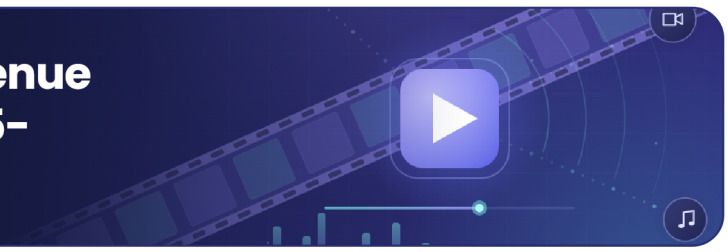
Protecting Subscription Revenue and Partner Trust Across a 15-Billion-Call API Ecosystem



How a global media enterprise shut down unauthorized plan extensions, stopped geo-pricing fraud, and made every partner API call attributable with discovery, testing, and runtime enforcement unified on one Business Logic Graph.

EXECUTIVE SUMMARY

A global media enterprise runs subscription video, broadcast, and digital content across multiple countries and price tiers. APIs drive entitlements, plan upgrades, and regional pricing, and a network of distribution and reseller partners extends the platform into new markets. That partner ecosystem fuels growth, but every integration is also an edge the security team must trust without fully seeing. AppSentinels brought discovery, testing, and runtime enforcement under one Business Logic Graph, turning three revenue-leaking blind spots into closed, monitored workflows and collapsing partner-incident attribution from days to minutes.

The Challenge

Three abuses were compounding faster than existing tools could track them, and each one mapped directly to leaked revenue.

01 Entitlements extended with no payment behind them

Renewal, trial, and upgrade endpoints were chained in sequences the enterprise's own apps never used, unlocking premium access with no payment event. Each call passed validation on its own; the abuse only appeared in the sequence, and nothing was watching sequences.

02 Geo-pricing claimed outside its market

Regional pricing relies on location signals to set the right price per market. Bad actors spoofed those signals to claim promotional rates never meant for them, turning a localization feature into a recurring margin leak.

03 Partner traffic no one could attribute

Each distribution and reseller partner connected through its own integration, but the team had no consistent way to see which partner called which API, or whether traffic matched the access actually granted. Attribution took days by which point the next abuse pattern was already running.

> "Our digital platforms rely heavily on APIs to power user experiences, and we constantly face attempts to gain unauthorized access or reach sensitive data. AppSentinels helped us uncover hidden vulnerabilities and significantly strengthen the security of our critical application workflows."
>
> — **Security Leader, Global Media Enterprise**

The Solution

AppSentinels mapped the enterprise's entire API estate into a **Business Logic Graph**: a live model of every API, partner identity, entitlement object, and access path. Behavior is evaluated against ownership and intent, not just request validity.

Continuous Discovery

Mapped every API across entitlement, pricing, and partner surfaces, attributing each endpoint to the identity authorized to call it.

Stateful Red-Teaming

Exercised entitlement workflows end to end, surfacing the exact sequences that could extend access without payment, the paths single-endpoint scanning cannot reach.

Runtime Protection

Correlated location, identity, and pricing signals to block geo-pricing fraud as it happened, and checked every partner call against that partner's real entitlement scope.

Unified Lifecycle Coverage

Closed the loop: a risky sequence caught in testing becomes a runtime rule, and a runtime anomaly traces straight back to the responsible partner.

15B	1K+	100%
API calls / month	APIs discovered & protected	UAT & production coverage

Business Outcomes

- **Revenue protected at the sequence, not the request**
  The workflows that let valid-looking calls chain into free entitlement upgrades are now closed in testing and enforced at runtime.
- **Geo-pricing fraud became a detectable pattern**
  Promotional pricing works as a growth lever again instead of a leak, with spoofed-location requests blocked in real time.
- **Partner traffic is attributable by default**
  Implicit trust gave way to continuous verification of what each partner's traffic is allowed to do and when something is off, it arrives already tagged with its partner, API, and workflow.
- **Investigation collapsed from days to minutes**
  At 15 billion calls a month, that is the difference between catching an abuse pattern while it runs and reconstructing it after the loss.

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.