Cloud Audit: Validation Report

Drop — Validation + Security + Cost Report

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

Executive Summary

Drop's AWS infrastructure has **3 CRITICAL** and **4 HIGH** security findings requiring immediate remediation. Current spend is ~$50-75/mo, well-optimized for scale. The application is cloud-portable (7.5/10) and the recommended path is to stay on AWS with security hardening + Terraform IaC.

---

1. Security Posture Assessment

Current vs Improved

Area	Current State	After Remediation	Risk Reduction
Secrets	Plaintext in App Runner env vars	AWS Secrets Manager	CRITICAL → LOW
RDS Access	Publicly accessible, SG open 0.0.0.0/0	Private, VPC-only access	CRITICAL → LOW
Encryption	RDS unencrypted at rest	AES-256 encryption enabled	CRITICAL → RESOLVED
Monitoring	None (no CloudWatch)	Basic alarms + Performance Insights	HIGH → LOW
WAF	None	Cloudflare WAF (free tier)	HIGH → LOW
CDN	None (direct App Runner URL)	Cloudflare CDN	HIGH → LOW

Area	Current State	After Remediation	Risk Reduction
SSL/TLS	App Runner managed cert	Cloudflare + App Runner	MEDIUM → LOW
IAM	Single user (john-deploy)	Least-privilege roles	MEDIUM → LOW

Security Findings Summary

#	Severity	Finding	Remediation	Effort
S1	**CRITICAL**	RDS publicly accessible with SG allowing 0.0.0.0/0:5432	Set publicly_accessible=false, restrict SG to VPC CIDR	1 hour
S2	**CRITICAL**	Database password in plaintext App Runner env var	Migrate to Secrets Manager, update App Runner to read from SM	2 hours
S3	**CRITICAL**	JWT_SECRET in plaintext App Runner env var	Migrate to Secrets Manager	1 hour
S4	**HIGH**	RDS storage not encrypted at rest	Enable encryption (requires snapshot + restore for existing DB)	2-4 hours
S5	**HIGH**	No monitoring or alerting configured	Add CloudWatch alarms for CPU, memory, DB connections	1 hour
S6	**HIGH**	No WAF protection	Add Cloudflare WAF (free tier)	30 min
S7	**HIGH**	No CDN (direct App Runner URL exposed)	Add Cloudflare CDN	30 min
S8	MEDIUM	Sentry DSN in plaintext (not secret, but cleanup)	Move to Secrets Manager for consistency	30 min
S9	MEDIUM	Docker image has build tools in runner (attack surface)	Remove python3/make/g++ from runner stage	1 hour
S10	MEDIUM	No structured logging (incident investigation gaps)	Add pino/winston with JSON output	2 days
S11	LOW	ECR image tag mutability (tag overwrite risk)	Set image_tag_mutability = IMMUTABLE	5 min

#	Severity	Finding	Remediation	Effort
S12	LOW	No lifecycle policy for ECR images	Add policy to clean old images	15 min

Compliance Checklist

Item	Status	Notes
GDPR data tables (consents, data_access_requests)	PASS	Schema includes consent tracking, DSAR, right to erasure
Audit logging	PASS	audit_log table with IP, user_agent, request_id
AML/KYC compliance	PASS	aml_alerts, str_reports, screening_results tables
Encryption at rest	FAIL	RDS storage unencrypted
Encryption in transit	PARTIAL	App Runner HTTPS, but RDS sslmode=no-verify
Secrets management	FAIL	Plaintext in env vars
Access control	PARTIAL	Single IAM user, no MFA enforcement
Backup & recovery	PASS	RDS 7-day automated backups
DeletionProtection	PASS	Enabled on RDS

---

2. Cost Comparison

Current AWS Spend

Resource	Monthly Cost	Notes
App Runner (1 vCPU, 2GB)	$25-35	Always-on, no auto-stop
RDS db.t3.micro	$15-18	Single-AZ, 20GB gp3
ECR	$1-2	Image storage
VPC Connector	$5	Flat fee
Data transfer	$2-5	Low traffic
Total	**$48-65**	

Optimized AWS (after fixes)

Resource	Monthly Cost	Change
App Runner	$25-35	No change
RDS (encrypted)	$15-18	No cost increase
ECR	$1-2	No change
Secrets Manager (3 secrets)	$1.20	+$1.20
CloudWatch (basic alarms)	$3-5	+$3-5
Cloudflare (free tier)	$0	Free CDN/WAF/DNS
Total	**$52-70**	**+$4-7**

Multi-Cloud Equivalent

Provider	Monthly	Annual	vs Current
AWS (optimized)	$52-70	$624-840	+$4-7/mo
Azure	$100-130	$1,200-1,560	+$50-65/mo
GCP	$35-60	$420-720	-$5-15/mo

Verdict: AWS is cost-effective. GCP saves ~$10/mo but migration effort not justified at current scale.

---

3. Risk Matrix

Risk	Probability	Impact	Current Mitigation	Recommended
Data breach via public RDS	HIGH	CRITICAL	DeletionProtection only	Restrict SG, disable public access
Secret exposure	MEDIUM	CRITICAL	None (plaintext)	Secrets Manager + rotation
Service downtime	LOW	HIGH	App Runner auto-scaling	Add health checks, CloudWatch alarms
Data loss	LOW	CRITICAL	7-day RDS backups	Add cross-region backup copy
Cost overrun	LOW	MEDIUM	None	Add AWS Budgets alarm at $100
Vendor lock-in	LOW	MEDIUM	Docker + PostgreSQL	Terraform abstraction modules
DDoS attack	MEDIUM	HIGH	None	Cloudflare WAF + rate limiting

Risk	Probability	Impact	Current Mitigation	Recommended
Compliance failure	MEDIUM	HIGH	Tables exist, no encryption	Enable encryption, structured logging

---

4. Implementation Roadmap

Phase 1: Security Fixes (Immediate — Day 1)

- ☐ Create Secrets Manager secrets (DATABASE_URL, JWT_SECRET, SENTRY_DSN)
- ☐ Update App Runner to read from Secrets Manager
- ☐ Restrict RDS security group to VPC CIDR
- ☐ Disable RDS public accessibility

- **Effort:** 4-6 hours | **Cost impact:** +$1.20/mo

Phase 2: IaC Migration (Week 1)

- ☐ Create S3 bucket for Terraform state
- ☐ Import existing resources into Terraform state
- ☐ Run `terraform plan` to verify no drift
- ☐ Add terraform-ci.yml to GitHub Actions

- **Effort:** 1-2 days | **Cost impact:** $0

Phase 3: Monitoring & Observability (Week 2)

- ☐ Enable RDS Performance Insights
- ☐ Add CloudWatch alarms (CPU > 80%, memory > 80%, DB connections > 80%)
- ☐ Add structured logging (pino) to application
- ☐ Configure Sentry properly (traces, breadcrumbs)

- **Effort:** 2-3 days | **Cost impact:** +$3-5/mo

Phase 4: Edge Security (Week 2-3)

- ☐ Set up Cloudflare (DNS, CDN, WAF)
- ☐ Custom domain (getdrop.no) through Cloudflare

- [ ] Enable Cloudflare WAF rules
- [ ] Add rate limiting at edge

- **Effort:** 1 day | **Cost impact:** $0 (free tier)

Phase 5: RDS Encryption (Week 3)

- [ ] Create encrypted snapshot from current DB
- [ ] Restore to new encrypted instance
- [ ] Update Secrets Manager with new endpoint
- [ ] Verify and swap

- **Effort:** 2-4 hours (with downtime) | **Cost impact:** $0

Phase 6: Multi-Cloud Readiness (Month 2+)

- [ ] Create Azure Terraform modules (optional)
- [ ] Create GCP Terraform modules (optional)
- [ ] Test migration to staging on alternative cloud

- **Effort:** 3-5 days | **Cost impact:** Only if migrated

---

5. Recommendations Summary

Priority	Action	Status
P0 (NOW)	Fix RDS public access + SG	Terraform module created
P0 (NOW)	Move secrets to Secrets Manager	Terraform module created
P1 (Week 1)	Enable RDS encryption	Requires snapshot/restore
P1 (Week 1)	Deploy Terraform IaC	Modules ready
P2 (Week 2)	Add monitoring (CloudWatch + Performance Insights)	In Terraform
P2 (Week 2)	Add Cloudflare CDN/WAF	Manual setup
P3 (Month 1)	Add structured logging	Application code change
P3 (Month 1)	Add graceful shutdown handler	Application code change
P4 (Month 2+)	Multi-cloud Terraform modules	As needed

Overall Assessment: Drop's infrastructure is functional but needs immediate security hardening. The Terraform IaC created by this audit provides a complete, reproducible foundation. Total

investment: ~1 week of engineering time, ~$5/mo additional cost, significant risk reduction.

Revision #6
Created 2026-02-23 11:28:58 UTC by John
Updated 2026-05-25 07:23:47 UTC by John