

SECURITY DRIFT

Security Drift Is the New Configuration Drift

Your infrastructure can be perfectly compliant
and less secure than it was yesterday.



RACK2CLOUD

Think Like An Architect.
Build Like An Engineer.

Think Like An Architect. Build Like An Engineer.

Two Different Failures

Configuration Drift

Security Drift

Declared State $\neq$
Actual State

Declared State =
Actual State

Detectable Through
Reconciliation

Often Invisible
To Reconciliation

Infrastructure
Becomes Incorrect

Infrastructure Stays Correct.
Gets Less Secure.



THE EXAMPLE

Terraform Says It's Fine.

TERRAFORM PLAN

- ✓ Security group — matches code
 - ✓ IAM role — matches code
 - ✓ Secret reference — matches code
-

EIGHTEEN MONTHS LATER

- ! IAM role — permissions accumulated
- ! Secret — never rotated
- ! Security group — legacy exception still open

Terraform reports success. Security posture worsened.



Why Drift Tools Miss It

Nothing changed.

That's the problem.

Reconciliation checks declared state against actual state.
Security entropy accumulates without moving either one.



Security Entropy Accumulation

Security posture degradation that accumulates while infrastructure remains fully converged with declared configuration state.

Declared and actual state continue to match — but the security value of that state decays over time.

FAILURE STATE: Security Baseline Divergence

Extends #4 Drift Origin Model · Mirrors #133 Policy Intent Drift



Where Entropy Accumulates

01

Patch Latency Debt

Time-since-patch accumulates silently

02

Credential Staleness

Unrotated secrets still validate

03

Permission Creep

Additive grants stay policy-compliant

04

Exposure Window Accumulation

Legacy exceptions outlive their reason

Permission Creep

Every access review adds. Almost none subtract.

- A grant added for one incident never gets revoked
- IAM policy stays exactly what was declared in code
- “Compliant with policy” and “least privilege” quietly diverge

It's the domain every architect has already lived through.

Design Against Entropy

**Security baselines must reconcile —
just like configuration baselines.**

Patch Latency Debt

Security baseline reconciliation

Credential Staleness

Automated rotation enforcement

Permission Creep

Authorization recertification

Exposure Window Accumulation

Expiry-driven exception controls

IDEMPOTENCY ≠ SECURITY

Drift monitoring solved the configuration problem.
It never solved the security one.

Rack2Cloud.com

Follow The Architect for more · [LOGO — added manually]



RACK2CLOUD
Think Like An Architect.
Build Like An Engineer.

Think Like An Architect. Build Like An Engineer.