approov
mobile security

CASE STUDY

Securing Democracy's Digital Infrastructure

How Approov Mobile App Protection Defended a National Election from Automated Voter Fraud

At a Glance

Client	National Election Commission (anonymized at client request)
Challenge	Emulator-based bots attempting mass fraudulent voter registration via the commission's mobile app API
Solution	Approov Mobile App Protection integrated with Cloudflare API Shield & Bot Management
Outcome	100% of fraudulent emulator-based registration attempts blocked; app remained fully operational through Election Day

The Stakes

Every democratic election depends on trust — trust that votes are counted fairly, that voter rolls are accurate, and that the digital systems underpinning the process are secure. When a national election commission deployed a mobile application to modernize its electoral process, it gave millions of citizens a powerful new tool: the ability to register to vote, request a paper ballot, and track its delivery — all from their phones.

But that same openness created a critical vulnerability. The mobile app's backend APIs, which processed voter registrations, were accessible to anyone who could imitate the app — and sophisticated bad actors knew it.

The Threat

In the lead-up to a hotly contested national election, politically motivated attackers identified that the commission's mobile API was a backdoor into the voter registration system itself. Using automated scripts and device emulators, they began attempting to register voters at scale — fabricating identities, flooding the system with fraudulent requests, and threatening to corrupt the integrity of the electoral roll before a single legitimate ballot was cast.

This was not opportunistic hacking. It was a coordinated, deliberate attempt to undermine a free and fair election through manipulation of the digital registration infrastructure.

The attack surface was the mobile app's API. With no mechanism to distinguish a genuine voter using a real device from an emulator running a bot script, the commission faced an existential threat to the credibility of the entire electoral process.

The Solution: Approov + Cloudflare

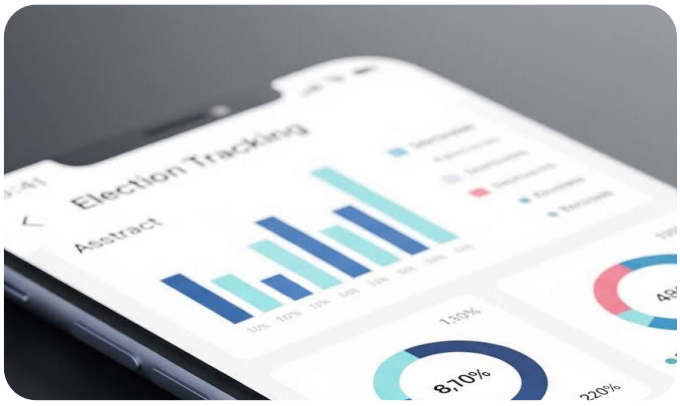
The Election Commission deployed Approov Mobile App Protection, integrated with Cloudflare's Enterprise Bot Management and API Shield services, to close that gap entirely. The solution operated on two reinforcing principles:

- **App Attestation at the Source:** The Approov SDK was embedded directly into the official mobile application. Before any request could reach the voter registration API, Approov's remote attestation service verified in real time that the request originated from a genuine, unmodified copy of the official app, running on a real, clean device. Emulators, rooted devices, repackaged apps, and automated scripts were blocked at the point of contact — before they could touch the API.
- **Unified API Defense with Cloudflare:** Cloudflare's API Shield and bot management layer provided network-level protection, filtering non-human traffic at scale. Combined with Approov's device-level attestation, the result was a closed loop: only genuine apps on genuine devices, verified in real time, could access the voter registration endpoints. The mobile app ceased to be a vector for API abuse.

The Result

The attacks failed. Every emulator-based attempt to register fraudulent voters was detected and blocked automatically. The voter registration API remained available exclusively to real citizens on real devices, ensuring the integrity of the electoral roll was maintained throughout the registration period and on Election Day itself.

The commission's mobile app delivered fully on its promise — enabling legitimate voters to register, request ballots, and track their receipt — without a single fraudulent registration bypassing the Approov-protected gateway. Essential election information reached hundreds of thousands of voters without interruption.



"Protecting a national election is one of the most consequential applications of mobile security technology. By ensuring that only genuine apps on clean devices can access voter registration APIs, Approov closes the door on the kind of automated, large-scale fraud that can corrupt an electoral roll before the election even begins. This is what defending democracy's digital infrastructure looks like."

- Ted Miracco, CEO at Approov

Summary

Election authorities worldwide are modernizing — and with modernization comes exposure. Mobile apps for voter registration, ballot tracking, and electoral information are powerful tools. But an unprotected mobile API invites manipulation at scale.

This threat isn't unique. Automated bot attacks on voter systems, emulator-based fraud, and mobile API abuse are growing global risks. The question is not if your election infrastructure will be targeted — it's whether you are prepared.

Approov's approach is decisive: if a request doesn't come from a verified app on a clean device, it never reaches your API. No token or workaround can grant an emulator or script access. Attackers find nothing to exploit.For election commissions committed to free, fair elections, Approov provides the same assurance for digital infrastructure that physical security provides for the ballot box.