AWS SECURITY

Cloud transformation security best practices for government

Table of contents

Introduction

With over 7,500 government agencies using AWS, we understand the requirements agencies have to balance economy and agility with security, compliance, and reliability. In every instance, we have been among the first to solve government compliance challenges facing cloud computing and have consistently helped our customers navigate procurement and policy issues related to adoption of cloud computing.

Moving to the cloud means making transformational changes to your processes, services, cost structure, and scale. It also requires you to modernize your approach to security. 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 new transformation architecture.

Organizations must meet and achieve thousands of third-party global validation compliance requirements. AWS helps support 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 organization.

How this eBook will benefit you

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.

"We deployed our first ever national security system, or Impact Level 5, to AWS GovCloud (US). We are working on automatic builds and deployment. But the real impact is that when we are done, we are going to take something that took three weeks down to 15 minutes."

Chris Lynch, Director at the Department of Defense's United States Digital Service (USDS)

"By relying on AWS, we can implement levels of authentication and security that are appropriate to the data."

Matt Lewis, Chief Architect, UK Driver and Vehicle Licensing Agency

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 operations and less on security by automating incident response for anomalies or deviations from your security baseline.

Five benefits of AWS cloud security

1. **Superior visibility and control of your data** give you critical insight into who is accessing your data and from where. AWS tools help you know where your data is stored and who can access it, as well as keep you informed on what resources your organization is consuming at any given moment. Reduce risk as you scale by using security automation and activity monitoring services to detect any suspicious activity across your ecosystem. Integrate AWS services with your existing solutions to streamline operations.

2. Automating security tasks with AWS not only increases security by reducing human configuration errors but also gives time to your security team to work closely with developers and operations teams to create and **deploy code faster and more securely**.

3. When you **build with the highest standards** for privacy and data security, you have access to world-class AWS security experts. The team is monitoring systems continuously, 24/7, to ensure your content is constantly protected.

4. AWS has the largest and most dynamic community, with tens of thousands of partners globally. **The AWS Partner Network (APN)** includes thousands of systems integrators that specialize in AWS services and tens of thousands of independent software vendors (ISVs) who adapt their technology to work on AWS. Access our trusted security partners and solutions that secure every stage of cloud adoption, from initial migration through ongoing day-to-day management.

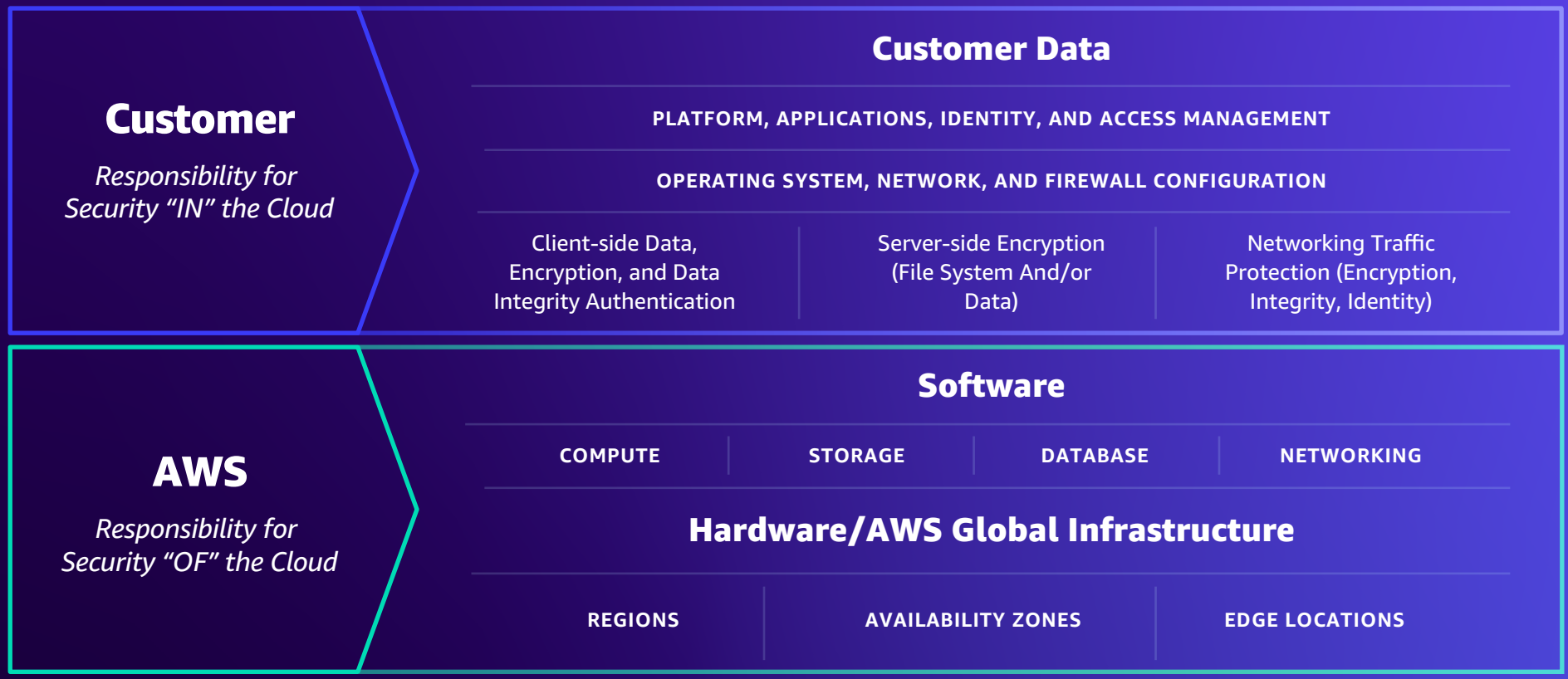
5. Inherit the **most comprehensive compliance controls** with AWS. AWS provides commercial cloud capability across all classification levels: Unclassified, Sensitive, Secret, and Top Secret. This empowers AWS Customers to complete missions with a common set of tools, a constant flow of the latest technology, and the flexibility to rapidly scale with the mission, supporting 143 security standards and compliance certifications, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, NIST 800-53, and more. ***Learn more*** about how AWS is earning data privacy trust through transparency.

THE HIGHEST STANDARDS

Designing the most secure, highest-performing, resilient, and efficient cloud infrastructures, world-class security experts at AWS build and maintain a broad selection of innovative security services, simplifying your own security and regulatory processes.

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.



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 the most 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 leverage 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. Leverage fine-grain 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

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

Visit *AWS Compliance* to learn more about AWS compliance offerings and why we serve government customers best.

AWS GovCloud (US) gives government customers and their partners the flexibility to architect secure cloud solutions that comply with the most stringent requirements. *Learn More*

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 customer 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 that 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 **here**.

Business 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 customer 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 provides fast, reliable recovery of physical, virtual, and cloud-based servers in AWS, minimizing downtime and data loss.

"In recent years, we solved a bunch of problems for disaster recovery by starting to use AWS because it's very important to have geographic diversity with disaster recovery."

Jonathan Feldman, CIO, City of Asheville, North Carolina

3 "TNEX Launches Vietnam's First Digital Bank in Nine Months on AWS, AWS Case Study," 2021

Customers—security in the cloud

While AWS does the heavy lifting for security of the cloud, customers 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

AWS Identity Services enable you to securely manage identities, resources, and permissions at scale. With AWS, you have identity services for your workforce and customer-facing applications to get started quickly and manage access to your workloads and applications.

Data Protection

AWS provides services that help you protect your data, accounts, and workloads from unauthorized access. **AWS Data Protection Services** provide encryption, key management, and threat detection that continuously monitor and protect your accounts and workloads.

Network Protection

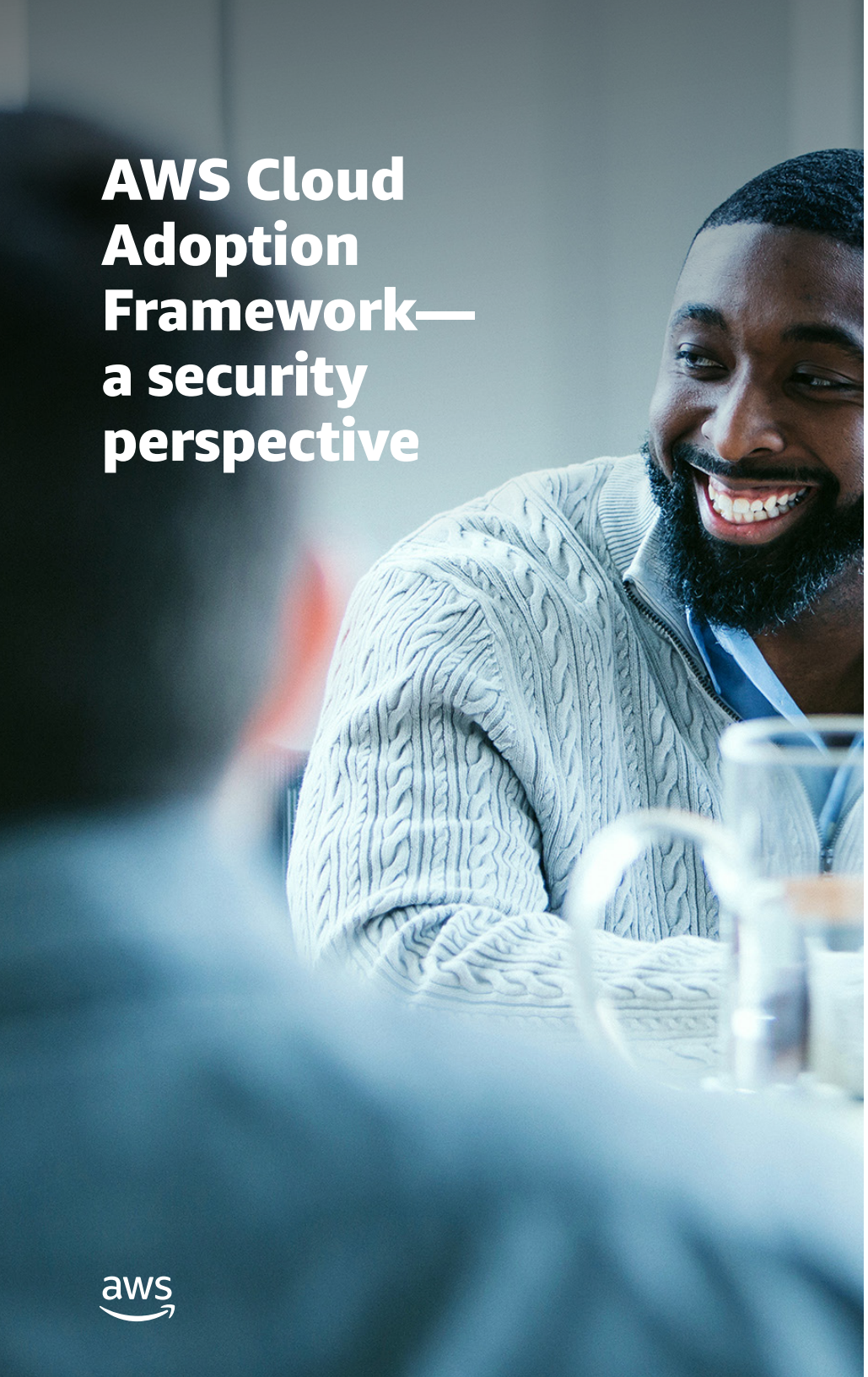
Network and Application Protection Services on AWS enable you to enforce fine-grained security policies at network control points across your organization. AWS services help you inspect and filter traffic to prevent unauthorized resource access at host-, network-, and application-level boundaries.

Threat Detection

Continuous Monitoring and Threat Detection on AWS identifies threats by continuously monitoring the network activity and account behavior within your cloud environment.

Data Privacy

Compliance and Data Privacy with AWS gives you a comprehensive view of your compliance status and continuously monitors 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)**. This framework provides best practices for building enhanced security capabilities and resilient workload, and the following nine capabilities can help you identify and prioritize security readiness and achieve the confidentiality, integrity, and availability of your data and workloads. Common stakeholders include CISO, CCO, internal audit leaders, and security architects and engineers.

Nine 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

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 in rest and in transit, and sensitive data should be stored in separate accounts reducing 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 business 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 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.

Conclusion

How to get started

AWS security solutions and services can help you transform how you operate and free up your time to focus on your core mission—all while making your organization more secure.

How to secure 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 ›

How to buy AWS

Buying cloud computing services takes different skills and strategies than buying traditional IT. Are you ready to move to the cloud but looking for practical guidance? Our experts at AWS have helped many government IT leaders select the right acquisition approach for their agencies.

Learn more ›