

Stop a surprise cloud bill

Low-effort guardrails for AWS · Azure · GCP — the one-page checklist.

smallestbusiness.com

cut your cloud bill 30–60%

1 PUT A REAL CEILING ON IT

- › Set **budget alerts** at 50 / 80 / 100 / 120% (AWS Budgets, GCP Budgets, Azure Cost Management).
- › **Alerts only email you — they don't stop spend.** Build an actual kill switch: GCP budget → Pub/Sub → Cloud Function that **disables billing**; AWS Budgets **Actions** → apply a restrictive SCP/IAM policy.
- › Turn on **anomaly detection** (AWS Cost Anomaly Detection; GCP/Azure anomaly alerts).
- › Send billing alerts to a channel you **actually watch** (Slack/SMS), not a forgotten inbox.

2 LOCK DOWN API KEYS & CLIENT APPS

- › **Never ship a paid-API key in a mobile/web client.** Proxy calls through your own backend.
- › Restrict every key: **app / bundle-ID** + an **API allow-list**. Firebase: enforce **App Check** (App Attest).
- › Set **hard quotas** (per-minute / per-day) on expensive APIs — Gemini, Maps, any LLM.
- › Scan repos + git history for leaked keys (`gitleaks`, `trufflehog`); rotate on exposure.

3 TAME EGRESS — THE METER THAT GROWS WITH SUCCESS

- › Find your **Data Transfer Out** line — it scales with traffic, not features, and it's usually bigger than you think.
- › Put a **CDN** in front and cache hard. Serve heavy assets from **\$0-egress** storage (Cloudflare R2, Backblaze B2).
- › Avoid **cross-AZ / cross-region** chatter — you pay per GB just to move data inside one region.

4 KILL THE QUIET WASTE

- › **Auto-stop dev/staging** out of hours; delete forgotten environments and demos.
- › **Right-size** over-provisioned instances & databases — routinely 20–30% off the compute bill.
- › **Storage lifecycle**: expire old logs, snapshots and backups; enable S3 Intelligent-Tiering.
- › Delete **unattached disks, idle load balancers, old AMIs/snapshots, unused IPs**.

5 LIMIT WHO, WHAT & WHERE

- › **Least-privilege IAM** — only a few people can launch expensive resources.
- › Keep **service quotas low** by default; raise them deliberately, not pre-emptively.
- › **Deny unused regions** (SCP / Org policy) — stops abuse spreading account-wide.
- › Separate **prod / dev / staging accounts** under consolidated billing.

6 SECURITY IS YOUR #1 BILL RISK

- › A **leaked credential** → **crypto-mining** is the classic five-figure overnight bill. Treat it as a security problem first.
- › **MFA** on root/admin; **no long-lived root access keys**; rotate keys regularly.
- › Turn on threat detection (**GuardDuty** / equivalents); alert on new-region or sudden-spend.
- › **Tag everything** (owner, env) so you can see — and charge back — what's running.

Start here: pull last month's invoice → sort by cost → look at **"Data Transfer"** and **"NAT Gateway"** first.

smallestbusiness.com