Runtime Protection for a Nation's Real-Time Payment Rails

How a country-scale payments operator used AppSentinels to stop business logic abuse in real time, from partner retry-flooding that games settlement to threat actors probing money-movement workflows, across 650M+ transactions a day that gateways and rate-limiters can't police.

EXECUTIVE SUMMARY

A national payments infrastructure operator runs the real-time rails that move money between hundreds of member banks and payment apps at country scale. Its APIs govern fund movement, settlement, refunds, and mandates — logic where valid-looking traffic can still do damage. The operator faced two runtime problems conventional controls couldn't address: partners abusing retry and reversal logic for competitive advantage on the rails, and threat actors probing money-movement workflows for authorization and sequencing gaps. API gateways and WAFs confirm a request is well-formed; rate-limiters cap volume bluntly. Neither can tell an abusive pattern of valid calls from legitimate use. AppSentinels applied runtime protection over the operator's APIs through a Business Logic Graph, evaluating behavior against ownership and intent, blocking abuse as it happens, at full payment-system scale.

The Challenge: Abuse That Hides in Valid Traffic

At payment system scale, the dangerous failures aren't malformed requests, they're patterns of perfectly valid ones. Three stood out, and none is something a gateway or rate-limiter can resolve.

01 Partners gaming the rails with aggressive retries

To win against competitors on settlement speed and success-rate optics, some payment apps flooded the system with aggressive retries and reversals, each call individually valid, the pattern abusive. It degraded the rails for every other participant, and blunt rate-limiting couldn't separate the abuse from legitimate spikes without harming good traffic.

02 Threat actors probing money-movement logic

Beyond partner abuse, the rails are a constant target for actors testing authorization, ownership, and sequencing in fund-movement workflows, the high-value failures that pass validation but violate intent.

03 Country-scale volume with zero tolerance for error

At 650M+ transactions a day, enforcement has to be real-time and precise: every false block is a failed payment; every missed abuse is financial and systemic risk. Manual review and syntax-based tools can't operate at that line rate or that level of nuance.

> "Our rails have to be fair and available to every participant, every second. AppSentinels lets us judge traffic by intent, not just whether it's well-formed, and stop abuse in real time without ever slowing a legitimate payment."
>
> — **Security Leader, National Payments Operator**

The Solution

AppSentinels brought runtime protection to the payment layer through the **Business Logic Graph**, a live model of every API, identity, object, and access path, so each call is judged against ownership and intent, not just whether it's well-formed.

Behavioral Abuse Detection

Distinguished abusive retry and reversal patterns from legitimate traffic spikes, so partner gaming could be throttled or blocked without penalizing good traffic.

Partner-Scope Enforcement

Checked every member-bank and payment-app call against the access actually granted to it, holding each partner to its real authorization boundary in real time.

Money-Movement Workflow Protection

Watched fund-movement sequences for authorization, ownership, and sequencing abuse, blocking the multi-step manipulation that single-request inspection misses.

Enforcement at Payment-System Scale

Ran inline at country-scale transaction volume, applying business logic judgment at line rate rather than after the fact.

650M+/day	15	99%
transactions protected in real time	APIs under runtime protection	reduction in abusive retry volume

Business Outcomes

Fair access restored to the rails

Partner retry-flooding meant to out-compete rivals is now detected as a pattern and contained, protecting performance and fairness for every participant.

Every partner held to its real scope

Member-bank and payment-app traffic is continuously verified against granted authorization instead of assumed trust.

Money-movement abuse blocked at intent, not syntax

Authorization, ownership, and sequencing manipulation in fund-movement workflows is caught in real time, where validity checks and rate-limiters are blind.

Abusive retry flooding contained at the source

Within the first weeks of enforcement, behavioral detection contained the retry-and-reversal flooding, reducing abusive retry traffic by 99% and returning headroom and predictable latency to the rails for every legitimate participant.

About AppSentinels

AppSentinels is the Business Logic Security platform for modern applications. Built around the Business Logic Graph, it delivers continuous discovery, automated stateful red-teaming, and runtime protection across AI agents, MCP servers, APIs, and the workflows that connect them. First-generation API security tools inventoried endpoints; AppSentinels secures the logic behind them, the layer where breaches happen.