30 august 2017 | Expert advices

Security or user experience : do you really have to choose?

Wannacry, NotPetya, Igexin, ... several names which have been making waves in the last few months. The recent increase in high-profile cyberattacks has reminded executives, CIOs and CISOs of the importance of security issues, as if such a reminder was needed.

In a world where digital is becoming the norm, protecting data used on devices is essential. To do so, there is one method: containerisation. This involves separating professional data from personal data on the mobile device in order to provide both with a greater level of protection. Today, two forms of technology exist: “native container” and “proprietary container”, each of which has a different approach.

The temptation to give absolute priority to security to the detriment of user experience is strong. But on the enterprise mobility market, good user experience is a key success factor. So, how can you make the right choice?

Proprietary container: security via restriction

Provided by EMM/MAM vendors, proprietary container consists of applying an extra layer to applications, which allows professional data to be **isolated and encrypted on the device**, **making them inaccessible**, even when the mobile OS is compromised (Root / Jailbreak).

For IT teams, proprietary container is difficult to maintain due to the quick rate of evolution of mobile OS; it also imposes constraints on development technologies.

For employees, **it makes access to professional applications more complex** by separating it from personal use, which can discourage uptake of digital tools within companies!

Native container- OS: a guaranteed hit!

Provided by mobile OS vendors, native container- (iOS, Android and Windows 10) is directly integrated into the OS of the mobile device. It accesses professional applications by operating the native applications on the device (mail, navigator, ...). With this technology, **users can maintain their usual habits** whether the device is used for professional or personal purposes. Adoption of applications is greatly enhanced!

Well aware of the importance of user experience, EMM/MAM publishers (Vmware Airwatch, IBM MaaS360, MobileIron and Jamf) have created the “AppConfig” community to promote native technologies alongside professional application publishers (e.g.: Salesforce 1, Box, Concur, ...).

In terms of security, native container- is often not rated as high as proprietary container because it is **more vulnerable to breaches** in the devices’s OS. Technologies provided by mobile OS vendors have, however, made a great deal of progress to integrate the enterprise requirements: this is the case for Apple on iOS 7, for Google with avec Android Enterprise on Marshmallow (6.0) and for Windows with WIP (Windows Information Protection).

It should be noted that **native container- cannot exist without the EMM solutions** which provide OS compliance policies management, but which mainly carry out remedial actions if the mobile OS is compromised (e.g.: automatic deletion of professional data on the device), an essential element for a security policy.

Nicolas Raison

Practice Manager at Digital Dimension, Nicolas is an expert in the field of OS and EMM infrastructures. He is particularly passionate about new technologies to improve business practices.

Security: even stronger!

Given the importance, indeed the critical nature of the issue of security, specialist publishers like Checkpoint, Lookout or Skycure are today going even further by providing **“MTD” (Mobile Threat Defense) solutions**. Their role is to analyse applications, network connections and OS behaviours and relay alerts in case of security issues.

These highly advanced solutions are a complement to containerization technologies. They are particularly effective in **preventing targeted attacks and the risk of spying**. These requirements do not, however, apply to all companies.

What to bear in mind

A high level of security and quality user experience are not contradictory. To guarantee the success of a project, CIOs need to – and can – bring these two elements together.

There is, however, no “good choice” given that the importance of the criteria needing to be taken into account varies so widely: requirement and resistance to changes of user, application requirements for business, criticality of the data used on mobile terminals, importance of exposure to risk of attack, … Each company has its own response!