Preventing Healthcare Fraud and Protecting Patient Data Across a Multi-Hospital Digital Ecosystem

How a leading healthcare provider secured AI agents, APIs, and business logic to prevent unauthorized insurance claims and protect PHI.

EXECUTIVE SUMMARY

A leading U.S. healthcare provider operating a large digital ecosystem of patient portals, insurance platforms, laboratory systems, pharmacy integrations, and AI-powered healthcare services faced growing risks from shadow APIs, business logic vulnerabilities, unauthorized insurance claims, PHI exposure, and insufficient governance of AI agents. To address these challenges, the organization deployed AppSentinels Business Logic Security Platform to continuously discover APIs and AI assets, identify business logic risks, and provide real-time protection for critical healthcare workflows.

The Challenge: Healthcare APIs are the Primary Attack Surface

01 Incomplete API Inventory

Hundreds of legacy, partner, and shadow APIs remained undocumented across acquisitions and digital transformation initiatives.

02 Business Logic Abuse

Attackers bypassed technical controls by exploiting legitimate healthcare workflows rather than breaking authentication.

03 AI Agent Risk

New AI-powered scheduling assistants and patient support agents accessed sensitive APIs with minimal visibility into downstream business actions.

04 Compliance Burden

Preparing evidence for HIPAA, GDPR, and HITECH audits required extensive manual effort across multiple environments.

> "AppSentinels gave us something we didn't have before: one place to see every API and every AI agent touching patient data. We went from reacting to fraud after the fact to stopping it in the workflow, before a claim was ever paid."
>
> — **VP of Information Security, Leading U.S. Healthcare Provider**

The Solution

AppSentinels delivered comprehensive business logic security by continuously discovering APIs and AI assets, proactively identifying exploitable business logic vulnerabilities, protecting healthcare workflows at runtime, and governing AI agents across the healthcare ecosystem.

Continuous Discovery

Continuously discovered APIs, AI agents, MCP servers, shadow assets, sensitive data flows, and healthcare business workflows to maintain complete visibility across the attack surface.

Automated Red-Teaming

24*7 simulation of real-world business logic attacks, including BOLA, BFLA, insurance fraud, prompt injection, and AI agent abuse to identify exploitable vulnerabilities before attackers could.

Runtime Protection

Monitored healthcare transactions in real time to detect and block unauthorized access, insurance fraud, AI agent misuse, and business logic attacks without disrupting clinical operations.

AI Security Governance

Continuously validated AI agent permissions, MCP server configurations, tool access, and policy compliance to ensure AI systems operated securely within approved healthcare workflows.

100%	99%	85%
API Visibility Across 4,500+ APIs and AI agents	Business Logic Attack Prevention Against insurance fraud and PHI abuse	Faster Compliance with HIPAA, GDPR & HITECH audit readiness

Business Outcomes

- **Full API Visibility**
  Discovered and secured shadow APIs across hospitals, partner systems, cloud applications, and legacy healthcare platforms.
- **Reduced Business Logic Exploits**
  Blocked nearly all attempts to manipulate insurance claims, abuse patient workflows, and exploit authorization weaknesses.
- **Accelerated Compliance**
  Automated evidence collection and continuous policy validation reduced HIPAA, GDPR, and HITECH audit preparation from weeks to hours.
- **Improved AI Security**
  Established continuous governance over AI agents interacting with patient records, scheduling systems, and insurance workflows.

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.