Improve your corporate risk management through advanced app risk evaluation. Appicaptor automatically analyzes app security relevance according to security quality and implementation characteristics. Its reports provide fast and reliable recommendations as well as full descriptions of the technical details where information is needed.

**Business Challenge**
According to our investigations among the top free iOS and Android apps more than 50% neglect basic security requirements and are therefore unfit for enterprise use. Apps represent a major threat for enterprise because uncontrolled installation by employees puts companies’ data, IT services and infrastructure at risk. Enterprises need to make sure that there is a quick reaction to the ever increasing number of app vulnerabilities and that they have reliable information at hand to make the decision which apps to whitelist and which to blacklist.

**How the Appicaptor MobileIron Integration Works**
The Appicaptor MobileIron Integration enables app risk management and mobile enforcement by connecting both specialized platforms by an automated interaction.

MobileIron App Inventory aggregates all installed apps on your company’s managed devices. Your MobileIron management platform (the integration supports MobileIron Core and MobileIron Cloud) transmits this app list to the Appicaptor backend, which is hosted and performs all security tests in Germany.

Appicaptor automatically scans all apps of your MobileIron App Inventory according to your Appicaptor service level agreement, analyses them with regard to IT security quality and compliance with defined data protection specifications. In order to evaluate if the apps are suitable for your business operations, Appicaptor transfers test results using a policy set into an app risk rating. The policy set will take your enterprise protection requirements into account or you use the standard policy set, which is best suited for enterprises with average protection requirements.

The integration of Appicaptor in MobileIron enables your administrators to quickly gain control over their mobile app risk problems by accessing detailed test results and reports and perform actions within your MobileIron management environment based on the risk assessment that allow them to make fast, comprehensive and well-based decisions.

**SOLUTION AT-A-GLANCE**
- Mobile app risk assessment for iOS and Android
- Security quality analysis
- Customizable reports for individual security requirements
- Deep Code Inspection
- Automated compliance monitoring and detailed reports
- Data security evaluation: behavior analysis, data access profile, activity check
- Easy business integration
**Key Features**

Appicaptor offers automatic app scanning and threat analysis for iOS and Android apps. It detects relevant app risks in the field of communication, data, input interfaces, privacy and runtime security. Appicaptor performs sophisticated static analysis of the app binaries in order to detect security relevant implementation errors, vulnerabilities or risky behavior.

Risk rating is supported by automatically classifying apps by their description texts within the App Markets. This classification determines the main security-related function (e.g. file viewer, organizer, calculator, password manager, etc.) and uses this information in the risk evaluation, in order to assess the risk more accurately.

The service generates an individual test report for each app and each operating system. The system issues a warning when detecting vulnerabilities or the insecure use of sensitive data. Appicaptor repeats the tests regularly, thus constantly evaluating the security features based on the latest technological knowledge.

Enterprises can use standard recommendations or create and deploy customized and fully automated policies to be in-line with their corporate IT security policy. More than 70 distinct parameters can be utilized to define specific custom policies to include App blacklisting or whitelisting based on app security quality, behavior and implementation or deployment characteristics. The complete Appicaptor infrastructure is operated in Germany.

**Use Cases**

A company that does not control the apps on its mobile devices takes unnecessary risks. Appicaptor evaluates if apps fulfill security requirements or not.

CIOs can subscribe to the test service and easily access the results via the MobileIron Enterprise Mobility Management System.

The integration provides reliable risk information in the forefront of an installation of apps from commercial app stores, enterprise app stores, or (third party) specific business apps on corporate devices or within BYOD programs. It facilitates and supports app approval processes. In case of a security incident or vulnerability disclosure Appicaptor provides tools and measures to evaluate if that pattern is applicable to approved and installed apps on managed devices.

Appicaptor supports to find apps with a specific functionality and the desired level of protection (e.g., searching for a PDF viewer that meets the demands the corporate IT policy).

**Appicaptor dashboard presents summarized app test results, facilitates mobile risk assessment and provides a direct entry point for analyzing specific app test results.**

**ABOUT PARTNER**

Fraunhofer SIT is one of the world’s leading research institutes for applied cybersecurity and data protection.

Fraunhofer SIT  
Darmstadt, Germany  
Tel. +49 6151.869.233  
Fax +49 6151.869.224  
appicaptor@sit.fraunhofer.de