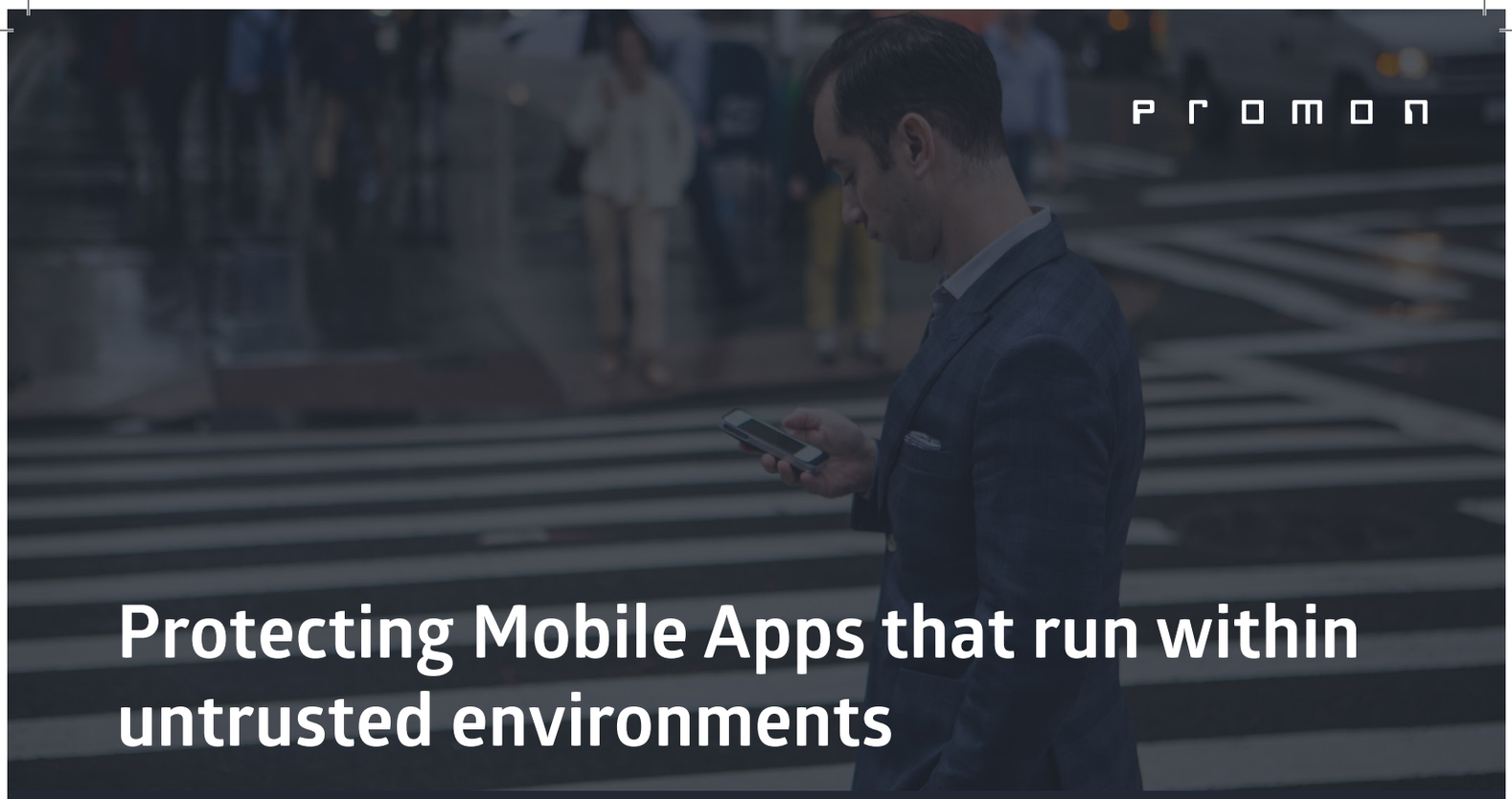

Protecting Mobile Apps that run within untrusted environments

Protecting mobile apps that run within untrusted environments is ever more crucial as mobile become ubiquitous. Hackers and their targeted malware is 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 Promon SHIELD™

Defeats targeted attacks

Promon SHIELD™ proactively protects your apps against targeted attacks, allowing apps to run securely. If a hacker attacks, Promon SHIELD™ will respond by taking necessary measures to fully protect your apps.

Quick to deploy

Promon SHIELD™ provides an automated implementation process. Once integrated, Promon SHIELD™ 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!

Doesn't affect user experience

Promon SHIELD™ 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.

Trusted by Tier 1 clients worldwide!

Promon 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. Promon's patented deep protection technology Promon SHIELD™, protects apps and applications used by more than 100 Million users.

Promon SHIELD™ protects your mobile 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 – for example by screen sharing).
- Asset integrity checks: Promon SHIELD™ can perform more in-depth integrity checks of files and assets inside the APK.
- Promon SHIELD™ 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

About Promon

Promon is a Norwegian firm specialising in app hardening, with our solutions focusing largely on Runtime Application Self-Protection (RASP). The company works with a variety of global Tier 1 clients, counting customers in industries such as finance, health and the public sector. Promon's technology originates from the internationally recognized research environments at SINTEF and the University of Oslo. Promon's patented deep protection technology Promon SHIELD™, has protected apps and applications used by more than 100 Mill users since 2009. Promon AS is a Norwegian limited company registered in 2006, with offices in Germany, the UK and India.

Promon AS
Stortingsgata 4
0158 Oslo
Norway
+47 22 02 11 30
info@promon.no
www.promon.co