Your First Cloud Security Fixes

A free plain-English guide from Sylvan Assurance

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-10-05

Contents

Why this guide exists 1
Move 1 — List every account 2
Move 2 — Lock the doors that matter 2
Move 3 — Turn on the lights 3
Move 4 — Close what's open to the world 3
Move 5 — Write the one-page incident card 4
The printable checklist 4
A short jargon translator 5
What not to do yet 5

About This Guide **7**

A plain-English guide to the five moves that start a real cloud security programme, for the person who just inherited "the cloud".

Why this guide exists

Somewhere between the client questionnaire, the insurance renewal, and the news story about the company whose storage bucket was open to the internet, you concluded that your organisation should be doing something about cloud security: knowing what you run online, locking the doors that matter, and noticing when something goes wrong.

Then you looked at the field and found a wall of acronyms, a dozen tools with four-figure price tags, and advice written for companies with a security department.

Here is the encouraging truth: a real cloud security programme starts with five moves, none of which needs a budget line or a specialist. Most of them are settings your cloud provider already offers, switched off by default. Organisations that make these five moves are meaningfully better defended (and can prove it) within a month. This guide walks through each move in plain English: what it is, why it works, and how to do it this week.

One note before we start. Everything here is general guidance drawn from widely recognised practice. Your organisation is specific. Treat each move as a recommendation to adapt, not a rule to obey.

Move 1 — List every account

The win: one current list of everything you run in the cloud.

You cannot secure what you don't know you have, and almost everyone has more cloud than they think. The cloud makes it effortless to create things: an account opened for one project years ago, a trial subscription that became production, an online tool someone signed up for with a company card. Each one is part of your estate whether or not anyone remembers it.

A spreadsheet is enough. Open one and list:

- **Cloud accounts**: every account, subscription, or project at every provider (AWS, Azure, Google Cloud, and any others). For each: what it is for, and a named person who answers for it. "The dev account" with no owner is where trouble starts.
- **Software-as-a-Service (SaaS)**. Every online tool the business uses: email and files, accounting, the customer system, design tools, the website host. Three places reveal them: the company card statement, the "connected apps" list in your Google or Microsoft admin console, and asking each team what they actually use.
- **What's reachable from the internet**. For each cloud account, note anything the outside world can reach: the website, any storage shared by link, anything with a public address. These are the assets attackers can try without an invitation.

The trick nobody tells you: read the bill. Every cloud resource that exists costs something, and every cost lands on an invoice with a service name and a region attached. A charge from a service you don't recognise, or a region you don't operate in, is a discovery, and occasionally an intruder. Ten minutes with the monthly bill is the cheapest security review you will ever run.

Time required: one honest afternoon, plus ten minutes a month for the bill.

Move 2 — Lock the doors that matter

The win: stolen passwords and forgotten keys stop being a way in.

In the cloud, identity is the perimeter. There is no office firewall standing between an attacker and your admin console. Whoever signs in with valid credentials is in. That makes three identity fixes worth more than everything else combined.

1. **Turn on multi-factor authentication (MFA) everywhere.** MFA is the second step at sign-in (a code or a prompt on your phone) and it means a stolen password alone is no longer enough. Enforce it for every user, starting with administrators. Most providers let you require it across the organisation with one setting.
2. **Audit your access keys.** Access keys are passwords for software: long strings that let scripts and tools call your cloud directly. They don't expire on their own. List every key (the provider's console shows them), and for each one ask: what uses this, and who owns it? Keys with no answer get switched off, especially any belonging to someone who has left. A leaver's forgotten key is one of the most common ways into a small cloud estate.

3. **Put the root account in the safe.** Every cloud account has one all-powerful login (the root or owner account) that can change anything, including the bill and every other control. The widely recommended discipline: strong MFA on it, no access keys attached to it, and no daily use. Do everyday work from a normal admin login. Write the root password down, seal it in an envelope, and put it in the safe. That envelope is a real security control.

Time required: an afternoon for MFA and the root envelope; the key audit takes an hour per account.

Move 3 — Turn on the lights

The win: a record of everything that happens, and an alarm that watches it.

Every cloud provider can keep a complete journal of every action taken in your account: every sign-in, every setting changed, every resource created. This audit log is the single most valuable thing you can have after an incident, and at small scale it costs little or nothing. It is also, in places, off by default.

Two steps:

1. **Enable the audit log in every region, every account.** Not just the region you normally use. Attackers deliberately work in the regions nobody watches. On AWS this is CloudTrail; Azure and Google Cloud have equivalents. If the provider offers it, deliver the logs somewhere your day-to-day accounts cannot delete them, so an intruder cannot erase their own footprints.
2. **Switch on the provider's threat detector and route it to a person.** The major providers each offer a managed detection service (GuardDuty on AWS, Defender for Cloud on Azure, Security Command Center on Google Cloud) that watches the logs for known attack patterns: stolen credentials in use, cryptocurrency mining, suspicious sign-ins. Switch it on, then connect its findings to an email address that a named person actually reads. An alert in a console nobody opens is not detection; it is decoration.

Time required: an hour or two, once. The watching is the provider's job; the reading is yours.

Move 4 — Close what's open to the world

The win: nothing is public by accident.

The most common cloud incident is not a sophisticated attack. It is a storage bucket, database, or server that was reachable from the internet without anyone intending it. The fix is a review plus one powerful setting.

1. **Review everything public.** Walk your provider's console and list what the internet can reach: storage buckets and their sharing settings, databases and whether they answer to the world, firewall rules that say "allow from anywhere". For each, ask one question: is this public on purpose? Your website: yes. Your backups: no.

2. **Block public storage at the account level.** The major providers offer an account-wide switch that stops storage being made public regardless of individual settings (on AWS: "Block Public Access"). If nothing in the account should ever be public, turn it on. It closes the most common exposure pattern in one step.
3. **Run the free posture check.** The providers all offer a built-in security check (Security Hub on AWS, and equivalents elsewhere). Check what it costs before you switch it on: AWS Security Hub is free for 30 days and then charges per resource. It compares your settings against a recommended baseline and lists what diverges. Run it, read the worst ten findings, and fix or consciously accept each one. That habit (a short list, reviewed monthly) is the seed of a real programme.

Time required: an afternoon for the review; the account-level switch takes minutes.

Move 5 — Write the one-page incident card

The win: the bad day runs on a card instead of on adrenaline.

Some day something will go wrong: a strange sign-in, a key in a public code repository, a bill that doubled overnight. The difference between organisations that handle it and organisations that flail is rarely tooling. It is whether anyone wrote down, in advance, who does what first.

Not a binder. A card. One page that answers:

1. **Who do we call?** The two or three people who act, with phone numbers, plus the provider's support contact and, if you have one, your insurer's incident line.
2. **What do we switch off first?** How to deactivate a user's access and revoke an access key, written as the actual console steps. The first response to a stolen credential is to make it stop working.
3. **What do we look at?** Where the audit log from Move 3 lives, so you can see what the intruder actually did.
4. **What do we not do?** Don't delete things (you may destroy the evidence that tells you what happened), and don't announce anything externally before the facts are clear.

Print it. Test it once by walking through a pretend bad morning with whoever is on it. Twenty minutes, and you will find at least one thing to fix on the card.

Time required: an hour to write, twenty minutes to test.

The printable checklist

```
THE FIVE MOVES - CHECKLIST

MOVE 1 - LIST EVERY ACCOUNT
[ ] Cloud accounts listed, each with a named owner
[ ] SaaS tools listed (card statement + connected apps)
[ ] Internet-reachable assets marked
[ ] Monthly bill review in the calendar
```

```
MOVE 2 - LOCK THE DOORS
[ ] MFA enforced for every user
[ ] Access keys listed; orphans deactivated
[ ] Root account: MFA on, no keys, sealed envelope

MOVE 3 - TURN ON THE LIGHTS
[ ] Audit logging on in every region and account
[ ] Logs delivered out of day-to-day reach
[ ] Provider threat detection on, routed to a reader

MOVE 4 - CLOSE WHAT'S OPEN
[ ] Public-access review done; surprises fixed
[ ] Account-level block on public storage (if possible)
[ ] Free posture check run; worst ten findings handled

MOVE 5 - THE INCIDENT CARD
[ ] One-page card written and printed
[ ] Walked through once as a drill
```

A short jargon translator

- **Control plane**. The steering wheel of your cloud: the console and commands that create and change things. The audit log records everything done to it.
- **CSPM (cloud security posture management)**: tooling that continuously checks your cloud settings against good practice. The free posture check in Move 4 is the starter version.
- **Root account**: the all-powerful original login at each provider. Belongs in the safe, not in daily use.
- **Access key**: a password for software. Long-lived, invisible, and the thing to audit in Move 2.
- **Shared responsibility**: the provider secures the cloud itself; you secure what you put in it and how you configure it. Every move in this guide lives on your side of that line.

What not to do yet

A short list of things that can wait, offered with respect for your time and budget:

- **Don’t buy a platform.** Until the five moves are routine, a paid security platform automates a process you don’t have yet.
- **Don’t chase a perfect inventory.** A 90% complete list maintained monthly beats a 100% complete list from last year.
- **Don’t aim for zero findings.** No estate on earth has zero findings. The goal is that the dangerous few are handled fast and the rest are handled deliberately.

- **Don’t wait for a quiet month.** There isn’t one. The five moves are sized to fit alongside a day job.

Want to see where your organisation stands? The free Cloud Security Assessment scores you across ten areas (including all five moves in this guide) in about ten minutes, entirely in your browser.

This guide offers general, plain-English recommendations drawn from widely recognised cloud security practice, not professional advice. Verify each step against your own circumstances and, where needed, a qualified professional.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience in the relevant practice area, translated into plain-language guidance for the people who run cloud security - from solo operators to security teams.

It provides **general guidance and recommended practices**. It is **not** legal advice (and not a professional audit). Every recommendation is **optional** - a widely accepted way to reduce a common risk - and following it reduces exposure to common problems but **does not guarantee security or any particular outcome**. Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with the Cloud Security Assessment.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here

Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-cloud-security

Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/cloud-security