The c-suite guide to Shared Responsibility for cloud security

What it is, and why it makes sense for enterprises

Security: your cloud priority

Migrating your business workloads over to the cloud is an exciting opportunity. It's a step towards greater flexibility, enhanced agility and advanced security measures. But it can also be a step towards greater visibility, control and innovation.

For a start, there are a lot of considerations, not least:

- Security
- Cost
- Compliance
- Disruption
- Ease of migration
- Ease of management
- Maintaining control
- And whether the move will help the business innovate and grow

All are important, but security is at the top of that list, and it's up there for obvious reasons. We're continually investing in cloud security to make sure our clients businesses are protected.

The method we use is called a Shared Responsibility security model. It's a data defence methodology that helps AWS form tightly bonded security systems, safeguarding the data that enterprises store in the AWS Cloud, while offering the flexibility you need to do business.

Over the next few pages we'll dive into:

- What it is and how it works
- The nuts and bolts of the responsibilities
- Why Shared Responsibility makes sense for enterprises
- Three Shared Responsibility stories
- Some links to help you get started

Let's go.

How Shared Responsibility security works

Shared Responsibility makes a clear distinction between **security of the cloud** and the **security in the cloud**.

We keep the cloud secure (security of the cloud). You keep your data inside the cloud secure (security in the cloud).

If you think of the cloud as a warehouse that contains your data, we own and control that warehouse. We keep it in a safe location for you, fenced off, and guarded with state-of-the-art, compliant security, with control over who's allowed in and out 24 hours a day. When you use AWS, you're hiring space and services inside the warehouse that we've built and secured for you.

So what's inside the warehouse? That's where your data, your content, and your applications are. You can implement your own Information Security Management System (ISMS) inside there to keep them secure, or use the controls we offer to configure the right security measure for you.

But the big thing to remember is that we secure the cloud itself, you secure the data inside it. Between us we form a tightly bonded framework that's trusted by banks, healthcare institutions, governments and even military organisations, all over the world.

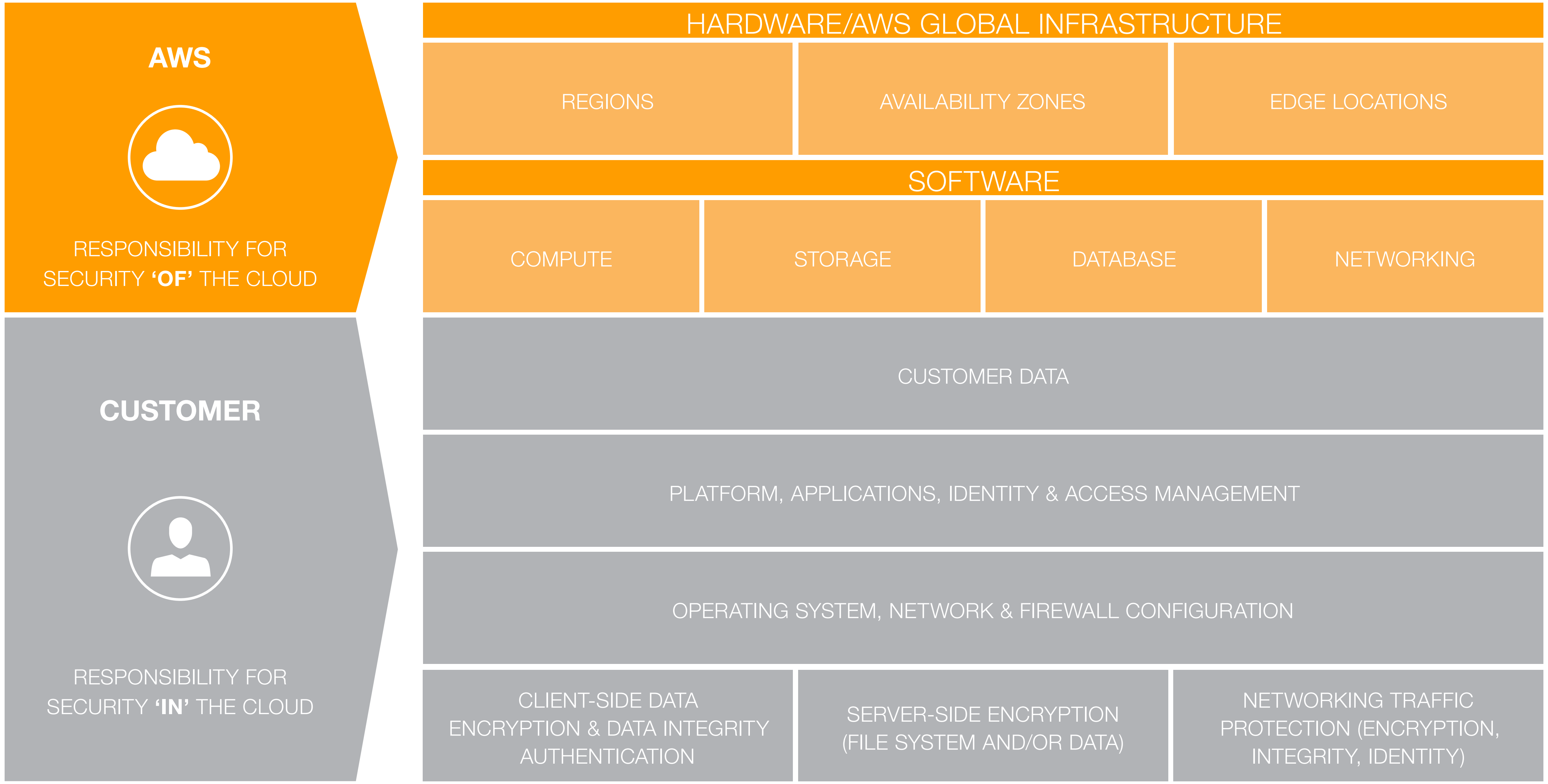
The nuts and bolts of the responsibilities

We control the security of the underlying hardware and software of the cloud

On the hardware side, we safeguard the AWS global infrastructure. That's the physical security of our global and regional data centres and the hardware of the network that connects them between each other, and to you.

On the software side, we control the compute, storage, database and networking layers – including data encryption services, and services like AWS Multi-Factor Authentication (MFA).

We also provide you with a cloud-architecture API. It gives your business access to a series of powerful security systems that your IT team can configure to protect data stored in the AWS cloud.



AWS

RESPONSIBILITY FOR SECURITY **'OF'** THE CLOUD

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS | AVAILABILITY ZONES | EDGE LOCATIONS

SOFTWARE

COMPUTE | STORAGE | DATABASE | NETWORKING

CUSTOMER

RESPONSIBILITY FOR SECURITY **'IN'** THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

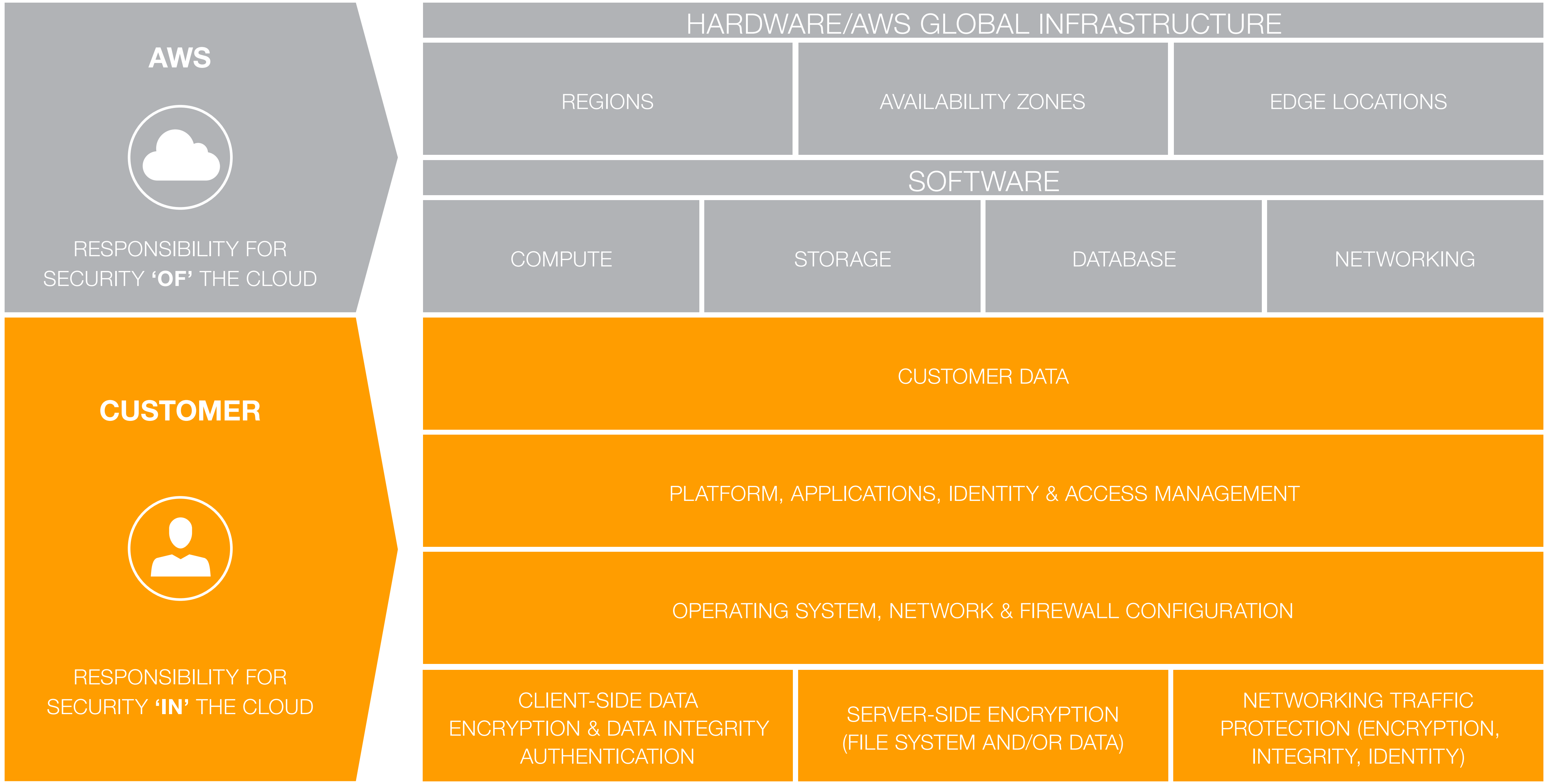
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION | SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA) | NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

You control the configuration of those security systems within the cloud

This is where your responsibility begins. We provide you with powerful Identity and Access Management tools, firewalls and a security API for you to configure to your business' needs. It's up to you to configure them to protect your business' assets.

You're in control of security baselines within data protection services (through the proper use of encryption), as well as access assignments, and permissions.

But you don't have to use and configure AWS-designed security measures to protect your data. If you prefer, you have the flexibility to implement your own Information Security Management System (ISMS) if that's the best approach for your business.



AWS

RESPONSIBILITY FOR SECURITY **'OF'** THE CLOUD

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

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)

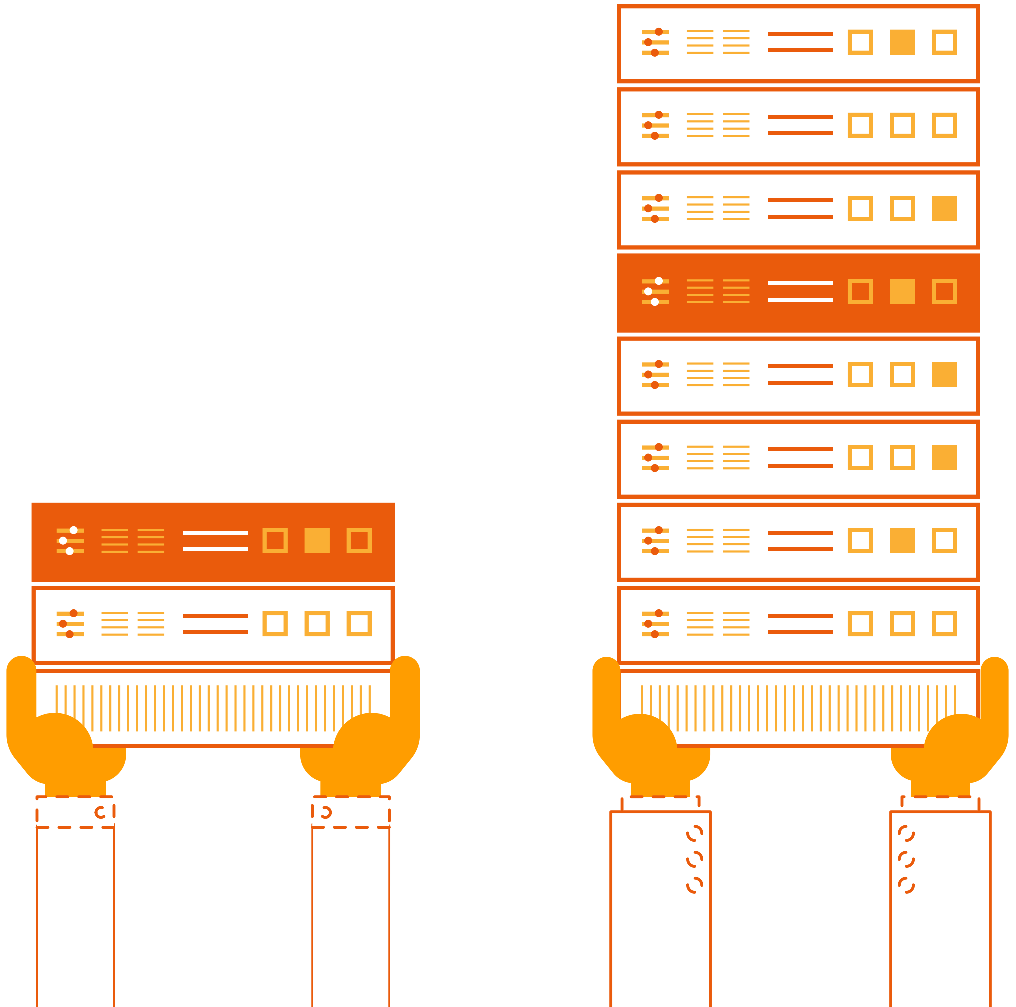
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

Why Shared Responsibility makes sense for enterprises

That's how the responsibilities are shared out between you and AWS, but how can your business benefit from this security model, long-term?

Here's what you can expect…

You'll do a lot less of the IT heavy lifting



By taking care of the security of the cloud, we're able to take thousands of accredited security controls completely off your hands.

That means there's no need for you to have acres of server warehouses, or reliable power supplies, or cooling systems, or security guards, or secure ways to connect your storage infrastructure to your network. You don't need any of that – we take care of it for you.

Having that secure, managed system gives you a huge amount of service consistency, without any of the maintenance and upkeep issues you'd normally associate with running an efficient IT infrastructure.

It'll also free up your IT team's time. They won't need to sweat the maintenance side of securing your business – instead, they'll be focusing on innovating new services for your customers.

> "AWS allowed us to store information in a cost-effective manner while alleviating the burden of supporting the necessary infrastructure since AWS takes care of that. It really is a win-win for us and our customers."

Jeff Kimsey, Associate Vice President of Product Management at Nasdaq

Strengthen your programmes by inheriting our strong security and compliance controls

Shared Responsibility is part of a number of compliance assurance programmes, from certifications like ISO27001 to regulations like the EU Data Protection Directive. You can find more about each of the assurance programmes here.

That gives you two big benefits.

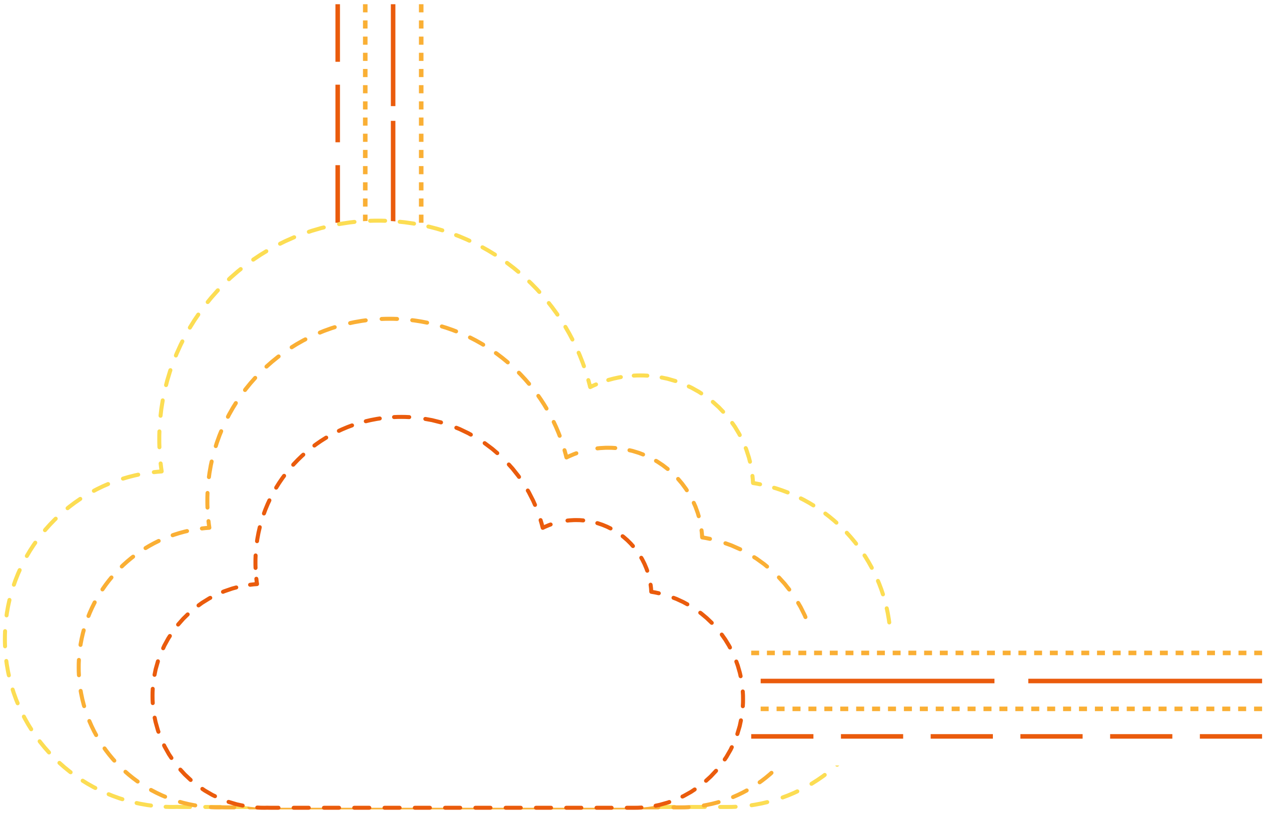
First, peace of mind, as you'll know your customers' data is being held in a cloud architecture that's been audited and accredited by some of the world's leading regulatory bodies.

Second, each cloud service has defined characteristics that we've designed from working closely with regulatory bodies. It means the security we implement is more than just compliant (that's the bare minimum). It's equipped with the most comprehensive security technology available today.

AWS Assurance Programmes

ISO 27001
International Organization for Standardization
ISO 27018
International Organization for Standardization
C5
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
AICPA SOC
HIPAA
PCI Security Standards Council
PARTICIPATING ORGANIZATION™
FR
FedRAMP
irap
iDA
SINGAPORE

You'll get scalable, responsive security



Picture this. Your sales people win a huge customer and you need more server space to handle all the new business. You call up IT, explain that they need to prepare for the tsunami headed their way, and the team comes back with their response: 'That's great news! We'll have the server spun up and compliant in… six months' time.'

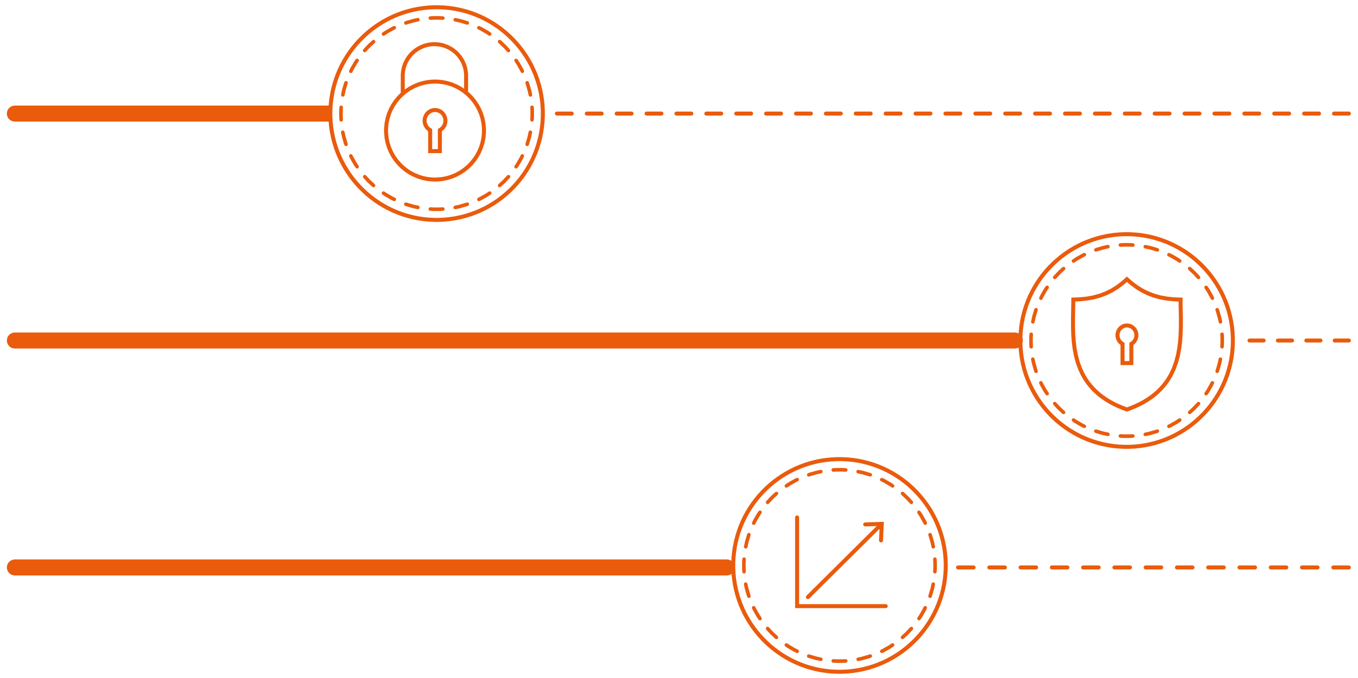
There was a time when that's just how it was. You'd just accept that there was either going to be a delay in starting work, or that in the early days of the new relationship there'd be a server bottleneck.

Things are different now. Organisations need to scale their IT infrastructure to service new business, fast. So they expect greater agility as standard.

Cloud-based Shared Responsibility security gives you instant and consistent access to a secure IT infrastructure at the scale you need, at exactly the time you need it. There isn't even an issue of scaling your team to fit the IT infrastructure – the server onboarding process is all carried out by software.

In effect, you can scale up to run servers in a week, and be safe in the knowledge they'll have exactly the same compliant security measures built into them that you're currently running. When that's out of the way you only need to concern yourself with serving your customers.

You'll get ownership and control



While the heavy lifting is taken off your hands as part of the security *of* the cloud, you'll still maintain close control of security measures *in* the cloud.

We provide powerful APIs that allow you to implement your own Information Security Management System (ISMS). That allows you to define the right security controls for your workload, data sensitivity, model, and the changing scale of your business.

Certain regulations might also require you to add an additional layer of protection between the services from AWS and your own operating systems and platforms. With AWS you can impose additional controls like protection of data at rest and in transit. You can also add an opacity layer between AWS services and your platform that includes data encryption, data integrity, authentication, software- and data-signing, secure time-stamping, and more.

Alternatively, you might introduce your own data protection tools, or take advantage of AWS partner offerings.

You'll save a lot of time and hassle

Keeping your IT infrastructure secure is a time-consuming business.

You have to keep your data centres secure, with safeguarded warehouse facilities that have tight surveillance and closely monitored Identity and Access Management systems.

Then there's the infrastructure upkeep, networking, software and upgrading.

But when all your security tasks are automated on AWS, you can redirect all this time and resources to doing what your company do best. And be way more secure in the process.

> "Using AWS, we were able to design and launch a security-compliant solution in three months while reducing our capital expenses by 30 percent,"

Online Senior Product Manager
for Vodafone Italy

You'll get continuous security innovation that evolves with you

Let's say you don't need to scale your business' IT infrastructure up or down for the foreseeable future – everything's staying consistent. That's great. From your side of things, you continue to pay a regular fee for the cloud storage you need.

On our side, we're constantly iterating new security measures to fortify our systems.

And you don't need to pay for upgrades – the security service you get from us is always improving.

> "The fact that we can rely on the AWS security posture to boost our own security is really important for our business. AWS does a much better job at security than we could ever do running a cage in a data centre"

Richard Crowley,
Director of Operations at Slack

In short, Shared Responsibility means...

You keep close control of the security you need to manage.

You can stop being concerned about the security of the foundational services your IT infrastructure is built on.

You get the benefits of a robust cloud infrastructure with a reliably secure service that's scalable, responsive, and efficient.

More control, more compliance, less time, less effort.

It's like a CISO's dream.

> "We had heard urban legends about 'security issues in the cloud,' but the more we looked into AWS, the more it was obvious to us that AWS is a secure environment and we would be able to use it with peace of mind."

Yoshihiro Moriya,
Certified Information System Auditor

Where can I find more info?

Head over to aws.com/compliance and aws.com/security.

In both you'll find more information about Shared Responsibility, as well as many case studies from enterprises that use the model.

You can also access our security webinars through https://aws.amazon.com/events/security-webinars. There's an archive of recordings from past security seminars in there, and if there's something you can't find, you can sign up for the next webinars we've got coming up to ask something new.

Or, if you'd like to speak to someone about Shared Responsibility

Click here to get in touch with our security team and they'll help set up a conversation about how Shared Responsibility could work for your business.

Further reading

The six core benefits of a secure cloud eBook:

aws

The Data-Safe Cloud

6 core benefits of a secure cloud

- See how software company Symantec used AWS to optimise its security solutions
- Get the full story on how data protection business Druva used AWS to automate tasks and achieve a faster time to market
- Read how cyber security solutions business Bitdefender uses AWS to deliver SaaS