AWS SECURITY

Cloud transformation security best practices for public sector organizations

Table of contents

Notices

This document is provided for informational purposes only. It represents the current product offerings and practices from Amazon Web Services (AWS) as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions, or assurances from AWS, its affiliates, suppliers, or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Introduction

Moving to the cloud means making transformational changes to your organization’s processes, services, cost structure, and scale. It also requires you to modernize your approach to security. Take the opportunity to make the move from self-managed, on-premises security and assurance techniques to a fully managed service architecture that will support and scale with your organization’s new cloud transformation architecture.

Organizations must meet and achieve thousands of third-party global validation compliance requirements. AWS helps support organizations to meet these requirements by sharing the responsibility of security and compliance while helping them scale in the cloud and automate security tasks. Evolving toward automated security also helps reduce human configuration errors and gives teams time to focus on other work critical to your mission.

How this ebook will benefit you

This eBook will appeal to security executives such as chief information security officers (CISOs) and security IT leaders. Discover how AWS protects the infrastructure that runs all of the services offered in the AWS Cloud. Better understand your role and responsibilities for security in the cloud and the security services you use.

““Under normal circumstances, migrating an institution’s entire infrastructure to the cloud could be a long and difficult process taking months or even years, but we couldn’t wait. Luckily, AWS and Ferrilli had all the tools, resources, and expertise we needed to rebuild our infrastructure very rapidly.”[1]

Dr. Chelsy Pham, Vice President of Information Technology Resources, Hartnell College

“We chose AWS because it helps us to meet data protection standards and provides the scalability we need.”[2]

Benjamin Sauer, Head of Backend Engineering, Climedo Health

[1] “**A Silver Lining in the Cloud: Ferrilli Helps Hartnell College Leverage Cyberattack Recovery to Modernize IT Infrastructure with AWS,**” AWS case study, 2023

[2] “**Climedo Health Captures Patient-Centric, Compliant, and Secure Clinical Data Using AWS**,” AWS case study, 2022

Cloud security in AWS

AWS is architected to be the most flexible and secure cloud computing environment available today, giving you the ability to control your environment so that it meets or exceeds the control capabilities of your legacy infrastructure. AWS offers tools and support for compliance, assurance, and monitoring of infrastructure and application changes. It also saves you time by helping you create guardrails to allow innovation and to ensure a security baseline without requiring manual security reviews. All of this helps your security and IT teams focus more on your core business and less on security by automating incident response for anomalies or deviations from your security baseline.

3 benefits of AWS Cloud security

1 Build, run, and scale your applications on infrastructure architected to be the most secure cloud computing environment available today. Benefit from a cloud and network architecture built to meet the requirements of the most security-sensitive organizations, including governments, education institutions, financial services, and healthcare.

2 Move fast and stay secure by confidently integrating and automating security into every part of your organization. AWS provides organization-wide controls that automate infrastructure and application security checks to continually enforce security and compliance controls. Customers can then implement automated reasoning tools to mathematically prove the highest levels of security.

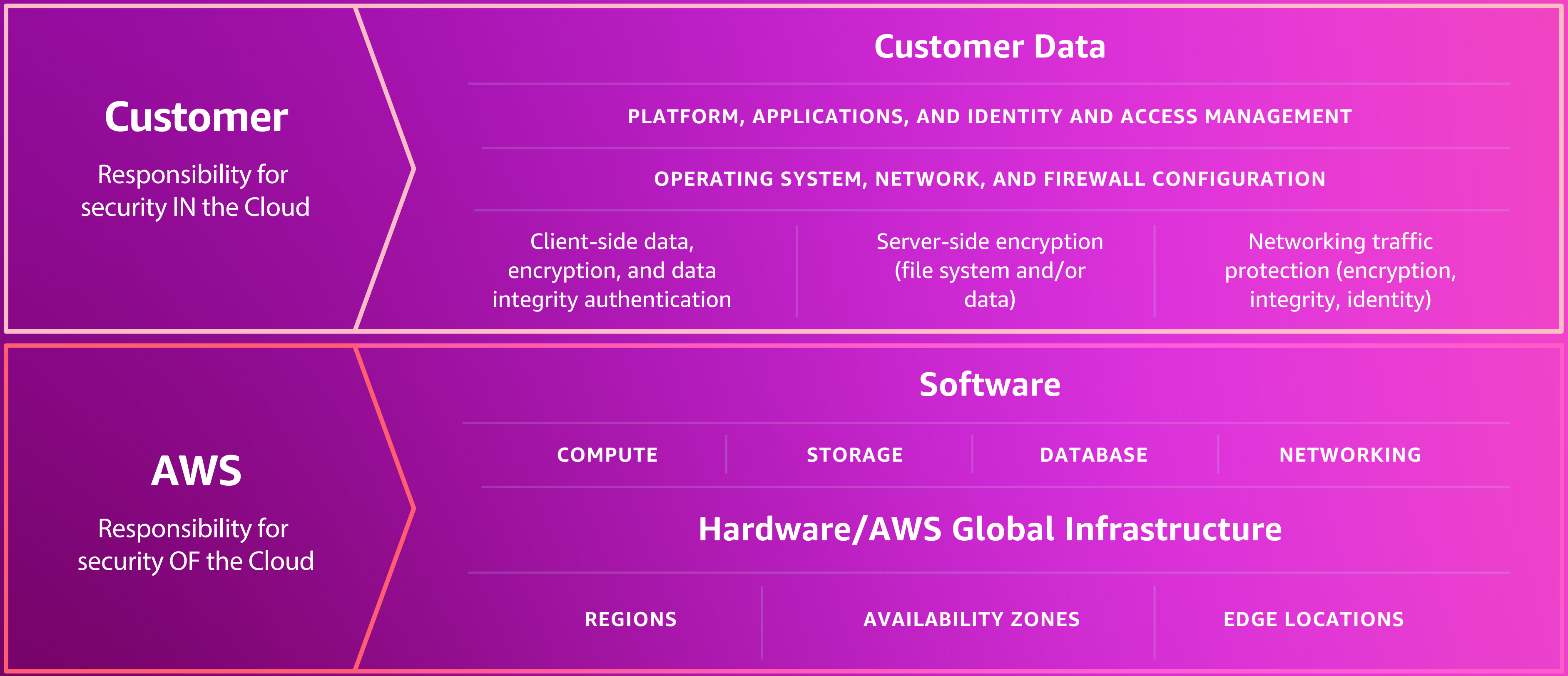
3 Innovate with a wide portfolio of security services and partner solutions to help achieve end-to-end security for your organization. AWS security services and solutions help customers implement every step of their organization's optimal security posture, from identifying risks to remediation. Customers can extend the benefits of AWS by using security technology and consulting services from AWS Professional Services and the AWS Partner Network.

THE HIGHEST STANDARDS

The AWS team is monitoring systems continuously, 24/7, to help ensure your content is constantly protected.

Cloud security—a shared responsibility

When you move your IT infrastructure to AWS, you adopt the model of shared responsibility. This shared model provides multiple benefits, including reducing your operational burden as AWS operates, manages, and controls the layers of IT components—from the host operating system and virtualization layer to the physical security of the facilities in which the services operate. Just as you share the responsibility for operating the IT environment with us, you also share the management, operation, and verification of IT controls.



Customer

Responsibility for security IN the Cloud

Customer Data

PLATFORM, APPLICATIONS, AND 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

AWS—security of the cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in AWS. AWS infrastructure is composed of hardware, software, networking, and facilities that run AWS services. From the host operating system to the physical security of the facilities, it reduces the operational burden for organizations. Gain peace of mind knowing your information, identities, applications, and devices are protected.

AWS security assurance

As the leading cloud provider, AWS has comprehensive compliance controls with established, widely recognized **frameworks and programs**. These controls help satisfy compliance requirements for regulatory agencies around the world, which you'll inherit automatically. Not only do they dramatically lower the costs of your security assurance efforts, but they also strengthen your own compliance and certification programs.

Third-party independent assessments validate the effectiveness and efficient operations of the ubiquitous AWS IT control environment and facilities across the globe. These include policies, processes, and control activities that use various aspects of the overall AWS control environment.

Privacy

Privacy is largely about having control of who can access data. With AWS, you know who is accessing your content and what resources your organization is consuming at any given moment. Provide the right level of access to your resources at all times. Use fine-grained identity and access controls and continuous monitoring for near real-time security information—regardless of where your information is stored.

Reduce risk and enable growth by using our activity monitoring services that detect configuration changes and security events across your system. Integrate our services with your existing solutions to help simplify your operations and compliance reporting. AWS gives you control that can help you comply with the regional and local data privacy laws and regulations applicable to your organization.

COMPLIANCE CONTROLS

AWS supports 143 security and compliance certifications, including:

- SOC
- PCI
- ISMAP
- FedRAMP
- DoD CC SRG
- HIPAA BAA
- IRAP
- MTCS
- C5
- K-ISMS
- ENS High
- OSPAR
- HITRUST CSF
- FINMA
- GSMA
- PiTuKri

Data residency

AWS data centers are built in clusters in various locations around the world and are known as AWS Regions. You choose the AWS Regions in which your content is stored. Deploy AWS services in the locations of your choice in accordance with your specific geographic requirements and to help you meet your compliance and data residency requirements. For example, if you are an AWS customer in Australia who wants to store your data only in Australia, you can choose to deploy AWS services exclusively in the Asia Pacific (Sydney) AWS Region. Discover other flexible storage options **around the world**.

Organization continuity

AWS infrastructure has a high level of availability and delivers the features you need to deploy a resilient IT architecture. Our systems are designed to tolerate system or hardware failures with minimal user impact.

Disaster recovery

Remain resilient in the face of most failure modes, including natural disasters or system failures by distributing applications across multiple AWS Availability Zones. **AWS Elastic Disaster Recovery** minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery.

> ***"As a collective, we were not only committed to solving for a solution that would improve our standard environments, but accounted for, planned, and tested a complete disaster recovery environment."***[3]
>
> Paula Mattingly, chief information officer (CIO), AZDHS

[3] "**Migrating and modernizing state WIC applications with AWS**," AWS case study, 2023

Organizations—security in the cloud

While AWS does the heavy lifting for security of the cloud, organizations are responsible for security in the cloud, including managing the guest operating system and associated application software.

How to securely manage your AWS resources

Your responsibilities will vary depending on the services you use, the integration of those services with your IT environment, and applicable laws and regulations. You should take all of this into consideration when you choose AWS services. AWS offers different levels of support to help you raise the security posture of your environment to meet the security and compliance requirements of your company. Tools and services available include documented best practices, professional services, and solutions that automate security and compliance posture checks.

Benefits of AWS security and identity services

To help establish security in the cloud, AWS offers a broad selection of innovative security services to meet your own security and regulatory requirements.

Identity services

Identity management, access controls, and governance are foundational security pillars for organizations of any size and type. With AWS, your security and IT teams can adopt modern cloud-centric identity solutions and zero trust architectures to securely support a hybrid workforce, improve access experiences, manage permissions, and help meet stringent compliance mandates.

Data protection and privacy

AWS provides **technical, operational, and contractual measures** needed to protect your data. With AWS, you manage the privacy controls of your data, control how your data is used, who has access to it, and how it is encrypted. We underpin these capabilities with the most flexible and secure cloud computing environment available today.

Network protection

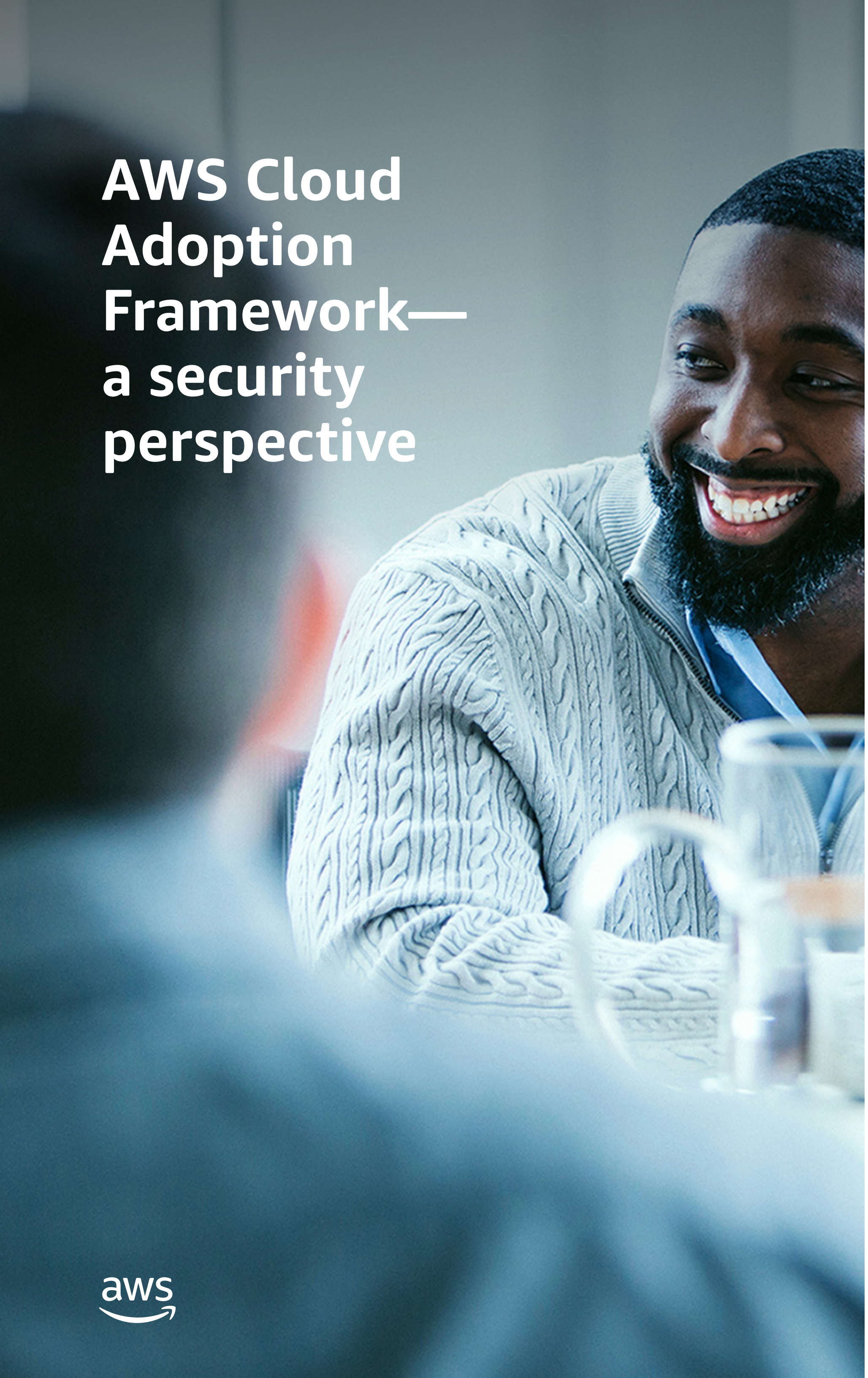
Network and application protection services on AWS enable you to enforce fine-grained security policies at every network control point across your organization. AWS network and application protection services then provide equally flexible solutions that inspect and filter traffic to prevent unauthorized resource access.

Detection and response

AWS detection and response services work together to help you enhance your security posture and streamline security operations across your entire AWS environment by continuously identifying and prioritizing security risks, while integrating security practices earlier in the development lifecycle.

Compliance

Compliance and data privacy with AWS give you a comprehensive view of your compliance status and continuously monitor your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows.



AWS Cloud Adoption Framework—a security perspective

A successful and secure cloud adoption journey starts with using AWS experience and best practices in the **AWS Cloud Adoption Framework (AWS CAF)**. From a security perspective, the framework provides best practices for building enhanced security capabilities and resilient workloads. The following nine capabilities can help you identify and prioritize security readiness and achieve the confidentiality, integrity, and availability that your data and workloads require. Common stakeholders include CISOs, chief commercial officers (CCOs), internal audit leaders, and security architects and engineers.

9 capabilities of the AWS Cloud Adoption Framework

1. Security governance
2. Security assurance
3. Identity and access management
4. Threat detection and monitoring
5. Vulnerability management
6. Infrastructure protection
7. Data protection
8. Application security
9. Incident response

9 capabilities of the AWS Cloud Adoption Framework—a security perspective *(continued)*

1 Security governance

An effective security program requires defining, developing, maintaining, and communicating certain items, including security roles, responsibilities, accountabilities, policies, processes, and procedures. A clear line of accountability ensures a more effective security program.

2 Security assurance

To improve the effectiveness of your security programs, continuous monitoring, evaluating, and managing are critical. Building trust and confidence around the controls you've implemented will enable you to meet regulatory requirements effectively.

3 Identity and access management

Ensuring the right people have access to the right resources under the right conditions is critical as you run more workloads and continue to scale on AWS. Identity and access management plays a central role when it comes to operating secure AWS workloads. Both human and machine identities need to be authenticated and authorized. Permissions management allows for broad and granular access controls with capabilities of least privilege.

4 Threat detection and monitoring

Threat detection is necessary to continuously monitor your environment to identify normal and legitimate behaviors of the assets and resources in use. Using techniques such as machine learning, anomaly detection, automated best practice checks, and intelligent vulnerability management of potential misconfiguration, misbehavior, or unauthorized usage, can be quickly determined and communicated to reduce the time to remediate.

5 Vulnerability management

You can have a broad range and a dynamic set of software and software versions across your server and container workloads. New software vulnerabilities are regularly announced—vulnerability management is critical to automate identifying and prioritizing potential exposures quickly to enable remediation to occur.

6 Infrastructure protection

Control methodologies are critical for successful ongoing operations in the cloud and to meet best practices and regulatory obligations. A key part of an information security program is infrastructure protection to ensure systems and services within your workload are protected against unintended and unauthorized access and potential vulnerabilities.

7 Data protection

Foundational practices that influence security should always be in place before architecting any workload. This is critical to supporting objectives such as preventing mishandling or complying with regulatory obligations. All data should be encrypted at rest and in transit, and sensitive data should be stored in separate accounts to reduce risk and vulnerabilities.

8 Application security

Keep security top of mind to save on time, effort, and costs when a security flaw is identified during the software development process. Putting policies in place for security at the development stage of your application provides peace of mind that security gaps are minimized.

9 Incident response

Preparation is key for your organization to respond to and mitigate the potential impact of security incidents. Minimizing organizational disruption and enabling your team to operate effectively during an incident—isolating, containing, and performing forensics on issues—requires putting the right tools and access in place ahead of a security incident.

Creating your AWS migration strategy

Whether you are creating and planning for a successful and secure cloud adoption journey or reworking your existing workloads on AWS, there are several industry-accepted standards and frameworks to help you build a strong security foundation.

When it comes to building your IT governance and security management systems, the AWS Cloud Adoption Framework helps you plan for a successful and secure cloud migration. The AWS Well-Architected Framework assists with building secure infrastructure while automated checks for AWS security best practices allow you to continuously evaluate AWS accounts from a security perspective.

AWS Well-Architected Framework

When it comes to building secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads, the **AWS Well-Architected Framework** is the go-to source to help cloud architects focus on the workload level. The security pillar of the framework is built around five components:

- Identity and access management
- Detection
- Infrastructure protection
- Data protection
- Incident response

The AWS Well-Architected Framework provides guidance for secure implementation and approaches for selecting the right AWS services, and it helps to implement these core security practices in your workloads.

Automated checks for AWS security best practices: AWS Security Hub

It is essential to detect when your deployed accounts and resources are deviating from security best practices to maintain your organization’s security posture. **AWS Foundational Security Best Practices standard** utilizes a set of controls to allow you to continuously evaluate all your AWS accounts and workloads, providing actionable and prescriptive guidance to continuously improve your cloud security.

Learn more

Get started securing your workloads in the cloud

Discover more about securing your move to the cloud with security, identity, and compliance on AWS.

Learn more ›

Access security content

Learn more about AWS offerings in security and customer-related content in the AWS Security Hub.
Find useful webinars, whitepapers, quick reference guides, and eBooks on various security topics.

Learn more ›