The Data-Safe Cloud

6 core benefits of a secure cloud

The evolving conversation around cloud security

Security will always be top of the agenda in any cloud conversation, but the way we talk about it is changing.

Early on, customer concerns centred around whether or not the cloud itself was secure: Can we trust the cloud with our data? Are we increasing our exposure to risk by migrating to the cloud?

But over time, the conversation has changed. Concerns are no longer about whether or not the cloud is secure – instead, they are about how to best secure data in the cloud.

Customers want to know: What kind of controls are available so I know who is accessing my data, and when? How do I access and audit my data so I know I'm in compliance? How can I secure a hybrid cloud environment?

The first wave of leaders to ask these questions were pioneering what was as much a cultural shift as a technological upgrade. Now, more organisations have realised that, one way or another, their future lies in the cloud and they are seeking the best way to secure their data with the right cloud provider.

As confidence in the public cloud grows, we see that the volume of applications being run on shared infrastructure is also growing. This gives us more and varied uses cases that reveal the benefits and best practices for a data-safe cloud.

51%

51 percent of IT managers said data security is better in the cloud than in their data centres.

58%

58 percent said public cloud was the most secure, flexible and cost-effective solution for their organisations.[1]

2020

Confidence is such that Gartner predicts that by 2020, more compute power will be sold via the cloud than what is deployed in customers' on-premise data centres.[2]

[1] SADA systems public cloud survey

[2] Gartner, Predicts 2016: Cloud Computing to Drive Digital Business, December 2015

6 Benefits of Cloud Security

One of the challenges of moving to the cloud is managing multiple stakeholders in an organisation with varying levels of enthusiasm for a cloud adoption journey.

Understanding the unique benefits of a secure cloud is the first step towards addressing the concerns of security and compliance professionals within your organisation.

A provider who demonstrates these six benefits can help you transform the way you operate, freeing up resources to focus on your core business – all while making your organisation more secure.

01

Inherit Strong Security and Compliance Controls

02

Scale with Enhanced Visibility and Control

03

Protect Your Privacy and Data

04

Find Trusted Security Partners and Solutions

05

Use Automation to Improve Security and Save Time

06

Continually Improve with Innovative Security Features

01

Inherit Strong Security and Compliance Controls

When you're choosing a cloud provider, remember that you'll inherit many of their security controls into your own compliance and certification programmes. If they're the right ones, they can dramatically lower the costs of your security assurance efforts. To ensure you select the right provider, look for third-party validation: internationally recognised security best practices and certifications, as well as industry-specific certifications.

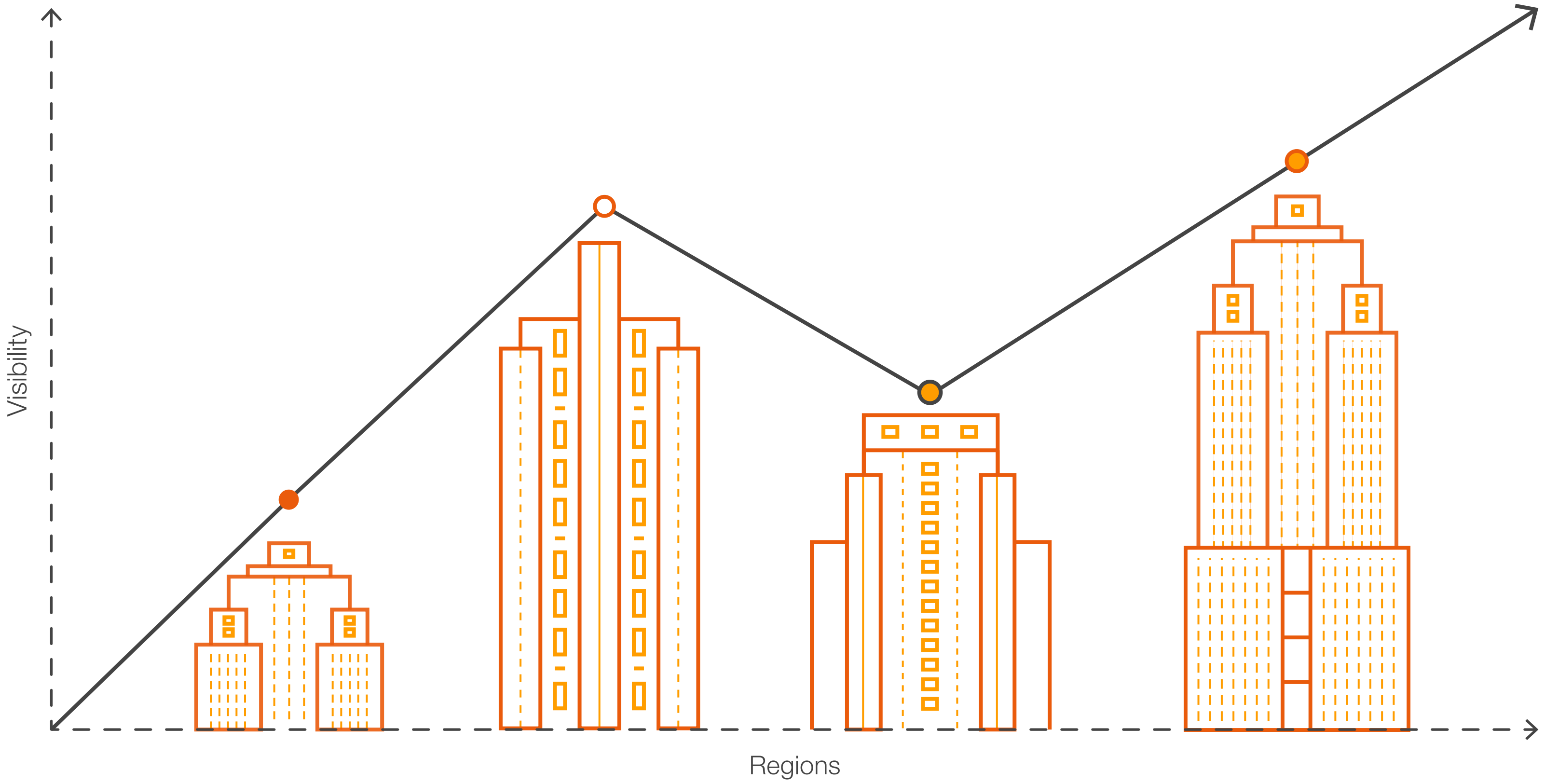
Examples of these controls include internationally recognised security best practices and certifications such as ISO 27001, ISO 27017 for cloud security, ISO 27018 for cloud privacy, and SOC 1, SOC 2, and SOC 3. The right provider will also offer services to help you achieve HIPAA or PCI-DSS compliance, and will have achieved many public sector certifications via FedRAMP and the DoD SRG in the US, C5 in Germany, IRAP in Australia, and MTCS Level 3 in Singapore.

> "Robust security in a retail environment is critical for us because of our many retail operations. By leveraging the security best practices of AWS, we've been able to eliminate a lot of compliance tasks that in the past took up valuable time and money."

Brian Mercer, Senior Software Architect, Delaware North

02

Scale with Enhanced Visibility and Control



The data you store in the cloud isn't out of sight, out of mind. You need to know where it is and who is accessing it at all times. This information should be available in near real time wherever you are, regardless of where in the world your data is stored. Imagine information about your infrastructure and your data being a simple software programming call away – you cannot get this kind of visibility with an on-premises datacentre.

Ensure you have the control you need by looking for key features like fine-grain identity and access controls combined with activity-monitoring services that detect configuration changes and security across your ecosystem.

Not only will these controls allow you to reduce risk, but you will be able to scale your organisation more efficiently. Ideally these cloud-based controls and services will even integrate with your existing solutions to simplify your operations and compliance reporting.

03

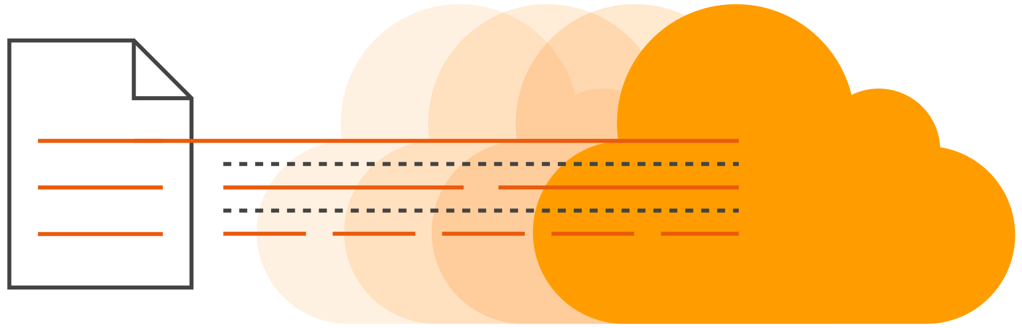
Protect Your Privacy and Data

When you move your data to the cloud, you don't surrender ownership of it – nor should you lose your ability to encrypt it, move it, and manage the retention. Look for a provider who is vigilant about your privacy and offers tools that allow you to easily encrypt your data in transit and at rest, to help ensure that only authorised users can access your data.

In addition, when you work with a global cloud infrastructure, you should make sure you can retain complete control over the regions in which your data is physically located. This will be key to your regulators, helping ensure you meet regional and local data privacy laws and regulations as well as data residency requirements.

> "[Using a vendor with a Sydney region] is very important to us from a product performance and a latency perspective. Our customers are in Australia and New Zealand, and data sovereignty was also a concern. We also wanted to use a range of flexible cloud services to optimise the ability of the system to meet customer needs."

Trevor Leybourne, Head of Delivery,
Mind Your Own Business



> “Our data is hosted in Europe, which is crucial for us from a security perspective. With AWS, we have complete control over where and how data is stored, and who has access to it. This control, along with the extensive encryption, means we feel safe. We know the Trust’s data is protected.”

Martin Brambley,
Director of MSP Sirocco Systems,
working with The National Trust U.K.

04

Find Trusted Security Partners and Solutions

One of the biggest advantages of working with a leading cloud provider is gaining access to their partners and the cloud security solutions and consulting services that they offer. There are thousands of security technology and consulting services out there, but knowing which ones are right for your particular use case, where to access them, and how to manage those engagements can be hard.

How can the right cloud security partners help you?

1. The right partner will have deep expertise and proven success with your stage in the cloud adoption journey, enabling you to find the right help at the right time. You can also find partners skilled in either hybrid or all-in migrations.
2. Use the solutions you already know and trust. Many cloud security partners offer the same tools and services you currently use on premises, providing a seamless transition to the cloud for your team and your data.
3. For highly regulated environments, you can find partners that meet stringent security requirements and have expertise in building, deploying, and managing the types of workloads you wish to migrate to the cloud.
4. The right cloud provider will even help you ease billing headaches with “pay as you go” partner pricing and unified billing so you can manage one invoice for all of your cloud spend.

05

Use Automation to Improve Security and Save Time

Automation is a vital component in any cloud security programme, not just to handle high-scale checks efficiently, freeing your team to focus on more business-critical areas, but also to reduce human configuration errors.

You should also be able to automate infrastructure and application security checks whenever new code is deployed, to continually enforce your security and compliance controls to help ensure confidentially, integrity and availability at all times.

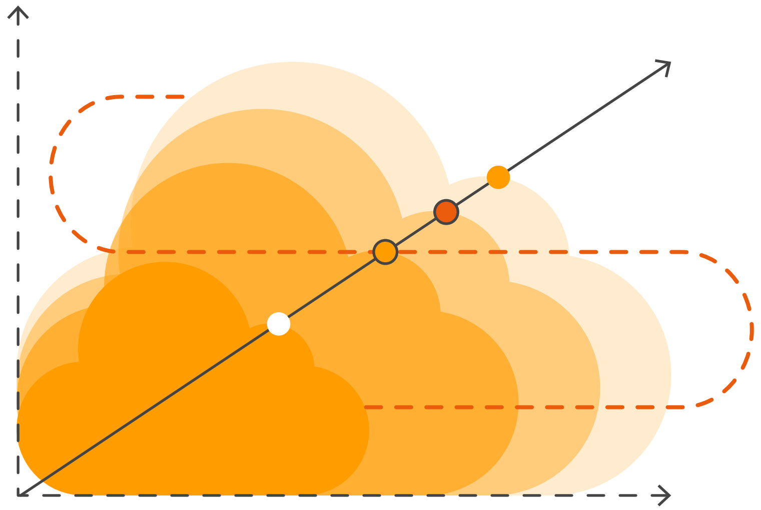
> “With AWS, IT is more agile than ever before and able to match the pace of business.”
>
> Balakrishna Rao, Chief Information Officer Manipal, Global Education

06

Continually Improve with Innovative Security Features

For too long, security has been seen by some as an innovation block, slowing down business. With the right services and tools in the cloud, you can secure your data with greater speed and agility, and your security team can rightly be called an enabler of innovation across the organisation.

To achieve this kind of transformation, scale matters. An experienced cloud provider working with millions of customers across the globe should have a team of experienced engineers with deep insights into global trends, giving them remarkable visibility into emerging security challenges. This knowledge, along with customer feedback, should be incorporated back into both their infrastructure and their services. This continual feedback and improvement should enhance core security services like strong identity and access management, logging and monitoring, encryption and key management, network segmentation, and DDoS protection – and everyone benefits.



Tips for a Successful Cloud Mindset

Today, CISOs are looking at security and risk in a new way. Just a few years ago, even considering a move to the cloud was controversial.

Recently the conversation has shifted to governance, and how leaders can guide their organisation through change to securely maximise new opportunities while still retaining the controls they need.

We're also seeing the beginnings of true integration of security planning into cloud strategy. In the past, enterprise customers might have asked vendors to help them write a cloud security strategy. Now they're realising that a more useful question is 'What's my overall security strategy, and how can I incorporate cloud into it as a deployment model?'

Adopting the right mindset can help your organisation adapt to what is new about security in a cloud environment. Here are some tips to keep in mind.

Build on what you have.
Don't think of your cloud security strategy in isolation. Instead, look at your wider security strategy and think about how you can incorporate cloud without losing sight of your control frameworks.

Remember the basics.
Most of it is still just good hygiene, and these principles will apply whether you're in an on-premise, hybrid, or all-cloud environment.

It's a well-trodden path.
Your peers are already there. These days you are not facing the risk of being one of the first organisations to migrate sensitive workloads to the cloud. 84 percent of IT managers reported are already using public cloud infrastructure.[3]

The real security conversation is about leadership.
To succeed in the cloud, many organisations choose to transform how they operate. Your leadership team should be prepared to define how you will lead your organisation through the change. Who will own the responsibility for security and compliance? How will roles or job skills need to change, if at all?

[3] SADA systems public cloud survey

Invest in cloud security in the same way you invest in the cloud.
Experiment with new ways to solve your security and compliance challenges. The cloud offers you a flexible, try-before-you-buy or try-as-you-buy model that also gives you the benefit of greater vendor accountability. So you can start small, test, then build as you need.

The best cloud security solutions are designed for speed and automation.
Cloud solutions give users the freedom to experiment and iterate, with the ability to make enhancements on the fly. Try a new security solution and, if you don't like it, you can make small, controlled changes to get it right – or you can roll it back, without getting locked in.

You're probably already in the cloud somewhere.
If you're securing a data centre today, you're probably using cloud computing somewhere in that supply chain already. This can give you leverage with your leadership team to start moving more sensitive workloads to the cloud.

Changing Compliance from a Roadblock to an Enabler

One of the main roadblocks to cloud adoption is concern over meeting strict risk and compliance requirements which are often industry – or country-specific. Finding a cloud provider with deep experience in building secure environments for the most risk-sensitive organisations is only the first step. Ideally you will find a provider who can make it easier for you to demonstrate to your internal and external risk stakeholders that your data is secure and meets the requirements of applicable third-party assurance frameworks.

At AWS, we think differently about security and compliance. As with everything at Amazon, our success is primarily measured by one thing: our customers' success. When it comes to security and compliance, our customers drive our portfolio of compliance reports, attestations, and certifications that support their efforts in running a secure and compliant cloud environment.

With AWS you can:

- Inherit many security controls operated by AWS, giving you the ability to strengthen your own compliance and certification programmes.
- Gain access to tools that will help you lower your cost to maintain and run your specific security assurance requirements.
- Save time by using AWS Artifact, our automated compliance reporting tool, to review and download reports and details about thousands of our security controls.
- Get started with confidence by following security configuration best practices outlined in our Quick Starts, laying a solid foundation for meeting your global compliance requirements.
- Tie together governance-focused, audit-friendly service features with applicable security compliance regulations or audit standards.
- With AWS Compliance you're able to build on legacy systems and help customers establish and operate in an AWS security control environment.

Sharing Security Responsibility with Your Cloud Provider

One issue that has gained prominence in cloud conversations is the question of who owns responsibility for security.

How does responsibility for security break down within your organisation, and how is it shared between you and the provider?

A surprisingly common assumption made by many cloud buyers is that once they migrate to the cloud, they've passed the responsibility for security on to the cloud provider. That's not the case for any provider. At AWS, our customer-first mindset shapes our view of how we share responsibility for security and compliance with our customers.

The AWS Shared Responsibility Model

Our model makes a clear distinction between the security of the cloud, and security in the cloud.

01

The security **of** the cloud

– refers to the measures that we, as the cloud service provider, implement and operate.

02

Security **in** the cloud

– refers to those measures that the customer implements and operates, and relates to the security of customer content and applications that make use of AWS services.

It helps the customer to share responsibility without handing over the reins. Organisations retain visibility and control of the security measures they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site data centre.

For a more detailed look at cloud security – and, ultimately, where the buck stops – take a look at this eBook on the AWS Shared Responsibility Model.

Your next move

You have many resources available to you when you are ready to get started with AWS:

1. Follow the security best practices outlined in our Cloud Adoption Framework (CAF).

2. Leverage our rich AWS Partner Network (APN) ecosystem comprised of partners and security services you may already know and use today – and check out the solutions available through AWS Marketplace.

3. Engage our Professional Services team to accelerate your migration to the cloud and help guide you through every step of securing your cloud environment.

Learn more about the benefits of AWS including details about our infrastructure and security and compliance features by visiting our website aws.amazon.com/security.