The Guardian

Guarding Mobile Apps

Protecting mobile apps that run within untrusted environments is ever more crucial as mobile become ubiquitous. Hackers and their targeted malware are an increasing threat to the mobile revolution. With the explosive growth of the mobile channel and user demand for anytime/anywhere access to mobile services, app providers are challenged to keep up with security, which increases exposure to malicious attacks.

Why The Guardian ?

Defeats Targeted Attacks:
The Guardian proactively protects your apps against zero-day and other targeted attacks, allowing mobile apps to run securely, even on highly infected devices. If a hacker attacks, The Guardian will respond by taking necessary measures to fully protect your apps.

Dosen't affect user experience:
The Guardian protects multiple business apps and is not bound to one application with one business logic, it allows for effective scaling across multiple apps of the organization while maintaining an optimal user experience.

Quick to deploy:
The Guardian provides an automated implementation process. Once integrated, The Guardian sifts through the business logic, event and data flows of the app, before binding itself to existing code. This allows organizations to quickly release protected apps, without affecting the development timeline!

Trusted by Tier 1 clients worldwide!
TrustSec works across a range of industries with a variety of global Tier 1 clients, counting customers in industries such as finance, health, IOT, and the public sector. TrustSec's patented deep protection technology The Guardian , protects apps and applications used by more than 100 Million users.

+48784784 504
info@trustsec.net
www.trustsec.net

The Guardian secures apps against:

- Malware
- Debugger (Java Debugger, Native debugger)
- Emulator/fake execution environment
- Cloning of the device
- Rooting/Jailbreak
- Code-Injection (prevent Runtime Library Injection)
- Hooking-Frameworks
- Repackaging (Fake, Manipulated Apps)
- System- and User-Screenshots
- Keylogging : untrusted Keyboards
- Keylogging and Screen-Scraping : untrusted Screen-readers
- Native Code-Hooks
- External Screen sharing (content being displayed 'outside' the screen of the device
- Asset integrity checks: The Guardian can perform more in-depth integrity checks of files and assets inside the APK.
- The Guardian will verify the integrity of the matched files when starting the application.
- API: Foreground override detection ("Overlay- Detection")

  This feature detects if another application is placed in front of the currently working application in order to perform a phishing attack. This is sometimes referred to as an overlay attack, which has been widely known to be done by certain types of Android malware.
- Whitebox-Crypto features, to prevent 'important keys' from being present (and possible stolen) in memory at any time.
- Stealing of sensitive data from the app (at rest or otherwise)
- Man-in-the-App Scenarios
- Man-in-the-Middle Scenarios (related to network communication)

Trusted By Customers Worldwide!

100's
of millions of users

+48784784 504
info@trustsec.net
www.trustsec.net