CASE STUDY

How Coinme replaced homegrown state management with enterprise-grade infrastructure governance

Role-based access control gives technical leads scoped self-service without bypassing infrastructure policy.

Spacelift provides a consistent, auditable deployment workflow from GitLab commit through to production.

Structured rollback paths cut incident recovery time compared to a manual approach.

Summary

The infrastructure team at B2B2C crypto-enablement platform Coinme had been managing Terraform state through Amazon S3 and a collection of homegrown scripts, but this approach did not scale. The company needed fine-grained access controls and a cleaner collaboration model for technical leads. Moving to Spacelift gave the team a structured, repeatable way to manage deployments across environments and bring technical leads into the workflow without sacrificing governance.

B2B2C crypto-enablement platform Coinme is in a near-continuous state of audit, with regulators, finance teams, and state attorneys general all periodically requiring evidence of who has access to what, who approved which changes, and how the company's infrastructure is governed. Chief information security officer (CISO) Michael McMillan joined the company about five years ago, at a point when the company was transitioning out of an early startup phase. Infrastructure had largely been built by developers shipping prototypes directly to production. "When I joined, I built out the infrastructure engineering team, and we started to re-look at how we are hosting our services, securing them, and creating a repeatable, disaster-resistant environment," Michael explains.

That journey led Coinme through a familiar infrastructure-as-code (IaC) maturity arc: from manual configuration, through Terraform with state stored in Amazon S3, and ultimately to a dedicated infrastructure orchestration platform. Each step was driven by the need for governance and control that could keep pace with a growing, distributed engineering team operating under regulatory scrutiny.

The challenge for Coinme

When Coinme's infrastructure team began codifying their environment in Terraform, Amazon S3 emerged as the logical place to store state. It was technically sound because state files were centralized, accessible, and could underpin a disaster recovery posture if a region went down. However, the model's limits began to emerge as the team grew and the number of concurrent deployments increased.

State management was managed through a set of homegrown scripts that engineers ran locally against remote targets. Those scripts had to be downloaded and kept current. There was no centralized view of what was running, no mechanism to prevent two engineers from stepping on each other's work, and a significant dependency on verbal or written communication to coordinate activity.

> Running things locally against a remote target meant there had to be a lot of communication about what was going on — a warning system of, 'okay, look out, we're gonna run this thing, don't do anything for a minute
>
> **Michael McMillan**
> Chief Information Security Officer (CISO)

Recovery from failed deployments compounded the problem. When something went wrong, the team had no built-in rollback path: They had to diagnose the failure, reverse changes manually, and then re-deploy. Although the system worked, it always carried an element of risk.

Coinme operates with a two-tier engineering structure: a core infrastructure team of two engineers who own the platform, and three technical leads who are senior software developers managing their own product teams. The technical leads needed access to certain repositories and the ability to deploy specific services — but not others. GitLab handled much of the repository-level access control, but it did not provide a natural path for technical leads to do infrastructure work correctly. Without a structured way to deploy through approved workflows, the path of least resistance was to go around processes entirely. "If you don't give somebody a way to do the right thing, they're going to find the easy way to do it. And sometimes that's just going around you or going around policy and best practices," says Michael.

Why Coinme chose Spacelift

After discovering Spacelift through a YouTube recommendation, Coinme ran a proof of concept, evaluated Spacelift against HCP Terraform Cloud, and moved fully to Spacelift for infrastructure orchestration in late 2023. The decision came down to two factors that mapped directly to the team's pain points: state management and fine-grained access controls. Where Amazon S3 and scripts had been functional but brittle, Spacelift offered a purpose-built platform with those capabilities built in. "The integration and streamlined state management solved a real problem. We had a POC and quickly moved to using it in our infrastructure deployments," recalls Michael.

Coinme's Spacelift experience

Spacelift's most significant contribution was to reduce the risk profile of every deployment. With state managed through Spacelift's platform rather than scripts, the infrastructure team can work concurrently without the coordination overhead that had previously been required.

> It's much more fluid. We're communicating, we're planning, all of that's still happening, but it requires so much less fear.
>
> **Michael McMillan**
> Chief Information Security Officer (CISO)

The safety mechanisms built into the platform change the calculus around failed deployments. Previously, a failure meant manual diagnosis and recovery. With Spacelift, rollback and recovery paths are structured into the workflow. Spacelift's role-based access controls gave Coinme a way to solve the technical lead problem cleanly by enabling the team to configure exactly which stacks each person can trigger, what they can approve, and what should be restricted to the infrastructure team. The platform enforces the boundary between self-service and managed deployment without requiring additional governance overhead.

Spacelift's impact on Coinme

Coinme's infrastructure is now fully managed through Spacelift, with any remaining services not yet on the platform slated to migrate. The team runs multiple deployments per day with the confidence that control is enforced by the platform rather than relying on manual discipline and communication.

Key governance outcomes include:

- Role-based access controls that give technical leads scoped self-service without bypassing infrastructure policy
- A consistent, auditable deployment workflow from GitLab commit through to production
- Structured rollback paths that reduce incident recovery time compared to the manual approach
- A single interface for demonstrating access controls and change approvals to regulators and auditors

Collaboration is also much easier. The shift from scripts to Spacelift eliminates the coordination overhead that concurrent deployments used to involve. Engineers no longer need to announce they are about to run something and ask colleagues to stand down. Work that previously required synchronous communication now happens asynchronously through the platform's built-in state management. That reduction in coordination overhead is the difference between a workflow that scales and one that requires constant manual management.

Although Spacelift did not accelerate deployments compared to the previous Terraform workflow, it changed the cost of failure significantly. Previously, when deployments failed, recovery was time-consuming and manual. Now, the Spacelift platform absorbs that cost through structured recovery paths, making the overall time investment lower even if individual deployment times are similar. "Even though it didn't really speed us up, from my perspective it was a net savings of time — because when things didn't go right, it was a lot more work for us to fix things," concludes Michael.