Quokka

Q vet SOLUTION SHEET

Automate Mobile App Vetting (MAV) for Android and iOS with Q-vet

Enterprise-approved apps have become essential for work-from-anywhere-flexibility and increased productivity. Yet, reliance on mobile to get work done also exposes organizations to risks that can lurk in the apps they deploy. Apps from public and private app stores can still contain security, privacy, and malicious threats that can be exploited for data exfiltration. Effective mobile app vetting enables risk-based decisions on which apps to deploy to minimize introducing vulnerabilities into enterprise environments.

Apps are the new endpoint

Many mobility products use network, identity, and device-based approaches that inadequately protect enterprises at the mobile app layer. App intelligence is needed to check apps for zero-day vulnerabilities that are exploited in supply chain attacks.

Common app vetting challenges include:

- **costly and time-intensive** manual testing, requiring mobile security expertise
- **inability to test apps** without source code or ability to scan compiled app binary due to in-app or run-time obfuscations
- **incomplete insights** into the latest emerging threats and zero-day vulnerabilities

Q-vet delivers automated app intelligence to test for security, privacy, and compliance risks before deployment

Automated security testing across platforms

Automated security testing platform for iOS and Android apps, no source code access needed.

Comprehensive coverage

Analysis of vulnerabilities in millions of apps helps preempt sophisticated zero-day threats, including data harvesting, MitM attacks, elevation of privileges, and app collusion.

App intelligence

Advanced algorithms and machine learning offer clear threat intelligence, enabling developers and analysts to identify and mitigate vulnerabilities early, addressing complex threats like app collusion and MitM attacks efficiently.

Rapid pass/fail decisions

Security and privacy testing can be done in as little as 30 minutes, ensuring only secure apps are deployed in enterprise environments.

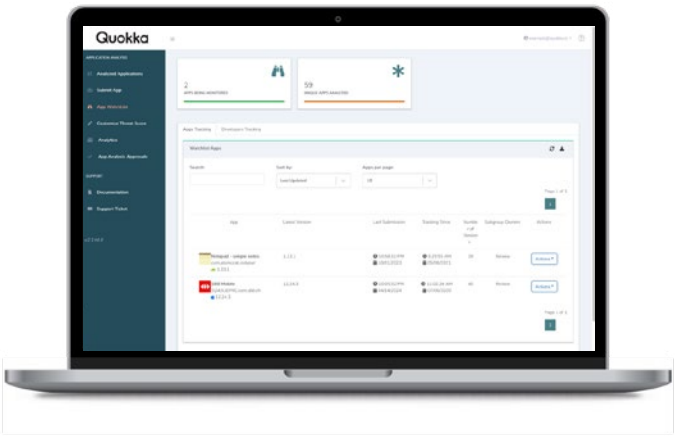
Trusted by the US Federal Government since 2011.

> “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

Q-vet capabilities

- Comprehensive static (SAST), dynamic (DAST), interactive (IAST) and forced-path execution app analysis
- Automated scanning in minutes, 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, HIPAA, GDPR, PCI
- 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



Integrate contextual mobile security intelligence with existing UEM tools

Explore Q-scout to future proof mobile endpoint protection.

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	210+ mobile CVEs
2M+ apps scanned	350+ academic citations
115K+ weaknesses found	75+ customer countries
500+ device vulnerabilities	11 academic papers

Quokka