecting your data. As an AWS customer, you will gain access to controls that have been tested and validated by third-party auditors across ISO 27001, ISO 27017, ISO 27018 PCI-DSS, PCI 3DS, SOC 1, SOC 2, SOC 3, and other certifications. AWS Financial Services security experts can also help you create a scalable, secure cloud platform specially designed to complement your organization's security goals, strategies, and tactics, while meeting the strictest regulatory requirements.

To help you get the most from the AWS security control framework, we developed AWS Security Assurance Programs to demonstrate how AWS's security controls align with different compliance standards. AWS also communicates security best practices and policies that customers can then incorporate into their compliance frameworks. In addition, customers can gain access to tools and documentation to learn about how AWS aligns to industry regulations as well as information on security frameworks, and certifications from independent, third-party auditors about AWS's alignment to certain compliance programs.

AWS also offers the AWS Compliance Center for Financial Services customers. The regulatory requirements that impact the industry. The AWS Compliance Center summarizes the position of regulators in over 58 countries[1] regarding the adoption of cloud services.

[1] As of August 2021

aws financial services

Our **core infrastructure** is designed to meet the most stringent security requirements in the world and is monitored 24/7 to ensure the confidentiality, integrity, and availability of customer data.

Maintain strong control of your data

Data doesn't do much good if it's difficult to access. With AWS, you can build on the most secure global infrastructure, knowing that you own and control access to your data, including the ability to encrypt it, move it, and manage retention. The fine-grain access controls built into AWS allow you to be confident that the right resources have the right level of access to the right data.

In addition, with 81 Availability Zones in 25 geographic Regions,[2] the design of our global infrastructure allows you to retain complete control over where your data is physically located, helping you to meet data residency requirements.

[2] As of August 2021

aws financial services

Use security automation and API integration to become more responsive and agile, making it easier to work closely with developer and operations teams to create and deploy code faster and more securely.

Reduce risk through automation

AWS services such as Amazon GuardDuty, Amazon CloudTrail, and AWS Lambda automate tasks like logging, monitoring, and remediation of malicious activities according to your specific security and compliance needs. This reduces human configuration errors, enabling you to be more secure and giving your team more time to focus on the work that is critical to the business so you can grow and innovate faster.

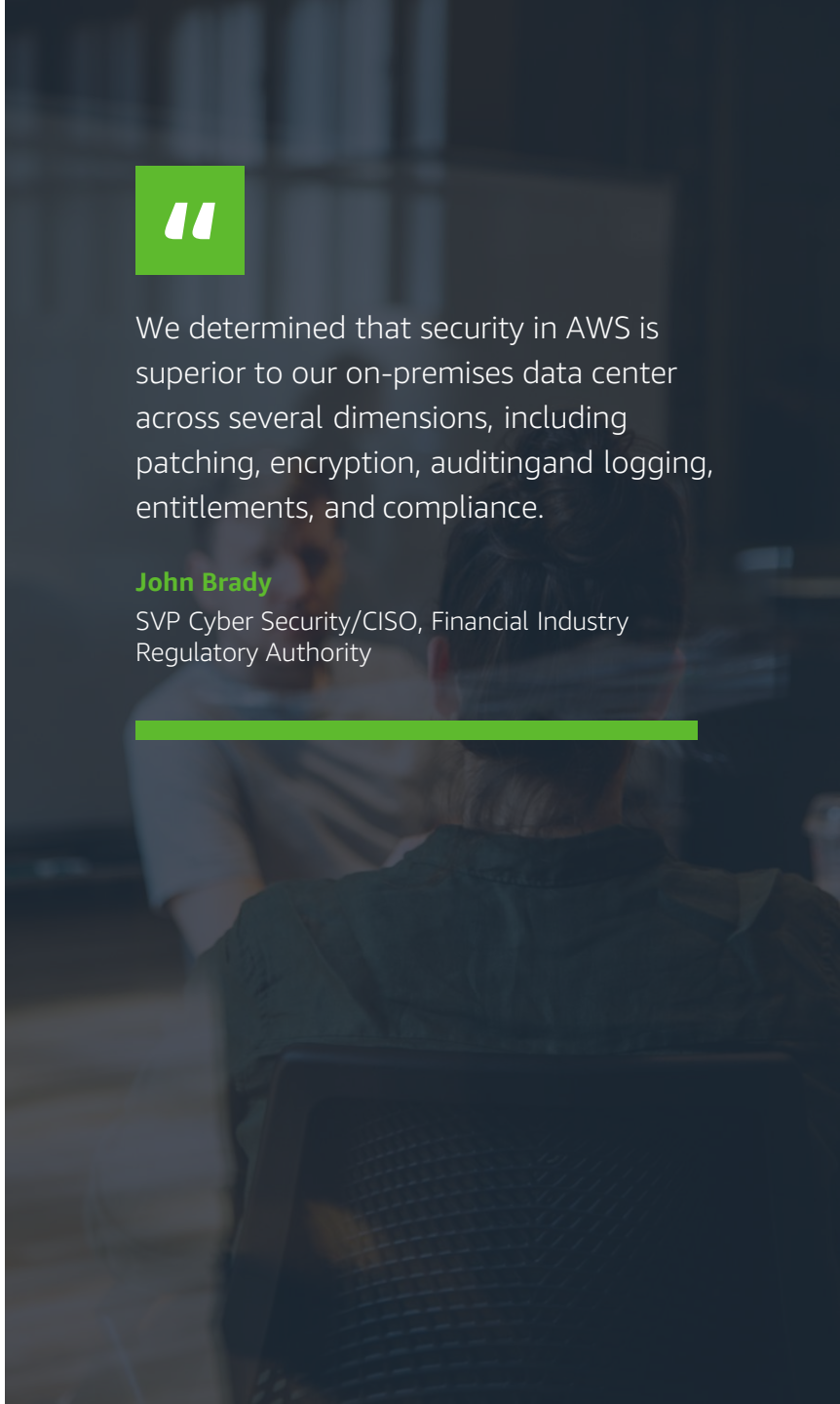
Automating infrastructure and application security checks whenever new code is deployed allows you to continually enforce your security and compliance controls to help ensure confidentiality, integrity, and availability. You can also automate infrastructure and application security checks in a hybrid environment with our information management and security tools to easily integrate AWS as a seamless and secure extension of your on-premises environment.

AWS in the Financial Services Industry

The **Financial Industry Regulatory Authority (FINRA)**—America's leading governance body for broker-dealers—used AWS to migrate 90 percent of its data to the cloud, enabling the organization to create a flexible platform for regulating the securities industry. FINRA made Security and Compliance key stakeholders in the migration of its applications, leveraged AWS security services such as **AWS Key Management System**, and inherited the security of other AWS services to reduce costs and enhance security maintenance efforts.

National Australia Bank (NAB) is working with AWS to accelerate its three-year enterprise transformation. NAB is adopting a cloud-first strategy using AWS compute, storage, database, and analytics capabilities to build new services to deliver better financial outcomes for its nine million customers around the globe. For enhanced security, NAB deployed **Amazon GuardDuty**, a fully managed intelligent threat detection service that continuously monitors account activity for malicious or unauthorized behavior, to help protect all of its AWS workloads and safeguard customer data in the cloud.

aws financial services



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

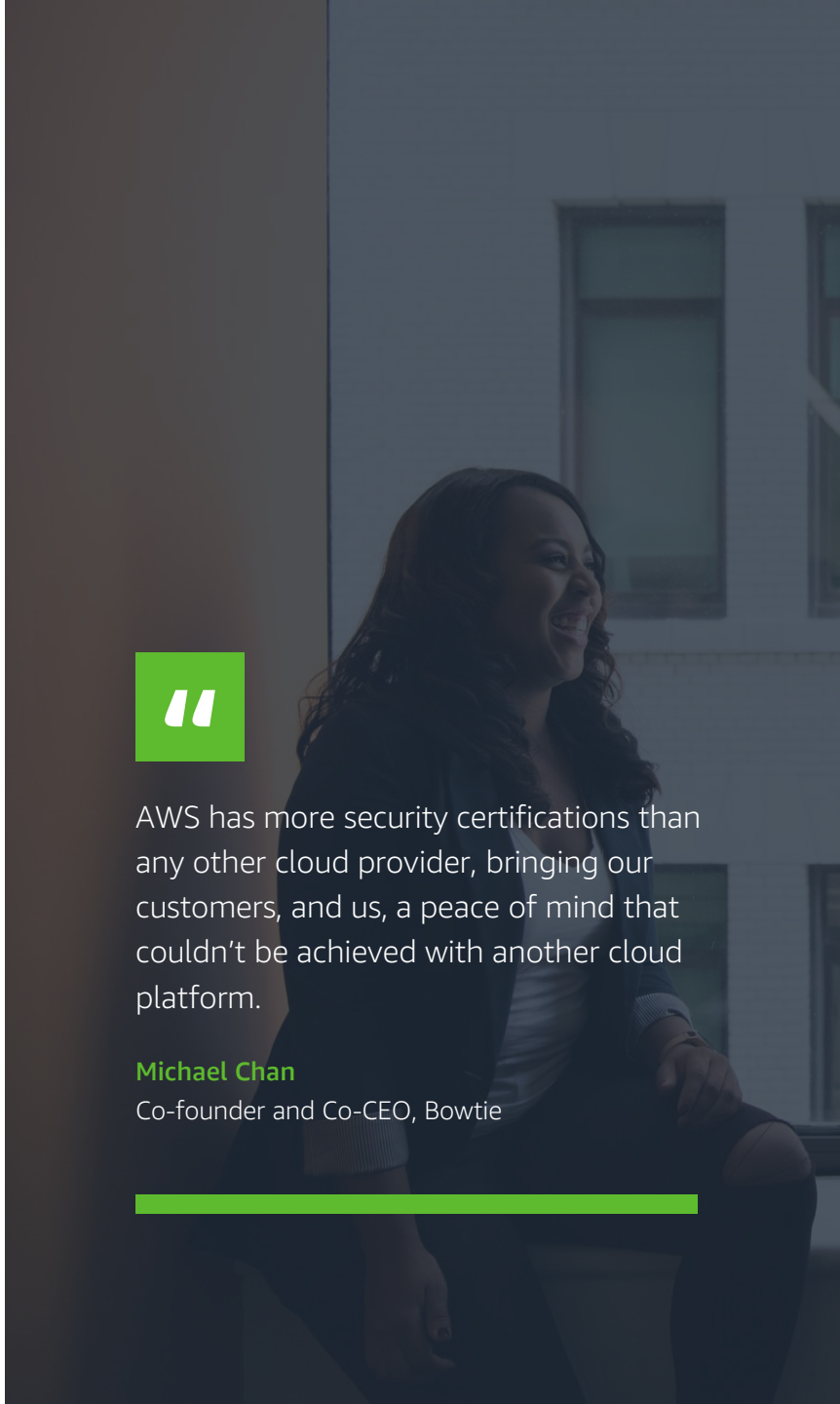
John Brady
SVP Cyber Security/CISO, Financial Industry Regulatory Authority

AWS in the Financial Services Industry

NuData Security, a MasterCard company, is a Canadian startup which has been running on AWS for over 10 years. NuData specializes in solutions that minimize the impact of attacks with offerings that are powered by machine learning on AWS. It uses **Amazon SageMaker** to improve detection of fraudulent attacks along with **Elastic Load Balancing** and **AWS Lambda** to provide real-time device intelligence and enable passive biometrics for account verification. The solution has mitigated over 250 million automated attack attempts with a 99% accuracy rate.

Bowtie, Hong Kong's first virtual insurance company, built its insurance platform on AWS as it needed to ensure it operated in a highly secure and available environment. With AWS, Bowtie built its own security alert system, using **Amazon GuardDuty** to monitor the logs of multiple AWS components like **Amazon VPC, Amazon Route 53**, and **AWS CloudTrail**. The system automatically notifies their cloud team when anomalies are detected, enabling quick responses and ensuring its platform is safe and secure while continuing to launch new services to its customers.

aws financial services



"AWS has more security certifications than any other cloud provider, bringing our customers, and us, a peace of mind that couldn't be achieved with another cloud platform.

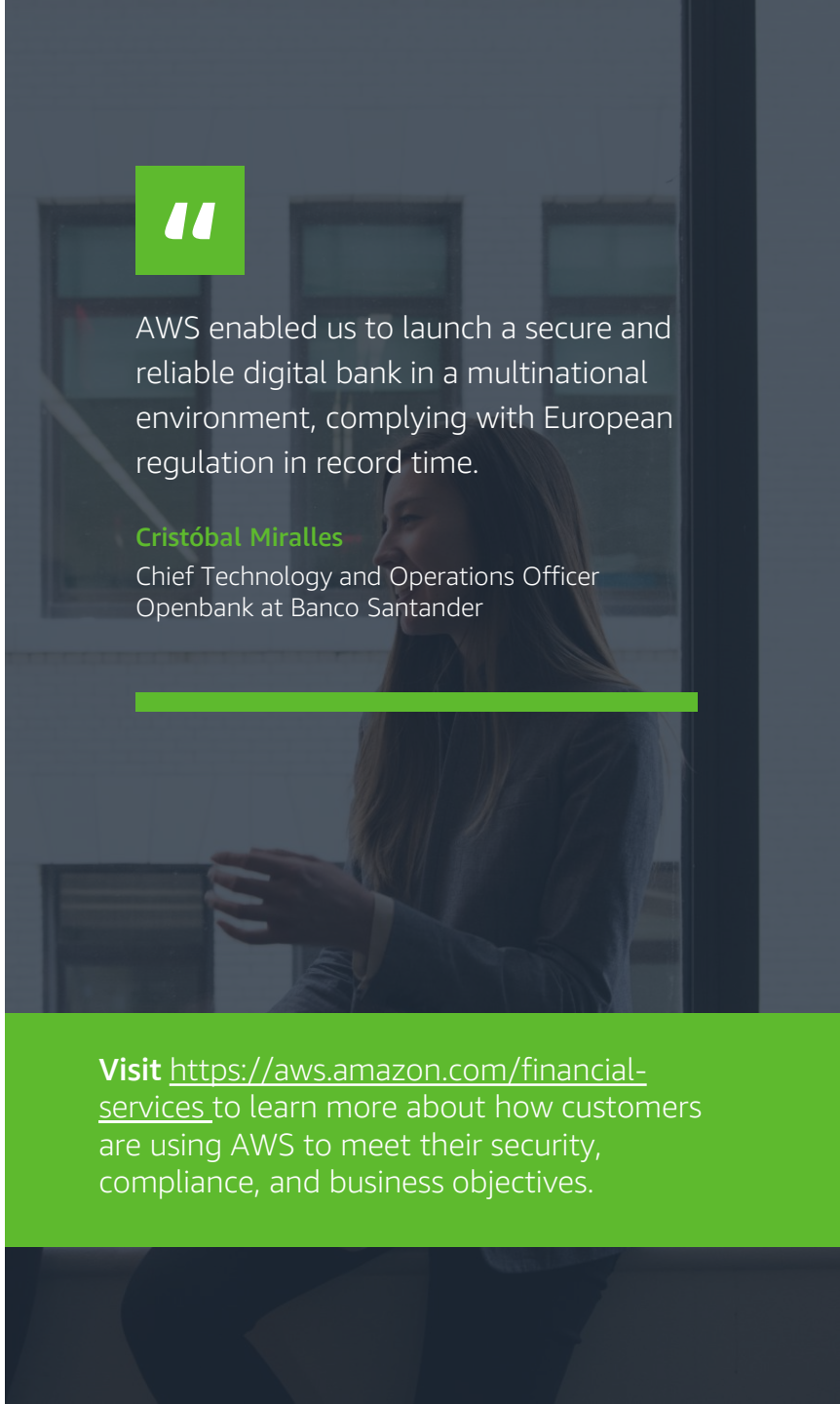
Michael Chan
Co-founder and Co-CEO, Bowtie

AWS in the Financial Services Industry

Openbank
Grupo Santander

Openbank, Santander Group's 100% digital bank, is all-in on AWS. Openbank worked with AWS to migrate its mission-critical data lake from on-premises to a cloud-based architecture and has relaunched its technology stack with a new set of cloud-based components and full machine learning capabilities for its AML, fraud, commercial, and credit risk activities.

Openbank is using a comprehensive set of AWS services to evolve its customer service models and help them provide proof of robust security architectures that protect both customers and proprietary data.



"AWS enabled us to launch a secure and reliable digital bank in a multinational environment, complying with European regulation in record time.

Cristóbal Miralles
Chief Technology and Operations Officer
Openbank at Banco Santander

Visit https://aws.amazon.com/financial-services to learn more about how customers are using AWS to meet their security, compliance, and business objectives.

aws financial services

Discover how AWS can improve your data security

At AWS, we innovate rapidly at scale, continually incorporating customer feedback into our services. This benefits you because our solutions improve over time, and we are constantly evolving our core security services.

aws financial services

AWS security, identity, and compliance solutions

AWS customers can access services that strengthen security postures in six key areas:

Identity and access management

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

AWS Identity and Access Management (IAM)
Securely control access to AWS services and resources.

Amazon Cognito
Add user sign-up/sign-in and access control to your web and mobile applications.

AWS Directory Service
Managed Microsoft Active Directory in the AWS Cloud.

Amazon Single Sign-on (SSO)
Centrally manage SSO access to multiple AWS accounts and business applications.

AWS Organizations
Policy-based management for multiple AWS accounts.

AWS Resource Access Manager
Simple, secure service to share AWS resources.

Detective control

Gain the visibility you need to identify and respond to issues before they can impact your business, improve your security posture, and reduce risk in your environment.

AWS Security Hub
Centrally view and manage security alerts, and automate compliance checks.

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

Amazon Inspector
Automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

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

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

Amazon CloudWatch
Complete visibility into your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes.

VPC Flow Logs
Capture information about the IP traffic going to and from network interfaces in your Virtual Private Cloud (VPC). Flow log data is stored using Amazon CloudWatch Logs.

Infrastructure protection

Manage and increase security of your overall infrastructure.

AWS Systems Manager

Easily configure and manage Amazon Elastic Compute Cloud (EC2) and on-premises systems to apply OS patches, create secure system images, and configure secure operating systems.

AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS.

AWS Web Application Firewall (WAF)

Protect your web applications from common web exploits that could impact availability, security, and resources.

AWS Firewall Manager

A security management service that makes it easier to centrally configure and manage AWS WAF rules across your accounts and applications.

AWS Control Tower

Set up and govern a secure, multi-account AWS environment, called a landing zone. AWS Control Tower creates your landing zone using AWS Organizations, bringing ongoing account management and governance as well as implementation best practices.

AWS Network Firewall

Define firewall rules that give you fine-grained control over network traffic, such as blocking outbound Server Message Block (SMB) requests to prevent the spread of malicious activity.

AWS Private Link

Set up private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet.

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 KMS and **AWS CloudHSM** integrate to help satisfy compliance obligations that would otherwise require the use of on-premises HSMs while providing AWS service integrations of KMS.

Data protection

Deploy more data protection features to enhance our automatic encryption and management service, including data management, data security, and encryption key storage.

AWS Key Management Service (KMS)

Create and control the encryption keys used to encrypt your data.

AWS CloudHSM

Managed hardware security module (HSM) on the AWS Cloud.

AWS VPN

Establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network.

Amazon Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycles.

AWS Certificate Manager

Provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates.

Amazon Macie

Leverage machine learning to automatically discover, classify, and protect your sensitive data, and even automate compliance checks.

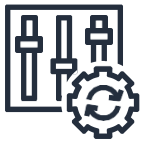
Server-Side Encryption

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

Incident response

AWS automated tools help you quickly contain events and return to a known good state.

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



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 CloudEndure Disaster Recovery
Minimize downtime and data loss by providing fast, reliable recovery of physical, virtual, and cloud-based servers into AWS Cloud, including public regions, AWS GovCloud (US), and AWS Outposts.

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

Streamline and automate compliance to simplify reporting, use activity monitoring services that detect configuration changes and security events across your system, and get on-demand access to more than 2,500 security controls.

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 with regulations and industry standards.

Resources

AWS Compliance Center

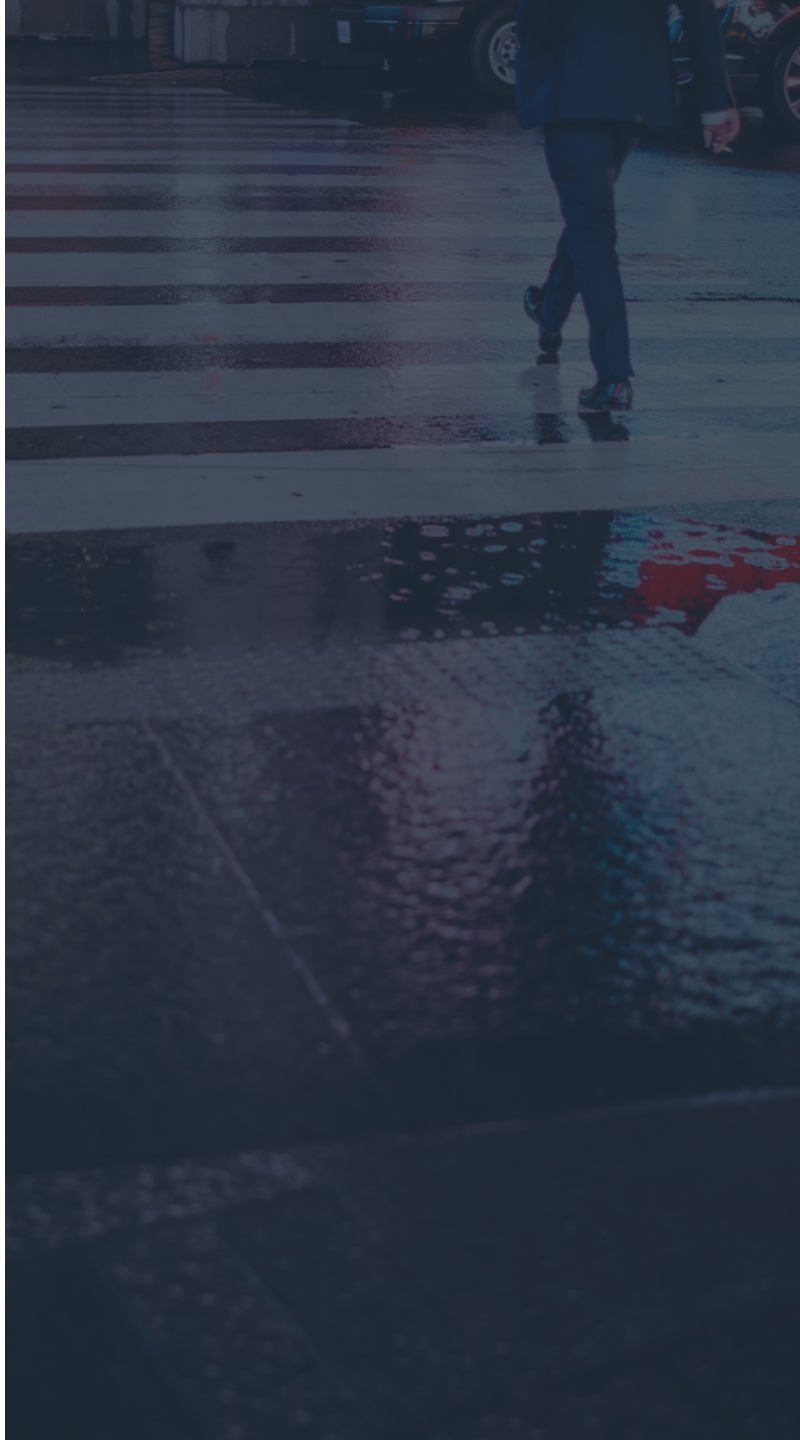
The AWS Compliance Center offers a central location to research cloud-related regulatory requirements. Simply select the country you are interested in, and the AWS Compliance Center will display the position of regulators in that country with regard to the adoption of cloud services.

For more information, visit https://www.atlas.aws and https://aws.amazon.com/compliance/programs.

Training

Whether you are just starting out, building on existing IT skills, or sharpening your cloud knowledge, AWS training can help you and your team advance your understanding so you can be more effective using the cloud.

For more information, visit https://aws.amazon.com/training/paths-specialty.



aws financial services

Resources

Well-Architected Framework

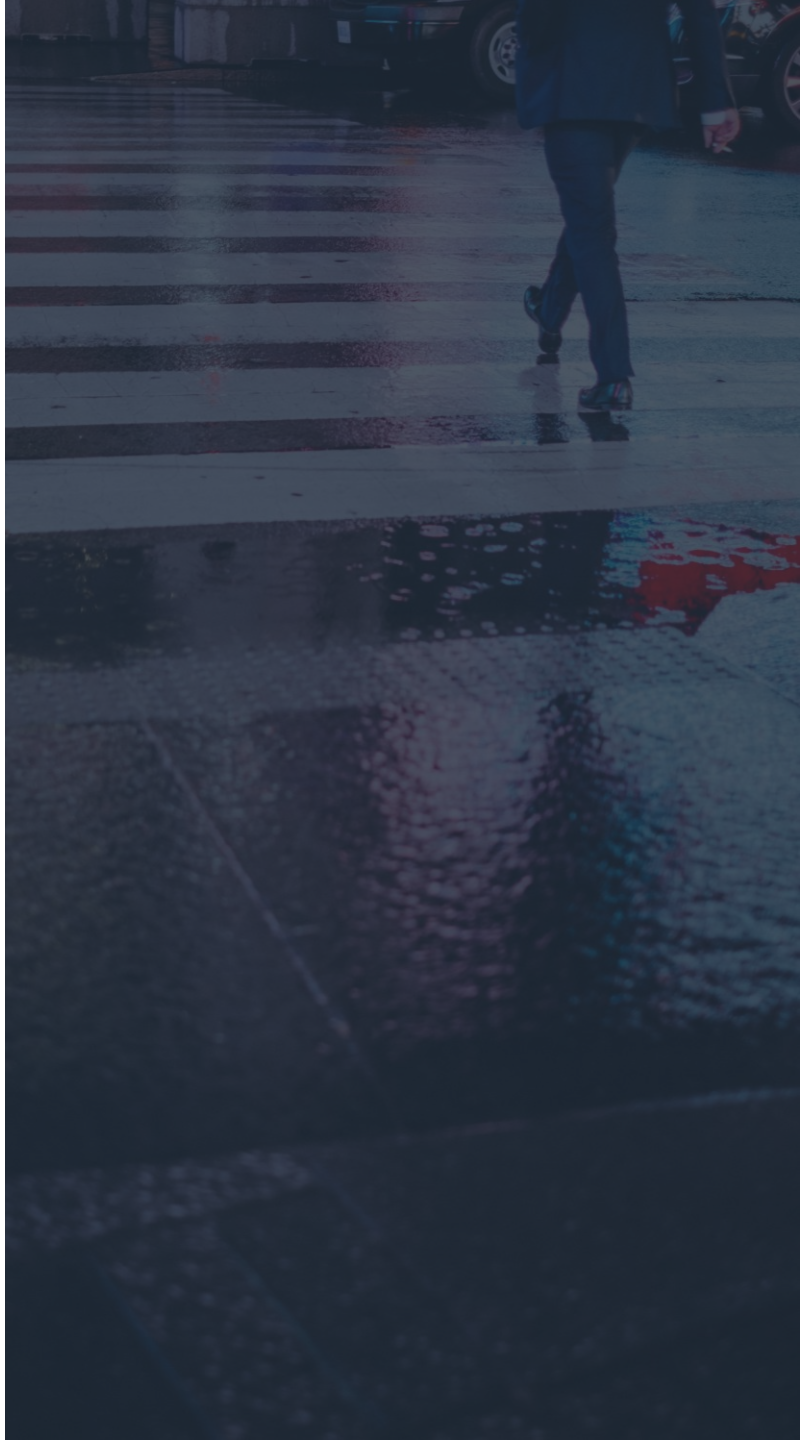
Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—the Well-Architected Framework provides a consistent approach for customers and members of the AWS Partner Network (APN) to evaluate architectures and implement designs that will scale over time. APN Technology and Consulting Partners are available to help you along the way as you build and manage your workloads.

For more information, visit **https://aws.amazon.com/architecture/well-architected** and **https://aws.amazon.com/architecture/well-architected/partners**.

Cloud Adoption Framework

AWS Professional Services created the AWS Cloud Adoption Framework (CAF) to help organizations design and travel an accelerated path to successful cloud adoption. The guidance and best practices provided by the framework help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle.

For more information, visit **https://aws.amazon.com/professional-services/CAF**.



aws financial services

Resources

AWS Partner Network (APN) and AWS Marketplace

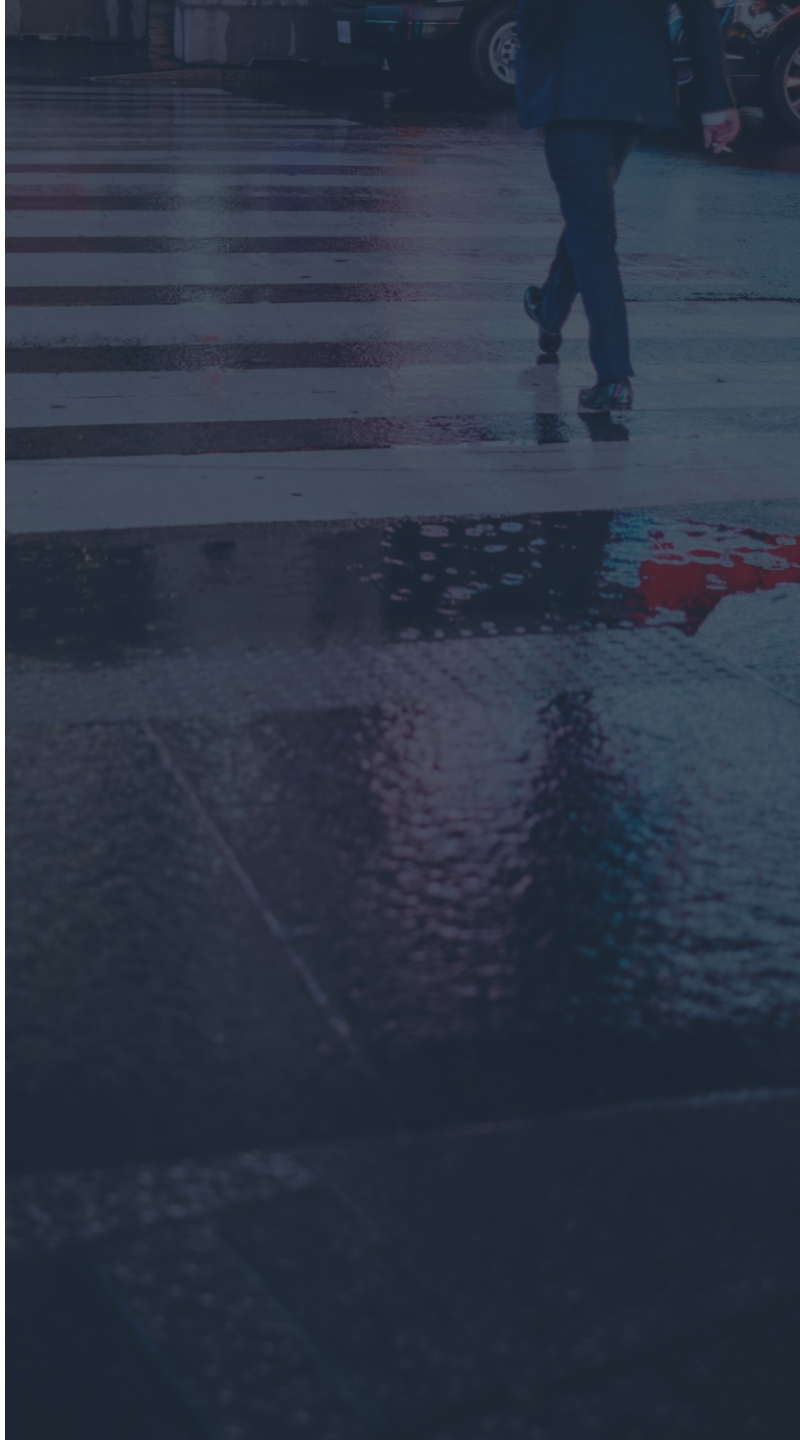
APN Partners are focused on your success, helping customers take full advantage of all the business benefits that AWS has to offer. With their deep knowledge of AWS, APN Partners are uniquely positioned to help you at any stage of your cloud journey, including managing risk. Work with Technology and Consulting Partners who have achieved AWS competencies in Security and Financial Services to protect customer data, support continuity of business-critical operations, and meet new standards in regulatory reporting.

For more information, visit https://aws.amazon.com/solutionspace/financial- services, https://aws.amazon.com/security/partner-solutions, and https://aws.amazon.com/marketplace.

Professional Services

AWS Professional Services provides strategic and technical guidance on security, governance, risk, and compliance to large enterprises that are migrating to AWS via executive support, enhancement of their security framework, and alignment of their risk operating models to cloud technology.

For more information, visit https://aws.amazon.com/professional-services.



aws financial services