What is App Protector?

Solution concept

What is App Protector

App protector is a solution which utilizes **R**untime **A**pplication **S**elf-**P**rotection (**RASP**) that is built on or linked into an application runtime environment. It is capable of controlling application execution, early intrusion detection and preventing real-time attacks.

App Protector is embedded within an application and kicks in when an application starts and runs. It's designed to detect attacks on an application in near real-time. When an application begins to run, App Protector can protect it from malicious input or behavior by analyzing both, the app's behavior and the context of that behavior. By using the application to continuously monitor its own behavior, attacks can be identified and mitigated immediately without human intervention.

How does App Protector work?

App Protector incorporates security into a running application by utilizing a mechanism that, regardless of the business logic in the application, checks for threats on the mobile device of an end user. The technology doesn't affect the design of the application because App Protector's detection and protection features operate on the OS platform the application is running on. When a security event in an application occurs, App Protector detects the threat, and following this detection, the app can be configured to react accordingly.

ASEE App Protector implementations

The App Protector solution has three options for implementation:

- App Protector SDK freemium
- App Protector SDK advanced
    - App Protector SDK offline
    - App Protector SDK online

App Protector SDK freemium is a free SDK that enables developers to implement the limited scope of detections and reactions within mobile applications. SDK is configured by hardcoding which threats to detect and how to respond to these threats (App Protector configuration). This configuration can only be changed in a way to change the hardcoded part of the App Protector

configuration. If mobile application vendors want the full scope of the product, the paid versions of SDK are required.

App Protector SDK advanced can be implemented in 2 ways: **online** or **offline**, each one can be configured in two dimensions: which tamperings should be detected and how to react to each detected tampering.

App Protector SDK offline is a type of implementation in which the SDK is configured by hardcoding which threats to detect and how to respond to these threats (App Protector configuration). This configuration can only be changed in a way to change the hardcoded part of the App Protector configuration.

App Protector SDK online is connected to App Protector Portal and configuration can be modified through the Portal, meaning that App Protector configuration is not hardcoded in the App Protector SDK.

The online SDK consists of everything that the offline SDK consists of; with an additional component, the App Protector Portal server, which can be used to monitor all attacks reported with App Protector SDK. The portal shows overall statistics and can be used to configure the initial behavior or to change behavior based on current or mostly detected attacks.

Along with App Protector Portal exists a mechanism that helps to manage the behavior of App Protector on a mobile device. App Protector SDK collects and sends security events from mobile applications to App Protector Portal. The portal can be used for analyzing security events/attacks on users' devices that have installed monitored production applications. Based on the received information, the behavior of App Protector (App Protector configuration) can be changed.

Changing configurations or responses to attacks can be done by sending change information over the App Protector Portal server to App Protector SDK on a mobile device.

> **NOTE:** App Protector offline/online is not related to the end-user device's internet connection - even if the end-user device has an internet connection (Wi-Fi, 3G, 4G, 5G), if App Protector SDK implementation type is set to offline, App Protector SDK is considered to be offline and there is no connection between App Protector SDK and App Protector Portal.

Supported platforms and languages

There are two versions of App Protector SDK, one is built for Android and one is built for iOS.

Android App Protector SDK is written in Java language but is fully compatible with other Java languages supported on Android, like Kotlin. This framework can be used for target devices from Android KitKat (API level 19) and higher.

iOS App Protector SDK, available in two builds, build for Swift and build for Objective-C. Both versions have all the capabilities in terms of runtime self-protection. This framework can be used for target devices iOS 8.0 and higher.