
SECURING
THE CLOUD
A Practical Guide to Implementing
6 Essential Steps for Cloud Security

6 STEPS TO CLOUD SECURITY

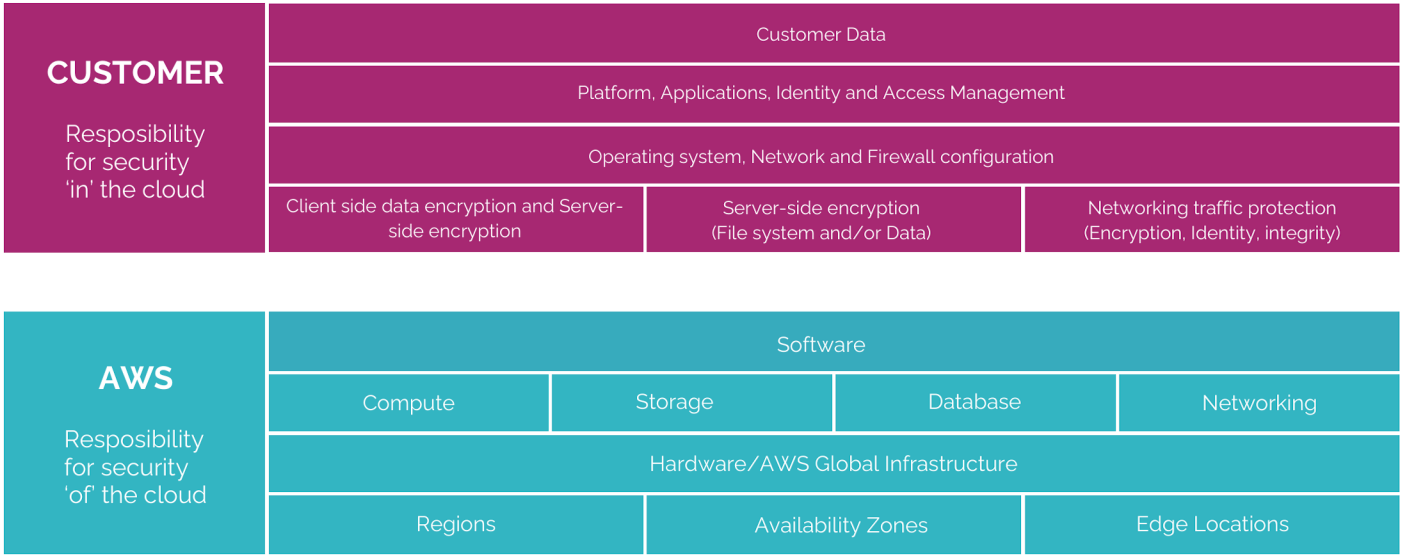
Yes, we know there are more than 6 things to consider when building security in the cloud! We've highlighted this half dozen as a starting point to help you along your journey to building and managing a robust, secure cloud environment. As with all IT solutions, success depends on the blend of technology, processes and people, and cloud is no different. If any one of these elements is lacking, then not only will the business fail to get their return on investment, but the risks of a security attack are significantly increased.

1 DON'T ASSUME YOUR CLOUD IS SECURE!

It's an urban myth that a company's data is automatically secure because it's in the cloud. Nothing could be further from the truth! A recent study by **CPR** shows there has been a 48% year-on-year increase in cloud based cyberattacks for 2022 globally, and 50% in Europe. Whether you're using wholly public cloud, private cloud or hybrid there is always a joint responsibility between the service provider and the organisation.

2 CHOOSING YOUR CLOUD PROVIDER

Not as straightforward as you might imagine. Whether you're a large enterprise or a small business, the **14 guiding principles** of cloud security apply and the provider must demonstrate its ability to meet these principles in line with your business requirements. Even when you've satisfied yourself that your shortlist of providers comply with the principles, you have to consider how they can keep ahead of the evolving threats, how they update their systems and how quickly they can respond and mitigate new threats. Of course, the three market leaders AWS, Microsoft and Google have it in their interest to be secure as possible, but it should be taken for granted and you remain vigilant! It's also very important to understand where you have responsibilities when it comes to public cloud services. Whilst each public cloud provider has some responsibilities for aspects of infrastructure, platform and network security, the client must take all reasonable steps to set up, configure and maintain its security posture. The diagram shows a summary of provider and client responsibilities.



3 GOVERNANCE IS CRITICAL

You've chosen your provider and set up your services, identity management, authentication, and all the other critical steps to create a secure operating environment, so you're done, right? Wrong! That's just the starting point. Many activities have negatively affected the security integrity of your cloud environment, two of the key ones being Shadow IT and Cloud Sprawl. Do you suspect or have you seen people in your business subscribing to cloud services outside of your corporate standard? Do you know what they're up to? They could have used their department's budget to use non-approved and unchecked cloud services and moved some company data into an insecure area. The results could be a lack of visibility and control, data loss, data that some users can't access and an expansion of the attack surface.

Let's assume that shadow IT has been squashed. What about sprawl? The uncontrolled, sometimes unintentional, growth of cloud usage is a real risk. Apart from the increased costs of unchecked cloud services consumption, it also increases the risks of attacks. The urgent need for data and applications often shortcuts the processes for correctly setting up and configuring assets such as new virtual machines, containers, new users and APIs to other applications, sometimes outside your domain.

Good governance is difficult to achieve but is critical to the ongoing security of an ever-changing and dynamic environment.

4 UNDERSTAND RISK

It's often said that if you don't take risks, you'll never make any big decisions. The day-to-day operation of your business depends on the processing of data and the sharing of information, so regardless of the steps you take to secure your business, there will always be inherent risks. How can you understand the risks and do whatever you can to mitigate and minimise them? We could spend all day talking to you about this, but we'd like to focus on one aspect of risk: people. You've risk-assessed your technology; you have a robust governance process but what about the users and the IT team? Two issues at stake here are skill sets and human behaviour. Running cloud services take people with the right set of skills and experience. Not having these will introduce unnecessary risks like misconfigurations, choosing inappropriate hardware and software, not knowing how to respond to critical events, and being unable to identify malicious behaviour, even if they have good tools.

Users, after all this time and the high-profile cases of phishing and malware, still do things they shouldn't! Clicking on rogue URLs, running executable files, installing things they shouldn't do, having weak passwords, and even sharing passwords!

5 DATA IN TRANSIT

Do you have visibility of the routes your data takes? Do you have a high level of confidence that each leg of its journey is secure? Data traverses many sections of physical wired networks, wireless networks, between virtual assets in the cloud, across internal and external networks. It's more likely that an attacker will target the weaker point of the infrastructure between the user and service, so understanding the components of the communications and identifying weak spots in things like authentications and encryption techniques is essential.

6 SUPPLY CHAIN

Most companies, whether they be global, international, or local are dependant on their supply chain. Manufacturers, for instance, run lean operations to achieve their 'just in time' production strategy. A recent study by AAG shows that 39% of British businesses reported a supply chain cyberattack in 2022. Companies in the supply chain will be using a combination of private, hybrid and public cloud services and exchange data between and within them. We've already discussed the importance of adhering to the guiding principles of cloud security and we've looked at the communications flow, but how do you know that your supplier is an rigorous as you are? Can an attacker use a weak point on your supplier's cloud back-end infrastructure to steal your data, causing collateral damage or service denial? The answer is yes, they can and do and it will always remain a constant threat. As usual, the successful blend of technology, process and people will help to mitigate this threat. Rigorous supplier assessments, implementing a zero trust model, incident planning and crisis simulations are a few things that should be done.

SUMMARY

Don't make it someone else's problem. Be aware of your responsibilities. Security is the responsibility of everyone in the company, not just the IT team. Security is a journey, not a one-off exercise. Governance is critical.

Look beyond your own company assets and cloud. Challenge your suppliers and partners. **NEVER** assume your data is safe in the cloud!