eBook

Security, Compliance, & the Cloud

How to enhance your cloud visibility and protection strategy

aws

Table of Contents

Introduction 3

Cloud Adoption Drivers 4

- Adoption Goals & Drivers 5

Security Use Cases 8

- Security & Compliance 9
- Security Information and Event Management (SIEM) 11
- Cloud Workload Protection for Storage 12

Tap Into the Extensive APN Partner Network 13

- Dome9 15
- Splunk 17
- Symantec 19

Next Steps 21

Introduction

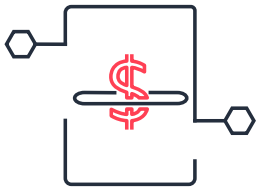
Earning and keeping your customer's trust is one key to long-term success. In today's digital world, your customers expect product and service innovations at an increasingly rapid pace. At the same time, customer privacy and data security are under close scrutiny.

These trends help to explain why organizations are migrating to Amazon Web Services (AWS): to benefit from the agility, scalability, and security that it offers.

AWS has always put cloud security first. This security-centric approach not only helps you more effectively protect your data on AWS, but can also help you meet security and compliance standards.

Cloud Adoption Drivers

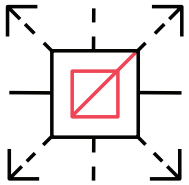
Adoption Goals & Drivers



Cost-Efficiency

Cost-efficiency is perhaps the most well-known driver of cloud adoption. Organizations flock to the cloud to reduce hardware setup, maintenance, and upgrade costs.

When you experience spikes in demand for compute power, you can avoid the costs of provisioning new on-premises services. Instead, you can quickly spin up more compute instances and get back to meeting business goals. When you no longer need them, you decommission them, paying only for what you used.



Flexibility & Agility

Architecting your environment on the cloud enables you to build agility in from the start.

Integrating new services, automating routine processes, collaborating more efficiently, and other maintenance is made easier with the numerous tools and offerings in AWS Marketplace that are designed to work seamlessly together.

Automating manual processes can be especially useful for your organization's security posture, by minimizing the chance of human error.

Freedom to Innovate

Technology is constantly evolving and the cloud is poised to evolve right along with it. Artificial intelligence (AI), machine learning (ML), the Internet of Things (IoT), containerization, advanced identity-based security solutions... These are areas where cloud technology is leading the pack. You have access to numerous AWS and AWS Partner Network (APN) Partner services that can help you streamline the implementation of these and other emerging technologies.

Figure 1: Journey to the Cloud

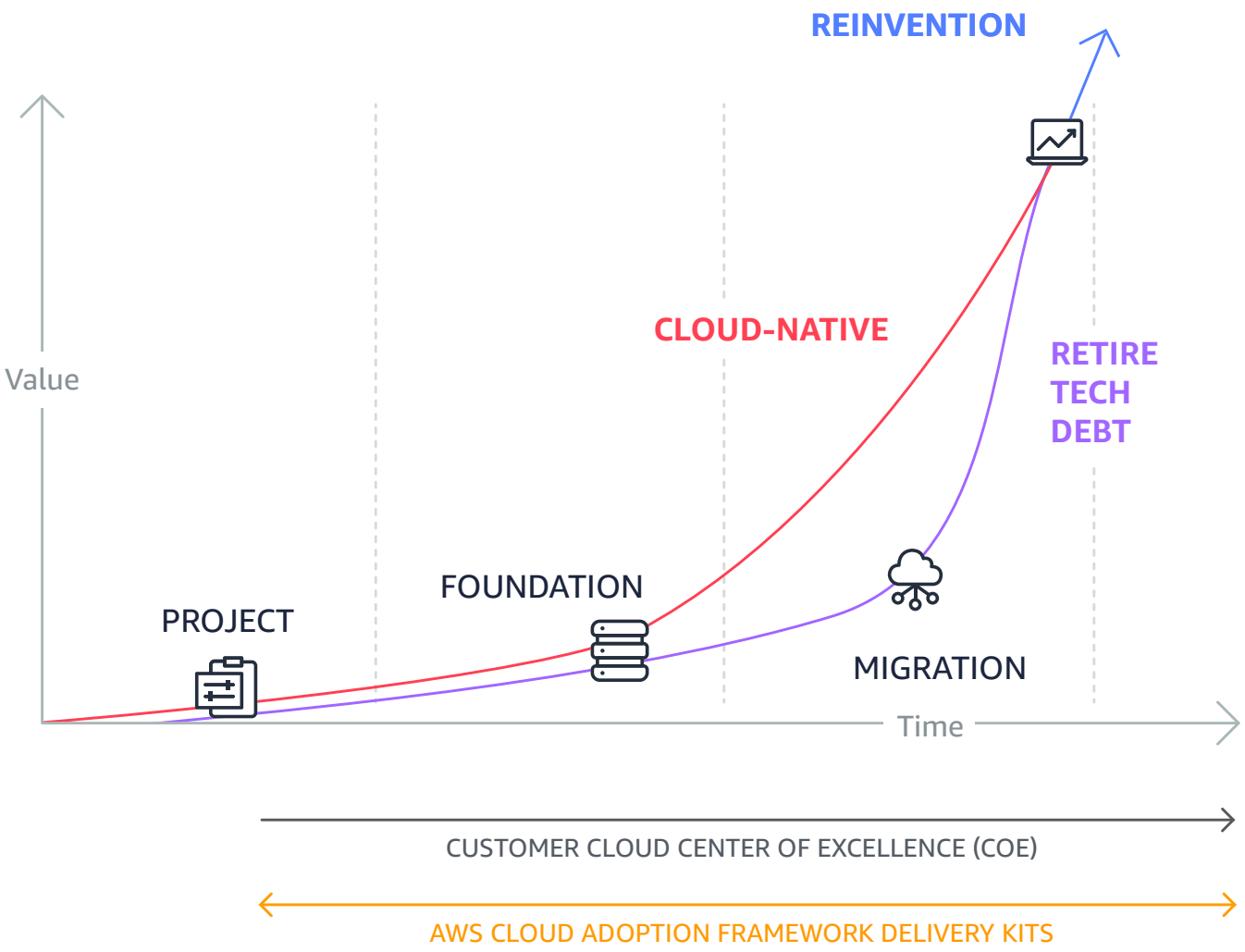
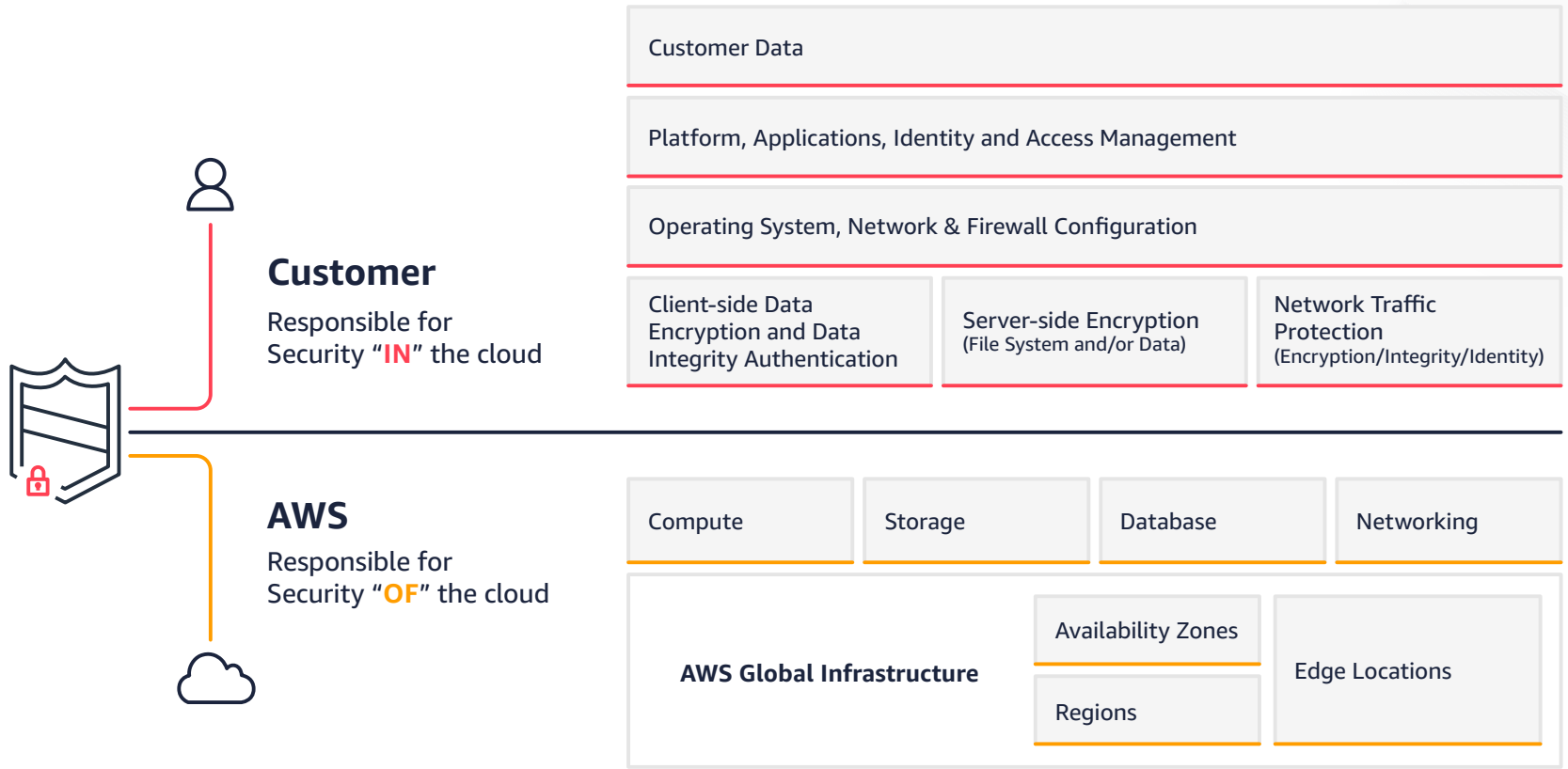


Figure 2: Security & Compliance is a Shared Responsibility



Security Use Cases

Security & Compliance

Depending on the type of data you are storing on AWS, you may be subject to organizational, industry, or government compliance standards. These standards will inform the way you create your cloud security posture, at every level.

AWS is committed to offering services and resources to enable organizations to protect their sensitive data and adhere to compliance standards, including the recently imposed General Data Protection Regulation (GDPR).

Compliance Enablers

Amazon Inspector

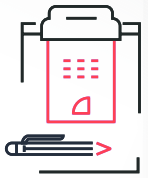
Amazon Inspector is an automated security assessment service, designed to improve the security and compliance of your applications deployed on AWS. Amazon Inspector provides you with a detailed list of security findings prioritized by level of severity.

Amazon Macie

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data on AWS. This fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks.

Amazon GuardDuty

Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior. When a potential threat is detected, Amazon GuardDuty sends a detailed security alert to your GuardDuty console.



AWS Artifact

AWS Artifact provides you with on-demand access to AWS compliance reports and audits.

Security Information and Event Management (SIEM)

The best security posture is the one that can prevent incidents from occurring in the first place, but is also poised and ready to react and mitigate risks at a moment's notice.

SIEM serves two purposes:

- Unifying security logs and security reports into a single view
- Detecting, investigating, and remediating security events.

There are numerous AWS services designed to aid you in securing your environment. These services include Amazon GuardDuty, AWS CloudTrail, VPC Flow Logs, Amazon CloudWatch Logs, and AWS Config. These services, among others, can come together to form a well-rounded SIEM strategy to deliver deep visibility into AWS.

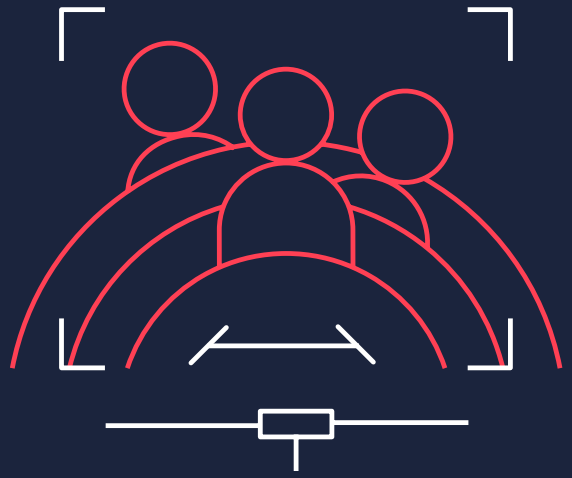
There's an emerging trend of organizations leveraging SIEM-as-a-service solutions which are ideal for organizations trying to reduce implementation time, scale more efficiently, and simplify the process of collecting and analyzing event logs.

Cloud Workload Protection for Storage

Storage makes up an essential piece of your operating environment on the cloud, storing the data you use to run your applications.

Some of the most common AWS storage services include:

- Amazon Simple Storage Service **(Amazon S3)** – Amazon S3 is object storage built to store and retrieve any amount of data from anywhere, designed to deliver 99.999999999% durability.
- Amazon Elastic Block Store **(Amazon EBS)** – Amazon EBS provides persistent block storage volumes for use with Amazon Elastic Compute Cloud (Amazon EC2) instances.
- Amazon Elastic File System **(Amazon EFS)** – Amazon EFS is a regional storage service designed for high availability and durability, that delivers scalable, reliable, and elastic file storage on AWS.



Tap Into the Extensive APN Partner Network

Tap Into the Extensive APN Partner Network

The AWS Partner Network includes tens of thousands of Consulting Partners and Technology Partners, and membership has grown more than 50% over the past 12 months.

APN Security Partners have shown proficiency in developing, implementing, and managing security solutions. These solutions, when combined with each other and with various AWS security services and resources, can form an end-to-end cloud security posture as powerful and agile as your cloud environment, itself.

Independent Software Vendor's (ISV's) security and compliance tools also help accelerate the process and implementation time. AWS Marketplace offers 35 solution categories and more than 4,200 software listings from over 1,400 ISVs.

APN Partner solutions: Dome9

Comprehensive Security and Compliance Platform

Dome9 Arc is an innovative software-as-a-service platform that delivers visibility across your security and compliance posture.

Use Cases

- Network security
- Advanced IAM protection
- Compliance management

Dome9 enables you to:

- Actively assess your security and compliance posture against business and regulatory requirements
- Gain comprehensive visibility across your AWS environments from a single pane of glass
- Customize and extend security and compliance policies across your AWS environments
- Automatically remediate misconfigurations

Customer Success Story: Centrify

Centrify, a cyber security company, combines Identity-as-a-Service (IDaaS), Privileged Access Management (PAM), and Enterprise Mobility Management (EMM).

Deciding to move their Software-as-a-Service (SaaS) applications to AWS, Centrify went through a Well-Architected Security Review with AWS to learn how to optimize the security in their SaaS environment.

After careful review of several companies, they chose Dome9 as the best candidate to help them efficiently monitor and control their security and compliance posture.

Dome9 worked with Centrify to streamline compliance adherence, simplify cloud inventory management, and increase network visibility.

APN Partner solutions: Splunk

splunk>

Intelligent Threat Detection and Edge Protection on the Cloud

The Amazon GuardDuty Add-on for Splunk helps you more quickly monitor, detect, investigate, and resolve advanced security threats.

Use Cases

- Security investigation and event management
- Security monitoring and troubleshooting
- IT operations and application monitoring

Splunk enables you to:

- More quickly monitor, detect, investigate, and resolve advanced security threats
- Monitor your AWS environments to understand anomalies, metrics, and billing
- Streamline investigations of dynamic, multi-step attacks with analytics-driven security event remediation
- Set threshold-based and conditional alerts and triggers to help warn of potential issues before they occur

Customer Success Story: REI

National outdoor retail co-op Recreational Equipment, Inc. (REI) is committed to "inspire, educate, and outfit for a lifetime of outdoor adventure and stewardship."

REI wanted to extend its security posture to include the edge protection of its Amazon Virtual Private Clouds (VPCs) as it migrated applications to Amazon Web Services (AWS).

REI deployed Splunk Cloud and Amazon GuardDuty managed threat detection service across its hybrid environment. With this Splunk and AWS solution, REI gained end-to-end security visibility during migration, revealed real-time insights into potential threats, and enabled a security-oriented mindset through DevSecOps transformation.

APN Partner solutions: Symantec

Workload Protection for Storage to Secure Data in Amazon S3

Protect your data stored in Amazon Simple Storage Service (Amazon S3) with the automated Symantec Cloud Workload Protection (CWP For Storage) security solution.

Use Cases

- Protect against malware and advanced threats
- Web form submission security
- Automatic scanning of all files when they are uploaded, downloaded, or modified

Symantec enables you to:

- Automatically run scheduled scans of Amazon S3 buckets to discover malware and secure cloud applications and services
- Protect against data breaches by discovering when Amazon S3 buckets are misconfigured and automatically sending alerts
- Discover and block the latest threats using Symantec anti-malware technologies
- Automate the protection of Amazon S3 buckets to minimize DevOps and administrative workloads

Customer Success Story: Snapper

Snapper, a New Zealand-based company, develops custom account-based payment solutions such as large-scale ticketing solutions for mass transit organizations.

Snapper needed to create a payment system to process the specific purchases attached to qualified offerings, while securing each transaction and protecting the stored data associated with each purchase. Symantec Cloud Workload Protection for Storage (CWP for Storage) enabled Snapper to automatically discover and sweep their Amazon S3 buckets, using Symantec's suite of anti-malware technologies, in order to keep their cloud storage clean and help to ensure that buckets are not publicly accessible.

This solution is helping Snapper to meet contractual requirements by scaling elastically to optimize cost.

Next Steps

Learn more about Security on AWS

- AWS Security Resources
- Coud Security, Identity and Compliance with AWS
- AWS Security Guidance