



NowSecure Workstation

The Ultimate Power Tool for Mobile App Security Analyst and Pen Tester Productivity

NowSecure Workstation centralizes and streamlines modern mobile app security and privacy testing within a single easy-to-use testing kit.

Purpose-built for mobile security analysts, the kit automates deep, full-coverage testing using a mix of open-source tools and proven, proprietary testing methodologies.

With a battery of built-in mobile security, privacy, and compliance tests, analysts are in full control and can conduct step-by-step interactive testing, pausing as needed to dig into individual units within those tests to investigate further. NowSecure Workstation can also be used to interactively test multi-factor authentication, mobile apps with IoT, and Bluetooth Low Energy equipment.

Preformatted and customizable reporting options speed dissemination of results across multiple stakeholders with actionable results users trust.

“ 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... The longer we use the product, the more efficient we have become at evaluation. ”

Derrick Smith, CEO
NSight365

NowSecure Workstation Speeds Security Testing Workflows

All-in-one pen testing kit to jumpstart mobile testing program

NowSecure Workstation is an all-in-one solution that combines a pre-configured laptop with mobile security testing software, iOS device, and an Android device.



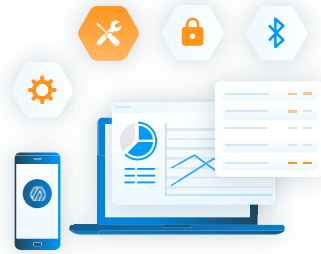
Within minutes, security analysts can load an app on one of the devices, configure sensitive data and search terms, and start testing.

Fast, stable and repeatable testing reduces manual inefficiencies

Rather than fighting test harnesses, setting up proxies and OSS/scripting configurations on each test run, automation enables repeatable processes that include unified testing environments, proper test configuration, automated diagnostics, security testing standards, and reporting guidelines.

NowSecure Workstation Highlights

- Preconfigured Hardware & Software Kit
- On-premises, Analyst-directed mobile appsec testing
- Easy-to-use interface with Intuitive UI and Wizard-driven Hands-on Testing
- Repeatability with Customizable Preferences for Speed
- Hands-on Testing & Report Generation Complete in 1-2 hrs
- Testing on Real Mobile Devices
- Flexibility to Test Jailed or Jailbroken Modes to Analyze Binaries for Latest iOS Releases
- Ideal for Complex Scenarios like MFA, CAPTCHA, IoT, USB, and Bluetooth
- Combines Leading Open Source Tools like Frida, Radare and r2frida with Proprietary Tests
- Updated UX and Architecture that Enables Teams to Complete Testing and Reporting Faster
- Findings that Include Prioritization and Remediation Instructions
- Near Zero False Positives



1 Install Binary on Device

Perform repeatable assessments for complex use cases.

- Custom and app store apps
- Device touch interactions
- IoT, USB, Bluetooth
- CAPTCHA
- Multi-factor authentication

2 Wizard-Driven Testing

Preconfigured hardware and software for deep analysis on binaries.

- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Interactive Application Security Testing (IAST)

3 Rich Output

Pre-formatted customizable reporting with contextual data.

- CVSS security scores
- Compliance checks
- Findings descriptions
- Remediation instructions

Advanced customization options allow analysts to leverage existing tools

Analysts can use additional tooling (eg. NMAP, Androguard, etc), advanced code testing using the remote shell, etc to ensure relevant results.

Deep-dive analysis at the analyst's fingertips

Analysts can leverage advanced capabilities for critical app analysis, such as dynamic code analysis via r2frida to complete complicated tasks very quickly. Similarly, easily bypassing certificate pinning enables analysts to eavesdrop on network traffic and perform man-in-the-middle attacks (MiTM).

Easy-to-use automatic report generation saves time

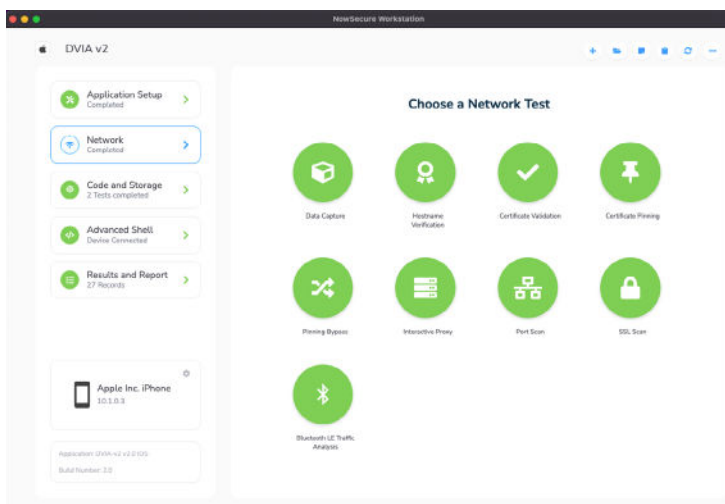
Automatically generates pre-formatted, ready-to-share reports combining results of all tests and tools used during the assessment, eliminating time-consuming frustrations of manual report assembly.

Rich output enables fast remediation with mapping to common compliance standards

Detailed remediation instructions show exactly where vulnerability or risk issues are located and how to fix them. Reports include mappings and reference details to common regulatory standards of OWASP Mobile Top 10, FFIEC, PCI DSS, HIPAA, GDPR, CWE, and more.

Testing Methodology

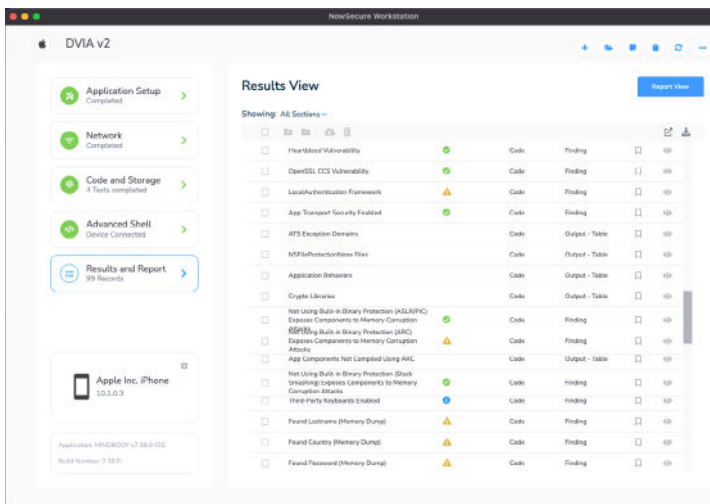
NowSecure Workstation provides an automated, wizard-driven test harness with hundreds of built-in tests, leveraging proprietary technology developed by the NowSecure Research team and best-in-breed tools from the open source community. NowSecure Research includes elite mobile app security experts, such as the creators of open source tools like Frida, a dynamic instrumentation toolkit, and Radare, a reversing framework — both popular globally and included in almost any mobile app security professional's pen testing toolbox. Workstation extensibility means analysts can tap into their favorite tools to leverage their own best practices as well.



NowSecure Workstation uniquely combines automated Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST) and API Testing for full testing on real mobile devices, not emulators. NowSecure Workstation reverses the mobile app binary and uses SAST to identify critical code issues first, then launches DAST+IAST+API security testing. DAST instrumentation hooks at the mobile OS kernel level to drive external attack scenarios and analyze how an app

interacts with the device, network and backend APIs from the “outside in”. IAST instruments an app from the “inside out” to inspect the app data and control flows. Leveraging the dynamic testing process, API security testing discovers and generates a list of all mobile-connected APIs further action.

This integrated DAST+IAST+API approach enables a security analyst using NowSecure Workstation to exercise the mobile app and backend APIs the exact same way an attacker would at runtime, probing the mobile attack surface to pinpoint and validate vulnerabilities. The depth of this attacker point-of-view approach results in full coverage of the mobile attack surface with near zero false positives.



Rich Reporting to Find and Fix Issues Fast

NowSecure Workstation eliminates manual test result analysis, interpretation and consolidation through a rich report engine. Across the large battery of tests, NowSecure Workstation automatically assembles rich, actionable and shareable reports including all key information to understand and fix issues fast:

- Description of issue and relevant supporting information
- Context details verifying finding such as actual interactive proxy traffic, passwords found in keychain, unencrypted sensitive data found in HTTP or local storage, application behaviors, endpoint connections found, and more.
- Includes severity and risk level using CVSS scores, a universal, open and industry standard method for rating risk and security vulnerabilities



- Easy-to-understand remediation instructions and links to additional resources for developers and security pros to fix issues quickly
- Regulatory mappings include PCI, CVE, CWE, NIAP, GDPR, FFIEC, FISMA, HIPAA, and OWASP Mobile Top 10

How It Works

1. NowSecure Workstation is a fully provisioned kit including a MacBook Pro, an iOS device, and an Android device.
2. Simply connect a device and load the application that the internal team builds or download public apps from the Apple AppStore™ and Google Play™, create a project, select the mobile app and begin the assessment.
3. Proceed through the intuitive setup wizard to set up a WiFi network and create sensitive data search terms relevant to the application. Then start a test.
4. During the test run NowSecure will apply SAST+DAST+IAST+API testing processes while searching for a myriad of critical vulnerabilities and sensitive data leakage on device, over the air and on the API endpoints.
5. The analyst has full control to review, modify and comment on the results under network, forensics, code and advance tabs.
6. Automatically generated reports are easily customizable and include vulnerability descriptions, CVSS 3.0 scoring, remediation recommendations, and regulatory mappings.



Boost Security Team Efficiency and Test Coverage

NowSecure Workstation is purpose-built for mobile app security teams. NowSecure Workstation turns new-to-mobile security analysts into mobile app security experts overnight, and empowers veteran mobile security analysts to speed through the mundane work and dig deeper into complex scenarios. By reducing mobile appsec testing time from weeks to hours, NowSecure Workstation drives massive 10x productivity gains for security analysts and substantial capacity gains across full security teams. Organizations that build and use mobile apps tap into NowSecure Workstation to enable their internal security teams with speed and depth to meet the needs of the business. Pen testing companies and Managed Security Services Providers (MSSPs) leverage NowSecure Workstation to scale their security testing business cost efficiently.



About NowSecure

As the recognized experts in mobile security and privacy, NowSecure protects the global mobile app economy and safeguards the data of millions of mobile app users. Built on a foundation of standards, NowSecure empowers the world's most demanding private and public sector organizations with security automation to release and monetize 30% faster, reduce testing and delivery costs by 30% and reduce AppSec risk by 40%. Only NowSecure offers a full solution suite of continuous security testing for DevSecOps, mobile app supply-chain monitoring, expert mobile Pen Testing as a Service (PTaaS) and training courseware. NowSecure actively contributes and supports the mobile security open-source community, standards and certification including OWASP MASVS, ADA MASA, NIAP and is recognized by IDC, Gartner, Deloitte Fast 500, and TAG Cyber. Visit www.nowsecure.com for more information.