aws FOR FINANCIAL SERVICES

Fortify Your Financial Services Institution with Security and Compliance on AWS

Table of contents

Introduction 3

Navigating a shifting landscape 4

Secure in the cloud: Building a culture of security 6

AWS shared responsibility model 7

Embrace AWS best practices 9

- Ensure the highest standards for security, compliance, and privacy 10
- Maintain strong control of your data 11
- Reduce risk through automation 12

The big picture: The power of AWS 13

AWS delivers 15

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

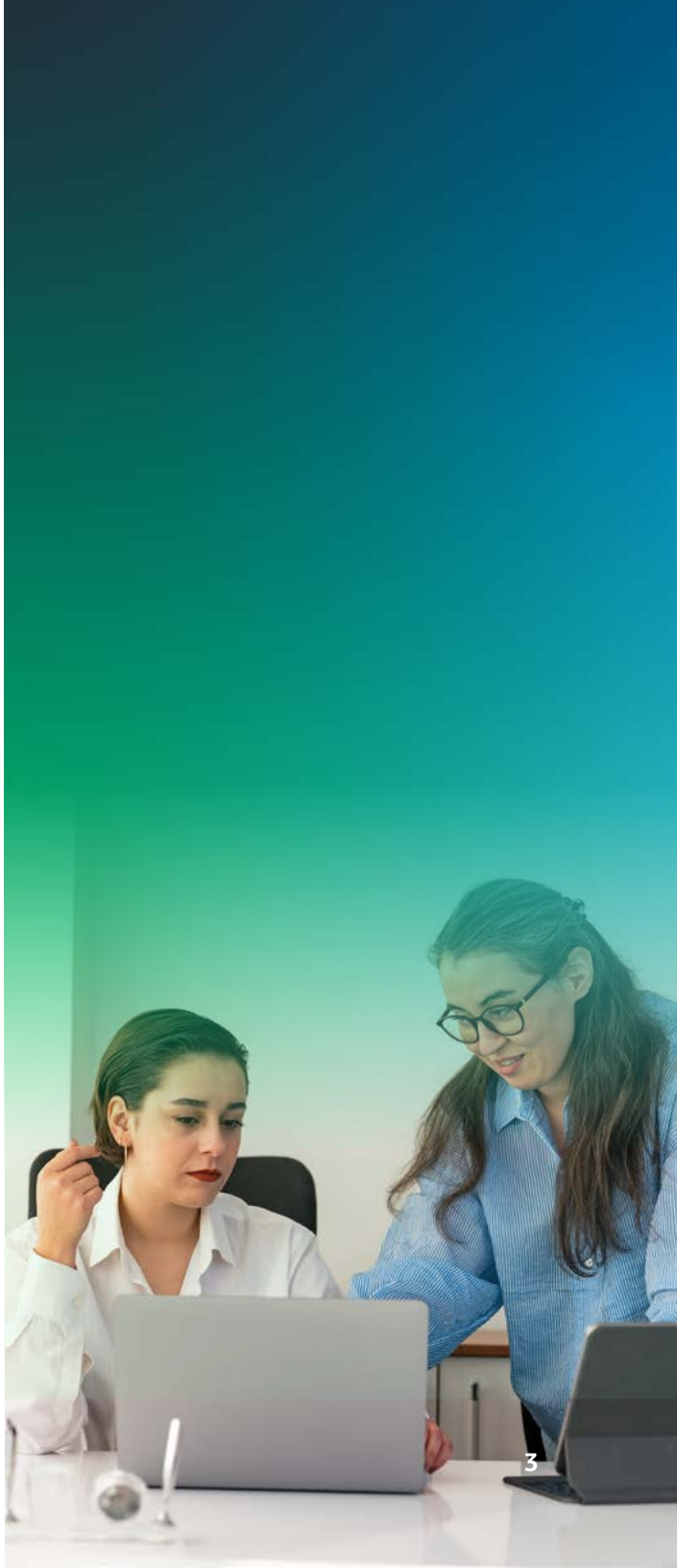
AWS delivers

Introduction

As financial services institutions migrate to and build on the cloud, resilience, security, data privacy, and regulatory compliance continue to be as important as ever.

Cloud technology is continuing to evolve in all types of enterprises. Financial services institutions are increasingly focusing on cloud migration at scale for business-critical applications, including trade lifecycle platforms, core banking and insurance systems, and payment processing software.

Amazon Web Services (AWS) offers financial institutions several advantages when moving their operations to the cloud. First, it enables a continuous approach to security, compliance, and resilience. AWS's core infrastructure is designed to meet the stringent security requirements of highly sensitive organizations, such as the military, global banks, and others. To support the shared responsibility model, AWS provides a wide range of services, tools, resources, best practices, and guidance to help customers implement application-level security measures and ensure compliance. Additionally, AWS specialists can assist financial institutions in setting up a control environment that meets or exceeds the control capabilities of their current legacy environments. AWS partners also offer tools and features to help financial customers achieve their security objectives, including network security, configuration management, access control, and data encryption.



Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

Navigating a shifting landscape

Financial services institutions face a complex landscape of ever-changing regulations and security requirements for data, applications, and infrastructure. The emergence of generative AI is further transforming both the security threat landscape and the requirements and policies needed to defend against those threats. AWS can help them confidently navigate this landscape.

Prime target for cyberattacks

The industry consistently ranks among the sectors most targeted for cyberattacks. There's no shortage of threat vectors, including phishing, ransomware, denial of service (DoS) attacks, and insider threats. And, the threats continue to grow in number and sophistication.

64%

of financial services organizations reported ransomware attacks in 2023, up from 34% in 2021[1]

[1]Source: Sophos

2X

as many cyber incidents in the financial sector in Q3 2023 vs. Q3 2022[2]

[2]Source: Positive Technologies

Fractured and complex regulatory requirements

The regulatory environment surrounding data privacy and cybersecurity is complex and becoming increasingly fractured.

Financial services institutions must navigate rigorous data privacy requirements. The most prominent and far-reaching of these is the European Union's General Data Protection Regulation (GDPR).

In the United States, California, Colorado, Connecticut, Utah, and Virginia have adopted distinct data privacy requirements. More states are set to implement similar legislation, including Oregon, Montana, and Texas. This ever-changing regulatory landscape creates complexity for organizations operating across multiple states.

In addition, governments and regulators around the globe are looking at the role of information and communication technology (ICT) in operational risk for financial services institutions. Notably, the European Union Digital Operational Resilience Act (DORA) broadens the components of operational risk to include ICT.

Generative AI and risk management

Generative AI could fundamentally change financial institutions' risk management by automating, accelerating, and enhancing everything from compliance to climate risk control.[3] At the same time, generative AI is unleashing concern regarding risks, triggering regulatory action such as the EU AI Act and the recent U.S. Executive Order on Artificial Intelligence. As institutions move forward, they will need to consider data privacy, security, and responsible design of the infrastructure and the large language models that utilize their data.

[3]Source: McKinsey and Co.

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

Further, in 2020, the U.S. Federal Reserve released Sound Practices to Strengthen Operational Resilience, which outlines steps for increasing operational resilience drawn from existing regulations, guidance, statements, and industry standards. The practices are grounded in effective governance and risk management techniques, consider third-party risks, and include resilient information systems.

Specifically related to the cloud, the U.S. Department of the Treasury (Treasury) released The Financial Services Sector's Adoption of Cloud Services in February 2023. This report identifies how consumers benefit when financial services institutions use cloud services, including "reduced costs, ability to rapidly deploy new information technology (IT) assets, shorter time to develop new products and services, and enhanced capabilities for security and resilience." It also outlines the Treasury's Strategic Vision for Supporting the Resiliency of the Financial Sector's Use of Cloud Services, including long-term objectives to promote the financial sector's operational resilience with the use of cloud services. This strategic vision will guide the Treasury's engagement in the coming months and years with the private sector, as well as with domestic and foreign counterparts.

Operational resilience in focus

- **Australia** issued market integrity rules intended to promote technological and operational resilience of securities and futures markets operators and participants.
- **Hong Kong** introduced a Supervisory Policy Manual that requires financial services institutions to develop a framework and timeline for achieving operational resilience.
- **Singapore** published guidance on operational risk management and the management of outsourcing and third parties. It also requires banks to benchmark their practices against this guidance.

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

Secure in the cloud: Building a culture of security

Cloud can be a powerful driver in creating a culture of security and streamlining compliance across a financial services institution.

Increasing threats and risk, along with growing operational resilience requirements, will continue driving a shift to the cloud, where security can be built into everything organizations do. We've seen from our customers, partners, and internal builders who work on delivering and maintaining AWS security services, that rapid innovation in cloud security services makes it easier to integrate security into every facet of an organization and drive continuous improvement.

The power of the cloud extends to operational resilience, where CSPs can effectively deliver the geographic diversity and infrastructure redundancies required to ensure business continuity. Building and managing these redundancies on their own would be capital- and resource-intensive for financial services institutions and would divert focus from projects that drive innovation and growth. AWS delivers the most secure, extensive, and reliable Global Cloud Infrastructure. Gartner has recognized our market leadership, naming AWS a Leader in the 2023 Gartner Magic Quadrant for Strategic Cloud Platform Services (SCPS) report. AWS also placed highest in the Ability to Execute axis of measurement among the top 8 vendors.

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

AWS shared responsibility model

Security and compliance are a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. For Amazon EC2, the customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software, and the configuration of the AWS-provided security group firewall. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits deployment. As shown in the diagram on the next page, this differentiation of responsibility is commonly referred to as "Security of the Cloud" versus "Security in the Cloud."

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

AWS responsibility: Security of the Cloud

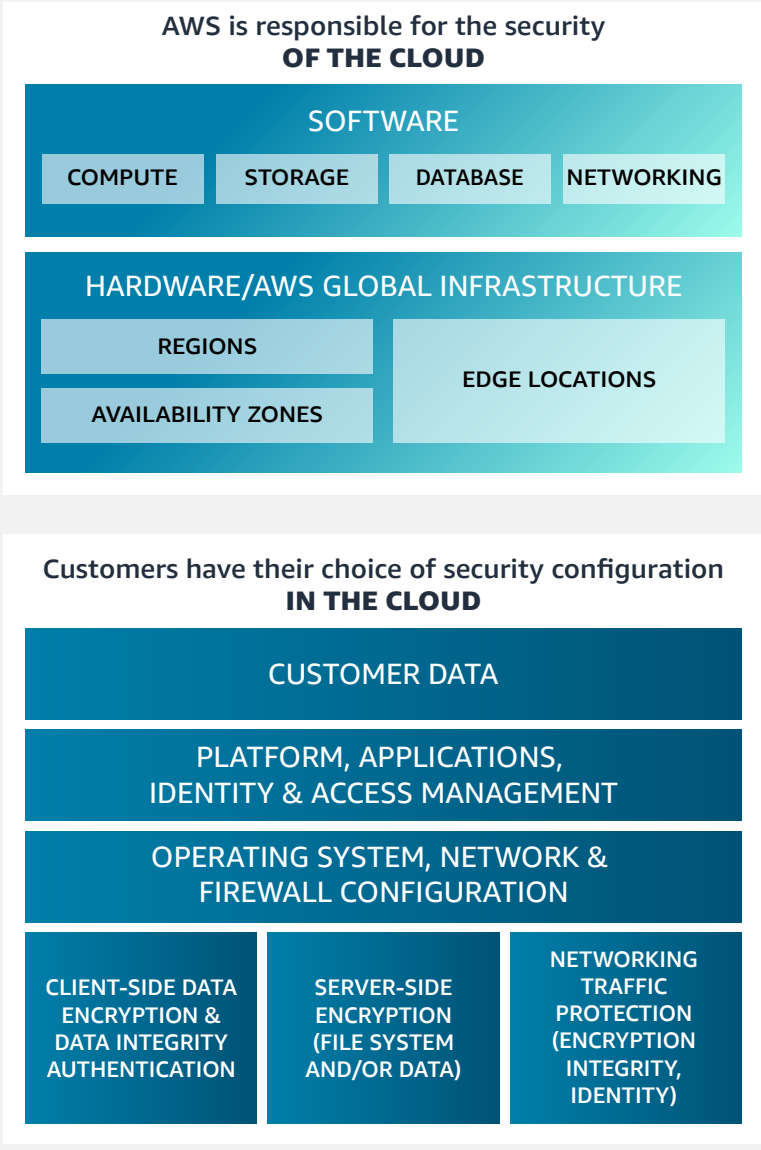
AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility: Security in the Cloud

Customers are responsible for managing their data (including encryption options), classifying their assets, and using identity and access management tools to apply the appropriate permissions.

This shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, the management, operation, and verification of IT controls are also shared. AWS helps customers by managing the controls associated with the physical infrastructure deployed in the AWS environment that may have been previously managed by the customer.

As every customer is deployed differently in AWS, customers can take advantage of shifting the management of certain IT controls to AWS, resulting in a new distributed control environment. Customers can then use AWS control and compliance documentation to perform their control evaluation and verification procedures as required.



Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

Embrace AWS best practices

Not all clouds are equal when it comes to ensuring and advancing security and compliance. Using AWS, financial services institutions gain the control and confidence needed to run their business with the most flexible and secure cloud computing environment available today. They benefit from the resiliency of AWS Regions and Availability Zones and an infrastructure architected to protect their information, identities, applications, and devices. Operating across multiple Availability Zones within a Region is a best practice, and allows customers to achieve very high availability. With AWS, financial services institutions can improve their ability to meet core security and compliance requirements, such as data locality, protection, and confidentiality with comprehensive services and features.

AWS allows financial services institutions to automate manual security tasks, such as detection and remediation, so they can shift their focus to scaling and innovating their business.

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

EMBRACE AWS BEST PRACTICES

Ensure the highest standards for security, compliance, and privacy

AWS is architected to be the most secure cloud environment available today, backed by a set of cloud security tools, with over 300 security, compliance, and governance services and features. This means AWS customers inherit the most comprehensive security and compliance controls available.

AWS supports 143 security standards and compliance certifications, including International Organization for Standardization (ISO), Payment Card Industry Data Security Standard (PCI-DSS), System and Organization Controls (SOC), FedRAMP, GDPR, and more, helping to satisfy compliance requirements for the vast majority of regulatory agencies around the globe.

AWS has the largest footprint of any cloud provider, spanning 105 Availability Zones within 33 geographic Regions (with announced plans for 12 more Availability Zones within four Regions) to support evolving operational resiliency requirements. And, AWS Global Infrastructure delivers the highest network availability of any cloud provider.

S&P Global
Market Intelligence

S&P Global Market Intelligence wanted to efficiently manage one of its flagship applications in the data center to be more agile and offer a better experience to its clients. With its application, IssueBook, customers can issue debt in near real time. In 2020, S&P Global Market Intelligence started migrating its systems onto AWS. Using the AWS Well-Architected Tool, which is designed to review the state of applications and workloads against architectural best practices, the company transformed its infrastructure. Now it delivers six times more releases each year and providing its clients with much higher availability.

Learn more ›

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

EMBRACE AWS BEST PRACTICES

Maintain strong control of your data

Data doesn't do much good if it's difficult to access. With AWS, financial services institutions can build on the most secure global infrastructure, knowing that they own and control access to their data, including the ability to encrypt it, move it, and manage retention. The fine-grained access controls built into AWS provide financial services institutions with the confidence that the right resources have the right level of access to the right data. In addition, AWS infrastructure is designed for customers to retain complete control over where their data is physically located, helping them meet data residency requirements.

JCB is one of the world's seven major credit card brands in Japan and wanted to adapt to changes in the business environment by migrating their on-premises business systems to AWS. Using the AWS Cloud Adoption Framework (CAF), Amazon Aurora, Amazon S3, and Amazon Athena, they have migrated 80 systems to AWS, advancing common infrastructure and data infrastructure to respond to changes in the business environment. They expect a 30% cost savings and improved business agility.

Learn more ›

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

EMBRACE AWS BEST PRACTICES

Reduce risk through automation

Financial services institutions are eager to expand automation of security processes to keep up with business requirements, ever-expanding and evolving threat vectors, and changing regulatory requirements. Automation reduces human configuration errors, enabling financial services institutions to become more secure while shifting resources to more innovation and growth-oriented projects.

AWS enables enterprises to automate security and compliance functions at a scale not possible with on-premises implementations. It's important to understand that end-to-end automation capabilities across the security lifecycle are critical to optimizing impact.

AWS delivers robust automation for numerous manual security tasks. For example, AWS Identity and Access Management Access Analyzer helps to automate away human intervention so enterprises can know more about their compliance posture and permissions levels before deploying changes to their IT infrastructure. AWS services such as Amazon GuardDuty and AWS CloudTrail automate tasks like logging, monitoring, and remediation of malicious activities according to an organization's specific security and compliance needs. AWS Audit Manager automates evidence collection for compliance frameworks rather than having customers rely on point-in-time, manual assessments.

Financial services institutions can also use AWS Systems Manager to automate infrastructure and application security checks in a hybrid environment. This allows them to easily integrate AWS as a seamless and secure extension of their on-premises environment.

bitbank

With distributed denial-of-service (DDoS) attacks on the rise, cryptocurrency exchange Bitbank Inc. (bitbank) changed its response workflow and upgraded its security using AWS. Bitbank created a new process for responding to DDoS attacks with a new process and using services, like AWS Shield. As result, it improved response speed to DDoS attacks, assuring there is no loss of opportunity for customers, and enabling secure service availability and stability.

Learn more ›

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

The big picture: The power of AWS—the world's most trusted cloud

Accelerate innovation confidently—move from idea to action faster

Financial services institutions can go from idea to implementation quickly and confidently with AWS solutions and services. Our deep security capabilities and focus on automation give financial services institutions the resources they need to "build it right" from the beginning and optimize the effort they spend on innovation while also maintaining the highest level of security.

Build operational resiliency

AWS is a valuable partner for financial services institutions as they face requirements to demonstrate operational resilience. We purposefully build to guard against disruptions and incidents and account for them in the design of our services—so when they do occur, their impact on customers and the continuity of services is as minimal as possible. The AWS Region and Availability Zone model has been recognized by Gartner as the recommended approach for running enterprise applications that require high availability.

- AWS infrastructure is geographically dispersed over five continents. It includes 31 geographic Regions, which are composed of 99 AWS Availability Zones that, in turn, include multiple data centers.
- AWS Availability Zones are physically separated and independent from each other and built with highly redundant networking to withstand local disruptions.
- AWS Regions are isolated from each other, and each Region has a dedicated infrastructure stack and services so that a disruption in one Region does not cause disruption in others. Compared with global financial institutions' on-premises environments today, the locational diversity of AWS infrastructure greatly reduces geographic concentration risk.
- AWS employs compartmentalization throughout our infrastructure and services and has multiple constructs that provide different levels of independent, redundant components.
- AWS uses cell-based architecture that contains multiple instantiations of a service—which are isolated from each other. This design minimizes the chance that a disruption in one cell would disrupt other cells.

Scaling cyber event recovery

Financial services institutions are building their cyber event recovery platforms on AWS because it's so easy to build a cyber data vault in minutes rather than the months it takes to build on premises. They can start small and pay only for what they use and then scale with the growth of data. They can also use multiple security services to build a modern cyber event recovery platform.

Learn more ›

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

Streamline and simplify security and compliance

Automation is key to streamlining and simplifying security and compliance, and AWS offers the industry's most extensive solutions to enable automation at scale.

AWS supports customers throughout control implementation

In addition, AI and ML, including generative AI, are playing a significant role in augmenting security engineers' capabilities, helping them to create more secure architectures and applications in the cloud and drive continuous improvement. The automation and intelligence capabilities that these technologies enable will be transformational as financial services institutions work to create a more proactive security stance in the face of an evolving threat landscape.

ekonoo

Innovation in Action

ekonoo SA sought to maintain security and compliance while avoiding the complexity of managing physical devices. Seeking cloud-native tools, ekonoo SA turned to AWS. "AWS provides us with many tools that we can use to implement virtually any kind of security or data protection that we need," says Julien Del Piccolo, DevOps and cloud architect at ekonoo SA. Using fully managed AWS services, financial technology company ekonoo SA achieved regulatory approval for its pension management solution and can focus on delivering value to its customers.

Learn more ›

aws

Introduction

Navigating a shifting landscape

Secure in the cloud

AWS shared responsibilty model

Embrace AWS best practices

Ensure the highest standards

Maintain control of your data

Reduce risk through automation

The power of AWS

AWS delivers

AWS delivers

AWS is architected to be the most secure, scalable, and resilient cloud environment available today. Fortified by the strongest set of cloud security tools, you'll find the technology, resources, and industry expertise you need to confidently embrace and experience the flexibility of the cloud.

Fortify your cloud and apps today