Temporal

The Missing Control Layer for AI Agents

A discussion around controlling tool calls, and sandboxes



Cornelia Davis

Principal Technologist
Temporal



Today, everyone is able to ship something that works quickly...

Code-gen IDEs | Agent scaffolds | Hosted LLMs | MCP / tool registries

The first 80% has never been cheaper.

You need to add...

Every team that **ships** an AI product ends up building a number of additional things.

✓ Longer-running sessions

Hours, days, weeks — the user expects to come back and pick up where they left off.

✓ State Persistence

Multi-turn context that survives crashes, restarts, and rolling deploys without losing the thread.

✓ Storage & context cost optimization

Token cache, prompt compression, history pruning — your bill scales with conversation length.

✓ Right-sized and shaped infrastructure

Horizontal worker scale, queue isolation, and fair scheduling so one tenant doesn't starve another.

✓ Visibility into every execution

Live timeline of every LLM call, tool result, and decision — for debugging, audits, and incident response.

✓ Resilience to external failures

Rate limits, timeouts, partial responses, sandbox crashes — retry policy you don't have to hand-roll.



You need to add...

Every team that ships an AI product ends up rebuilding the same six things.

✓ Longer-running sessions

Hours, days, weeks — the user expects to come back and pick where they left off.

✓ State Persistence

✓ Storage & context cost optimization

oken cache, prompt compression, story pruning — your bill scales ith conversation length.

And CONTROL!!

✓ Right-sized and shaped infrastructure

Horizontal worker scale, queue isolation, and fair scheduling so one tenant doesn't starve another.

✓ Visibility into every execution

Live timeline of every LLM call, tool result, and decision — for debugging, audits, and incident response.

✓ Resilience to external failures

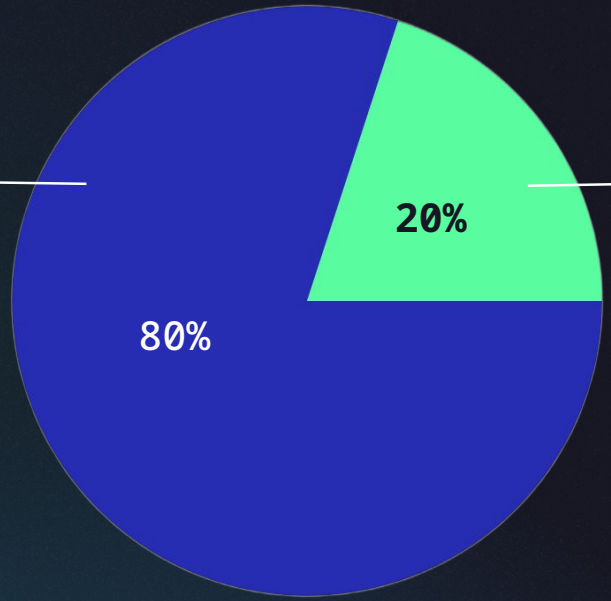
Rate limits, timeouts, partial responses, sandbox crashes — retry policy you don't have to hand-roll.

There's a fundamental challenge with modern applications

Too much of software development is spent on work that should **not** be the developer's responsibility.

Plumbing

Reliability
Scale
Data Integrity



Business Logic

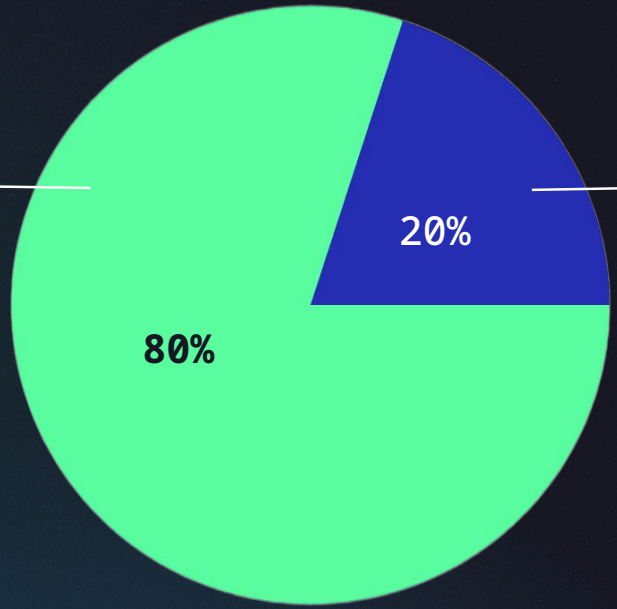
Value
Differentiators
Innovation

What if you could flip the script?

Remove the **tax** on development that slows iteration and pulls focus away from building differentiated products.

Business Logic

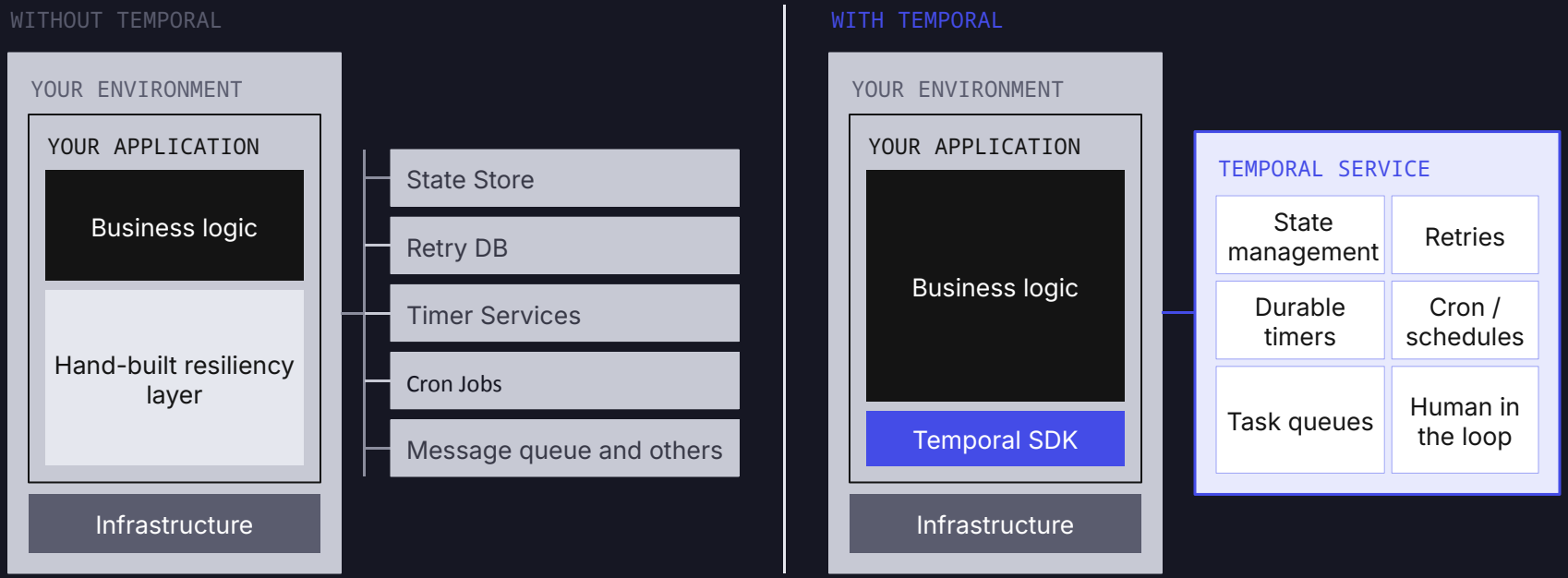
Value
Differentiators
Innovation



Plumbing

Reliability
Scale
Data Integrity

Temporal moves reliability and agent plumbing out of app code



Teams keep their application code and business logic. Temporal maintains execution state, manages retries and timers, schedules work, and waits for human decisions.

Temporal helps give AI agents more responsibility

1 LLM	2 AGENT HARNESS	3 APPROVAL	4 TRUSTED SERVICE
Requests an action	Checks policy and authority	A person decides when required	Carries out the permitted action

TEMPORAL RUNS THE BUSINESS PROCESS - THE AGENT LOOP WITH CONTROLS APPLIED

YOU OWN
Policy
Agent and approver identity
Permissions to government systems
Approval rules and interface
Preventing agents from bypassing the process

TEMPORAL PROVIDES
Durable execution
Runs the process, including government-defined checks and approvals, in the required order
Waits for approvals and continues after failures or delays
Records the request, decision, and result reported by the government service



Demo!!



WHERE IS TEMPORAL USED?

A **Temporal Workflow** defines any process or series of events that you want to guarantee execute correctly and reliably.

PROCESS

- Payment Processing
- Money Movement
- Order Management
- Bookings
- Payment Gateway
- Shopping Cart
- Logistics Management
- Customer Service
- Customer Notifications
- Marketing Campaigns
- Supply Chain

LIFECYCLE

- Inventory Management
- Menu/listing Versioning
- User Management
- Customer Lifecycle
- Subscription Lifecycle
- Inventory

OPERATIONAL

- Infrastructure Services
- CI/CD Workflows
- SaaS Provisioning
- Software Provisioning
- Server Provisioning
- Software Upgrades
- Compute Optimization
- Data Pipeline
- ETL

AI WORKFLOWS

- Agentic AI Processes
- RAG flows
- Orchestrating LLMs / GenAI
- Chatbots & Assistants
- Machine Learning
  - Training & Inference
  - Data Pipelines
- GPU Lifecycle Mgmt

Guardrails for Durable Workflows at Scale



USE CASE: AI – Internal Agent Platforms

CHALLENGES

- Supporting many teams across Ruby, Java, and Go
- Reliability is critical for payments, billing, and control planes
- Preventing workflow bugs (retries, replay, versioning) at scale

SOLUTION

- Central Temporal platform with distributed worker ownership
- Wrapped SDK with a “fat client” to simplify usage and enforce patterns
- Built guardrails: idempotency checks, replay safety, and strict versioning

"I'm ex Facebook, and I always say that privacy is to Facebook as reliability is to Stripe."

Drew Hoskins
Software Engineer, Service Platform



Source: Stripe & Temporal Webinar

One Workflow, Many AI Agents

block

USE CASE: AI – Internal Agent Platforms

CHALLENGES

- Synchronous agents timed out under heavy workloads
- AI workflows needed human-in-the-loop control
- Rapid changes risked workflow non-determinism

SOLUTION

- Rebuilt KGoose agent loop on Temporal
- Kept orchestration in Temporal and data in DynamoDB
- Added retries, guardrails, interruption, and recovery

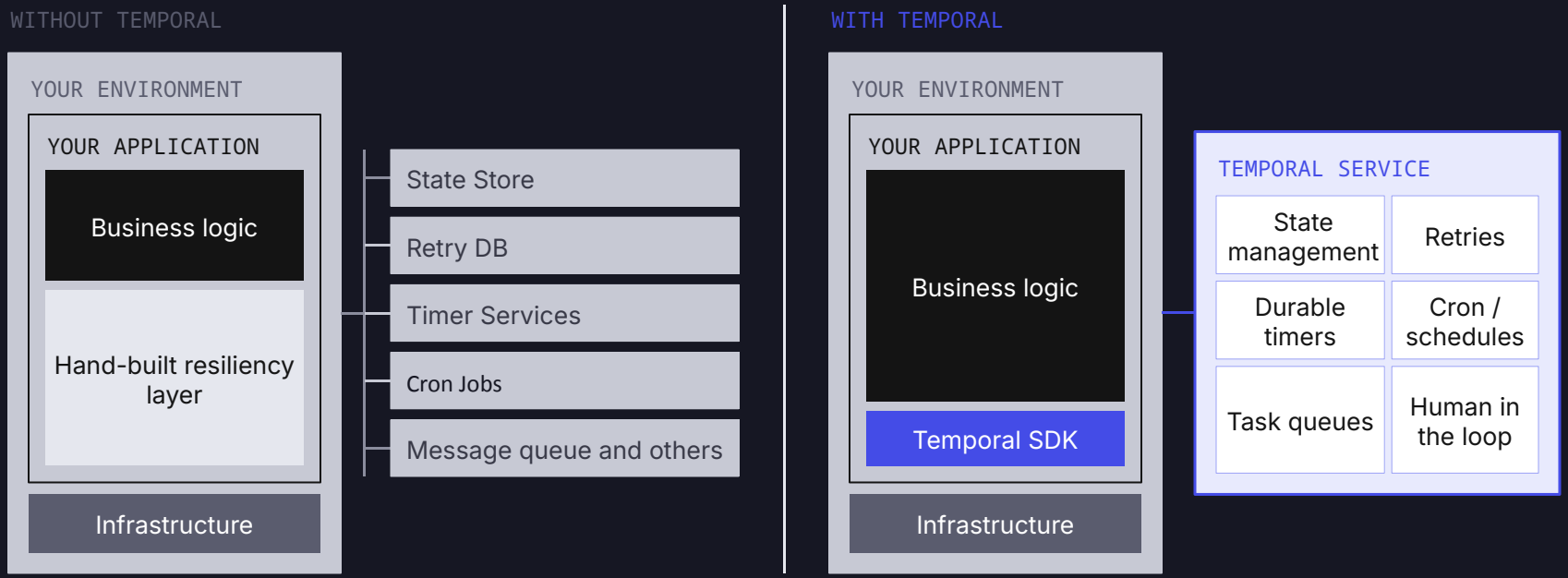
"We trust Temporal for its durability and reliability, which is key when you wanna have long-running agent loops."

Catherine Zhang
Software Engineer

100M+
weekly activities per namespace

Source: Replay 2026 presentation

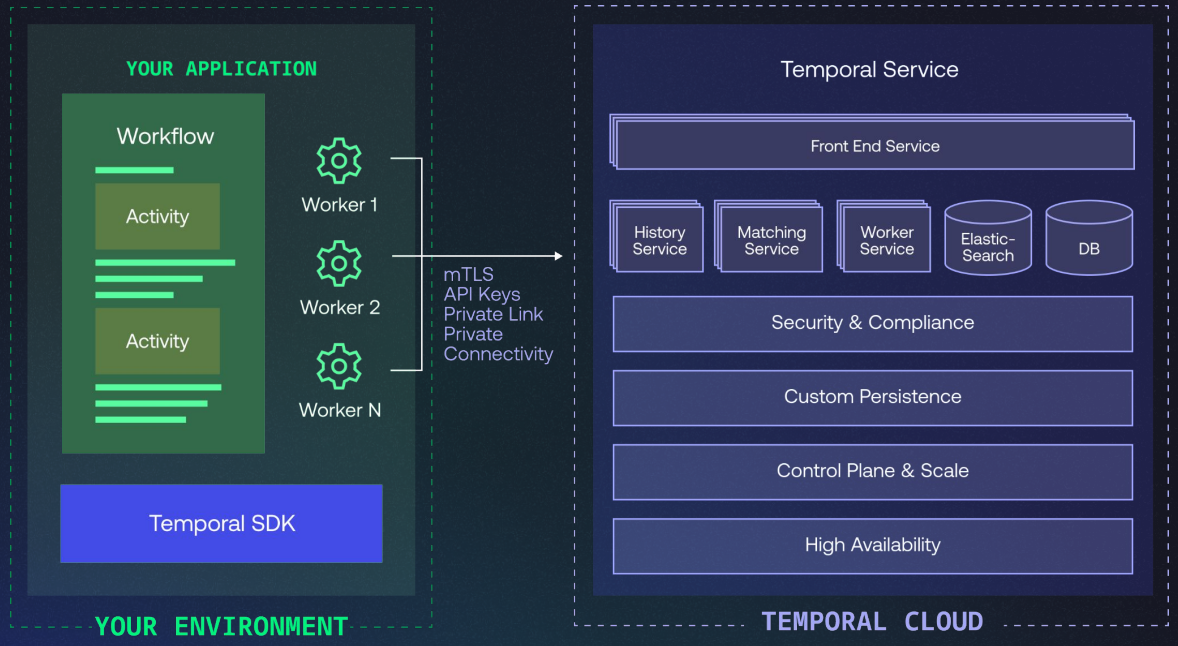
Temporal moves reliability and agent plumbing out of app code



Teams keep their application code and business logic. Temporal maintains execution state, manages retries and timers, schedules work, and waits for human decisions.

Temporal Cloud: How does it work?

Continue executing your workflow code in your environment; our team manages the Service

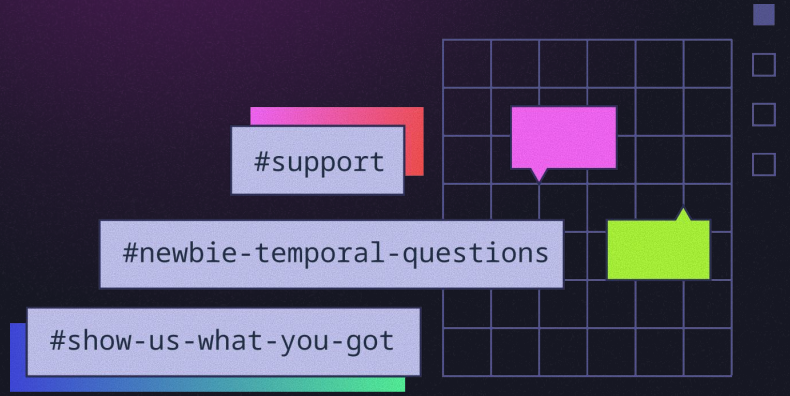


Eliminate the need to manage a complex, highly available Service

Temporal Cloud Service is optimized with:

- Security (RBAC, SSO with SAML, etc.)
- Compliance
- Control Plane
- Custom Persistence Layer
- Highly available out of the box

Join the Conversation



Ask questions in the Temporal Slack community.

t.mp/slack to join

Subscribe for our monthly community newsletter.

Stay up to date with the latest product updates, releases, and more.

temporal.io/community to subscribe

