How World-Class Organizations Scale Mobile App Security & DevSecOps

Discover seven proven ways to drive speed and productivity while reducing risk.

NowSecure™

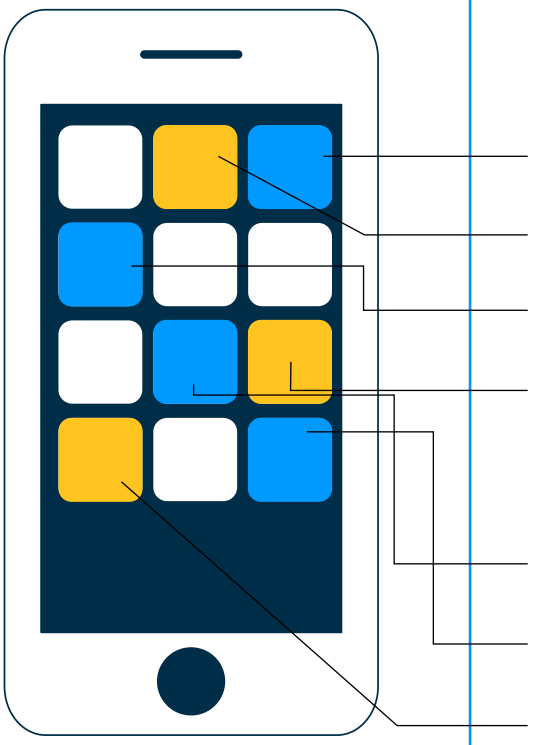


TABLE OF CONTENTS

Introduction

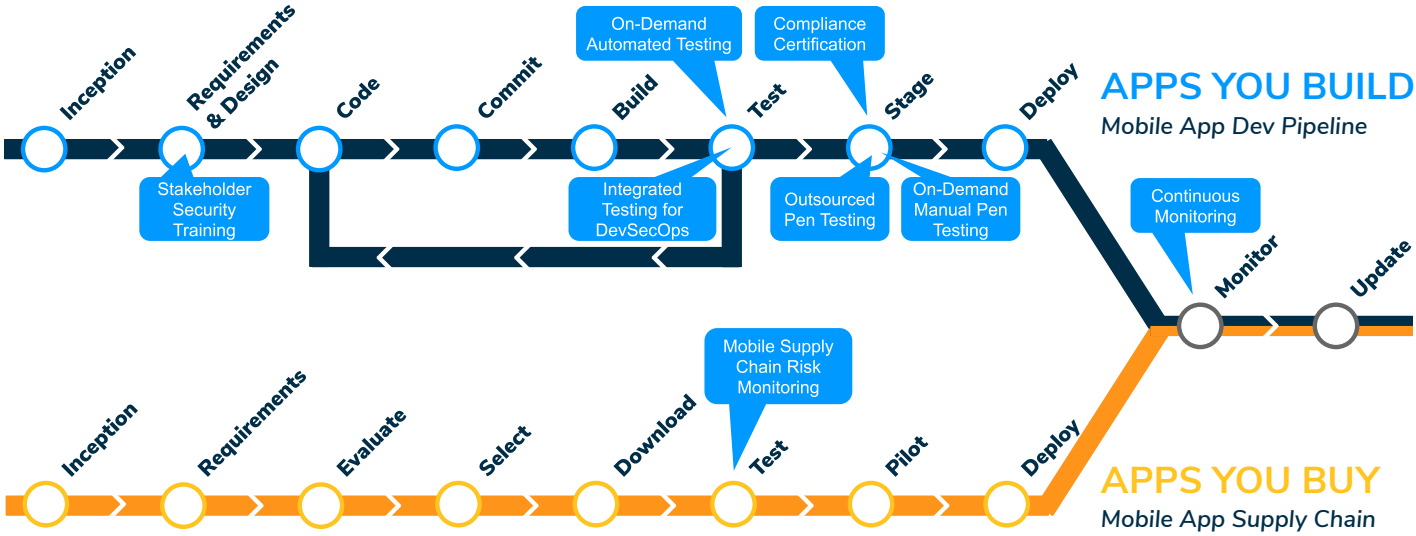
Virtually all organizations rely on mobile apps, yet none have the exact same requirements, development methods and risk tolerance. Perhaps your organization is standing up or growing a mobile application security, mobile application development or mobile DevSecOps program, building a new flagship mobile app, responding to a mobile data breach or seeking to reduce risk in the supply chain posed by the hundreds or thousands of mobile apps found on employee and corporate devices.

Mobile appsec and mobile DevSecOps teams play a critical role in supporting development teams to achieve common business goals while conquering security, privacy and compliance challenges. Maybe you want to enable mobile digital transformation, maximize resource efficiency, speed the release of high-quality apps, streamline the mobile app software development lifecycle or effectively manage overall risk. Granted their wishes, senior executives probably want to accomplish all of those objectives.

With more than a decade of mobile security expertise, NowSecure offers a comprehensive suite of automated mobile app security and privacy testing software, penetration testing services and training courseware to help organizations succeed throughout the software development lifecycle. Our portfolio of solutions protect millions of mobile apps across finance, high tech, Internet of Things (IoT), retail, hospitality, transportation and government sectors.

Organizations partner with NowSecure for everything from addressing a specific training or pen testing need to establishing and growing a complete mobile appsec or DevSecOps program. From mobile-powered digital transformation to mobile-first innovators, the most successful mobile appsec and mobile DevSecOps programs across our customer base rely on a blend of NowSecure software, services and training to reduce risk in the apps they build and use.

Whether you seek to speed releases, improve quality, manage risk or scale efficiently, NowSecure can help you accomplish those goals. Based on our experience with hundreds of customers, what follows are sample success stories about how companies in a range of industries conquer their challenges and benefit from NowSecure software and services at every phase of their mobile journey.



Outsourced Pen Testing

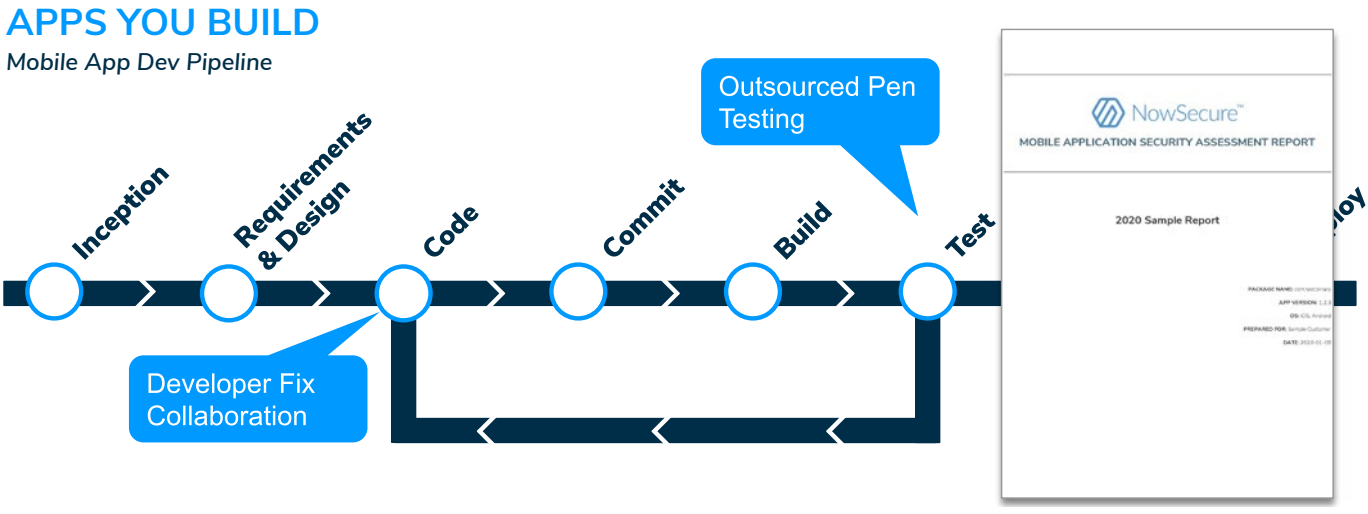
Many companies lack the mobile appsec staff or skills to conduct manual mobile app penetration testing to identify critical issues prior to release. For example, those in certain regulated industries such as finance and healthcare must engage an outside third party to conduct pen tests to comply with security and privacy requirements. Others opt for periodic pen testing of highly sensitive apps that contain Personally Identifiable Information (PII), unique intellectual property (IP), or mobile-connected IoT to gain assurance of independent certification. And some may be standing up a new flagship mobile app or embarking on a major app update. What all of these organizations have in common is a desire to protect their users and brand by finding and fixing security, privacy and compliance issues before they go into production to avoid damaging the business.

A large financial institution has upgraded its app with Artificial Intelligence (AI) technology and features to help consumers project spending, retirement and investment strategies. Given the sensitive and high-risk nature of financial transactions, the company engages in full-scope pen tests for each of its quarterly app releases. In addition, this fulfills the industry requirement of independent review by a third party in order to maintain regulatory compliance.

The last time the business outsourced a mobile app pen test, it took several weeks to receive the results which delayed the release. Worse, the appsec team later discovered that the pen test missed critical items which created a false sense of security. What's more, the pen testing provider sent senior staff to an initial consultation but then handed actual testing off to junior associates who lacked mobile expertise.

After that disappointing experience, when the company needed another quarterly pen test, the appsec manager sought out a provider with an exclusive focus on mobile apps. He selected NowSecure because its world-class services team has performed thousands of mobile assessments to uncover security, privacy and compliance issues.

NowSecure kicked off the engagement by consulting with the financial institution about its threat modeling and testing requirements. Instead of adopting a cookie-cutter approach, the team took the time to listen to the mobile appsec manager and his team's needs, complete a detailed threat model and build trust before developing a custom plan of attack. Leveraging industry standards, NowSecure Android and iOS mobile app pen tests deeply probe the



mobile attack surface for security, privacy and compliance vulnerabilities. To ensure client success, the scope of the pen test and methodologies employed vary depending on client need and timeline. As part of the initial preparation, the pen testing team obtained the binaries and provisioned the Android and iOS credit card apps on an assortment of smartphones and tablets.

Next, NowSecure experts performed black-box testing using a mix of custom, commercial and open-source tooling and techniques derived from a dozen years of dedicated mobile experience. The team deeply explored the app for issues with data storage, network transmission, backend APIs and code functionality while maintaining close communication with the customer.

The NowSecure assessment revealed a cryptography problem and additional vulnerabilities that others missed. The customized high-quality report not only identified all the vulnerabilities that were found, but included important context about severity level, potential impact and remediation guidance. NowSecure also provided screenshots and other visual evidence to support findings and make the report easy to consume.

The appsec manager invited stakeholders from the financial company's appsec and mobile app development teams to join an advisory call with the NowSecure services group to review the results and obtain consulting and remediation advice from a trusted partner. Once the DevSecOps team fixed the bugs, the NowSecure services team retested the mobile app to confirm that the issues were properly remediated. NowSecure certified the app, enabling the financial institution to use the NowSecure Security Certified logo and gain competitive advantage by meeting a high level of security and privacy standards.

The company published the update in Google Play and the Apple App Store. Through proper testing and consultation, the financial business released the major update on time, met regulatory requirements and avoided potential brand and shareholder disaster and regulatory fines.

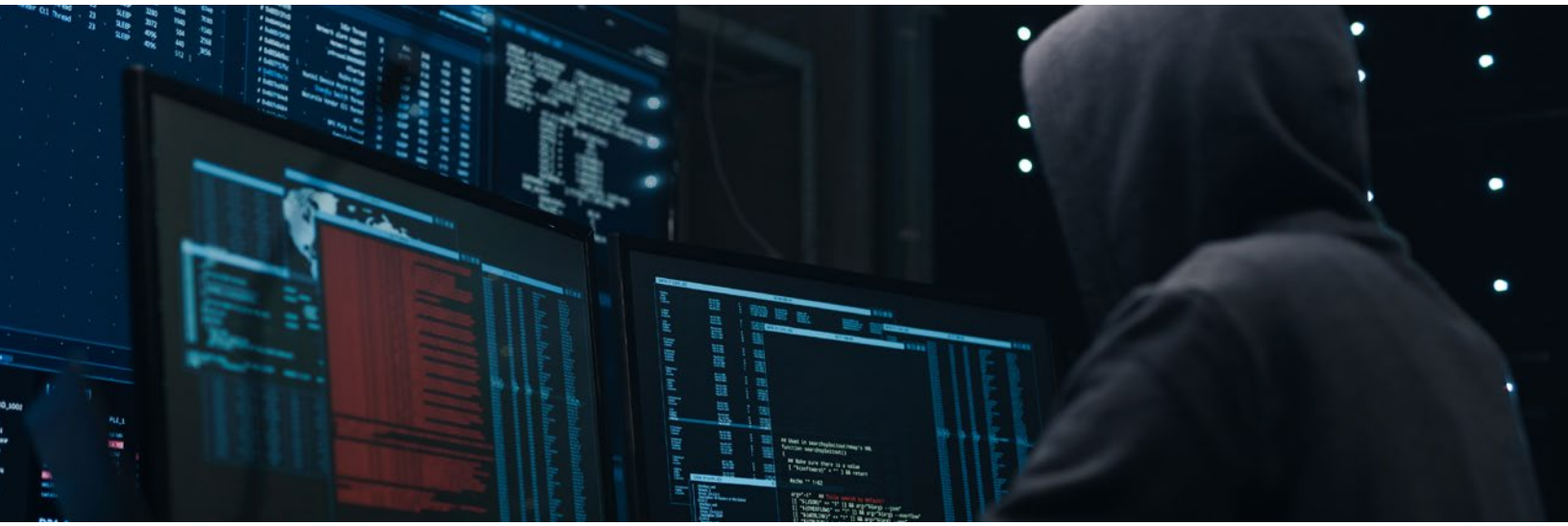
On-Demand Manual Pen Testing

Organizations with security analysts on staff often perform their own manual penetration testing of high-risk mobile apps that contain sensitive data and/or sensitive IP, or need to meet certain compliance mandates. But the onerous nature of manual pen testing combined with an ever-increasing volume of mobile app releases often creates lengthy backlogs. In addition, a lack of repeatability in manual testing makes it difficult to assess apps with complex workflows.

A medical equipment manufacturer developed a mobile app that uses Bluetooth to communicate with its IoT cardiac care device. The mHealth app provides diagnostics to physicians while also enabling patients to monitor their health. Security flaws would not only compromise sensitive information protected by the Health Insurance Portability and Accountability Act (HIPAA) standard, but could jeopardize the user's health if an attacker seized control of the IoT medical device. Disruption can range from merely annoying to life threatening.

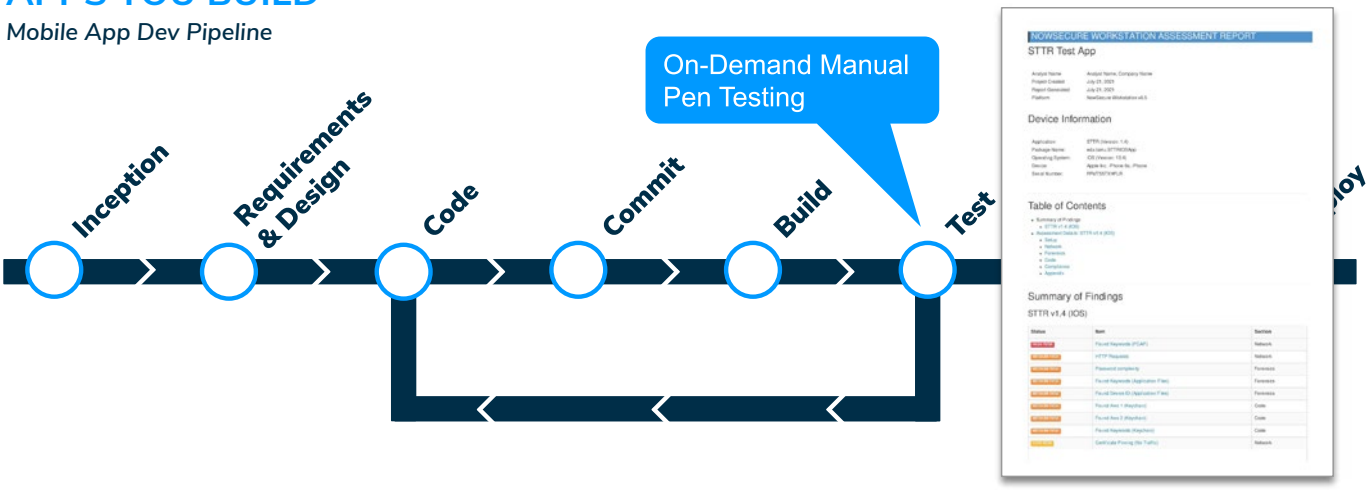
A skilled senior mobile app security analyst faces an ever-growing backlog of apps to test to ensure the protection of sensitive data and IP. It took her about two weeks to complete a manual pen test due to the work entailed in configuring a homegrown test environment of open-source and commercial tools, all running differently and none sharing data. She covered as much of the mobile attack surface as she could with the time and tools available, but found the work frustrating, repetitive and error prone. In addition, the mobile app dev team often pressured her to go faster so they could meet a release deadline. And once the pen test was finally complete, the analyst faced the pain of documenting her results, writing a report, explaining issues to the developers and showing them where fixes were needed.

Seeking to shrink the two-week pen testing process and increase efficiencies, the medical device maker's application security director deployed NowSecure Workstation to ease the task of pen testing complex apps. The NowSecure Workstation preconfigured hardware and software kit empowered her to thoroughly test her company's IoT-connected mobile mHealth app in about a day. In addition, she gained consistent, repeatable assessments for complex use cases such as CAPTCHA, biometrics and multi-factor authentication.



APPS YOU BUILD

Mobile App Dev Pipeline



The analyst unboxed the NowSecure Workstation kit which includes a laptop and two mobile devices, installed the iOS and Android mobile app binaries on the respective devices, then navigated the point-and-click interface to perform wizard-driven hands-on testing. She used NowSecure Workstation to deeply exercise the mobile apps with a combination of Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST) and API Security testing for a dramatic boost in security test coverage.

The senior mobile appsec analyst methodically used NowSecure Workstation to conduct step-by-step interactive testing, pausing to dig into individual units within tests such as device memory or network packet data. She also interactively tested the app with the IoT-connected cardiac device over Bluetooth Low Energy. Skipping the hassle of configuring and troubleshooting the old manual multi-tool test environment allowed her to dedicate more time to the intricate work of testing the many features and risks of the complex apps.

When it came time to document the test findings, NowSecure Workstation automatically generated rich output of pre-formatted customizable reporting with contextual data including CVSS security scores, compliance checks, findings descriptions and remediation instructions for developers.

Automating the mundane aspects of manual testing, analysis and reporting enabled the analyst to complete the mobile app testing in a single workday for a 10x productivity gain compared to the previous timeline of two weeks. The dev team was happily surprised that the hands-on assessment was completed so quickly, that the results were accurate and contained no false positives, and that the issues included remediation assistance to speed their work.

The appsec and dev teams and overall organization reaped tremendous productivity and security benefits from NowSecure Workstation. The analyst finally caught up with the testing backlog and her job satisfaction has improved. In fact, now she even has time to attend her son's soccer games to cheer on his team. The developers appreciate the accuracy and efficiency of finding only real issues and help in fixing them. And the manufacturer releases regular updates of its mHealth mobile apps on schedule to positive reception from customers with the confidence that they are safe and compliant.

On-Demand Automated Testing

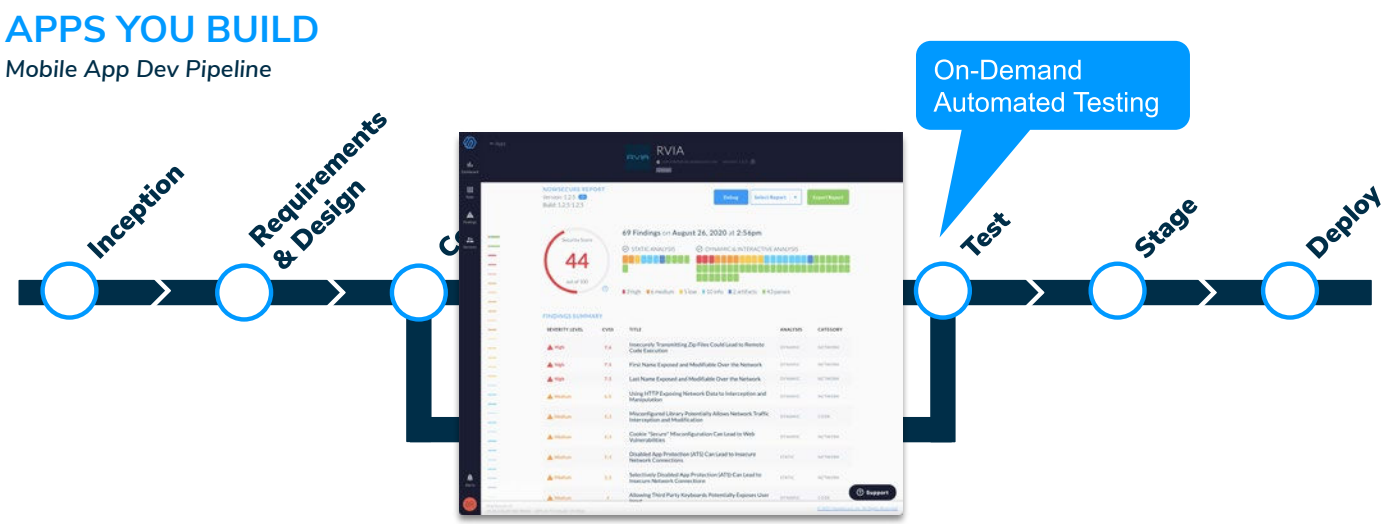
As mobile apps have become crucial to ecommerce, companies rush to get new features and capabilities to market to fend off the competition. But because developers generally outnumber security analysts by a ratio of 100:1, mobile appsec teams struggle to handle the growing frequency and volume of releases. Limited resources and increased demand create substantial security testing backlogs. Fundamentally the appsec program cannot scale to meet the needs of the business.

The time-consuming nature of traditional manual mobile appsec testing causes friction with developers and executive teams. The mobile app owner faces a losing proposition: either delay the release or push it through with little to no security testing. As a result, organizations often release mobile apps without full security testing and miss critical vulnerabilities. Or worse, perhaps devs bypass security altogether and expose the business to risk. Traditional mobile appsec testing or manual pen testing alone are insufficient for meeting the needs of a growing enterprise.

A discount retailer pivoted during the pandemic shutdown when its digital channel became the major source of revenue. It flipped from 90% in-store revenue to 90% mobile sales and the remainder via web. The company quickly rolled out new mobile app features such as a larger product catalog, curbside pickup and augmented reality virtual clothing try-on to facilitate safe ease of purchasing and business growth. Mobile dev and appsec teams adjusting to working fully remotely endured intense sprints and tremendous pressure to quickly test major new features while ensuring no critical vulnerabilities escaped undetected.

One looming obstacle was the appsec team lacked physical access to their offices during the early days of the pandemic when Los Angeles County businesses were subject to stay-at-home orders. Another problem was the short-staffed group was ill-equipped to scale to keep up with a crushing workload. Testing was time consuming and tedious and gaps in coverage created a lack of confidence in results among security analysts. Meanwhile, delays and a slew of false positives caused contention with developers. The mobile appsec team rallied to rise to the challenge, but at a significant cost to morale.

The retailer's director of appsec realized traditional manual mobile appsec testing was inefficient and unsustainable and automation was the answer. He deployed NowSecure Platform automated mobile application security testing to



Successful Teams Apply Multiple Solutions

NowSecure customers with the most effective mobile application security and mobile DevSecOps programs tend to use complementary software and services to meet their goals. NowSecure offers the flexibility for successful mobile appsec, DevSecOps and compliance teams to scale and evolve their programs as they go.

For example, some organizations may start with outsourcing all of their mobile app pen testing, then realize they can save money and time by training their own security analysts via NowSecure Academy and using NowSecure Workstation for on-demand manual testing of complex apps.

Some organizations may migrate from contracting semi-annual pen testing to continuous mobile appsec testing using NowSecure Platform. They may even cover all the bases by conducting continuous security testing and supplement that with independent third-party pen testing certification for major new releases.

Those in highly regulated industries may combine external pen testing with compliance reporting for the mobile apps they build with NowSecure Services, and then tap NowSecure Platform to vet third-party mobile apps used by employees and in the supply chain for security and privacy vulnerabilities.

Other organizations initially task security analysts with on-demand automated testing of mobile apps using NowSecure Platform while the mobile app developers hone their skills with in NowSecure Academy secure coding courseware. Eventually the enterprises fully integrate continuous security testing into the DevSecOps toolchain and empower developers to find and fix bugs to speed release.

boost speed, accuracy and depth of coverage. The software leverages standards such as OWASP, NIAP and ioXt to automatically assess Android and iOS mobile app data at rest, data in motion, code quality and API backends using a mix of static, dynamic, interactive and API application security testing.

He got his team started using NowSecure Platform quickly thanks to fast onboarding, an intuitive interface, and easy configuration assistance from NowSecure Services. Today, they test mobile apps to catch security, privacy and compliance issues before they're released. Analysts simply upload a mobile app binary on demand via a web portal or API to conduct a battery of tests for security, privacy and compliance issues. NowSecure Platform runs hundreds of tests automatically and returns results in about 30 minutes in the form of reports that feature risk-based security scores, CVSS scored findings, issue description, business impact, evidence, and embedded developer remediation assistance such as instructions, code samples and links to resource guides.

Thanks to NowSecure Platform, the retailer's mobile appsec team enjoys a dramatic productivity gain. They collapsed weeks of manually testing to a test run in less than an hour whenever needed at an overall security cost savings of more than 30% compared to a manual approach.

The small team scaled operations to keep pace with development and analyst confidence improved due to consistent, accurate results. The mobile appsec director can use the automated testing tool to plug knowledge gaps and assign junior staffers to mobile app security reviews. In addition, he has peace of mind that the test automation evolves along with new and updated standards, regulations and policies.

In fact, not only has the mobile appsec team increased efficiency while reducing risk and scaling to meet the needs of the business, but security has become an enabler at the company rather than a blocker.

Integrated Testing for DevSecOps

Organizations with DevSecOps practices seek to shift left and build security into the software development lifecycle to get secure mobile apps to market faster. Developers don't have the time to wait for mobile appsec testing results, the patience to sort through a slew of false positives or the desire to learn yet another tool. What's more, they want to be able to quickly fix the most important security bugs and then move on. True mobile DevSecOps needs full automation and integration into the toolchain to reduce friction, drive fast feedback loops and enable faster release cycles.

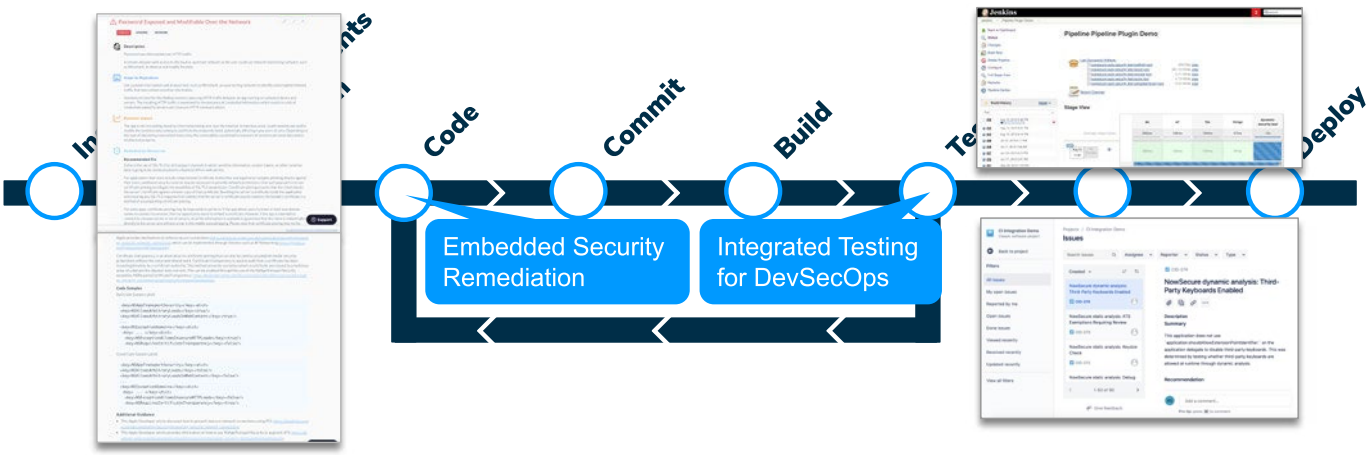
A customer relationship management (CRM) company operating in a highly competitive market needs to accelerate on many fronts. The vendor deals with sensitive customer data so can't afford to release bad code, nor can it handle any last-minute release blockers from security that delays getting new features into the hands of customers and prospective buyers.

The CRM maker is gradually shifting to a built-in security model by training devs in secure coding best practices and integrating continuous automated security testing into the mobile app dev lifecycle. The director of mobile engineering and his counterpart on the mobile appsec team wanted to tap automation and tool integration to reduce friction and enable their teams to work faster and more efficiently. The pair partnered to drive a mobile app development culture of 'secure by design' using standards-based security requirements.

Together, the leaders brought in NowSecure mobile appsec courseware targeted for the dev and security teams and deployed NowSecure Platform for continuous security testing integrated directly with the CI/CD via pre-built connectors. The director implemented NowSecure Platform directly in the DevSecOps toolchain to run a full battery of SAST/DAST/IAST and APISec tests autonomously in the background without human intervention.

APPS YOU BUILD

Mobile App Dev Pipeline

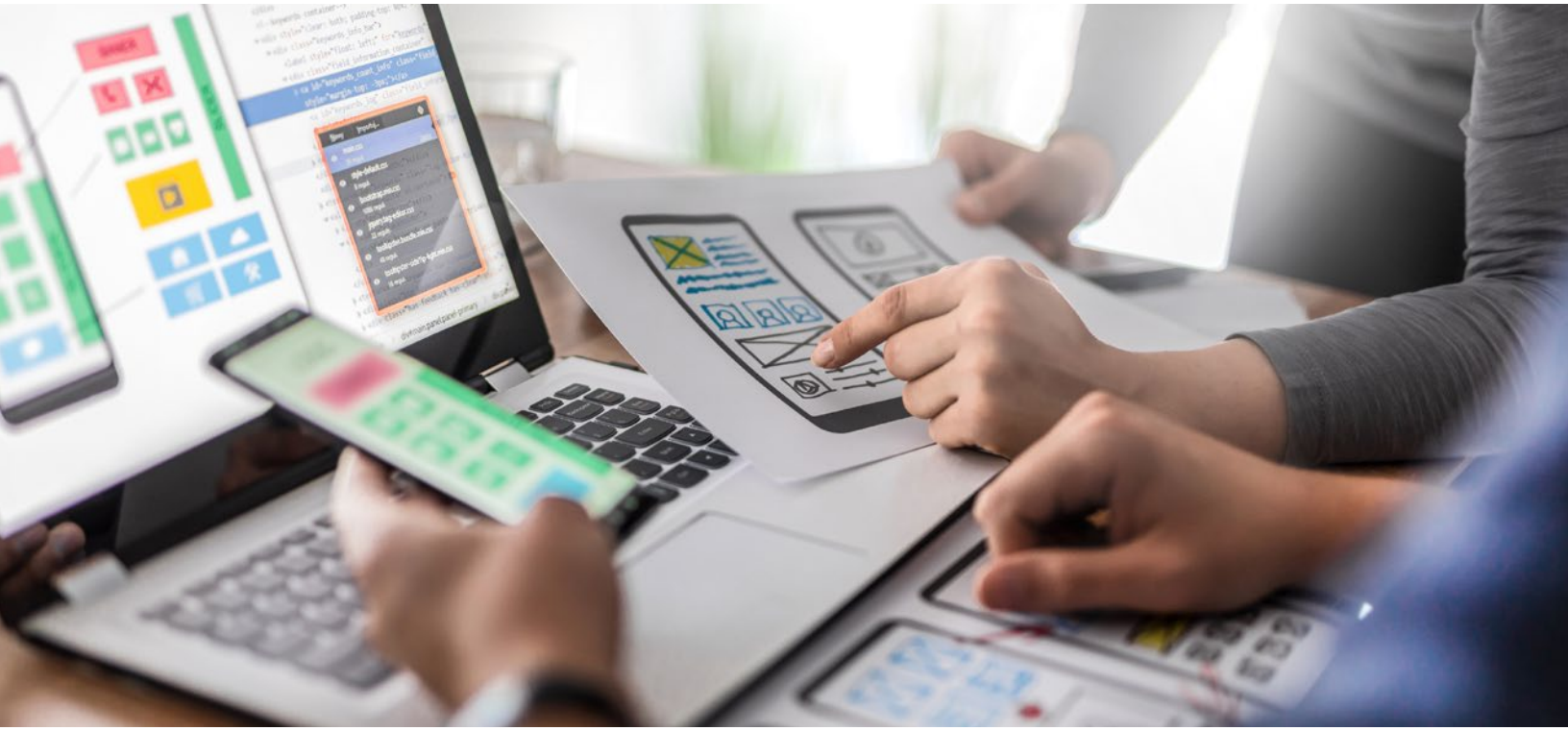


He configured his Jenkins CI/CD system to send daily Android and iOS builds of the company's flagship CRM app to NowSecure Platform to assess security, privacy and compliance. After automatically testing the mobile app, Platform feeds bugs into a Jira ticketing system so devs can quickly fix them. This level of integration enables fast feedback loops to streamline workflow and collapse the software development lifecycle.

NowSecure Platform delivers highly accurate results that are easy for dev, QA and mobile appsec teams to understand. The dev-friendly tickets contain embedded remediation assistance such as priority, evidence, fix instructions, code samples and links to Apple iOS and Google Android developer docs that helped the dev team fix issues faster, driving down their mean time to repair metrics.

The CRM maker was able to dramatically speed each phase of the SDLC with NowSecure, moving from quarterly to monthly to weekly and now daily releases and going from commit to test to production in just a few hours. It accomplished those time savings by setting mobile appsec policy based on standards up front, adding mobile appsec training courseware for all stakeholders, continuously security testing every mobile app build, generating tickets with embedded dev assistance, and quickly retesting to verify that issues were resolved.

In addition to speeding release cycles, the DevSecOps team improved the overall quality of the company's CRM app. Not only did it eliminate late-stage release blockers and shrink the defect escape rate by implementing NowSecure Platform, but developers no longer suffer from unpredictable late-stage security issues and app store rejections. Devs are empowered to focus on writing secure code and delivering competitive new CRM features faster with the confidence that security is baked in. What's more, collaboration between the mobile appdev and appsec teams has never been better.



Stakeholder Security Training

High-performing organizations with successful mobile appsec programs invest in training and building internal security expertise to enable dev and appsec teams to understand and remediate findings raised by assessments. For example, DevOps teams might set up a DevOps Dojo to help upskill stakeholders in best practices for delivering high-quality mobile apps faster. Such knowledge would help mobile devs to apply secure coding techniques and appsec analysts to better test mobile apps. In addition, employees would be motivated to demonstrate their skills and improve their professional opportunities by earning certifications.

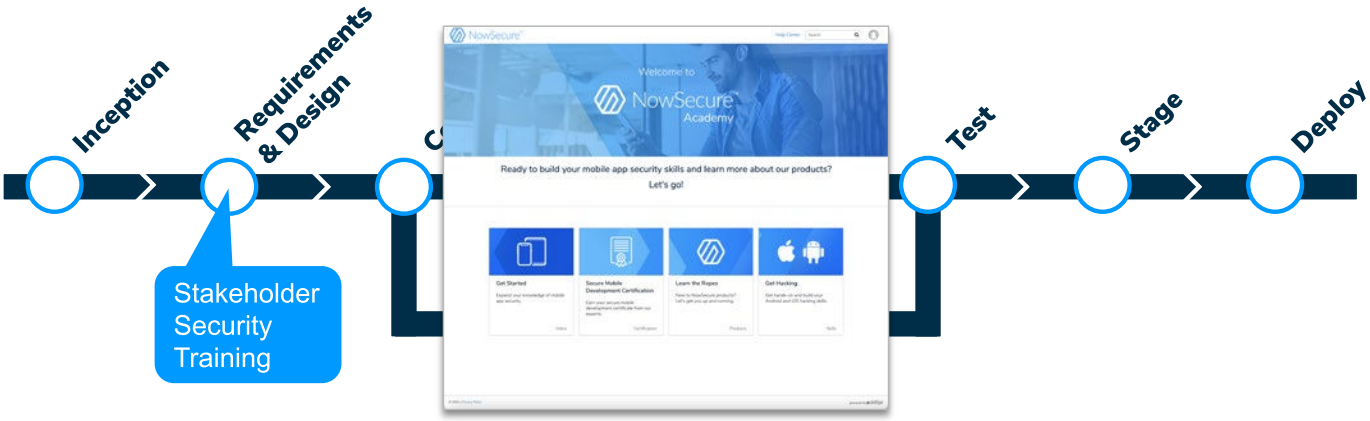
In a quest to increase code quality and speed secure mobile app releases, a growing entertainment company recently embraced the development philosophy of 'secure by design.' Recognizing that the furthest way to shift left is into the mind of the developer, the mobile app maker sought to impart best practices for secure coding throughout the mobile app dev team. Improving code quality from the start would eliminate coding errors, reduce security bugs and shrink issue repair times.

As part of this initiative, the DevSecOps leader wanted to improve collaboration with the mobile appsec team to drive efficiencies. So they partnered to agree in advance on clear security standards for secure mobile app coding and testing, leveraging the training aligned with industry security standards to help ensure success.

Many of the entertainment company's developers and security practitioners came from web app development and security. As the company's revenue channels and traffic steadily shifted to mobile, web dev and security pros transitioned over to fill the need. However, both groups lacked mobile knowledge and experience and leadership soon recognized there was a skills gap to bridge.

APPS YOU BUILD

Mobile App Dev Pipeline



With teams stretched to full capacity to build a mobile app for a new line of business, nobody in the company had the bandwidth to train their colleagues on specialized mobile appsec skills. Nor did anyone have a particular comfort for teaching large groups of their peers. The entertainment company turned to NowSecure Academy for expert-led, mobile-specific computer-based training that participants could learn from at their own pace and obtain certifications.

NowSecure Academy is an online resource for mobile app developers and new mobile security analysts to learn mobile appsec best practices and get certified. The centralized repository of resources includes self-service learning modules for professional skills development, education and certifications.

The entertainment company enrolled a dozen devs into the NowSecure Academy secure coding program to upskill them on code quality, reduce security issues and speed mobile app releases. The individuals participated in expert-led interactive training videos with quizzes about commonly found mobile appsec issues such as insecure storage or weak cryptography and how to avoid them. After taking the courses on timelines that best suited their schedules, each developer had specialized knowledge to help ensure mobile code they write is secure. Upon successful completion, each also received a NowSecure Academy Secure Mobile App Development Certification and badge to add to their resumes and LinkedIn profiles. At the same time, the entertainment business's new security analysts completed Introduction to Mobile AppSec Hacking 101 training modules to gain mobile pen testing skills.

This professional development initiative helped the DevSecOps team create a culture of security champions. As a result, the security and devs team improved collaboration and devs gained confidence in their ability to deliver high-quality mobile apps to market. The mobile app development team morale soared and the entertainment company drove its DevSecOps initiative forward by releasing mobile apps in scope that met agreed security standards on time.

NowSecure Academy

Free Mobile Security Courses For The Community

Expert-Led Online Mobile AppSec Certifications

Self-Service Training Modules For NowSecure Products

Mobile Supply Chain Risk Monitoring

Whether they support BYOD, COPE, COBO, CYOD or some other mobility model, organizations use hundreds or even thousands of mobile apps from public app stores on employee devices. In turn, those apps create millions of points of mobile app risk to the enterprise.

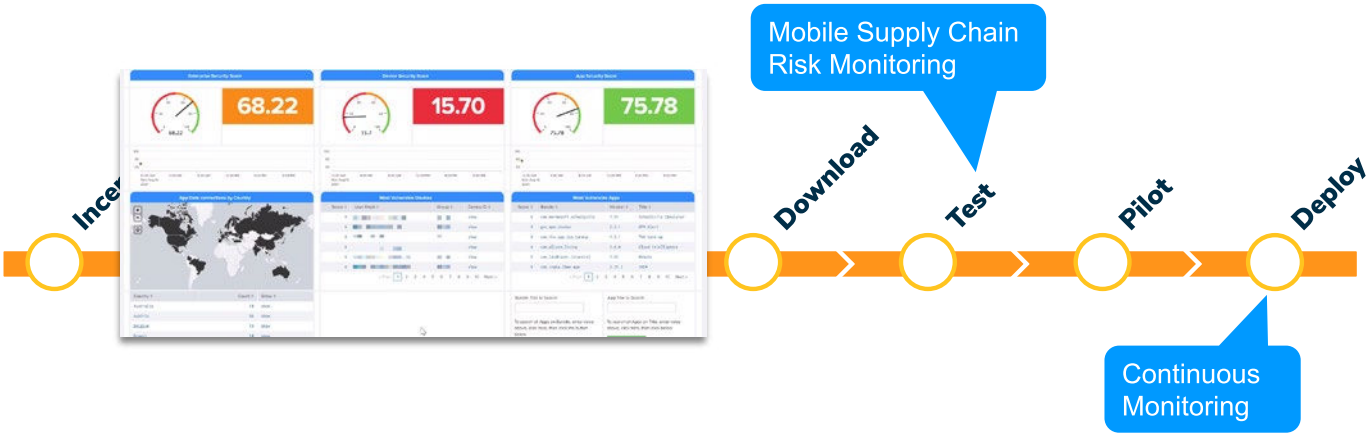
How can security leaders truly be confident that the mobile apps their employees use at work and home are secure? A mobile risk management program requires proper vetting of the third-party mobile app supply chain to provide a complete picture of the risk level of the entire portfolio.

A U.S. federal government agency lacks visibility into the third-party mobile apps that its employees use on government-furnished equipment and personal devices around the world. Leaders are deeply concerned by the reach of the SolarWinds supply-chain vulnerability. They're also worried about nation-state threat actors from adversaries such as China, North Korea and Russia mounting mobile attacks to track and surveil U.S. government workers around the globe.

Seeking a way to better manage overall mobile application security and privacy risk for a high volume of mobile apps, the federal agency's Chief Information Security Officer mandated the use of NowSecure Platform for mobile app supply chain monitoring. After purchasing NowSecure Platform, the CISO directed his team to rapidly inventory, assess and triage the existing installed base of mobile apps through a large-scale automated mobile risk analysis process. The agency found more than 12,000 unique mobile apps and versions on more than 20,000 devices connected to its networks.

Integrating NowSecure Platform mobile app vetting with its VMware AirWatch mobile device management system (MDM) enabled the security team to automatically and continuously monitor mobile app inventory and risk, delivering actionable intel for approval or denial of any apps deemed too risky for use.

The tool alerts administrators to updates and changes that present new security, privacy and compliance risks so they



can take action. For example, the CISO was relieved when NowSecure Platform found a new mobile app vulnerability and his team blocked and uninstalled it before news of the vulnerability even made the press, protecting agency personnel.

Security analysts on staff can also use NowSecure Platform to manually select mobile app binaries from the Apple App Store and Google Play for examination. The agency incorporated the portal's automated risk analysis capabilities into its procurement workflows for purchasing new systems that have mobile apps. For instance, say an industrial HVAC system can be managed via an IoT app. This visibility helps ensure apps are safe to use before being brought into the organization.

NowSecure Platform automates analysis of an expansive volume of apps found in the agency's MDM/Enterprise Mobility Management inventory; third-party apps downloaded from public app stores and those built by suppliers. The agency gained complete visibility into the security, privacy and compliance posture of each and every app with continuous monitoring giving them the ability to understand and manage risk at scale. In addition, public servants were pleased that the new approach allowed them the freedom to download the mobile apps they need to remain productive.

Compliance Certification

Governance, Risk and Compliance (GRC) departments manage the increasingly complex risk landscape and ever-growing regulations. Typical responsibilities of a compliance manager include setting policy and enabling controls.

Many companies must comply with several industry-specific regulations such as the Payment Card Industry Data Security Standard, NIAP, ioXt or HIPAA and general regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act, depending on the location of their customers. That means the mobile apps they develop need to meet standards for security and privacy.

A global airline offers a mobile app for ticket purchases, bidding on upgrades, boarding passes and its mileage rewards program. The apps include sensitive data such as first name, last name, passport number and payment information and are subject to GDPR laws. The company needs to conduct mobile appsec testing and furnish a report that demonstrates the apps meet GDPR privacy requirements.

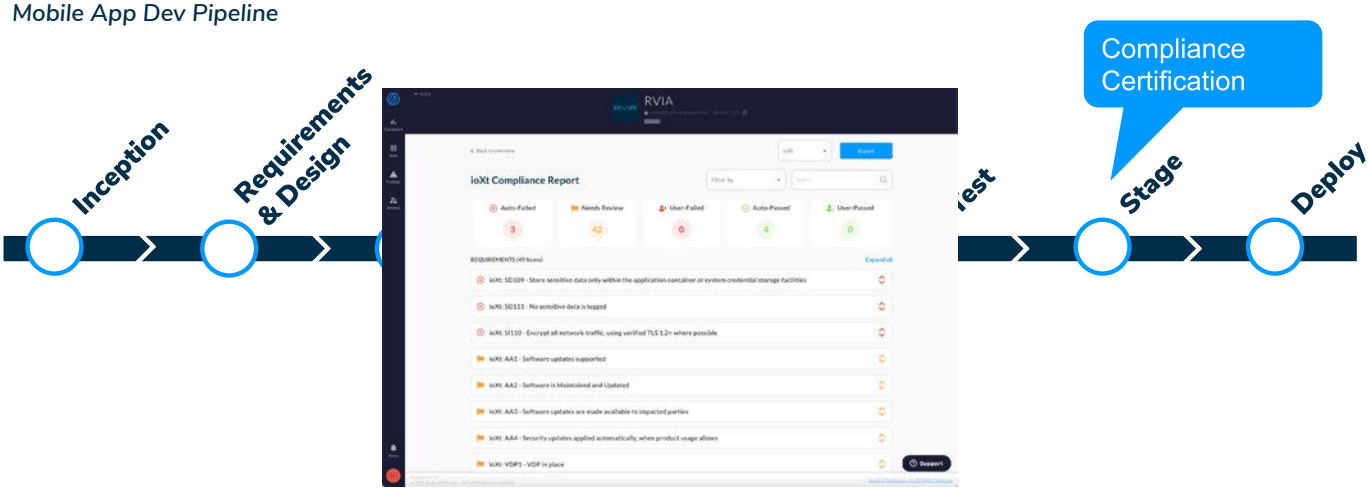
The compliance manager endured intense migraine headaches stemming from stress about the business's risk exposure. It's always a tense time in her department when compliance reports are due and the team experiences a huge spike in work. In addition, she felt uneasy about her ability to stay abreast of evolving standards and cobble together reports without holding up releases.

Looking to streamline the compliance reporting process, the compliance manager purchased NowSecure Platform to generate third-party reports attesting that the insurance company's apps meet the required standards for security and privacy. She or one of her team members simply uploads her employer's mobile apps to the NowSecure portal for rigorous security, privacy and compliance testing. Once testing is complete and the app meets the GDPR security requirements, she can simply generate a high-quality report to demonstrate compliance.

NowSecure Platform removes the guesswork of what tests

APPS YOU BUILD

Mobile App Dev Pipeline



need to be completed for compliance and eliminates the pain of manual reporting. Continuous testing helps the compliance team avoid deadline-driven spikes in workload that consume their weekends and provides the consistency that risk management professionals crave. Best of all, the compliance manager uses the clear reports to drive alignment with the mobile appsec and mobile appdev teams and achieve executive visibility.

Not only can the compliance manager more easily meet business policy requirements, but she can do it with less risk and more certainty. That's a win for the entire airline.

NowSecure Helps Organizations Achieve NIAP and ioXt Compliance

Standards-based testing and certification create predictability and governance for organizations to differentiate and safeguard the brand and protect customers. They also foster alignment between mobile app development and security teams.

NowSecure products and services test mobile apps using industry standards such as the OWASP Mobile Top 10 and OWASP Mobile Application Security Verification Standard (MASVS). In addition, NowSecure assesses mobile app compliance with privacy standards such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR).

NowSecure Platform and NowSecure Pen Testing Services provide two options for testing and certification of National Information Assurance Partnership (NIAP) Mobile App Vetting Protection Profile to protect Department of Defense and civilian agencies. NowSecure Platform offers an interactive workflow NIAP assessors use to review mobile apps and generate a detailed, high-quality report ready for ATO submission. NowSecure Services also partners with federal teams to perform the NIAP pen testing certification, help developers address issues with their mobile apps and smooth the overall NIAP certification to ATO process. These solutions dramatically compress months of testing and documentation into a few days of work for a massive productivity gain.

NowSecure Platform and NowSecure Pen Testing Certification Services also empower vendors and developers of IoT-connected mobile apps and VPNs to rapidly certify their apps for the industry-standard ioXt Mobile Application Profile. The ioXt Alliance is an industrywide security certification standards group for IoT devices, mobile apps that connect to and manage IoT devices, and mobile VPNs. As an ioXt Authorized Lab, NowSecure provides fast and high-quality results and assistance for customers to quickly complete ioXt compliance certification.

Conclusion

As you've discovered in the use-case scenarios detailed above, NowSecure helps customers tackle an array of mobile appsec, mobile DevSecOps, supply-chain monitoring and compliance challenges. Our software, pen testing services and training courseware supports thousands of mobile security analysts and developers who are responsible for millions of apps running on billions of mobile devices around the world.

NowSecure offers a complete suite for mobile app security and risk management programs that includes NowSecure Platform for on-demand automated testing, integrated testing for DevSecOps, supply-chain monitoring and compliance reporting; NowSecure Workstation for manual testing; NowSecure Pen Testing Services for expert assessments, and NowSecure Academy for security training and skills certification.

Take an important step towards solving your mobile application security, privacy and compliance issues by contacting us to discuss our solutions and read a few case studies to see how we've helped other organizations in a variety of industries succeed.

About NowSecure

NowSecure offers a comprehensive suite of automated mobile app security and privacy testing solutions, penetration testing and training services to reduce risk. Trusted by many of the world's most demanding organizations, NowSecure protects millions of app users across banking, insurance, high tech, retail, healthcare, government, IoT and others. As the recognized expert in mobile app security, the company was recently named a mobile security testing leader by IDC, a DevSecOps transformational leader by Gartner, a Deloitte Technology Fast 500 winner and a TAG Distinguished Vendor.