MINISTRY OF DEFENSE LEVERAGES PRADEO SECURITY GLOBAL APPLICATION DATABASE

In highly sensitive sectors such as politics and intelligence agencies, the zero-trust policy is more heavily applied than anywhere else, and mobile users are restricted from downloading apps from public app stores. Regardless, individuals constituting these units still need to access some services offered by mobile applications.

One of the Federal IT security team we work with is relying on a mobile device management (MDM) solution to distribute applications to mobile devices locked into a kiosk-mode. In addition, the IT security team was looking for a way to ensure that all public apps pushed on that store would strictly follow internal security guidelines.

By using Pradeo Security Global Application Database, the team members diagnose the security level of the selected public applications before distributing them to highly restricted mobile devices.

Ministry of Defense	thousands+ applications already audited	**A global database with 98 million+ public application reports**

Core business need: Vetting mobile applications before their distribution to kiosk-mode mobile devices

This Ministry of Defense is providing locked down devices to its field operatives. Those devices' usages are highly restricted and can't download apps from public stores nor be used outside the Ministry's premises. Yet, the security team is, among other, pushing public mobile applications to those devices through the application management functionality of the MDM in place. It uses Pradeo Security Global Application Database to **assess the security level** of those apps prior their distribution.

The Pradeo Security engine has gathered detailed security analysis of over 98 million applications. These audits have constituted and continuously complete a global database of mobile app security reports. For the past 3 years, the security team has leveraged Pradeo Security global database to review any public application to be deployed against their tailored security policy.
As a first step, the team was exclusively using the web platform. Then, they strengthened their security process by integrating one of Pradeo Security APIs to extract the list of all network accesses required by the mobile applications distributed to their fleet. With that list, they were able to filter the communications of these apps.

Applications' flaw remediation, the final piece of the puzzle

Unsurprisingly, a no-negligible portion of audited applications did not comply with the security policy of the Ministry, preventing users to benefit from their useful services.
To address the security issues of those public apps and fill the gap to make them compliant and usable, the Ministry IT security team leverages Pradeo Security **remediation capability**. The IT security team is able in few clicks to specify for each application unwanted behaviors and fix them before pushing them to users.

Industry

- Government

Technical environment

- Mobile applications: **Android and iOS**
- UEM: **MobileIron**
- **Integration of Pradeo Security APIs**
- **Remediation** of apps

Why Pradeo Security?

- **Ready to use** platform
- **Full visibility** on behaviors and vulnarabilities
- **Customizable** security policy
- Compliance with **regulations**
- Mobile app security expertise recognized by **Gartner**, **IDC** and **Frost & Sullivan**