

Shared Responsibility Playbook



Contents

- 3 Introduction
- 4 A false sense of data security
- 5 What is the shared responsibility model?
 - 5 Different types of shared responsibility models
 - 6 What leading Cloud Service Providers say about the shared responsibility model
- 7 How to uphold your end of the shared responsibility model
- 8 Shared responsibility — Own alignment



Introduction

Scalable, cost-effective and customizable, software as a service (SaaS) continues to gain dominance as the preferred method of enterprise applications delivery.

But while cloud service providers cloud environments with proven infrastructure far beyond what most enterprises can achieve with on-prem solutions, data resiliency and security need to remain in clear focus for all companies using cloud services.

So that leads to the question: what exactly is the customer's role in keeping their cloud data secure?

The answer lies in the **shared responsibility model**.

A false sense of data security

Before we explain the model and **who** is responsible for protecting SaaS data, let's explain; what are we protecting it from exactly?

According to Gartner, 99% of cloud security failures and resulting data loss will be the customer's fault through 2025. This includes things like lax permissioning, social hacking, insider threats, poor physical security controls and other vulnerabilities.

Despite these risks, most people still assume that their cloud service provider is protecting their data, because 'it's on the cloud'. As part of our annual **State of SaaS Data Protection Survey**, we asked respondents who was responsible for protecting the information kept in SaaS applications such that, if there was a data loss or corruption incident, it could be recovered. Approximately 40% of respondents said these responsibilities sat with their SaaS provider or were unsure where that responsibility sat.

What is a (or the) shared responsibility model?

A shared responsibility model is a cloud security framework that dictates the security obligations of a cloud service provider (CSP) and its users to ensure accountability.

In short, this model states that CSPs, such as Salesforce, Microsoft Dynamics, Workday, etc are responsible for security of the cloud, and customers are responsible for security in the cloud:

- **CSPs:** Responsible for configuring, managing and securing applications, network controls and the host infrastructure
- **Customers:** Responsible for all data stored in the cloud, endpoints (devices), and account and access management

A good way of thinking about shared responsibility in the cloud is the relationship between a landlord and apartment renter. The landlord is responsible for making sure your roof doesn't leak, for example, and you're responsible for items located inside of the apartment, such as your TV.

It's the organization's responsibility to safeguard data from any threat—internal or external—and ensure that their cloud providers deliver bulletproof security and compliance guardrails.

Different types of shared responsibility models

While all cloud service models — infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) — subscribe to the shared responsibility model, a users' responsibilities increase as they move from SaaS to PaaS to IaaS.

- **IaaS:** The cloud provider is responsible for services and storage — the basic cloud infrastructure components such as virtualization layer, disks and networks. The provider is also responsible for the physical security of the data centers that house its infrastructure. IaaS users, on the other hand, are generally responsible for the security of the OS and software stack required to run their applications, as well as their data.
- **PaaS:** When the provider supplies a more comprehensive platform, the provider assumes greater responsibility that extends to the platform applications and OSes. For example, the provider ensures that user subscriptions and login credentials are secure, but the user is still responsible for the security of any code or data — or other content — produced on the platform.
- **SaaS:** The provider is responsible for almost every aspect of security, from the underlying infrastructure to the service application, such as an HR or finance tool, to the data the application produces. Users still bear some security responsibilities such as protecting login credentials from phishing or social engineering attacks.

Source: <https://www.techtarget.com/searchcloudcomputing/definition/shared-responsibility-model>

What leading CSPs say about the shared responsibility model

Today, nearly all CSPs subscribe to this shared responsibility model. Here's what some of the most prominent ones say about data protection responsibilities:



"Security and Compliance is 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. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall."

AMAZON WEB SERVICES



"Google does not control security on the operating system, packages or applications that are deployed by customers on GCP. It is the customer's responsibility to comply with the requirements of PCI DSS that relate to operating systems packages and applications deployed by customer, or to customer's configurations in multi-cloud or hybrid cloud models outside the GCP boundary"

GOOGLE



"While AWS secures and maintains the cloud infrastructure, you (the customer) are responsible for securing everything that you put in the cloud. This includes your data, the applications that you build, your configurations, and so on."

SALESFORCE



"For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control."

MICROSOFT AZURE



"An easy way to understand this is with a simple analogy: we provide a box and secure it (hosting), and you, as our customer, decide what is put in the box and who can access it (storing)."

SERVICENOW

How to uphold your end of the shared responsibility model

Through 2022, it's estimated that at least 95% of cloud security failures will be caused by missteps on the part of customers. That's why it's more important than ever before to clear up confusion around the shared responsibility model, get clarity and set yourself up for success.

While the shared responsibility model says you're responsible for backing up your data, it also means you're responsible for configuring your security controls.

Here's a checklist to help you get started:

Identify security vulnerabilities

Classify your data

Ensure the principle of least privilege

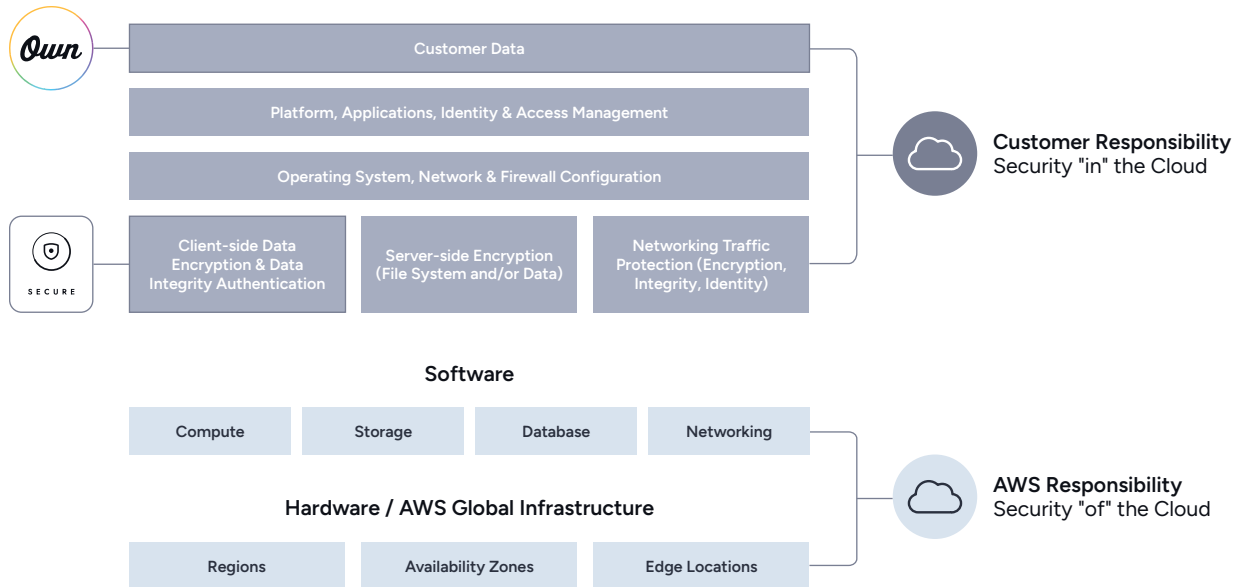
Encrypt your data

Anonymize data in non-production environments

Back up your data regularly

Have a data recovery solution in place that meets your RPO and RTO

Shared responsibility — Own alignment





O W N Y O U R O W N D A T A

About Own

Own is the leading data platform trusted by thousands of organizations to protect and activate SaaS data to transform their businesses. Own empowers customers to ensure the availability, security and compliance of mission-critical data, while unlocking new ways to gain deeper insights faster. By partnering with some of the world's largest SaaS ecosystems such as Salesforce, ServiceNow and Microsoft Dynamics 365, Own enables customers around the world to truly own the data that powers their business.

It's their platform. It's your data. Own it.

Learn more at owndata.com