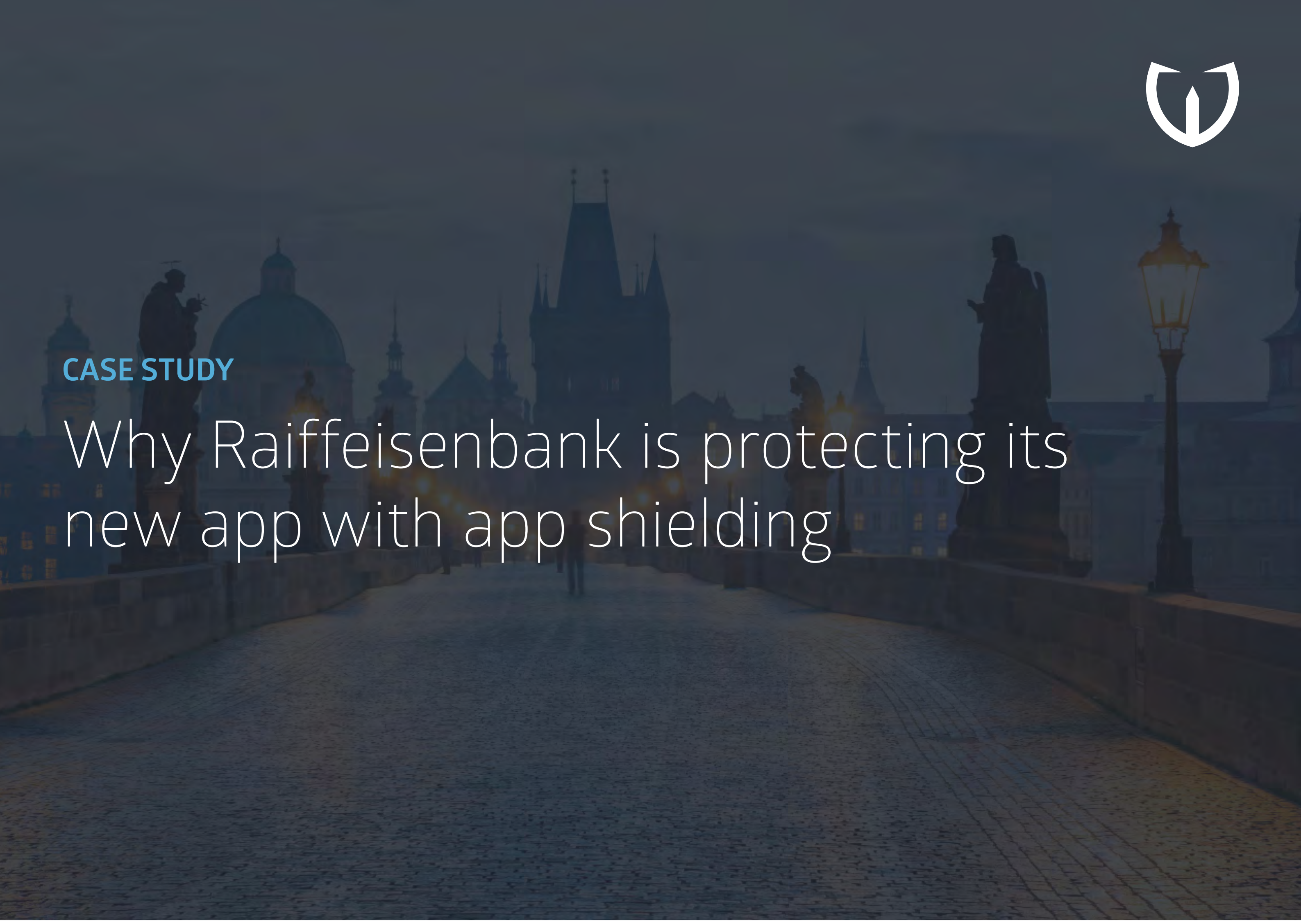


CASE STUDY

Why Raiffeisenbank is protecting its new app with app shielding

Raiffeisen
BANK
Banka inspirovaná klienty

Raiffeisen Bank International AG is an Austria-based company and part of the Raiffeisen Banking Group Austria (RBG). It serves commercial customers and financial institutions in Austria and Central and Eastern Europe through its network of subsidiary banks, leasing companies and specialized financial service providers.

Raiffeisenbank in the Czech Republic has been firmly established since 1993 and provides a wide range of banking services to private and corporate customers. It services its clients through 132 branch offices and client centres as well as specialised mortgage centres and private and corporate advisors. Raiffeisenbank's wide range of awards confirms the outstanding quality of the services it offers. One distinction that stands out is the repeated success in the Hospodářské noviny awards where Raiffeisenbank managed as first and still only bank to win in both main categories in the same year. It was awarded as Most Client-Friendly Bank of the Year for the third time in a row in 2017.

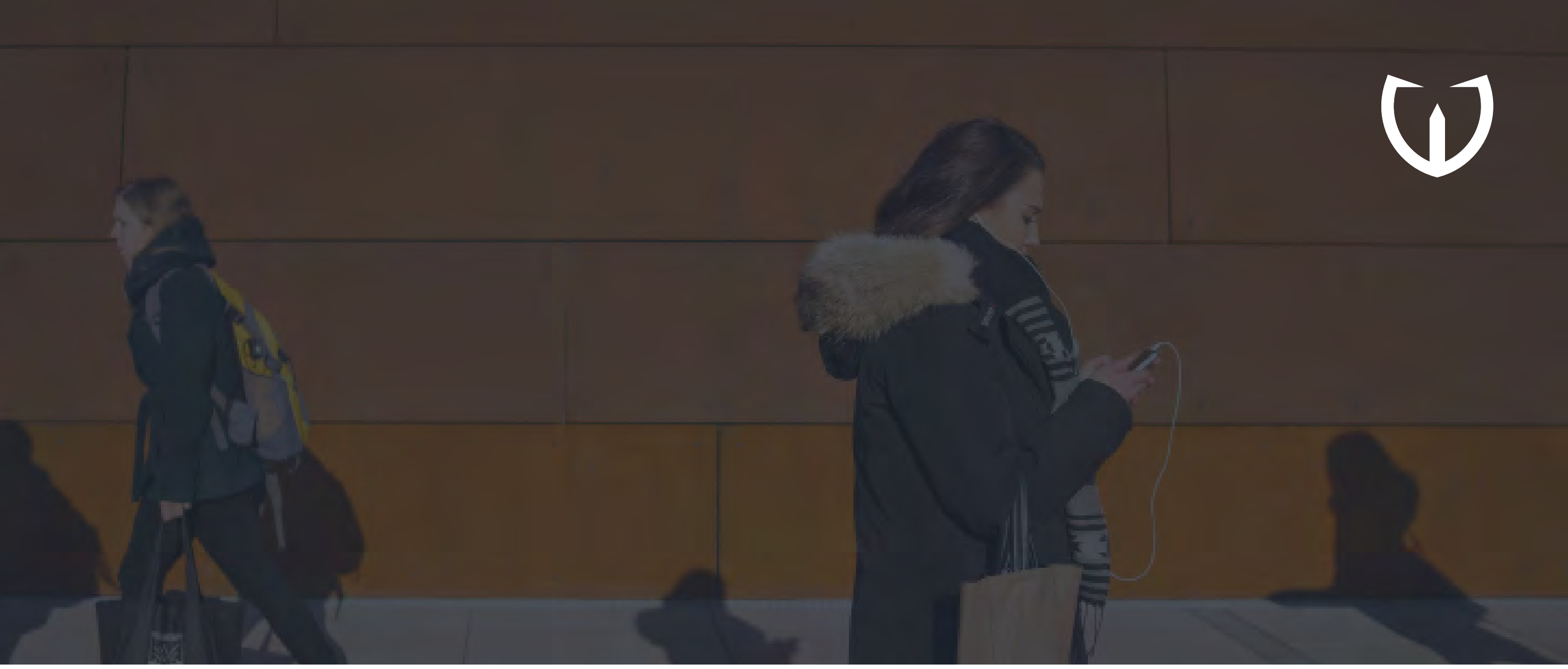
Mobile security threats on the rise

Mobile device security threats are both increasing in number and evolving in scope. And assuming that the mobile operating system alone can keep apps safe is a naïve approach.

Mobile banking apps reside on end-users' devices, which is an environment largely outside of banks control. The sensitive nature of unique identifiers such as passwords and other personal data makes them an ideal target for malware.

Cybercriminals use sophisticated tools to learn more about the inner workings of a banking app and its cryptographic key protection. Through these processes, hackers can plan their attack. By identifying entry vectors in an unprotected app, malware can steal sensitive user data through techniques such as keylogging and screenshots containing private password information. This approach, combined with efforts to steal cryptographic keys, make hackers a force to be reckoned with.

In addition to the security threats, the regulatory technical standards (RTS) for PSD2 define a whole range of new requirements for digital banking.



Compliant and secure with app shielding

App shielding technology protects mobile banking app users against malware and threats related to operating system weaknesses. At the same time, it helps banks to stay PSD2 compliant.

Raiffeisenbank recently released a new version of their mobile eKonto app. The new app is better, faster and more secure than ever before - and importantly, protected by app shielding. The bank is now protecting its new Mobilní eKonto app against threats including:

- Malware attacks
- Vulnerabilities related to rooting or jailbreaking
- Debugger connection
- Code or framework injection
- Application repackaging and app integrity breaches
- Malicious screen readers or untrusted keyboards
- Overlay attacks
- Man-in-the-app and man-in-the-middle scenarios

From the user perspective, nothing changes. The shielded app operates as usual—it doesn't require any additional permissions, and it doesn't alter the user experience in any way.

Fast and easy deployment

You can easily turn your app into a self-protecting app. Your Android or iOS app can quickly be uploaded and secured in minutes by using our integration tool, or an SDK that's easily integrated into the app.

App shielding was delivered to Raiffeisenbank in only a couple of weeks. Most of the time was spent on user testing; the shielding itself only took a few hours. The shielding process is fully automated and does not require any programming. Shielding the app is just a matter of running the scripts with an existing iOS or Android app package.

With the new mobile app by Raiffeisenbank, we can see a new trend emerging: Banks care about protecting mobile app runtime, and they seem to invest more resources in mobile app security in general.

Wultra

Wultra, s.r.o. helps the leading European banks to make secure and engaging digital channels faster. Their range of security-related software technologies covers the whole digital banking application stack.

Wultra is headquartered in Prague, the Czech Republic.

Wultra, s.r.o
Bělehradská 858/23
120 00 Prague 2
Czech Republic

+420 728 727 714

hello@wultra.com

www.wultra.com