Business Description

Malwarelytics

wultra

Company Information

Basic Information

Company name	Wultra s.r.o.
Company address	Bělehradská 858/23, 120 00 Prague, Czech Republic
Registered at	235343 C, Municipal Court in Prague
Company ID	03643174
VAT ID	CZ03643174
Bank account	CZ3855000000003643174999 Raiffeisenbank a.s.

Contact Information

Business contact	Mgr. Petr Dvořák, CEO petr@wultra.com +420 728 727 714

Company Introduction

Wultra helps the leading European banks to make secure digital channels. Our range of security-related software technologies covers the whole digital banking application stack, be it on the web or mobile. Founded in just 2014, security solutions by Wultra already secure the best rated mobile banking app in the Czech Republic, an open banking gateway for the retail bank with over 300k clients, or a premium Internet banking for the most affluent clientele.

Raiffeisen BANK	ČSOB	CNB CZECH NATIONAL BANK
MONETA MONEY BANK	VISTA BANK	POSTA SHQIPTARE

Executive Summary

Advanced cyber-attacks that arise these days are based on misusing the weaknesses in mobile operating system and mobile programming models. Examples include attacks through mobile malware, jailbreaking and rooting, active memory manipulation, app repackaging, or injecting a foreign code or a framework. These attacks are impossible to mitigate using the standard security measures, such as cryptographic protection since in most cases, the attack principle invalidates the preconditions for such methods. As a result, makers of mobile apps must introduce the active in-app protection. By robust obfuscation and self-protecting code, it is difficult for the attacker to understand the inner workings of an application, and to prepare and execute a well-suited attack.

We want to help your company to be prepared for these new types of attacks. To help you avoid possible financial damage as a result of the new sophisticated threats, and to prevent potential damage to your brand reputation, we are introducing **Malwarelytics**.

The solution includes an extensive range of runtime application self-protection (RASP) features for iOS and Android platforms to make the mobile application runtime secure without impacting the user experience. At the same time, Malwarelytics provides an active anti-malware protection on Android. Either of these features does not have any significant impact on other mobile app attributes, such as application launch speed, UI responsiveness, or bundle size.

The integration into your mobile app cannot be any simpler and it **can be done in literally 10 minutes.** Therefore, using the Malwarelytics does not negatively impact your development resources or the go-to-market project schedule.

We believe that you will find the Malwarelytics value proposition appealing and that you will build a secure world of mobile applications with us.

Solution Trusted By Many

Over 500 banks and fintech companies world-wide already trust our mobile security technologies. Thanks to our proven track record, excellent partnerships, and strong focus on digital banking security, you are making the right and safe choice.

Raiffeisen BANK	ČSOB	MONETA MONEY BANK
VISTA BANK	Equa bank	zonky.cz
POSTA SHQIPTARE		… and more

> “Thanks to the security components by Wultra, we quickly responded to an increasing threat of mobile malware attacks and hardened our application security.

Tomáš Rosa
Chief Cryptologist, Raiffeisenbank

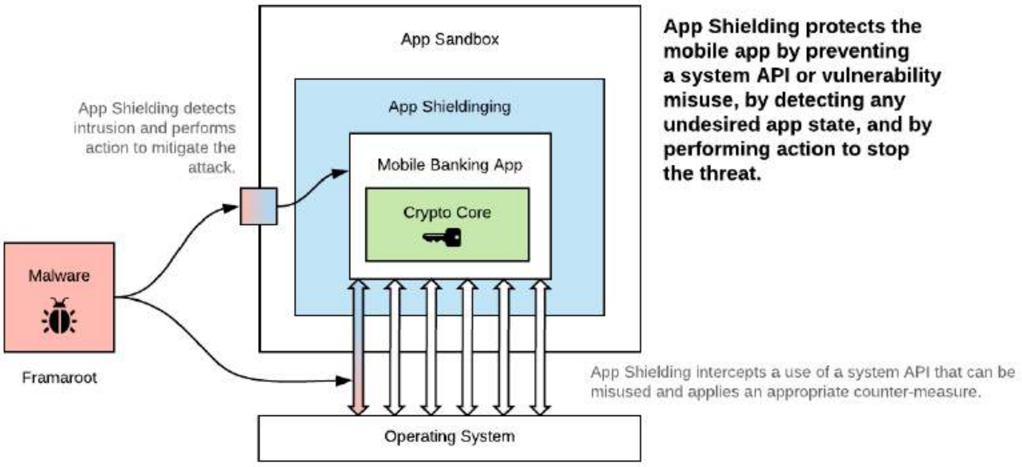
Technology Description

Malwarelytics provides additional protection to an app runtime against highly sophisticated attack scenarios that target the application in a potentially insecure mobile operating system, as well as active anti-malware protection on Android.

Malwarelytics works in three stages to protect your mobile app:

- ✔ Prevent non-standard situations by obfuscating the app and protecting runtime.
- ✔ Detect mobile malware or other non-standard situation whenever it happens.
- ✔ React to the discovered problematic situation and stop the possible attack.

These three stages of protection are implemented through integrating an SDK into your application, with just couple lines of code.



App Shielding protects the mobile app by preventing a system API or vulnerability misuse, by detecting any undesired app state, and by performing action to stop the threat.

App Shielding intercepts a use of a system API that can be misused and applies an appropriate counter-measure.

The technology is integrated on the mobile application side only and it automatically connects to our cloud interfaces hosted in the Azure cloud, making the data instantly visible via our online dashboard. There is no need to modify your in-house back-end components or deploy new ones. However, you can integrate your back-end systems with our cloud through RESTful APIs or via asynchronous webhooks to, for example, enhance data in your fraud detection system (FDS).

Solution Features

Malwarelytics protects your app from:

- ✔ Mobile malware.
- ✔ Screen-scraping via misuse of accessibility features.
- ✔ Keylogging and untrusted keyboards.
- ✔ Debugger connections (Java Debugger, Native debugger).
- ✔ App repackaging.
- ✔ Running in an emulator or insecure virtual environment.
- ✔ Device cloning.
- ✔ Rooting / Jailbreaking.
- ✔ Code-injection (Runtime Library Injection).
- ✔ Screen sharing (Chromecast, AirPlay, . . .)
- ✔ System or user screenshots.
- ✔ Foreground override attacks.
- ✔ Man-in-the-App, or Man-in-the-Middle.
- ✔ Untrusted installation sources.
- ✔ Tapjacking protection.
- ✔ Insecure configurations (disabled Google Play Protect, no screen lock).
- ✔ Outdated operating system or missing security patch.
- ✔ Detection of HTTP proxies or VPNs.

The Malwarelytics also adds more resilience by:

- ✔ Checking the integrity of application executables.
- ✔ Verifying the integrity of application assets (images, texts, . . .).
- ✔ Obfuscating the application code.
- ✔ Key protection using the "white-box crypto".
- ✔ Process cloaking (renaming the name of process).

Benefits for CISO

Comply with the PSD2 legislation requirements and the strictest OWASP security standards in mobile app security.

PSD2

OWASP
Mobile Application Security
Verification Standard
V8: Resilience Requirements

Solution Benefits

✔ Expert Threat Evaluation

By using Malwarelytics, you will outsource the security expertise and workload related to the new threat evaluation to our team of experts. We are dealing with the subject of mobile security 24x7 and we know mobile platforms inside-out. You do not need to hire an in-house security analyst who will have limited capabilities to evaluate and resolve the issue in time, and whose know-how will be limited to the view of a single organisation.

✔ Always There, Always Up-To-Date

Developing any security components, especially a malware detection and runtime application self-protection, is an ongoing research-heavy process that requires a knowledge of both the current threat landscape and the mobile operating system ecosystem. As Apple and Google keep updating their mobile operating systems, finding and implementing the right solution for a given security problem can quickly become a slippery slope. We make sure our components keep up with the ever-fast changing mobile ecosystem, and we deliver frequent updates of our components to protect your mobile apps.

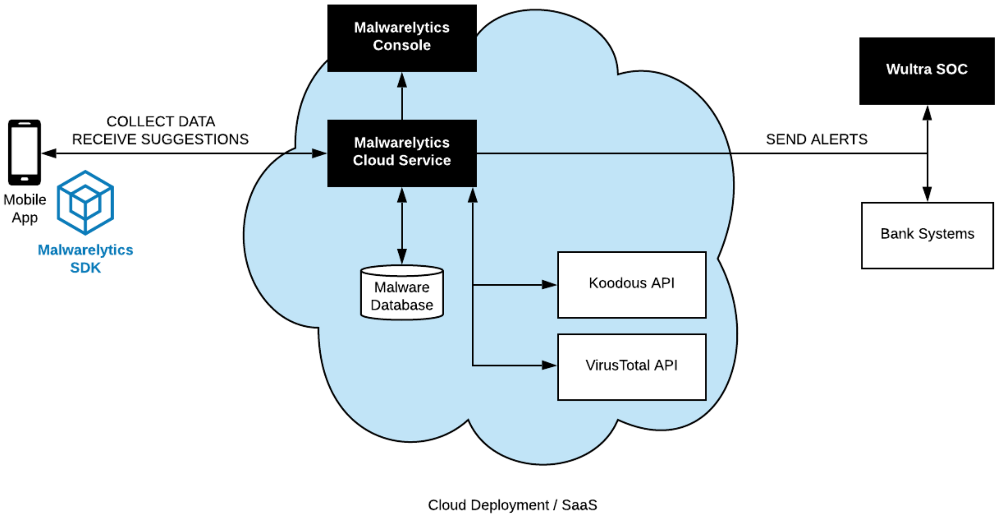
✔ Cross-Customer Knowledge

We deploy our SDK with multiple banks, and we collect threat intelligence from the best sources. Therefore, our know-how is not limited to the situation in a single organisation and a single approach. As a result, you and your mobile apps will benefit from security findings made elsewhere, before you can even experience the problem.

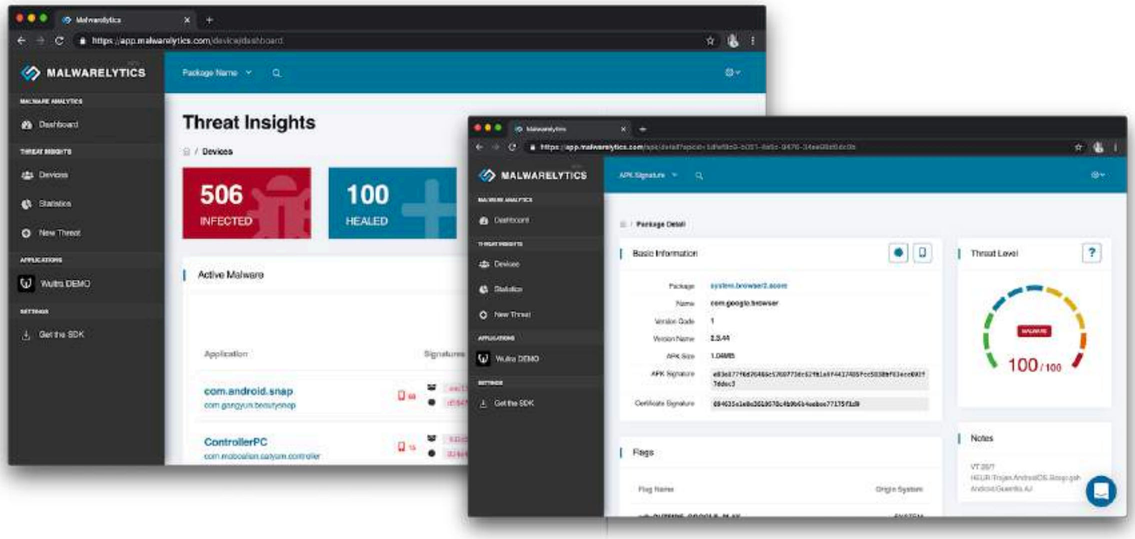
Threat Intelligence Dashboard

Besides the persistent on-device protection, we also provide visibility into the mobile device security landscape with our threat intelligence dashboard (provided as SaaS).

Malwarelytics is connected to our cloud components where our security operations center (SOC) carefully investigates all detections that need further examination.



Through easily accessible web interface, you can monitor current threats, see the important trends, stop mobile malware from causing any damage, and examine in-depth device security attributes (rooting, outdated OS, missing screen lock, etc.)



Threat Insights

/ Devices

506 INFECTED

100 HEALED

Active Malware

Application	Signatures
com.android.snap com.gangyun.beautysnap	
ControllerPC com.mobcalism.calyum.controller	

/ Package Detail

Basic Information

Package: system.browser2.acom
Name: com.google.browser
Version Code: 1
Version Name: 2.3.44
APK Size: 1.04MB
APK Signature: [illegible]
Certificate Signature: [illegible]

Threat Level

MALWARE

100 / 100

Notes

VT 26/7
HEUR:Trojan.AndroidOS.Boogr.gsh
Android/Guerrilla.A!

Flags

Flag Name	Origin System

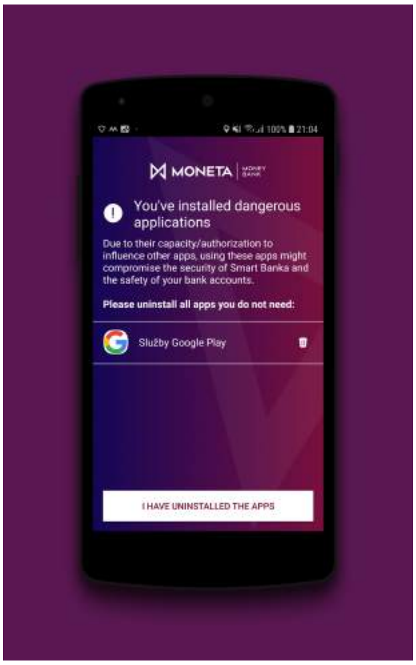
Persistent Malware Protection

With the rise of mobile malware on Android, it is no longer possible to dismiss the threat that applications installed on the end-user device pose to mobile banking. The banking malware is often very well prepared. Distributed via Google Play, it uses evolving and ever more sophisticated attack techniques that are tailor-made for the mobile ecosystem. These attacks are no longer just a theory. The end customers are already a target, the banks are losing money, and the situation is only about to get worse. To help you stay ahead of these threats, Malwarelytics protects your mobile banking from malware on the Android platform by turning your mobile banking into an antivirus app.

Malwarelytics helps you tackle mobile banker malware by:

- ✓ Detecting malware, dangerous apps and apps that are potentially unwanted.
- ✓ Indicating the reason why the app was classified in a given category.
- ✓ Protecting from malware even if the app is not running.
- ✓ Dynamic threat suggestions via on-line threat intelligence.
- ✓ Ready-to-use UI components to speed up mobile development.

Malwarelytics examines all applications installed on the end user's Android device. It checks if any of them use suspicious permissions (read SMS, install packages, uninstall software), registers accessibility services (ability to read screen content or perform gestures), performs overlay attack scenarios (task hijacking detection) or attempt any other suspicious activities. The device can then immediately notify the end user about a potential issue, or send a "call for help" to the bank's server, to be used by a fraud detection system (FDS) or by the security first-response team.



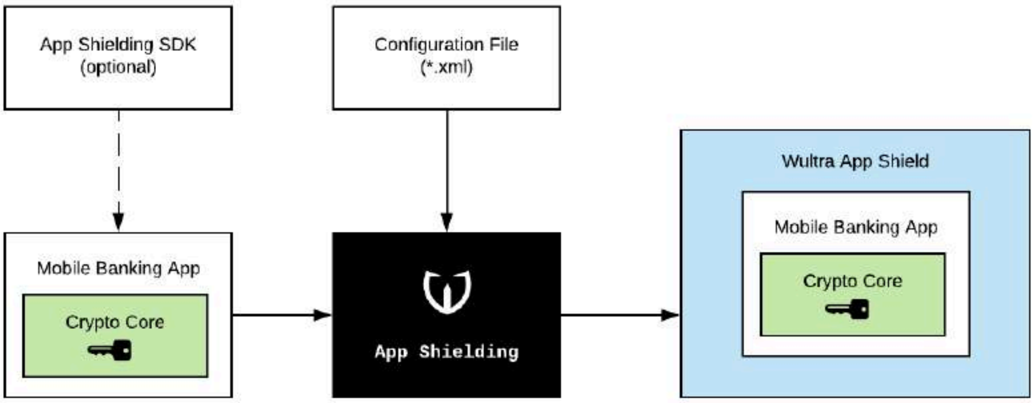
You've installed dangerous applications

Due to their capacity/authorization to influence other apps, using these apps might compromise the security of Smart Banka and the safety of your bank accounts.

Please uninstall all apps you do not need:

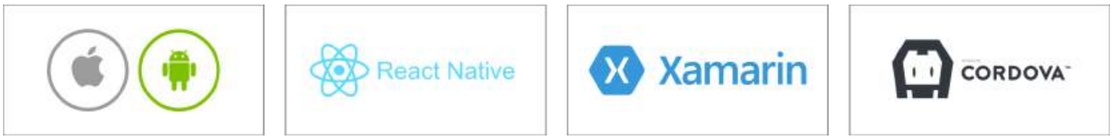
Additional Bundle Protection

Malwarelytics proposition contains a tool for „re-wrapping“ the application packages (*.ipa, *.apk) to achieve a highly obfuscated and hardened app version, automatically enhanced with a protective code.



Rich Mobile Platform Support

Besides native development, we support the most popular iOS and Android app development technologies to simplify your work during the solution implementation.



Licensing Model

The cost structure for the Malwarelytics consists of three cost components:

- ✔ Monthly developer support fee during the implementation phase.
- ✔ Annual license fee, price tiers based on the number of monthly active users.
- ✔ Enterprise support, price tiers based on the required support level (SLA).