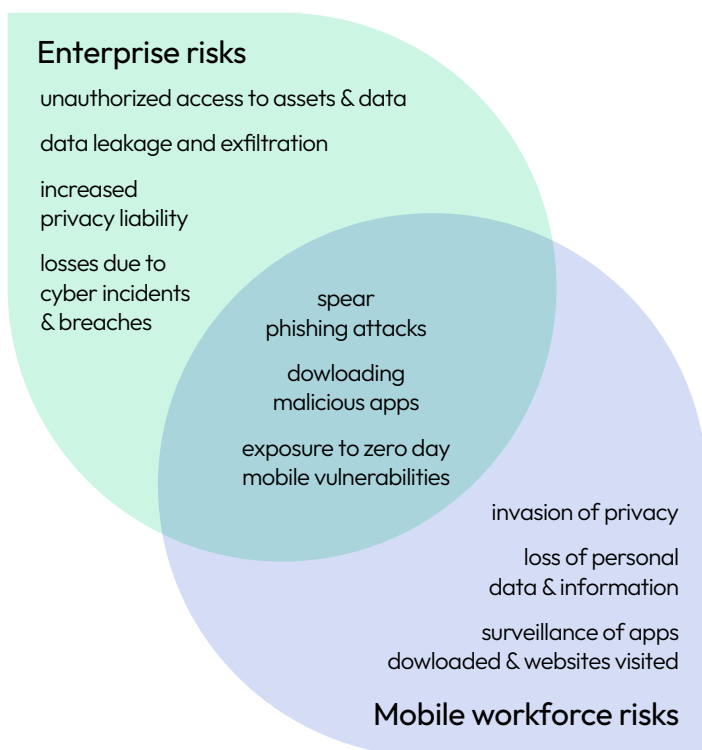# Privacy-first mobile endpoint protection with Q-scout Security

BYOD needs to work for the enterprise and the mobile workforce

It's common practice to allow or even require employees to use their personal mobile devices to reduce equipment costs and increase worker productivity. Using mobile devices provides workers the flexibility to work from anywhere. Yet, BYOD opens up risks for both the enterprise and the workforce.

Securing BYOD environments is challenging for organizations constrained by budget and IT resources, particularly due to limited insight into personal mobile devices and app download risks. Solutions such as MDM, MAM, and MTD are costly, complex, and:

- **fail to detect** zero-day threats residing in mobile devices and/or personal apps

- **escalate IT workload** without delivering adequate protection

- often **infringe on employee privacy**

Enterprise risks

unauthorized access to assets & data

data leakage and exfiltration

increased privacy liability

losses due to cyber incidents & breaches

spear phishing attacks

dowloading malicious apps

exposure to zero day mobile vulnerabilities

invasion of privacy

loss of personal data & information

surveillance of apps dowloaded & websites visited

Mobile workforce risks

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

NIST reports a rise in BYOD security threats

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

86% 86% of IT managers reports mobile attacks are becoming more frequent

Q-scout is the industry's only mobile endpoint protection that scans all apps, device configurations, and data destinations in the context of each device – all without collecting or sharing personal information. Q-scout delivers zero trust for mobility by validating connecting mobile devices and their apps meet compliance standards at every login. Q-scout aligns with NIST standards [1] to enhance mobile security and privacy in BYOD settings, offering a cost-effective, privacy-centric solution for SMBs. Q-scout simplifies security management, making it ideal for businesses prioritizing ease of use and minimal IT involvement.
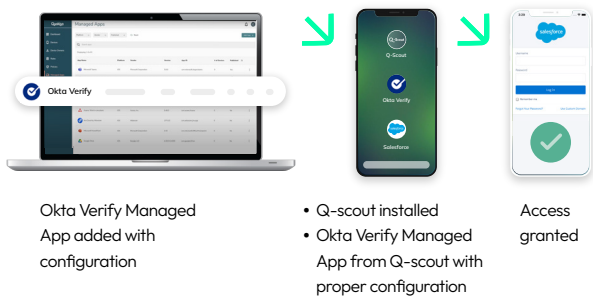
Quokka enables IT teams to proactively protect their organizations and mobile workforce from zero-day mobile exploits.

With Q-scout, IT teams leverage Quokka's unsurpassed mobile security intelligence – backed by original research, real-world contextual awareness, privacy-first architecture, and defense-grade app scanning engines – to set and enforce policies to secure their BYOD environments.

1 | 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 app management, identity & access tools to enforce BYOD security

Q-scout allows IT to securely manage its mobile workforce by distributing, administering, and revoking corporate apps through an enterprise app store that can remove access whenever necessary. It ensures secure app management by integrating with Okta Verify, allowing enterprises to control app access based on the security posture of devices and apps while maintaining user privacy and enhancing productivity. IT administrators can manage access and settings from one screen, ensuring productivity without compromising privacy. The Okta Verify integration provides multi-factor authentication (MFA), verifying user devices/apps and identities during sign-in.

Okta Verify Managed App added with configuration

- Q-scout installed
- Okta Verify Managed App from Q-scout with proper configuration

Access granted

"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 [2]"

– **Gartner**

Q-scout + Okta Verify = Zero-trust, privacy-first mobile endpoint protection

Enhanced Security

Integrating Q-scout's mobile endpoint management with Okta Verify's MFA ensures device attestation, creating a secure mobile environment at the login point.

Streamlined Authentication

Users can seamlessly authenticate their devices using Okta Verify's push notifications or one-time codes, ensuring frictionless and secure access to business resources.

Compliance and Privacy

Employee privacy is ensured since personal apps and data cannot be accessed at any point during or after the authentication process.
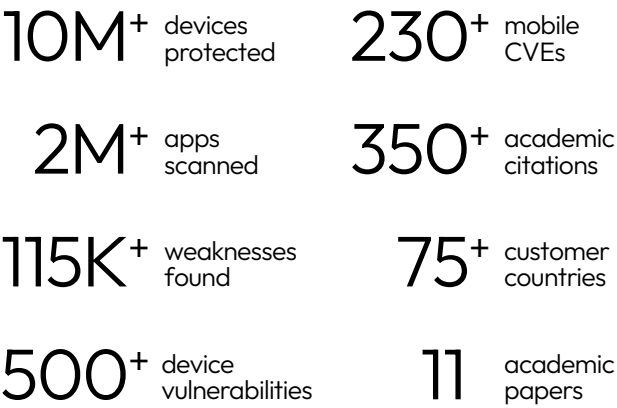
Employee Convenience

Users can enjoy the convenience of using their mobile devices for work while maintaining personal privacy and security.

Consolidated view of BYOD mobile fleet

Provides IT and security teams a single source of device security and regulatory compliance without user privacy concerns.

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

2M+ apps scanned

115K+ weaknesses found

500+ device vulnerabilities

230+ mobile CVEs

350+ academic citations

75+ customer countries

11 academic papers

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