SYNOPSYS®

Managed Mobile Application Security Testing (MAST)

Reduce your risk of a breach by identifying and eliminating critical security vulnerabilities across your mobile application ecosystem with on-demand MAST expertise

Change

The mobile landscape is evolving rapidly. Each new mobile operating system version, new mobile application development framework, and newly discovered attack opens new security issues that may affect your applications.

Overview

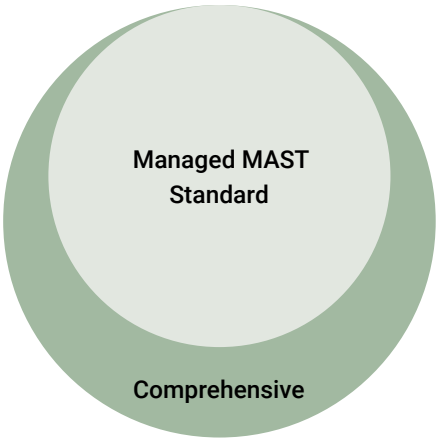
The roles of today's security professionals and software developers have become multidimensional. With their increased responsibilities, they must do more in less time, all while keeping applications secure. Mobile application security testing is an essential part of application security testing, but what if your team lacks the resources or skills to apply MAST effectively across your full mobile application portfolio? Synopsys Managed MAST enables you to implement client-side code, server-side code, and third-party library analysis quickly so you can systematically find and fix security vulnerabilities in your mobile applications, without the need for source code.

Key benefits

- **Flexibility.** Our on-demand, easy-to-use portal empowers you to manage your assessments. Schedule tests, set the desired depth of testing, and make modifications as business requirements change and threats evolve.
- **Coverage.** Test mobile applications you might miss owing to resource constraints.
- **Consistency.** Get the same high-quality MAST results all the time for any mobile application.
- **Enablement.** We walk you through your test results and help you develop a remediation plan best suited to your needs.
- **Scalability.** We provide scalable MAST delivery through our Assessment Centers without compromising manual reviews.
- **Comprehensiveness.** Our blended manual and tool-based assessment approach includes a thorough analysis of results, detailed reporting, and actionable remediation guidance.

Get access to the resources you need to scale at speed

Keeping your applications secure calls for continuous access to the people, processes, and technologies that make it possible to scale efficiently and scan with speed. Our Managed MAST assessments give you the testing flexibility, scalability, and cost-effectiveness to deliver the application testing coverage required to achieve your risk management goals. Through our Assessment Centers, you'll have continuous access to teams of security testing experts with the skills, tools, and discipline to analyze your mobile applications anytime. You can close testing gaps, conduct testing at any depth, and quickly scale to manage high-demand testing periods.



Top mobile risks

- Weak server-side controls
- Insecure data storage
- Insufficient transport layer protection
- Unintended data leakage
- Poor authorization and authentication
- Broken cryptography
- Client-side injection
- Security decisions via untrusted inputs
- Improper session handling
- Lack of binary protections

Choose from 2 depths of Managed MAST

Managed MAST helps you identify common to critical software security vulnerabilities in your running mobile application by using an application security testing suite designed specifically for mobile environments. We use a combination of proprietary static and dynamic analysis tools working together rather than in isolation to discover vulnerabilities accurately and efficiently. We offer multiple depths of analysis so you can tune the level of testing based on the risk profile of each tested application.

Managed MAST–Standard

Uses a blend of automated and manual analysis to identify vulnerabilities in application binaries running on mobile devices that cannot be found through automated analysis alone. Examples include authentication and authorization issues, client-side trust issues, misconfigured security controls, cross-platform development framework issues, and more. Includes a manual review to identify false positives and a read-out call to explain findings.

Managed MAST–Comprehensive

Expands Managed MAST–Standard by applying a blend of automated and extended manual analysis to find vulnerabilities in both application binaries running on the mobile device and corresponding server-side functionality. Example server-side vulnerabilities include session management, cryptographic issues, authentication and authorization issues, and other common web service vulnerabilities. Includes a manual review to identify false positives and a read-out call to explain findings.

Focus on actionable solutions

We'll never leave you with a laundry list of issues. At the end of each assessment, our experts will conduct a read-out call with the appropriate development/security team to review each vulnerability we identified during the assessment, answer your team's questions, and discuss actionable mitigation and remediation strategies.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com