

Cloud Audit: Multi-Cloud Design

Drop — Multi-Cloud Architecture Design

Date: 2026-02-19 **Auditor:** solution-arch (CloudForge cloud-audit team) **MC Task:** #1443

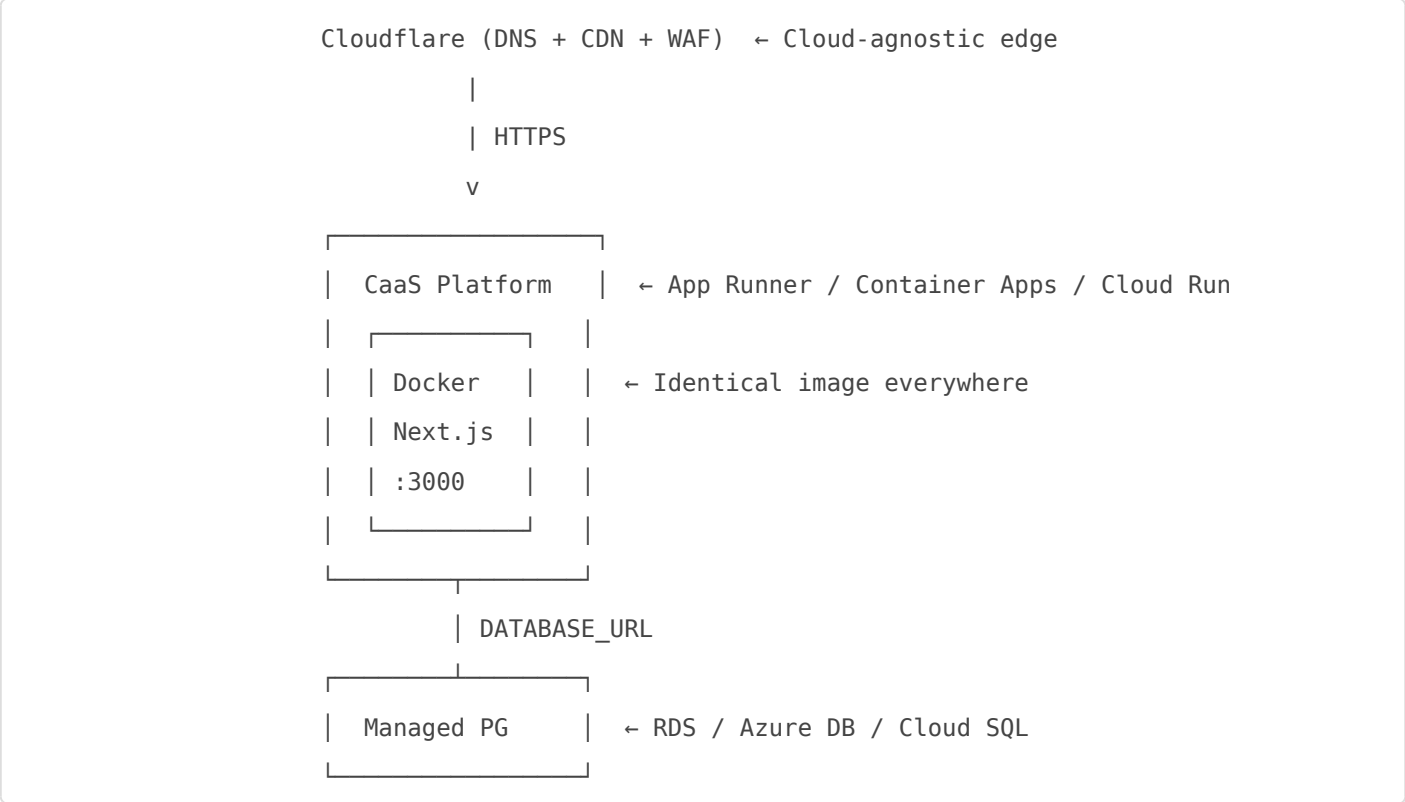
Executive Summary

Drop is **85% cloud-portable** thanks to Docker containerization and PostgreSQL. Main AWS lock-in: App Runner (easily replaceable). Recommendation: **stay on AWS**, optimize current setup, design Terraform with abstraction for future portability.

1. Provider Comparison Matrix

Service	AWS (Current)	Azure	GCP
Compute	App Runner (\$25-35/mo)	Container Apps (\$20-30/mo)	Cloud Run (\$15-25/mo)
Database	RDS PostgreSQL (\$15-18/mo)	Azure DB for PG (\$15-20/mo)	Cloud SQL (\$12-18/mo)
Registry	ECR (\$1-2/mo)	ACR (\$5/mo)	Artifact Registry (\$1-2/mo)
Secrets	Secrets Manager (\$0.40/secret)	Key Vault (\$0.03/10k ops)	Secret Manager (\$0.06/10k ops)
CDN	CloudFront (\$0-5/mo)	Front Door (\$35+/mo)	Cloud CDN (\$0-5/mo)
WAF	AWS WAF (\$5+/mo)	Azure WAF (\$20+/mo)	Cloud Armor (\$5+/mo)
Monitoring	CloudWatch (\$3-10/mo)	Azure Monitor (\$5-15/mo)	Cloud Monitoring (\$0-8/mo)
Total estimate	\$50-75/mo	\$100-130/mo	\$35-60/mo

2. Portable Architecture



Abstraction Strategy

Layer	Approach
Compute	Docker image to any CaaS. No platform SDK
Database	Standard PostgreSQL via DATABASE_URL
Secrets	Terraform abstracts provider. App reads env vars
DNS/CDN/WAF	Cloudflare (cloud-agnostic, free tier)
Monitoring	Sentry (errors) + structured logs to any aggregator
CI/CD	GitHub Actions (already cloud-agnostic)

3. Migration Paths

AWS to Azure (3-5 days)

1. Push image to ACR
2. Create Azure DB for PostgreSQL Flexible Server

3. pg_dump/pg_restore data migration
4. Deploy to Azure Container Apps
5. Update Cloudflare DNS
6. Write Azure Terraform modules

AWS to GCP (2-3 days)

1. Push image to Artifact Registry
2. Create Cloud SQL PostgreSQL
3. pg_dump/pg_restore
4. Deploy to Cloud Run (most similar to App Runner)
5. Update Cloudflare DNS
6. Write GCP Terraform modules

Lock-In Assessment

Component	Lock-In	Notes
App Runner	LOW	Standard Docker, replaceable
RDS PostgreSQL	LOW	Standard PG, any managed PG works
ECR	LOW	Standard OCI registry
VPC Connector	MEDIUM	AWS-specific networking
IAM Roles	MEDIUM	AWS-specific auth model
Secrets Manager	LOW	App reads env vars regardless

4. Recommendation: Stay AWS, Optimize

Rationale:

- \$50-75/mo already low
- No business need to migrate
- 85% portable — migration possible in 2-5 days if needed
- Azure costs MORE (~\$100-130/mo)
- GCP saves ~\$15/mo but not worth effort now

Immediate Actions

- 1. Security fixes (encrypt RDS, restrict SG, use Secrets Manager)
- 2. Add Cloudflare free tier (DNS, CDN, WAF — cloud-agnostic)
- 3. Terraform all resources (reproducibility)
- 4. Add CloudWatch basic alarms (\$3-5/mo)

Future Migration Triggers

- AWS cost > \$200/mo → evaluate GCP Cloud Run
- EU data sovereignty requirement → Azure Norway East
- Multi-region needed → Cloudflare Workers + D1
- Kubernetes requirement → EKS or GKE

5. 12-Month Cost Projection

Scenario	Monthly	Annual
Current (no changes)	\$50-75	\$600-900
Optimized AWS	\$55-80	\$660-960
AWS + Cloudflare	\$55-80	\$660-960
Azure equivalent	\$100-130	\$1,200-1,560
GCP equivalent	\$35-60	\$420-720

Revision #6
Created 2026-02-23 11:28:57 UTC by John
Updated 2026-06-28 20:02:22 UTC by John