Quokka

GUIDE

From Overpriviledged to Shifty

A guide to mitigating mobile app threats

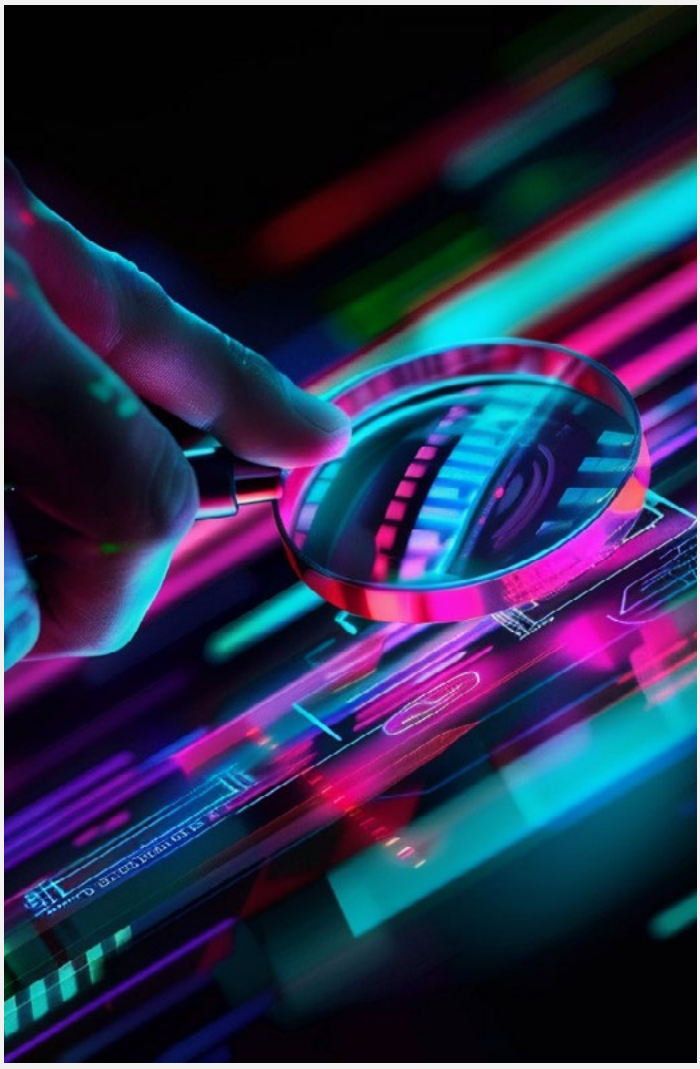
Quokka

GUIDE

Executive Summary

Apps have become the new endpoint for the modern enterprise, driving productivity, revenue, and customer engagement. However, their widespread use has also made them prime targets for cyberattacks. This guide will introduce you to various types of mobile app threats, using Quokka's unique view into this threat landscape.

We'll explore the latest threat vectors, offer insights into the risks posed by both in-house and third-party apps, and share proven strategies for mitigating these threats. Whether you're a seasoned CISO or mobile app developer, our goal is to arm you with the knowledge and tools you need to protect your most valuable assets.



Introduction

Mobile apps have become an integral tool for enterprise productivity and customer engagement. However, their security has never been more critical nor more challenging. Once simply a driving force for innovation, the mobile app ecosystem has rapidly transformed into a complex environment where threat actors are continually searching for vulnerabilities, exploiting code weaknesses, and aiming to compromise the tools organizations rely on to succeed.

For enterprise security teams and CISOs, this presents a daunting challenge: safeguarding a widespread, evolving landscape of mobile apps, while enabling the organization to innovate and grow. The stakes are high—not just in terms of potential data breaches and financial losses, but also in the loss of trust that can result from the exposure of sensitive information.

Mobile Apps: The new endpoint in the enterprise

Mobile apps are no longer just add-ons or conveniences—they've become essential to modern enterprises.

Globally, approximately 4 billion iOS and Android mobile devices are in use, each with **an average of 80 apps** that receive updates around **12 times a year**. This results in trillions of app endpoints that routinely handle sensitive data, connect to cloud services, and access critical enterprise systems. In contrast, there are about 1 billion active desktops worldwide, making mobile apps the newest and largest attack surface in today's digital landscape. The sheer volume of mobile endpoints and the frequency of their updates underscore the massive scale at which data is harvested, transmitted, and potentially exposed to security threats on a daily basis.

Recent data shows that 31% of decision-makers report that mobile deployments significantly boost employee productivity, 27% attribute increased revenue to these tools, and 26% highlight their role in improving customer service. These statistics reflect the deep integration of mobile devices and apps into core business operations.[1]

Types of mobile apps in the ecosystem

First-party apps (in-house developed):
These are apps developed by a company specifically for its own use, whether for internal productivity or consumer engagement. They are tailored to the company's specific needs but must be carefully secured and tested to prevent vulnerabilities.

Third-party apps:
These apps are developed by external companies and are widely available in app stores like Google Play and Apple's App Store. They range from productivity tools (e.g., Microsoft Office, Slack) to specialized business apps (e.g., Salesforce, QuickBooks). Third-party apps are not under direct control of the organization, presenting unique security challenges.

Unmanaged personal apps:
These are apps that employees install on their personal devices, which can also be used for work purposes (BYOD). These apps can range from social media and games to personal productivity tools. They often introduce risks due to lack of vetting and potential exposure to malware.

Beyond One App: The risks of a mixed app ecosystem

Mobile apps present countless inherent risks that organizations must navigate, impacting both the apps they build in-house and those they deploy for productivity. These risks stem from insecure coding practices, inadequate testing, and the integration of third-party libraries and software development kits (SDKs). Both first-party and third-party apps can introduce security risks. Below, we categorize these risks into business and cybersecurity threats.

Risks of mobile apps by type

First-party apps:

- **Data exposure and privacy risks:** Since these apps often handle sensitive data, such as customer information, financial records, or proprietary business information, any security flaw could lead to data breaches. If encryption, secure storage, or data transmission protocols are not properly implemented, sensitive data can be exposed.

Third-party apps

- **Lack of control over security:** Organizations have limited control over the security practices of third-party app developers. This can lead to risks, such as vulnerabilities in the app's code, weak encryption, or poor handling practices beyond the organization's control.
- **Data privacy concerns:** Third-party apps used for work can require access to sensitive enterprise data, such as usernames and passwords, including email accounts. This can result in data breaches or violations of data privacy regulations.
- **Inconsistent updates and patch management:** Third-party apps may not be updated regularly, leaving them vulnerable to newly discovered threats. Without consistent patch management, these apps can become entry points for attackers.
- **Compliance issues:** Depending on the jurisdiction and industry, third-party apps may not meet necessary compliance requirements for data protection and security, leading to potential legal liabilities.

Unmanaged personal apps (BYOD)

- **Malware and phishing threats:** Personal apps, particularly those not vetted by corporate IT, can introduce malware or be exploited for phishing attacks. Employees might unknowingly download compromised apps that put company data at risk.
- **Data leakage:** Unmanaged apps might access and share sensitive corporate data without proper encryption or security controls, leading to potential data leaks. This is especially concerning when apps request broad permissions that overlap with work-related data.

1 | IDC: 2023 U.S. Enterprise Mobility Decision Maker Survey: Devices, August, 2023

- **Lack of compliance:** Personal apps are often not subject to the same regulatory scrutiny as enterprise apps. If these apps access or store company data, they may inadvertently cause the organization to violate data protection regulations.
- **Difficult in monitoring and control:** IT departments often struggle to monitor and control personal apps on BYOD devices, leading to blind spots in the organization's security posture.

Overall business risks

- **Increased attack surface:** Each app, whether developed in-house or a third-party app used to run a business, introduces new endpoints that attackers can exploit. Failure to control this expanded attack surface can lead to multiple entry points for cybercriminals, making it easier for them to infiltrate the organization's network.
- **Financial impact and operational disruption:** Security breaches in mobile apps can lead to direct financial losses through theft or fraud, and incur indirect costs such as legal fees, incident response, and customer compensation.
- **Customer trust and business continuity:** A security incident that impacts a mobile app can impact customer experience and trust, resulting in customer attrition and a decrease in brand loyalty.
- **Intellectual property theft:** Proprietary algorithms, business logic, and sensitive product information embedded within apps can be reverse-engineered or stolen by competitors or malicious actors. Protecting intellectual property through secure coding practices, code obfuscation, and encryption is essential to prevent unauthorized access and safeguard competitive advantage.

In reviewing the risks associated with different types of mobile apps–whether they are developed in-house, sourced from third-parties, or installed by users–reveals a complex multifaceted security landscape. Each category presents unique vulnerabilities that are enticing for adversaries to exploit.

The new frontier of mobile app threats

Quokka has identified several critical threat vectors that represent the most pressing risks in the mobile app landscape. These vectors are not just abstract concepts – they reflect real-world tactics used by attackers to compromise mobile apps, including the sensitive data they handle. Understanding and addressing these vectors is essential for any organization building apps or using mobile devices for work.

Overprivileged apps

Overprivileged apps abuse unprotected permissions, gaining more access than necessary, which can lead to data exposure and exploitation by malware. Quokka's research and development team discovered that TikTok requires an excessive number of permissions from users, surpassing the data access norms of most social media platforms. Specifically, TikTok was found to gather an abundance of data, with permissions enabling access to unnecessary information, such as all data contained in a user's notifications. These actions sparked serious concerns regarding user privacy and security.

Harvester apps

Harvester apps collect data users willingly share with them, but they tend to collect more information than necessary for their stated purpose. An example of this is the popular fitness app Strava, which was found to collect and share users' location data even when they were not actively using the app. These harvester apps also pose a security risk if the collected data falls into the wrong hands.

Colluding apps

Colluding apps expose their data to other installed apps without the user's knowledge or consent, making them particularly challenging to detect. Unlike benign apps that share data by design–e.g., Google or Office365– colluding apps expose these data exchanges to create hidden networks or unauthorized data flow. A seemingly harmless social media app could access notifications from other apps and covertly share this information with other third-party entities, posing a significant risk to security and privacy.

Shifty apps

Shifty apps change drastically between versions, often introducing malicious features or vulnerabilities from one version to another. An application that adjusts music speed, available in Google Play Store version 12.6.2, is considered more secure than the later release, 13.1.1. Quokka's Q-mast report flagged the later version with a

risk rating of 99.3 compared to 34.8 for the earlier version. Whether intentional or not, this highlights the crucial need to thoroughly test mobile apps before their release to the public and continually vet the apps on devices used for work.

Sloppy apps

Sloppy apps contain poorly written code that doesn't follow security best practices, leaving them vulnerable to exploitation. An popular mobile app aimed at helping locate a user's Android device harbors hard coded cryptographic keys. As per a recent Q-mast report, the app has the potential to inadvertently disclose a user's password through network transmissions, local device storage, or logs. This scenario serves as a poignant illustration of the hazards stemming from negligent app development practices.

Chatty apps

Chatty apps can interact with SMS or MMS to make calls without prior authorization. A popular AI-powered photo editing app was found to interact with sending SMS/MMS messages. Accessing the ability to send SMS messages should be approached with caution. The application has the capability to transmit content of the app's choosing to any SMS-enabled number, potentially enabling deceptive communications and subscriptions to paid SMS services.

Leaky apps

Leaky apps reveal personally identifiable information (PII), putting users at risk. At DEF CON 32, Ryan Johnson, Quokka's Principal R&D Engineer presented the multifaceted Android ecosystem, highlighting examples of leaky apps found across several major vendors. His research uncovered how app usage reveals the subset of the apps that the user actually interacts with, which can be collected, combined with location data, and analyzed for advertising, profiling, and establishing user pattern-of-life.

Sticky apps

Sticky apps remain active in the background, continuing to collect data and operate without users' awareness, posing ongoing security risks. The app may employ this permission to terminate background processes of other apps on the device, potentially causing a denial of service to those apps. Developers must thoughtfully evaluate the necessity of this permission for the app's core functionality.

Quokka's unique categorization of mobile app threats provides more insight and enables security teams to enhance their framework for understanding and mitigating the diverse risks associated with mobile apps. As mobile app usage continues to rise, it is crucial for both developers and users to be aware of these potential threats and take steps to protect their data and devices.

Strategic pillars for effective mobile app security

For effective mobile app security, executives must take the lead by prioritizing and investing in security measures, especially as the mobile attack surface expands in both size and complexity. Rather than constantly reacting to threats and managing the consequences of data breaches, organizations can adopt preventative strategies to mitigate risks before they manifest. We don't have to accept risky apps as the norm. Instead, by fostering a proactive approach, we can create a safer mobile environment for everyone.

Develop a mobile security-first culture

Creating a security-first culture within an organization involves embedding security into every aspect of mobile app development and deployment.

- **Encouraging a security-first mindset:** Security should be prioritized across all departments. Regular training between development, operations, and business units is essential for a unified security strategy. Educating users on how to responsibly use the mobile app can greatly improve its security.
- **Collaboration between app developers and security teams:** Collaboration between developers and security teams is crucial for ensuring a secure mobile app. This includes integrating security reviews and audits into the development process, along with open communication to tackle security issues.
- **Regular testing and monitoring apps:** It is important to regularly test and monitor mobile applications for vulnerabilities and potential threats, otherwise known as "mobile app vetting."

Future-proofing mobile app security

Effectively addressing mobile app risks requires a holistic strategy involving development practices, security measures during production, and end-user perspectives. While eliminating all code weaknesses is challenging, organizations can proactively enhance their mobile app security by taking the following:

Secure development practices

- **Integrate security throughout development:** Incorporating security checks at every stage of the development life cycle helps identify weaknesses and vulnerabilities early. This includes static and dynamic testing, secure coding practices, and regular code reviews.
- **Regular app security testing and patching:** Regular security testing and promptly patching identified vulnerabilities are crucial to maintaining robust security. This includes static and dynamic analysis, as well as penetration testing to simulate real-world attacks.
  - **Static AST (SAST):** This approach analyzes the app's binary code before compilation to uncover security flaws at the code level. SAST is typically employed early in the development process.
  - **Dynamic AST (DAST):** DAST assesses the app's behavior during runtime, simulating attacks to detect vulnerabilities in production.
  - **Interactive AST (IAST):** IAST inserts agents into the app to analyze both its code and behavior during manual or automated testing. Unlike SAST and DAST, IAST focuses on specific parts of the app, as defined by the tester, rather than the entire code base.
- **Vetting third-party libraries and SDKs:** Given the widespread use of third-party components in app development, it's essential to vet these for security vulnerabilities and maintain an updated inventory of approved libraries and SDKs.

In-production security

- **Code obfuscation:** Implementing code obfuscation techniques can protect against reverse engineering, making it harder for attackers to deconstruct the app's logic and identify vulnerabilities.
- **Continuous monitoring for malicious activity:** Utilizing tools that provide real-time monitoring and alerting can help detect anomalous behaviors indicative of a breach or ongoing attack.

End-user security considerations

- **Managing user behaviors:** Educating users on safe practices, such as recognizing phishing attempts or avoiding sideloading apps, helps mitigate risks associated with human error.
- **Ensuring secure access to corporate resources: E**nforcing strong authentication mechanisms and access controls ensure only authorized users can access sensitive corporate data and resources.

By integrating security into organizational processes, mindsets and practices, companies can better protect sensitive data, enhance user trust, and maintain business continuity in an increasingly mobile-centric world.

Leveraging contextual app intelligence

Traditional mobile defenses are no longer sufficient to protect against the sophisticated and diverse threats facing mobile apps. Contextual mobile security intelligence bridges this gap by utilizing ML-based engines to detect malicious intent and unknown threats before an app is executed, enabling proactive detection of anomalies and potential threats. This multi-dimensional approach goes beyond mere app analysis, focusing on understanding app interactions and behaviors within the mobile environment to provide a stronger, more resilient security posture.

- **Integrate with existing security infrastructure:** Contextual intelligence should be integrated with existing mobile security tools, such as mobile threat defense (MTD), mobile app vetting (MAV), and mobile device management (MDM) and processes, to provide a complete view of the mobile threat landscape.
- **Invest in advanced analytics and machine learning:** Leveraging advanced analytics and machine learning algorithms to power detection engines can enhance the ability to dynamically detect and respond to advanced persistent threats.

- **Continuous monitoring and update of contextual data:** Maintaining up-to-date mobile threat intelligence is crucial for effective threat detection and response. Organizations should ensure continuous monitoring and regular updates to their contextual app intelligence engine.
- **Context-aware security:** The multi-dimensional approach enables a deeper understanding of how apps interact and behave within the mobile environment. This context-aware security framework allows for more accurate threat assessments and tailored responses, enhancing overall security posture.

Conclusion

As mobile security remains under-invested, the mobile attack surface continues to increase in size and complexity across all sectors. Unvetted, high-risk apps are proliferating on mobile devices that access enterprise data and assets. This whitepaper highlights various mobile app threats, from over privileged and colluding apps to shifty and leaky apps, each posing unique risks to organizational security and user data. Addressing these threats is crucial for maintaining a secure and resilient mobile app ecosystem.

To effectively manage mobile app risks, organizations should take a comprehensive approach to security. This involves secure development practices, ongoing monitoring, testing, and utilizing advanced tech like ML for contextual app intelligence. Fostering a security-first culture, prioritizing collaboration between developers and security teams, enhances data protection and business continuity.

Quokka

Let us help secure your mobile apps today

By partnering with Quokka, organizations can ensure that their mobile app ecosystem is protected against emerging threats and vulnerabilities. We work closely with our customers to understand their specific needs and customize our solutions to fit their unique security requirements. With our cutting-edge technology and experienced team, we are committed to providing the highest level of protection for your mobile apps.

Quokka offers two powerful solutions to meet the needs of both developers and organizations:

Qmast

> **Q-mast is an all-in-one SAST/DAST/IAST solution** that secures your mobile apps by scanning the compiled version—just like what you publish to the store. This approach ensures comprehensive coverage, including your custom and third-party code bundled with your app, without needing the source code.

Qscout

> **Q-scout provides actionable insights into the managed and personal apps** installed on mobile devices accessing enterprise resources and data. By analyzing malicious behaviors, security vulnerabilities, and privacy issues, enterprise security and IT teams can receive alerts and enforce proactive security measures based on risk-based policies they set for their organization.

Powered by the industry's only Contextual Mobile Security Intelligence engine, Quokka delivers actionable insights to proactively protect against malicious apps and zero-day exploits. Request a demo today and discover how Quokka can help safeguard your organization.enhancing their security posture and minimizing threats.

Learn more at www.quokka.io or email info@quokka.io.