Quokka

carahsoft.

Quokka

Qmast CASE STUDY

Q-mast for Federal Agencies

Q-mast for Federal Agencies

Case Study

Thank you for downloading this Quokka Case Study. Carahsoft is the aggregator for Quokka DevSecOps solutions available via NASA SEWP V, ITES-S2 and other contract vehicles.

To learn how to take the next step toward acquiring Quokka's solutions, please check out the following resources and information:

For additional resources:
carah.io/QuokkaResources

For upcoming events:
carah.io/QuokkaEvents

For additional Quokka solutions:
carah.io/QuokkaSolutions

For additional DevSecOps solutions:
carah.io/QuokkaDevSecOps

To set up a meeting:
Quokka@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/QuokkaContracts

For more information, contact Carahsoft or our reseller partners:
Quokka@carahsoft.com | 888-662-2724

Q-MAST Solution Spotlight:

Federal Agency Use Case

When security, privacy, and discretion are key, federal agencies lean on Q-MAST to establish trust.

The Need:

Reliably and proactively vet federal employees' mobile applications, eliminating vulnerabilities before use.

Government agencies are tasked with protecting information critical to the nation's success. Today, the nation's infrastructure, economy, and security hinge on digital workflows: workflows that must be thoroughly and proactively protected and increasingly transact on mobile and personal devices.

On today's virtual battlefield, offense is the best defense, making early detection a core imperative. Ensure your agency's mobile device security and privacy is in the best hands possible by placing your trust in the team with deep roots in—and wide knowledge of—the government sector.

The Solution:

Introducing Q-MAST, the mobile application vetting solution with roots in military security.

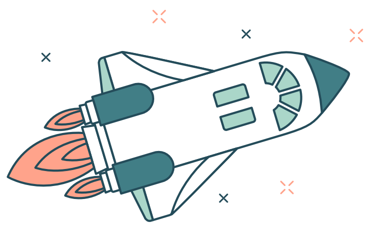
Q-MAST offers government agencies advanced analysis engines that dig deeper and test more thoroughly than any other mobile application security testing (MAST) solution in the market. **Leading organizations within the sector, including CISA and NIST, trust Q-MAST's superior technical capabilities and flexible deployment to deliver the fastest time-to-value possible.** With a proprietary combination of static analysis, dynamic analysis, and forced-path execution, we test all code that goes into your application, whether you wrote it or not.

Developed initially with funding from the US Department of Defense and selected by CISA as the tool of choice for all federal agencies, Q-MAST addresses specific security and privacy concerns held by government agencies. Using our mobile application security testing platform, agency leaders can address five critical security pillars:

Coverage: MAST sees through the behavior of an app at a level of comprehensiveness (both analysis depth and breadth-wise) that no manual analyst can match. Using MAST, organizations can easily get a comprehensive understanding of the behavior of an app and the security gaps in it with a high level of assurance.

Continuity: Q-MAST eliminates human error (omission, knowledge gaps), allowing organizations to turn mobile security testing into a continuous process that easily integrates into modern software development pipelines.

Evidence: Q-MAST provides concrete technical evidence, insight into each identified finding, and valuable information for remediation, significantly reducing debugging and remediation time.



Speed: Q-MAST does it all at a fraction of the cost and the time it would take organizations for manual testing or verification, giving them time back to focus their efforts where it matters most.

Compliance: We continuously assess the security and privacy of mobile apps against the highest internationally recognized software assurance standards published by:

- National Institute of Standards and Technologies (NIST)
- National Information Assurance Partnership (NIAP)
- Open Web Application Security Project (OWASP)

Real-World Results:

We've helped government agencies identify vulnerabilities and start the remediation process.

Q-MAST has helped leading government agencies identify vulnerabilities in over 200 applications in the real world. 16% of these applications, both Android and iOS, were vulnerable to known OS attacks, and 18% of Android apps scanned contained a known vulnerability.

A proprietary combination of static analysis, dynamic analysis, and forced path execution, we test all code that goes into your application, whether you wrote it or not.

- Each application tested offers a full Software Bill of Materials (SBOM), including a complete analysis of all third-party code in your app.
- Q-MAST identifies both known vulnerabilities (ex. log4j) and weaknesses that may lead to critical data being exposed.

The ability to configure both security and privacy protocols, ensuring total visibility and control over the flow of sensitive data.

- In the same way static and dynamic analysis work better together, so does stewardship of security and privacy; harmony is crucial.
- We understand that every system has its own unique risks, which is why Q-MAST allows organizations to customize the risk profiles applied to your scans.

Q-MAST integrates easily with leading software development tools, such as:

GitHub GitLab Azure DevOps Jenkins

Get Started with Q-MAST

Quokka is making the world of mobile security and privacy more positive, proactive, and conducive to peace of mind. Now, we'd love to help your team strengthen its security and privacy initiatives.