NowSecure™

U.S. MARSHALS SERVICE PURSUES MOST-WANTED MOBILE APPS

Federal protection agency arms itself with NowSecure application security testing to guard against unsafe commercial apps and aid mobile transformation.

ABOUT

Formed in 1789, the U.S. Marshals Service was the first federal law enforcement agency in the United States. Today, more than 5,000 marshals, deputy marshals, criminal investigators, detention enforcement officers and administrative staff work for the Department of Justice component. The U.S. Marshals Service mission includes protecting the federal judiciary, apprehending fugitives, seizing assets, housing and transporting prisoners, operating the Witness Security program and operating the "15 Most Wanted" program.

EXECUTIVE SUMMARY

The U.S. Marshals Service faced challenges determining which commercial mobile apps from the public Apple® App Store® and Google Play™ stores were trustworthy, potentially putting the lives of officers and those they protect at stake from data loss or privacy compromise. Seeking greater insight into the trustworthiness of apps, the agency sought a mobile testing solution and expert services to better manage risk and found a solution in NowSecure.

The NowSecure mobile application security deployment achieved the following benefits:

- Granular mobile app security assessment provides a high degree of confidence and coverage
- Speedy testing cut through the backlog to allow employees access to more third-party apps
- Strengthened application security and increased mobility

"We rarely get things that are ready to go out of the box, but when we received the NowSecure solution, we were up and running the same day."
— Derrick Smith, CEO, NSight365

THE STORY

Given the sensitive and confidential nature of U.S. Marshals' investigations at home and abroad, the cybersecurity team frequently nixed user requests for access to particular mobile apps. Of immense concern is the prospect of third-party iOS and Android apps leaking data or communicating with adversarial nations like China or Russia.

"You don't know who has developed an app, what kind of coding practices they've used, is there malicious intent, who these apps talk to, what kind of access the apps can gain on mobile devices, there are really a lot of unknowns," says Derrick Smith, CEO of NSight365, a government subcontractor company that aids the U.S. Marshals with application security.

Although the agency received reports from an outside vendor, they contained generic information such as whether apps used a camera or microphone. The reports "weren't that helpful and took

hours or days to receive." That led Smith to perform a deeper analysis of mobile apps by manually sniffing packets and compiling reports, but that was a laborious, painstaking, process that he sought to automate. Compounding the problem, the mobile security team faced a surging backlog of commercial apps to evaluate amidst the agency's migration from 5,000 BlackBerry devices to Apple iPhones.

THE SEARCH FOR A SOLUTION

After the U.S. Marshals CISO agreed more robust insight and coverage of mobile apps used by the agency would be beneficial, Smith began exploring automated mobile application security testing solutions.

Some companies required the customer to submit apps to review, but omitted specific details behind their recommendations when returning results. "I didn't want to rely on something that someone else was saying and sign the verification without knowing exactly how those results were created," Smith explains.

> *"If apps are developed by high-threat nations, we won't use them."*

As part of the evaluation process, one of the products Smith's team experimented with was the NowSecure mobile application vulnerability assessment and penetration testing tools. Analysts used the solution to launch man-in-the-middle attacks and obtain feedback about potential security shortcomings, such as retaining sensitive information in memory or transmitting passwords in cleartext. "The level of detail that we were able to obtain really drove excitement," Smith says.

Given the results of the evaluation, Smith felt assured that the NowSecure partnership met the agency's needs. "I did not want to make a mistake on the government's behalf," he says. "By the time I made this recommendation, I felt confident that NowSecure was the right vendor and the product was best."

NowSecure provided the U.S. Marshals team with training, making it easy for the group to quickly utilize the testing tool. "We rarely get things that are ready to go out of the box, but when we received the NowSecure solution, we were up and running the same day," Smith says.

ENHANCING MOBILE APPSEC

Faced with a backlog of about 150 user-requested apps to evaluate, the U.S. Marshals mobile app security team hit the ground running to keep up with an onslaught of new requests. After performing an environment-wide app discovery initiative, the team discovered that there were about 4,800 untested apps in the mobile environment. But by the time the iPhone rollout was complete, Smith's team had tackled the queue of requested apps, and focused the bulk of their time and attention on mission-critical apps.

Smith brought in two additional security professionals to test apps. The NowSecure solution enables them to quickly test an app in less than an hour, leaving more time for them to devote to analysis. "The longer we use the product, the more efficient we have become at evaluation," Smith says. The group provides the CISO with a report summarizing key test areas, noting issues identified, risk level of those findings, overall risk level for the application, and any recommendations.

The level of detailed testing enables the agency to permit the use of more apps, including lifestyle apps such as fitness trackers or games. "It helps boost morale of our users," says Smith. When apps are denied or restricted, his team recommends workaround measures to reduce the risk of compromise or data loss, such as disabling access to the camera.

Going forward, user requests continue to grow thanks to the availability of thousands of third-party apps. "We've been gaining more experience and skill sets in performing deep assessments of mobile apps," Smith says. "I'm proud of my team for contributing to mobile application security and helping to make the U.S. Marshals stronger."