



# Bolster AI App Store Monitoring & Takedowns

**Eliminate Fake Apps. Defend Your Brand Across Apple, Google Play, and Beyond.**

Fake and malicious apps are showing up across official and third-party app stores—undermining customer trust and putting user data at risk. Bolster’s App Store Monitoring & Takedowns module scans the full mobile app landscape to identify and remove fraudulent apps fast, keeping your brand and users safe.

## Why Monitor the App Store?



### Protect Brand Trust

Counterfeit apps confuse customers, erode confidence, and damage your reputation.



### Prevent Malware and Data Theft

Fake apps often contain spyware or credential-stealing code—putting users and your brand at legal and financial risk.



### Stop Revenue Diversion

Unauthorized apps steal installs, in-app purchases, and subscription revenue meant for your legitimate offerings.



### Avoid Platform Policy Violations

Fake apps can trigger IP conflicts, negative reviews, or get your real app flagged or delisted.



### Keep Up with a Fragmented Threat Landscape

New marketplaces and upload methods emerge constantly—automated monitoring is essential.



## Key Benefits

### AI-Powered Detection of Fake and Impersonated Apps

Identify unauthorized listings using advanced models trained on your brand assets, keywords, publisher history, and behavioral signals.

### Coverage Across Global App Stores

Monitor Apple App Store, Google Play, and a wide range of third-party and regional marketplaces, including APK sites and OEM-specific stores.

### Automated Takedown Workflows

Submit and track takedowns with one click. Bolster handles platform-specific forms, follow-ups, and escalations.

### Centralized Visibility and Control

Triage incidents, prioritize enforcement, and track outcomes in a unified dashboard that integrates with your broader threat response stack.

### Repeat Offender and Trend Analysis

Track malicious publisher patterns and identify recurring abuse themes to get ahead of future threats.



# Bolster AI App Store Monitoring & Takedowns

## ✓ Core Capabilities



Detection of fake, cloned, and malicious mobile apps



AI analysis of app metadata, branding, publisher behavior, and permissions



Global monitoring across Apple, Google, third-party Android, and regional app stores



End-to-end takedown automation and case tracking



Centralized dashboard for response and reporting



Intelligence on abuse trends, threat actors, and high-risk regions

## What Makes Bolster Different



### Best-in-Class Detection Accuracy

Bolster's models are trained on billions of real-world threats for unparalleled precision—no keyword lists or static rules.



### Industry-Leading Takedown Success

Over 95% takedown success rate across supported platforms, with average response times measured in hours—not days.



### Lightning-Fast Deployment

Get up and running in days with no heavy integration lift.



### Seamless Security Stack Integration

Connect to SOAR, SIEM, Slack, and ticketing systems to streamline enforcement and reporting.



### Hybrid Automation + SOC Support

Automated detection and takedowns backed by human analysts for edge cases and escalations.

## Get Started with Bolster

Fake apps are more than a nuisance—they're a brand and security risk. Bolster helps you find and remove them before they reach your customers.

[Request a Demo](#) 