NowSecure | U.S. Department of JUSTICE

Case Study | **Federal**

# Department of Justice Enforces Mobile Policy

NowSecure Platform, Academy and Workstation empower the agency to better manage mobile app risk.

## About

The United States Department of Justice federal executive department aims to uphold the rule of law, keep the country safe and protect civil rights. Under the leadership of the Attorney General of the United States, the Justice Department employs more than 115,000 people and comprises more than 40 separate component organizations such as the Civil Rights Division, Federal Bureau of Investigations, Drug Enforcement Agency and Bureau of Alcohol, Tobacco, Firearms and Explosives.

## Executive Summary

Entrusted with protecting national security, the U.S. Department of Justice (DOJ) needs to be cautious about the mobile apps employees use to avoid compromising sensitive data or placing them at risk. The DOJ proactively manages its mobile app portfolio by vetting mobile apps from the public app stores prior to installation.

The Justice Department uses the NowSecure Platform automated mobile application security testing software, NowSecure Workstation pen testing toolkit and NowSecure Academy online learning to achieve the following benefits:

- Gain visibility into the security and privacy risks of Android and iOS mobile apps
- Continuously monitor its mobile app portfolio for new supply-chain risks
- Enforce policy and comply with an array of federal mandates

> **"It's a huge workload lifted from my mobile security team."**
>
> — Mike McHugh, *Mobile Security Program Manager*, Department of Justice

## The Story

Mobile apps power productivity across the agency, but vulnerable mobile apps and those that violate regulations or policies present risks to the public sector and businesses alike. U.S. government agencies must ensure the mobile apps used by their workforces guard against supply-chain vulnerabilities and data collection by adversaries.

Privacy poses a key concern for the DOJ. "Location services may be completely necessary for weather apps so you can get accurate forecasts," says U.S. Department of Justice Mobile Security Program Manager Mike McHugh. "But if you're a member of the FBI tracking a suspect, your location becomes a very sensitive piece of information."

The DOJ reduces risk by controlling mobile app usage, proactively evaluating mobile apps for security, privacy and compliance issues and approving only those deemed safe. McHugh's team relies on NowSecure Platform for mobile app vetting and continuous supply-chain risk monitoring to whitelist mobile apps and gain visibility into changes that introduce security or privacy vulnerabilities. In addition, it uses the NowSecure Workstation pen testing toolkit for hands-on analysis of mobile apps that require a deeper investigation.

Assessing each and every mobile app that users request simply isn't possible without automated mobile application security testing. Manually pen testing a single mobile app

takes days and cannot scale to accommodate hundreds of mobile apps. But NowSecure Platform enables the DOJ to vet mobile apps in as little as 30 minutes. "It's a huge workload lifted from my mobile security team," says McHugh.

## Automation in Action

The DOJ established its mobile app vetting program because it suffered from a lack of visibility into the risks of mobile apps used by its workforce. After evaluating several solutions, McHugh selected NowSecure Platform as a key element of his agency's Mobile Risk Dashboard.

NowSecure Platform conducts static, dynamic, interactive and API security testing of Android and iOS mobile apps published in mobile app stores to check for security and privacy issues, calculate a risk score and generate a list of third-party components and dependencies. The agency integrated NowSecure Platform with VMware AirWatch enterprise mobility management software and Splunk for analytical insights.

The Mobile Risk Dashboard empowers McHugh's security team to track mobile app and mobile device risk and move to a whitelist approach in which only approved mobile apps are allowed to be used on government-issued mobile devices. The AirWatch suite performs an inventory of the mobile apps running on government devices and checks against the master list of allowed apps. NowSecure Platform conducts continuous monitoring of mobile apps as new versions get released and the dashboard will notify the security team if a mobile app falls below a certain risk score threshold.

When users request to use a mobile app that's not on the approved list, the security team tests it in NowSecure Platform and occasionally calls on NowSecure Workstation to perform a deeper review using pen testing techniques.

## Partnering with NowSecure

McHugh likes the NowSecure Platform Policy Engine feature that enables him to customize security policies tailored to risk level. The agency enforces four different policies depending on the department. He also appreciates the reporting capabilities of NowSecure Platform. The NowSecure executive reports contain a concise summary, recommendations and evidence so his team no longer has to compile their own reports.

The third-party component list that NowSecure Platform generates also proves helpful to the agency's supply-chain risk management team.

> **"The level of customer support is a huge differentiator for NowSecure and the product is great."**
>
> — Mike McHugh, *Mobile Security Program Manager, Department of Justice*

"We have a long history of working with NowSecure," says McHugh. He chose to partner with the company because of its maturity, expertise, completeness of the solution and fact that NowSecure Platform integrates with AirWatch and Splunk. "The level of customer support is a huge differentiator for NowSecure and the product is great," he says. McHugh marvels at the access he has to NowSecure Founder Andrew Hoog to make product suggestions.

"DOJ has led a market-leading implementation of mobile app security through the integration of automated security testing to help achieve a well-managed and controlled mobile app portfolio," says Hoog. "Mike's ability to implement a combined service with a robust outcome has driven transformational improvements in the agency's visibility into and management of mobile supply-chain risk."

The DOJ recently began integrating NowSecure Academy online mobile app security and developer training into its onboarding program for new and existing cybersecurity personnel. The NowSecure Academy expert-led learning program and certifications impart foundational knowledge of the growing mobile AppSec arena as well as best practices for mobile app pen testing.

Going forward, McHugh plans to expand the Mobile Risk Dashboard throughout the DOJ and will soon offer the mobile app vetting service to other federal civilian agencies. "Agencies are keen to offload the responsibility of mobile security and we can do that for them at a cost-effective rate," he says.