BLOG POST

Securing the cloud (by design *and* by default)

To reduce data breaches from cloud services, seek out providers who ensure functionality is ‘secure by default’

Andrew A

In any conversation about cloud security, it won’t take long before someone will mention the shared responsibility model. It ultimately comes down to the fact that the cloud service itself needs to be designed and operated securely by the cloud provider, and their customers need to configure and use it in a way that appropriately secures their data.

We know that doing security well can be hard, whether that’s getting architectures and configurations right, or the more routine things such as patching. It can feel like a never-ending battle, which means that it’s easy to forget to do all of the things that are important.

Make it somebody else’s problem

We’ve advocated for a while now that you should assign as much responsibility for security to your competent cloud provider as you can. Doing that lets you make use of your cloud provider’s security expertise, and reduces the burden on your own IT teams and developers (while still giving you enough confidence that the service is healthy).

Choosing to prefer SaaS and serverless components will make things a lot easier for you. However it will only get you so far; it will always be **your** responsibility as the customer to configure your cloud services well. And sadly, quite a few cloud providers have some pretty insecure default configurations including:

- weak default authentication policies (with no multi-factor authentication)

- weak default authentication policies (with no multi-factor authentication)
- data encryption as an optional add-on
- collaboration environments accessible by anybody on the internet, by default
- logs (which are very useful to incident handlers) being initially disabled
- legacy protocols (such as IMAP) being enabled, by default
- letting you set your root account password as ‘password’, while also not requiring you to set up multi-factor authentication

I’ve seen all the above in live services, but they’re examples of a wider pattern of insecure defaults. Especially when I map those things back to the misconfigurations that come up time and time again in cyber incident investigations.

Security shouldn’t be opt-in

The NCSC believe it’s important to use a cloud provider that is **secure by design and by default**, and one where **the provider helps you to meet your security responsibilities**.

Some providers may state that certain areas are **not** their responsibility. We think you should choose providers that make it easier for you to differentiate between a ‘good-enough service', and a ‘better service’.

We understand the argument that customers need the flexibility to use services in ways that meets their specific needs. Some people will be using a cloud storage ‘bucket’ to publish documents on the internet, whereas others need the data they’re storing in the cloud to remain private. However, we’ll all end up in a better place if:

- the **default configuration** for the cloud service is a robustly secure one
- relaxing the settings (so the service is more permissive) can only be achieved through an **intentional** action

Updating our guidance

The ‘secure by default’ message is one that you’ll now see throughout the updated cloud guidance. If several providers promise the same security feature, you should prefer the provider that has it enabled by default.

Many organisations don’t yet provide services that are natively secure by design and by default. While they work on this, they should - as a minimum - give you security templates, blueprints, scripts or guides to make it easy for you to secure their service.

As the guidance explains, there are many factors you will need to consider when choosing a cloud provider. When assessing whether they’re ‘secure enough’, you should choose one that makes it easier for you to meet **your** security responsibilities, as well as being secure in its own right.

Andrew A
Cloud Security Research Lead, NCSC

WRITTEN BY

Andrew A
Cloud Security Research Lead, NCSC

PUBLISHED

10 August 2022

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

PART OF BLOG

NCSC publications