Quokka

Qmast CASE STUDY

Q-mast for Medical Schools

Q-MAST Solution Spotlight: Medical Schools

Leading medical institutions trust Q-MAST to vet mobile device applications. **Here's why.**

The Need:

Ensure the security and privacy of patients, employees, and the organization at large.

In today's world, practitioners, administrative staff, and other employees at large medical schools use mobile devices (such as iPads and other tablets) to record patient interactions, manage workflows, and execute other mission-critical tasks. The applications used to facilitate these tasks are often numerous, diverse, and have different authors, including the University itself and/or third party developers. Additionally, the COVID-19 pandemic greatly accelerated the existing move towards mass medical digitization, increasing the amount of sensitive data contained within these applications.

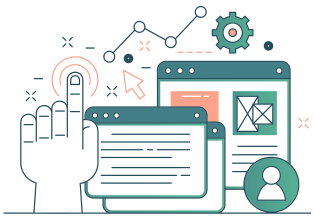
Accordingly, medical organizations are tasked with keeping this information safe and secure in an increasingly complex digital environment where information is highly decentralized. Robust, proactive protection requires organizations to trust every application on every device in their environment, from pre-installation through every automatic update.

The Solution:

Meet Q-MAST, the industry's leading mobile application security testing solution (MAST).

Q-MAST offers medical schools an advanced analysis engine that digs deeper and tests more thoroughly than any other MAST solution in the market. **The industry's most demanding customers trust Q-MAST's superior technical capabilities and flexible deployment to deliver the fastest time-to-value possible.**

Originally developed for the US Department of Defense – Quokka digital security solutions are currently being **used by Health and Human Services agencies**, setting the standard for mobile application privacy where it counts.



Complex Interactions: Applications in this type of environment frequently interact with each other, pushing and pulling information and leveraging broader device functions (such as camera, microphone, and GPS). For instance, an application that controls insulin monitoring may interact directly with the patient's EMR to update records.

That’s why Q-MAST uses static analysis, dynamic analysis and Forced Path Execution, testing all entry and exit points within a set of applications.

- Each application tested offers a full Software Bill of Materials, negating the possibility of supply chain attacks.
- Using the Watchlist feature, these protocols are executed automatically every time an application in the ecosystem is updated, allowing automated tracking of every update.

Privacy Concerns: Most security solutions focus on preventing breaches at the expense of privacy best practices. A robust SDK doesn’t guarantee that sensitive information, such as data covered under HIPAA, arrives and departs in an ideal fashion.

That’s why Q-MAST allows administrators 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 medical system has it's own unique risks, that's 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 OPENAPI INITIATIVE

Real-World Results:

How we’ve helped leading medical schools stay proactive and achieve peace of mind.

In the real-world, Q-MAST has helped leading medical schools:

- Create an App Watchlist capable of vetting thousands of application updates each month
- Create an OpenAPI-based, closed-loop reporting system capable of automatically importing security and privacy issues into a vulnerability management system
- Automate deployment of corresponding solutions to distributed development teams for integration into broader DevSecOps environments
- Ensure efficient, productive communication between multiple security teams within a large organization

- **Speed:** Rapid onboarding of large application portfolio across hundreds of mobile devices, as well as the ability to quickly add or expand scanning capabilities at scale
- **Efficiency:** Improved security testing suite coverage with less manual effort required, improving efficiency
- **Ease of Use:** Designed with usability in mind, our portal reduces the need for training and accelerates the onboarding process.
- **Confidence:** Proactive risk mitigation to reduce the possibility of patient and/or organizational exposure¬

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 organization.