Quokka

Qmast SOLUTION SHEET

Automate Mobile App Security Testing with Q-mast

Mobile applications are essential for business success, necessitating secure and seamless user experiences. The growing reliance on mobile apps and the surge in security threats highlight an urgent need for comprehensive Mobile Application Security Testing (MAST). Despite several MAST tools on the market, many solutions fail to adequately address the breadth and sophistication of mobile app vulnerabilities.

>50%	More than 50% of organizations reported **experiencing a mobile-related compromise,** highlighting the prevalent risk of cyber threats targeting
76%	**Insecure data storage** was the most common issue, found in 76% of mobile applications, putting passwords, financial information, personal data, and correspondence at risk
77%	77% of financial apps have **at least one serious vulnerability** that could lead to a data breach

Complexity of development exposes apps to zero-day vulnerabilities

Mobile apps are crucial for digital interactions, managing sensitive data, and enterprise access. However, their growing functionality makes them more susceptible to cyber-attacks, data breaches, and compliance issues, with the diverse mobile platform landscape adding to the security complexity.

> "MAST identifies and helps remediate vulnerabilities within mobile apps for iOS and Android devices. It analyzes source, byte, or binary code and observes or attacks mobile apps to identify coding, design, packaging, deployment, and runtime conditions that introduce security vulnerabilities"
>
> - GARTNER

Common challenges for testing apps

- **Limited Testing Scope**

  Many MAST solutions only focus on pre-deployment or post-deployment, failing to protect the entire app lifecycle.

- **Integration Difficulties**

  Incorporating MAST solutions into DevSecOps workflows remains challenging, impeding agile and secure development.

- **High Complexity and Cost**

  The complexity and expense of implementing comprehensive security testing are prohibitive for many organizations.

Rely on Q-mast automated Mobile App Security Testing for Android and iOS

Q-mast delivers defense-grade mobile app scanning capabilities, leveraging extensive threat research to identify zero-day vulnerabilities and deliver unsurpassed insights. Q-mast enables security and development teams to proactively mitigate issues early in development, saving costs and minimizing exposure to zero-day attacks.

- **Comprehensive Coverage**

  Q-mast offers a broad and in-depth range of tests covering every stage of the software development lifecycle (SDLC), from design to deployment, without requiring source code.

- **Seamless DevSecOps Integration**

  With a design tailored for DevSecOps workflows, Q-MAST supports continuous, automated security testing that aligns with tools like Jenkins, GitLab, and GitHub.

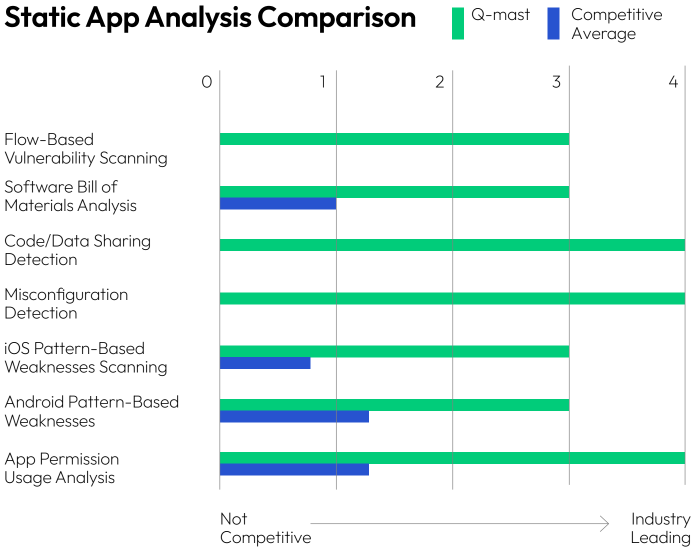
Q-mast capabilities

- Comprehensive static (SAST), dynamic (DAST), interactive (IAST) and forced-path execution app analysis
- Automated scanning in minutes, no source code needed, even for latest OS versions
- Analysis of compiled app binary, regardless of in-app or run-time obfuscations
- Malicious behavior profiling, including app collusion
- Checks against privacy & security standards: NIAP, NIST, MASVS
- Precise SBOM generation and analysis for vulnerability reporting to specific library version, including embedded libraries
- Cloud-based platform to avoid drag on hardware or bandwidth`
- Fewer false negatives with fewer false positives

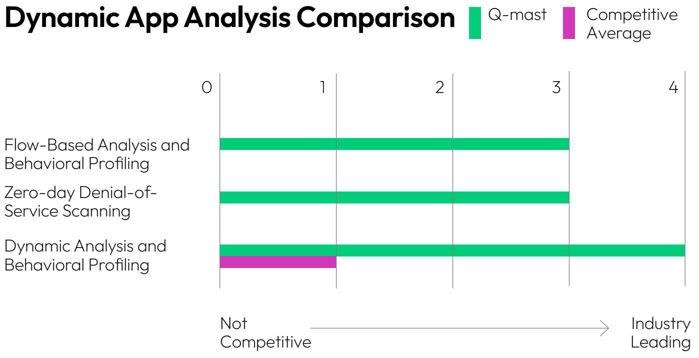
> "Of the 33 mobile apps evaluated by Quokka (formerly Kryptowire), 32 had security or privacy concerns (access to camera, contacts, or SMS messages); 18 of the apps contained critical flaws (hardcoded credentials stored in the app, app accepts all SSL certificates, and is susceptible to man-in-the-middle attacks)."
>
> – DEPARTMENT OF HOMELAND SECURITY
> Science and Technology Directorate

Competitive comparison: Q-mast vs. 5 nearest competitors

Static App Analysis Comparison



Dynamic App Analysis Comparison



About Quokka – Quokka protects mobile apps and devices used by millions globally. Formerly known as Kryptowire, the company was founded in 2011 with grants from DARPA and NIST, making Quokka the first and now longest-standing mobile app security solution for the US Federal Government. In over a decade since, defense-grade technology has enabled organizations from all sectors to deliver secure mobile apps to their customers and employees, while respecting privacy. With investment from USVP and Crosslink Capital, Quokka is bringing trusted mobile privacy and security to millions more.

Learn more at www.quokka.io or email info@quokka.io.

10M+ devices protected

230+ mobile CVEs

2M+ apps scanned

350+ academic citations

115K+ weaknesses found

75+ customer countries

500+ device vulnerabilities

11 academic papers

Quokka