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.

Quokka products:

1. Q-mast: Automated mobile app security testing product
2. Q-vet: Automated 3rd party mobile app vetting product
3. Q-scout: Privacy-first mobile endpoint protection product

With a layer on the top of App Intelligence : Contextual mobile security intelligence product

Qmast: 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-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

Q-scout integrates with MDM tools, empowering IT teams to establish and uphold robust security policies across mobile environments. Leveraging Quokka's contextual mobile security intelligence, Q-scout delivers deep app scanning to detect security vulnerabilities and malicious behavior, including zero-days, for discrete apps and, more importantly, sets of apps installed on each mobile endpoint.

- Real-world context : Apps do not exist in isolation. Rather, they are installed as a collection of different apps on each device, with different settings, OS versions, and form factors.
- App security intelligence : Whether COPE, BYOD, hybrid, MDM, or no-MDM, the enterprise needs app-level scanning analysis to detect vulnerabilities and malicious behavior – including zero-days – for discrete apps and sets of apps.
- 100% automated coverage : Make risk-based decisions about which mobile apps from the Google Play and Apple App Store – personal or managed – end users install on devices
- Privacy-first approach First and only mobile endpoint protection trusted by users because no personal information or data is collected or shared.
- Employee convenience : Users can enjoy the convenience of using their mobile devices for work while maintaining personal privacy and security

Q-mast and Q-Vet 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

Quokka product structure :

Quokka Core

- External code fetches, websites visits, network traffic
- Hard coded keys, Weak hash, Insecure web-views, permission usage analysis
- RASP & TLS friendly dynamic analysis
- Covers crypto best practices, dynamic code, inter-component and inter-app communication, tapjacking, PII leaks, input validation, tracking, webview weaknesses, and many more.

Quokka Advanced

- Code/Data Sharing Detection (App Collusion)

- In-app purchase vulnerability, unprotected permission exploit
- Exploitable inter-app communication vulnerabilities:
    - Message to app to crash or brick the device
    - Message to app to leak recording of device screen
- Advanced SBOM:
    - Transitively identifies common libraries used by an app, their version, and their public CVEs
    - Novel ways to handle obfuscations and code shrinkage

Quokka NextGen

- Malicious code that runs only after app runs for a long time
- Remote Command & Control to give access to app, device or files
- Read sensitive PII data like device location and send over network

Quokka serves the following personas/teams/departments

for Security teams

Your mobile app and data attack surface keeps expanding, with increasing complexity
Get the mobile app security visibility and actionable insights you need to make risk-based decisions about how to protect your organization from zero-day mobile vulnerabilities and exploits.

for IT teams

You can balance enterprise mobile security and privacy
Manage apps as endpoints and leverage Quokka intelligence to secure all mobile devices and apps – even personal ones – without invading privacy

for DEVSECOPS

Speed and complexity of development exposes your apps to zero-day exploits
Rely on defense-grade Mobile App Security Testing (MAST) for DevSecOps to remediate mobile security zero-day vulnerabilities — before they become incidents that threaten privacy, intellectual property, sensitive data, and brand reputation.

Quokka serves the following industries:

- Financial Services

Managing money from mobile apps is the norm – financial fraud doesn't have to be
Rely on Quokka Contextual Mobile Security Intelligence to proactively secure financial services apps. Discover and remediate mobile zero-day vulnerabilities that can be exploited for fraud, data breaches, and privacy violations.

Helping financial institutions protect the mobile ecosystem
Mobile security has historically been underfunded – Quokka can cost-effectively reduce your mobile app threat risk.
Prevent fraud & breaches
Mobile financial services apps are high-value targets for malicious actors, and worldwide mobile app fraud is estimated at over $2.64B USD.[1]

Protect your mobile workforce
Nearly everyone in your organization, from executives to frontline agents, accesses sensitive business and customer data from their mobile devices.

Comply with regulatory requirements
Around the world, financial institutions must comply with complex governmental regulations to protect consumer information, including on mobile apps.

- Healthcare

Patients expect mobile healthcare access – and privacy for personal info
Rely on Quokka Contextual Mobile Security Intelligence for proactive healthcare mobile app security. Mitigate zero-day vulnerabilities that can be exploited for ransomware, data breaches, and privacy violations.

Helping healthcare institutions protect the mobile ecosystem
Mobile security has historically been underfunded – Quokka can cost-effectively reduce your mobile app threat risk.
Protect against ransomware
Mobile app vulnerabilities can be exploited to exfiltrate data for follow-on fraud attacks or be the target of ransomware.

Prevent malicious data breaches
Personal healthcare data need to be protected to maintain patient trust & regulatory compliance.

Comply with privacy regulations

Healthcare institutions must comply with governmental regulations to protect patient information.

Enable mobile treatment & admin
Healthcare staff and patients need to know they can trust the apps they're using to access medical information.

- MSSP

Your customers need protection against evolving security risks from daily business use of mobile devices
Sell Q-scout privacy-first mobile endpoint protection as an MSSP to deliver 100% fleet coverage to your customers

Fill a recognized gap in your portfolio
Provide a service for customers who can't, or haven't, committed to an MDM yet need to protect COPE, BYOD, or mixed fleets

Zero-trust BYOD security
Validate whether managed or personal mobile apps do not contain malicious code and meet security and privacy compliance standards

App security intelligence for UEM
Integrate with existing MDM and MTD solutions to detect and block zero-day threats residing in managed and/or personal apps

- mCommerce

Your customers love your brand enough to download your mobile app – keep their trust
Rely on Quokka Contextual Mobile Security Intelligence for proactive mCommerce and retail app security. Mitigate zero-day vulnerabilities that can be exploited for data breaches that harm consumer confidence and brand reputation.

Helping retailers protect their mobile apps and ecosystem
Retail mobile app security has historically has underfunded – Quokka can cost-effectively reduce your mobile risk.
Protect your brand
Keep trusted brand names out of the headlines for mobile app breaches that expose login credentials, personal info, and payment details.

Prevent malicious data breaches
Retail mobile apps are complex, relying on payment integrations and 3rd party code libraries that can contain supply chain vulnerabilities and zero-day threats.

Comply with regulations
Mobile retail apps requiring login and/or processing payment information must comply with multiple government regulations.

Enable your mobile workforce
Apps your corporate employees and retail workers use for business must be as secure as your consumer-facing apps.

- Mobile Gaming

The success of your mobile games depends on thwarting cheating and piracy
Rely on defense-grade Mobile App Security Testing (MAST) to remediate mobile game security, code weaknesses, or zero-day vulnerabilities that can be exploited for cheating and piracy.

Helping game studios protect their gaming apps and mobile ecosystem
Mobile security has historically been underfunded – Quokka can cost-effectively reduce your mobile risk.
Protect your brand
Trusted game studios keep their games out of headlines for breaches that expose login credentials, personal info, and payment details.

Prevent piracy & cheating
Once a new game has been cracked for cheating or piracy, your studio loses out on revenue potential from that release and beyond.

Comply with regulations
In-game purchases requiring login and/or payment information must comply with multiple government regulations.

Enable your mobile workforce
Apps your employees and contractors use for business need to be as secure as the mobile games you produce.

Meet mobile app security security standards

OWASP
NAIP
NLST
CVE
Sarif

NIST 1800-22
BYOD Guidelines – Quokka participated in creating the NIST Special Publication 1800-22 and its insights and technologies were part of the example solutions used in the guide under the Cooperative Research and Development Agreement

NIST 1800-21
COPE Guidelines – Quokka (then Kryptowire) participated in creating the NIST Special Publication 1800-22 and its insights and technologies were part of the example solutions used in the guide under the Cooperative Research and Development Agreement

NIST 800-163
Vetting the Security of Mobile Applications – Quokka developed an automated mobile app vetting solution

Automating NIAP Requirements Testing for Mobile Apps
Quokka contributed automated analysis using proprietary mobile app vetting infrastructure

NIAP v1.4
Protection Profile for App Vetting – Quokka has worked with federal agencies to meet both the functional and assurance requirements outlined in this profile

.