Future-Proof Mobile Endpoint Protection for Android & iOS

Ensuring mobile security is vital to safeguarding sensitive data and protecting against endpoint-centric cyber threats

Using personal mobile devices for professional purposes is commonplace in corporate environments, presenting a pressing need for robust security measures. However, this widespread adoption also brings about the proliferation of unvetted personal applications, introducing potential vulnerabilities into enterprise networks.

> " Mobile applications are central to digital transformation for many organizations. Ensuring these apps do not present vulnerabilities that can be exploited is essential to enable this transformative process.[1]"
>
> - **Gartner.**

Securing mobile environments is challenging, especially when mobile security is underinvested and security risks from mobile apps are rising, especially since today's mobility products fail to meet today's threats. MDMs and MTDs cannot:

- **Detect zero-day threats** residing in mobile devices and/or personal apps

- Deliver adequate **mobile protection** for all mobile users and minimize IT workload

- Ensure employee **privacy**

## Mobile devices are a business necessity and likely risk

+95% Over 95% of businesses allow personal devices for work

90% 90% of successful cyber attacks originate from endpoint devices [2]

Zero-trust, privacy-first mobile endpoint protection for the enterprise

Q-scout aligns with NIST standards[3] enhancing mobile security and privacy for all mobile environments, COPE, BYOD, or mixed environments, with or without MDMs. It streamlines security management, making it ideal for organizations prioritizing ease of use and minimal IT involvement. Q-scout analyzes every managed and/or personal app for malicious app behavior and enforces data transmission policies while ensuring employee privacy and support for compliance standards.

Quokka enables IT teams to proactively protect their organizations and mobile workforce from zero-day mobile exploits.
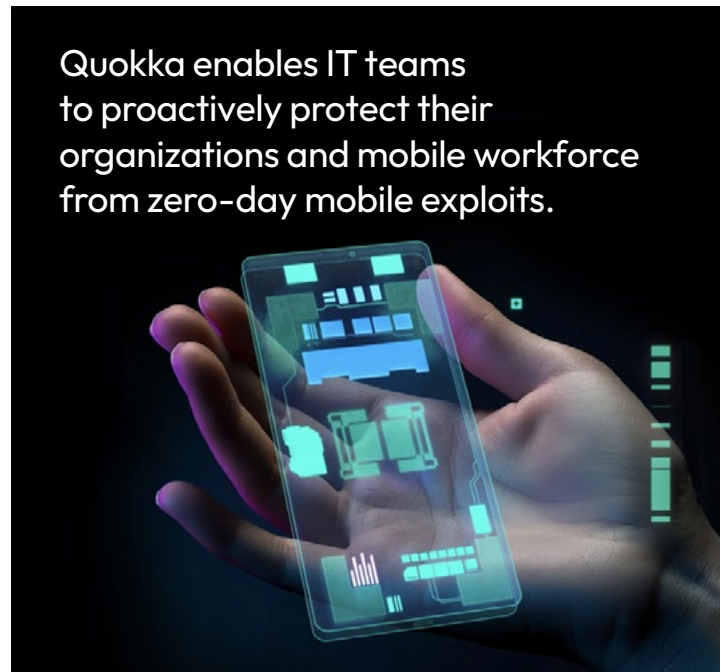
With Q-Scout's ability to integrate with existing UEM tools, IT teams can set and enforce policies to secure their mobile environments utilizing Quokka's unsurpassed mobile security intelligence. This intelligence is backed by original research and real-world contextual awareness obtained from defense-grade app scanning engines.

1   Gartner Research: A Guidance Framework for Building an Application Security Program 20 February 2024

2   Verizon Business 2023 Mobile Security Index

3   https://csrc.nist.gov/pubs/sp/1800/22/final 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.

Integrate defense-grade app security intelligence with mobile device management to enforce mobile security

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.
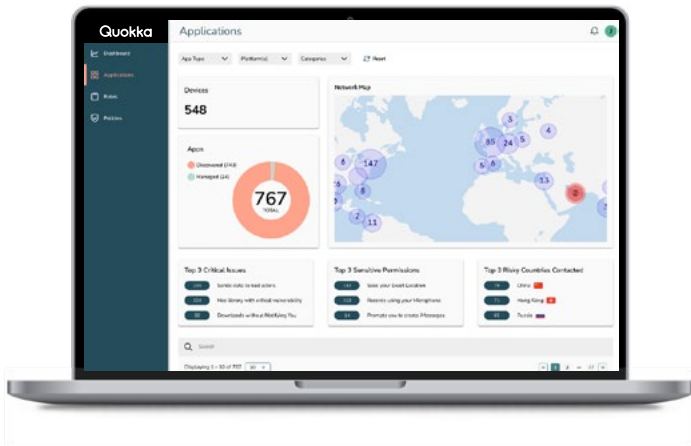
Real-world context

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

---

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, 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.

To learn more visit **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