FREE GUIDE

Your First 5 Cloud Security Fixes

Five plain-English moves that pay off fastest, from the access-key audit to the one-page incident card.

Cloud security is shared work between you and your provider: they secure the building, you secure your apartment. Most cloud trouble comes from a handful of basics left undone on your side. These five fixes close the gaps that cause the most incidents, and you don't have to do them all at once.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Fix 1: Know your accounts and lock the front door

What it is

A list of every cloud account and console you use, with strong login protection on the powerful ones.

Why it's first

Many of the most damaging cloud incidents start with a single over-powered login that wasn't well protected. The "root" or top administrator account can do anything, so it's the first thing to lock down.

Do this

List your cloud accounts and who has access. Turn on two-step login (multi-factor authentication, or MFA) for every administrator, lock away the root account, and use it only when you truly must.

Fix 2: Audit your access keys and give least privilege

What it is

Reviewing the long-lived keys and accounts that software uses, and trimming each one to only what it needs.

Why it matters

Access keys are among the cloud's most commonly leaked secrets: they end up in code, laptops, and chat histories. A key with broad permissions is a master key; a key with narrow permissions is a limited one.

Do this

Find your access keys, delete the ones nobody uses, and rotate the rest. Give each person and service the least access that lets them do the job, not "administrator" by default.

Fix 3: Close anything open to the whole internet

What it is

Finding the storage, databases, and ports reachable by anyone, and closing the ones that shouldn't be.

Why it matters

A storage bucket or database left open to the public internet is one of the most common causes of a data leak, and it's usually an accident, not an attack.

Do this

Check your storage buckets and databases for public access and turn it off unless it's truly meant to be public. Review your firewall and security-group rules and close ports that don't need to be open.

Fix 4: Turn on logging so you can see what happened

What it is

Switching on the cloud's built-in activity record so there's a trail of who did what.

Why it matters

If something goes wrong, logs are the difference between knowing what happened and guessing. Most clouds can record this for you. It just has to be turned on before you need it.

Do this

Turn on your provider's activity logging (for example, the account-wide audit trail), store it somewhere it can't be quietly deleted, and set a couple of basic alerts, like a new administrator being created.

Fix 5: Back up what matters and write a one-page incident card

What it is

A tested copy of your important cloud data, plus a single page on what to do if something goes wrong.

Why it matters

Cloud data can still be lost, deleted, or locked by ransomware, and "it's in the cloud" isn't a backup. A one-page plan removes most of the panic in the moment.

Do this

Set important data to back up automatically, then do one test restore. Write a one-page incident card: who to call, where the backups are, and the first three steps. Keep a copy you could reach even if your main account were locked.

Where to go from here

The free Cloud Security Assessment shows where you stand across these areas in a few minutes, and it runs entirely in your browser, so we never see your answers: sylvanassurance.com/free/cloud/

When you're ready to turn that snapshot into a full programme with ready-to-use templates and runbooks, the Cloud Security toolkit lays it out: sylvanassurance.com/cloud-security

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-cloud-security