



Is Your **Mobile App** a Gateway for **Attackers** or a **Fortress** for Your Business?

Mobile Application Risk Assessment & Security Evaluation,
Briskinfosec Your Cyber Risk Management Partner



CREST Registered
Region - Global



Your Mobile App Holds Your Customer's Trust, and Their Data

Your mobile application isn't just software, it's a direct line to your customers' most sensitive information. Every login, every transaction, every personal detail flows through code that lives on devices you don't control, in environments you can't predict. When mobile security fails, it fails publicly, catastrophically, and with lasting damage to customer relationships.

The modern threat landscape doesn't distinguish between enterprise infrastructure and mobile endpoints. Your app runs on devices shared with malicious applications, connects through untrusted networks, and stores sensitive data in spaces accessible to sophisticated attackers. A single vulnerability in your mobile application can expose millions of customer records, disrupt revenue streams, trigger regulatory penalties, and permanently damage brand reputation built over decades.

Every CTO Should Ask

If our mobile app was compromised tomorrow, what would be the business impact, and how long before we'd even know?

Your Cyber Risk Management Partner Reducing business uncertainty from mobile application risk, not just finding technical flaws.

The Business Impact of Mobile Security Gaps

Data Breach Exposure

Customer credentials, payment data, personal information stored insecurely on millions of devices

Revenue Disruption

App store removal, payment processor suspension, transaction fraud losses

Regulatory Penalties

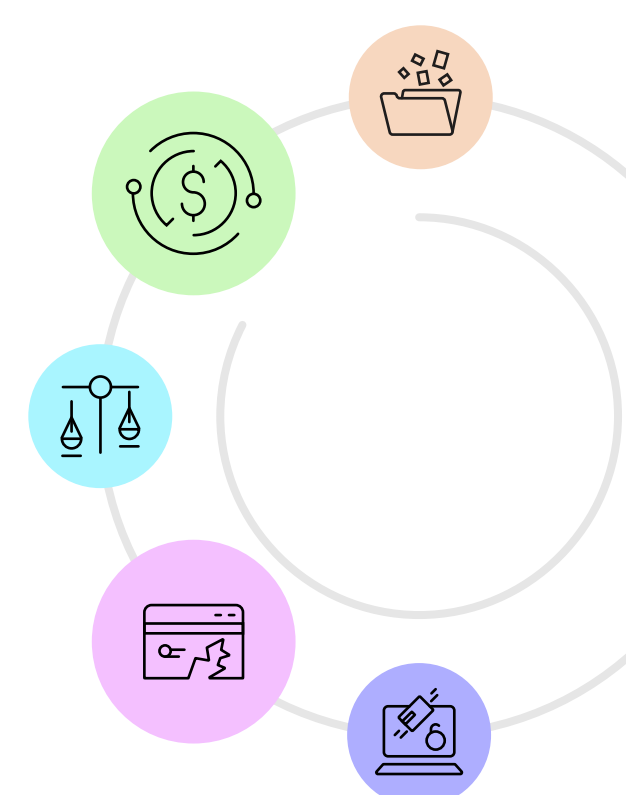
GDPR, DPDPA, PCI-DSS violations with fines reaching 4% of global revenue

Brand Devastation

App store reviews, social media backlash, customer exodus to competitors

Intellectual Property Theft

Reverse engineering exposing business logic, algorithms, API keys



No Shortcuts, No Sampling

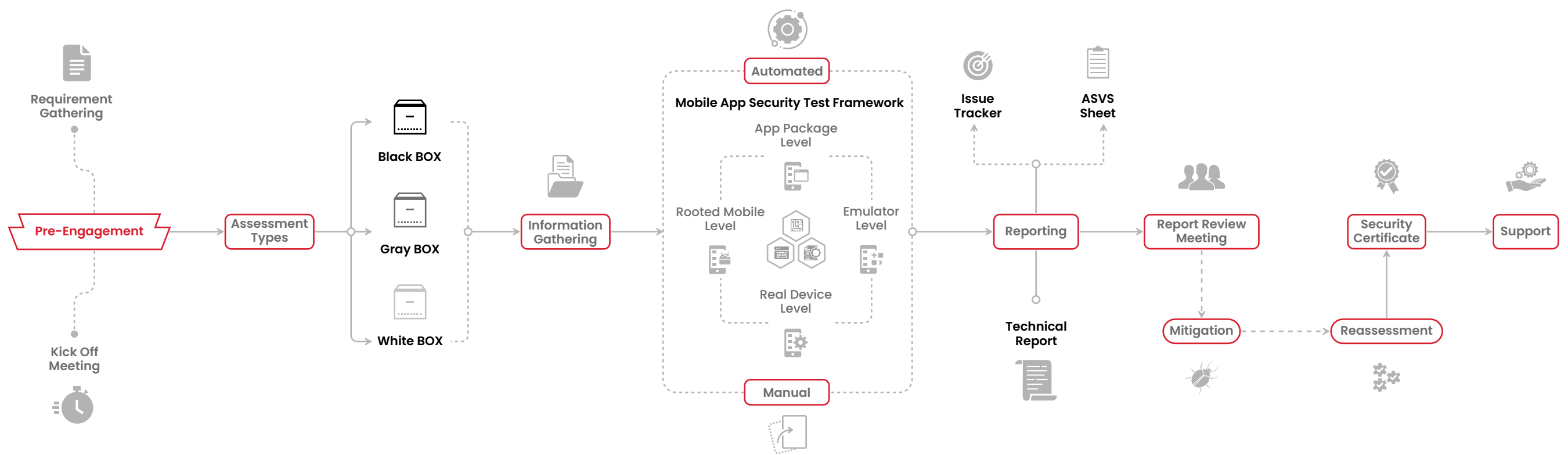
Mobile security isn't about running automated tools and generating reports. It requires understanding how your app behaves in hostile environments, how data flows between components, and how attackers think when targeting mobile platforms. We test like adversaries, not auditors.

Our mobile security engineers combine advanced technical capabilities with business context awareness. We don't just identify vulnerabilities, we map security findings to business consequences, helping you understand what matters most to your operations, your customers, and your compliance obligations. Every test is customized to your specific application architecture, business model, and risk tolerance.

NOT a Vulnerability Scan Report	NOT a Checklist Compliance	NOT a Generic Findings List	NOT a One Time Test
A Risk Register with Business Impact connecting findings to business	A Comprehensive Assessment covering iOS, Android, APIs, and backend integrations	Platform-Specific Analysis addressing unique risks of each mobile ecosystem	Continuous Risk Visibility through our LURA platform for ongoing posture management

What Our Mobile Security Engineers Actually Test

Binary Analysis & Reverse Engineering Decompilation, code analysis, hardcoded secrets, obfuscation bypass	Data Storage Security Keychain/Keystore implementation, SQLite databases, shared preferences, cache analysis	Network Communication Certificate pinning bypass, man-in-the-middle testing, API security, traffic analysis
Authentication & Session Management Token security, biometric bypass, session fixation, credential storage	Runtime Manipulation Frida/Objection hooking, method swizzling, root/jailbreak detection bypass	Business Logic Testing In-app purchase bypass, premium feature unlock, workflow manipulation



What We Need From You

No documentation? No problem.

We'll conduct discovery and help you understand your mobile risk surface first.

Application Access



Binaries (IPA/APK) or TestFlight/Play Store access

Test Accounts



Various privilege levels for comprehensive testing

Documentation



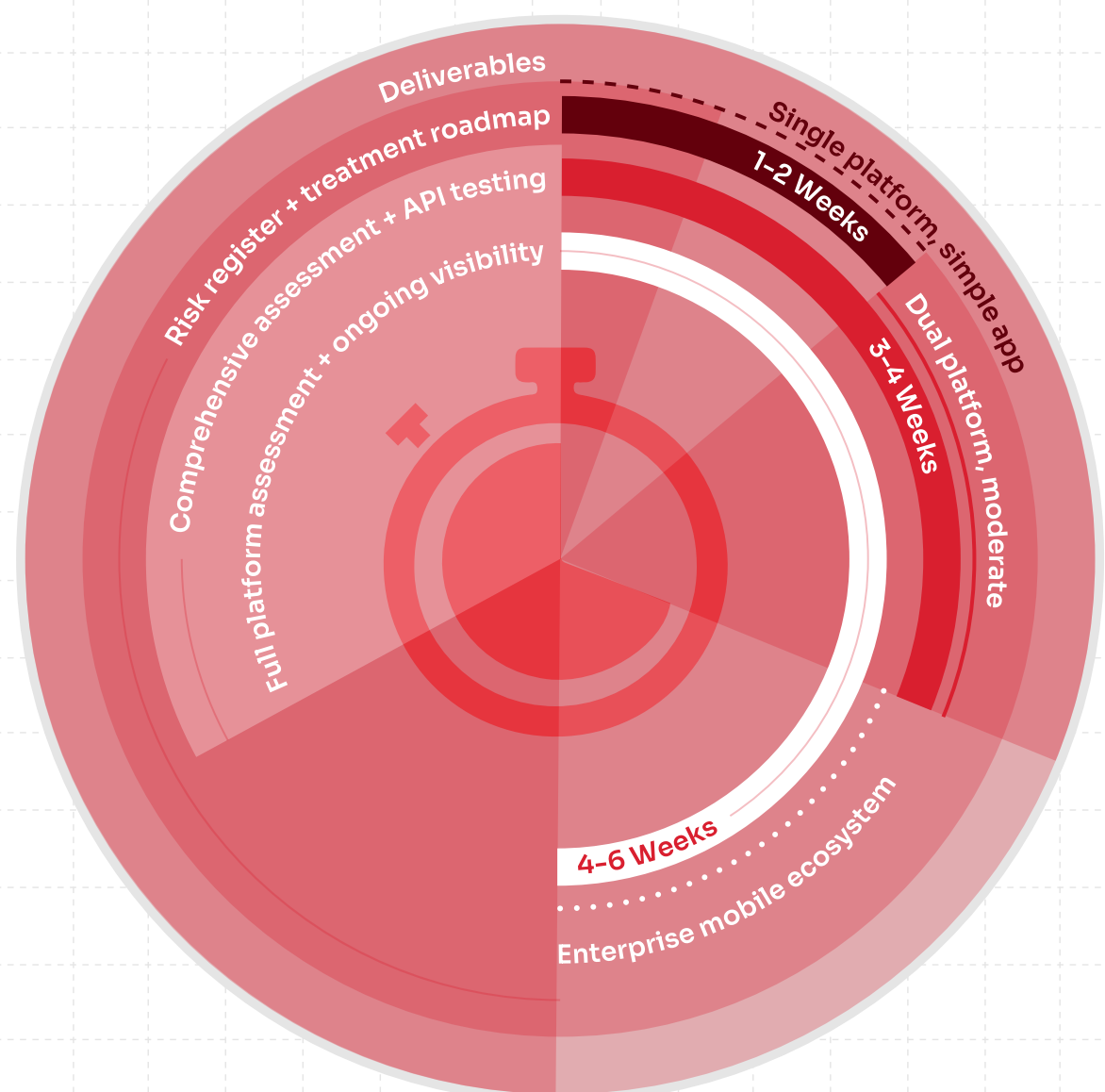
API docs and backend architecture overview (helpful but not required)

Business Context



Critical features and business priorities

Timeline & Investment



App Scope	Assessment Duration	Deliverables
Continuous partnership	Risk treatment lifecycle management	Ongoing

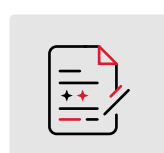
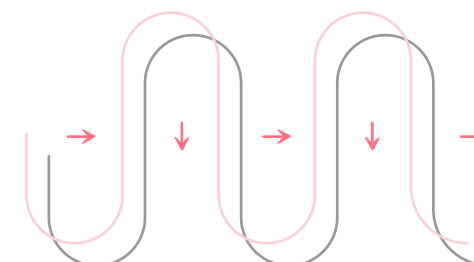
Standards we follow

Platform coverage (iOS, Android, or both), app complexity and feature set, backend API integration depth, compliance requirements (PCI-DSS, HIPAA, etc.), and current security maturity baseline.

Our Deliverables

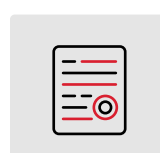
Every engagement produces actionable intelligence designed for both technical teams and executive leadership. Our deliverables translate technical findings into business risk language, enabling informed decision-making at all levels of your organization.

We don't just hand you a report and walk away. Each deliverable is accompanied by consultation sessions where we walk through findings, answer questions, and help you build a practical treatment roadmap aligned with your business priorities and resources.



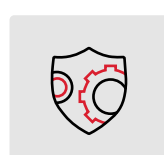
Risk Register

Business-contextualized findings with impact analysis showing what matters to your operations



Platform Specific Reports

Detailed iOS and Android findings with reproduction steps



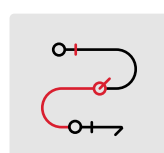
API Security Assessment

Backend endpoint testing specific to mobile app flows



bSAFE Score

Maturity rating aligned with OWASP MASVS for industry benchmarking



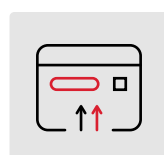
Risk Treatment Roadmap

Prioritized actions by business value with effort estimates



Executive Summary

Board-ready risk communication in business language



LURA Platform Access

Continuous risk visibility and treatment tracking

Our Commitment

Every engagement we undertake is built on understanding your business first, technology second. We measure success not by the number of vulnerabilities we find, but by the amount of business risk we help you reduce.

Your mobile application is a critical business asset and a direct channel to your customers. It deserves a security approach that protects both.

” We don't sell tests. We sell risk clarity and treatment.

Ready to Start?

The conversation begins with understanding your mobile app, your users, and your business objectives. Let's talk about what keeps you up at night, we'll show you how to sleep better.

Schedule Discovery Call

Mobile App Security Report

What Happens Next?



Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

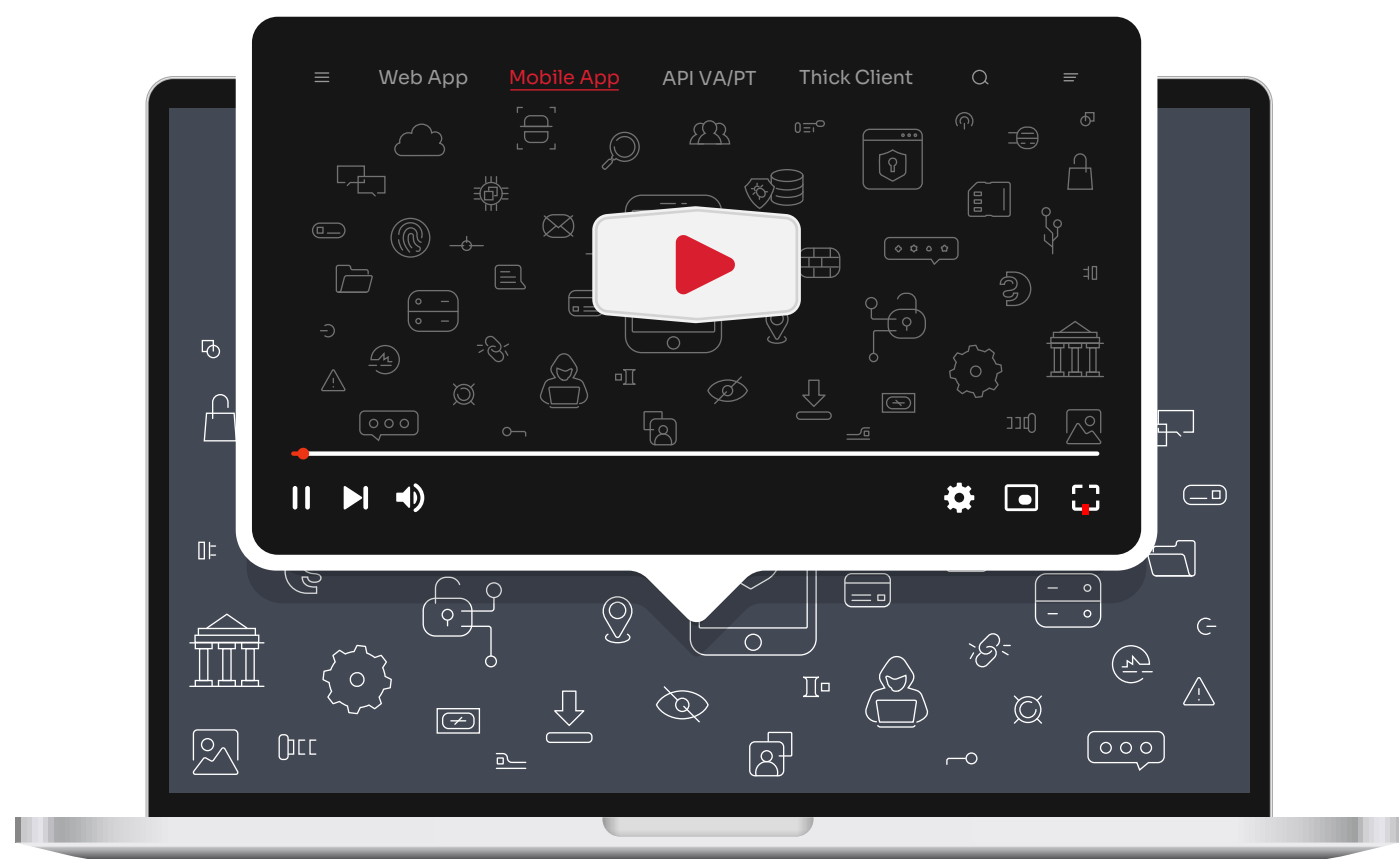
Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited Internationally certified penetration testing excellence	CERT-IN Empanelled Government-recognized trusted cybersecurity assessment provider	ISO 27001 : 2022 Certified Our own security practices are independently audited and verified annually
---	--	---

25+ Countries Client Portfolio	67% Logic flaws missed by bots	98% Client retention	640+ Successful Customers	5600+ Delivered in 24 countries
--	--	--------------------------------	-------------------------------------	---



Reach us for FREE

consultation



Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence

