The Utility Executive's Guide to Cloud Security

aws power and utilities

CONTENTS

The AWS cloud is trusted by some of the world's most security sensitive and highly regulated Power & Utility organizations. **Here's why.**

Empowering the digital utility

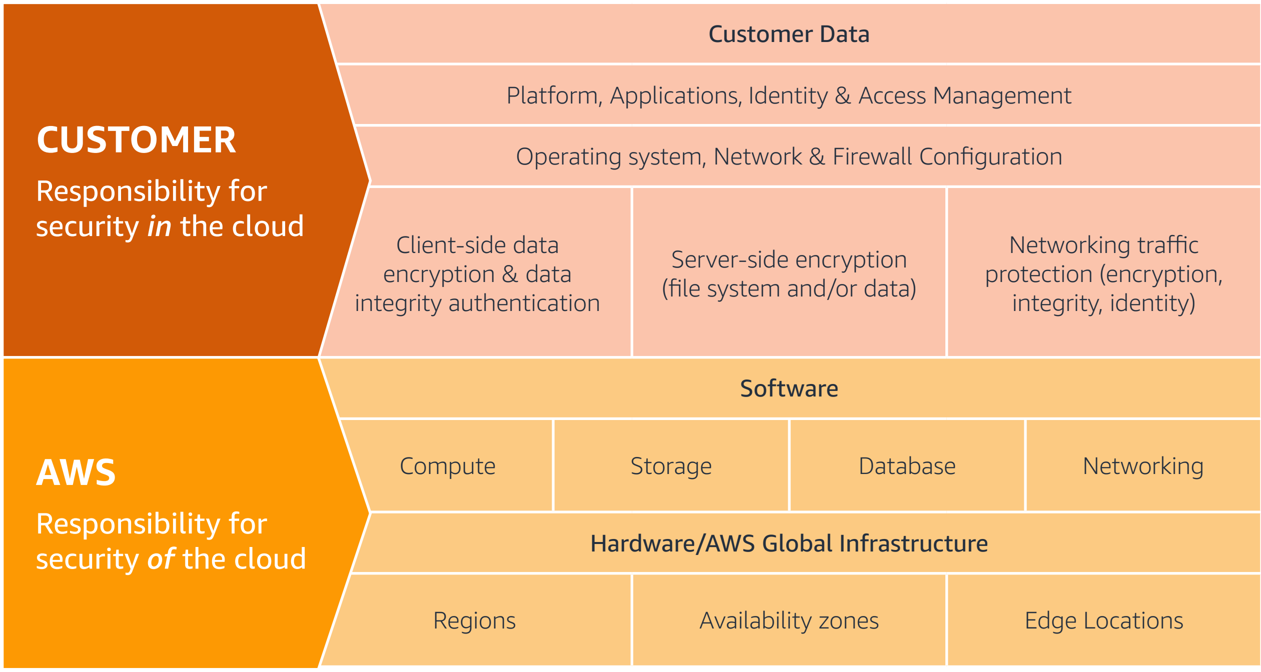
The Power & Utility industry is one of the most regulated industries in the world. Yet in order to deliver reliable service and respond to emerging customer needs, Power & Utility companies need to push the boundaries of innovation while continuing to deliver on their security requirements.

AWS understands the reliability, security, and compliance obligations utilities face and has worked with the industry's most complex organizations to meet their requirements at every stage of their cloud journeys.

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. You retain control of your security protocols, and in support, AWS provides access to guidance materials and industry-leading security teams to maintain your specific security assurance requirements.

AWS Shared Responsibility Model



CUSTOMER

Responsibility for security *in* the cloud

Customer Data

Platform, Applications, Identity & Access Management

Operating system, Network & Firewall Configuration

Client-side data encryption & 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

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, PCI, SOC, FedRAMP and other certifications. AWS Power & Utility security experts can also help you create a scalable, secure approach specially designed to meet your business objectives and 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 security standards. AWS also communicates security best practices and policies that customers can incorporate into their compliance frameworks. Customers can gain access to tools and documentation to learn about how AWS aligns to industry regulations such as NERC CIP. The AWS well architected framework also provides system configuration guidance.

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 76 Availability Zones in 24 geographic Regions*, 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.

All customers, regardless of size, benefit from AWS's ongoing investment in our secure infrastructure and new security offerings, such as **AWS Security Hub**, which enables you to centrally view and manage security alerts and automate compliance checks.

*As of July 2020

Reduce risk through automation and managed security services

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 availability, confidentiality, and 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.

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.

AWS in Power & Utilities

xylem
Let's Solve Water

Xylem (XYL) is a leading global water technology company committed to solving critical water and infrastructure challenges with technological innovation. Xylem's more than 16,000 diverse employees delivered revenue of $5.25 billion in 2019. Xylem is creating a more sustainable world by enabling its customers to optimize water and resource management, and helping communities in more than 150 countries become water-secure. Hear Xylem's AWS security story

ENGIE

ENGIE is a global energy company with 160,000 employees serving customers in nearly 70 countries. ENGIE's purpose is to accelerate the transition towards a carbon-neutral economy through reduced energy consumption and more environmentally-friendly solutions. With AWS ENGIE has accelerated development and solution roll out processes. Running SAP HANA on AWS, ENGIE has increased data transparency for internal business organizations with continuous financial reporting. AWS supports ENGIE's goal to rapidly and securely innovate at scale on a global basis.

Hear ENGIE's AWS Security Story

> "There are so many audit requirements and governance rules — General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and more — AWS checks the box for us so all we have to do is bring an additional layer of security on top of that."

Grant Muller, Vice President of software at Xylem

> "Using the cloud is vital for making new applications available and deploying them internationally; this is why we have chosen Amazon Web Services. AWS is the unrivaled leader in its field."

Gérard Guinamand,
ENGIE Group Chief Data Officer

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.

The same world-class security experts who monitor our core infrastructure also build and maintain our broad selection of innovative security services, which can help you simplify meeting your own security and regulatory requirements.

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 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.

Detection

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 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

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, and 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 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

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 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 operating systems.

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 Cloud HSM

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

AWS Secrets Manager

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

AWS VPN

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

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.

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 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 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 Artifact

No cost, self-service portal for on-demand access to AWS' compliance reports to help you deliver on your compliance obligations.

AWS IoT Device Defender

A fully managed service that helps you secure your fleet of IoT devices. AWS IoT Device Defender continuously audits your IoT configurations to make sure that they aren't deviating from security best practices.

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://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.

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.

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/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 power and utilities