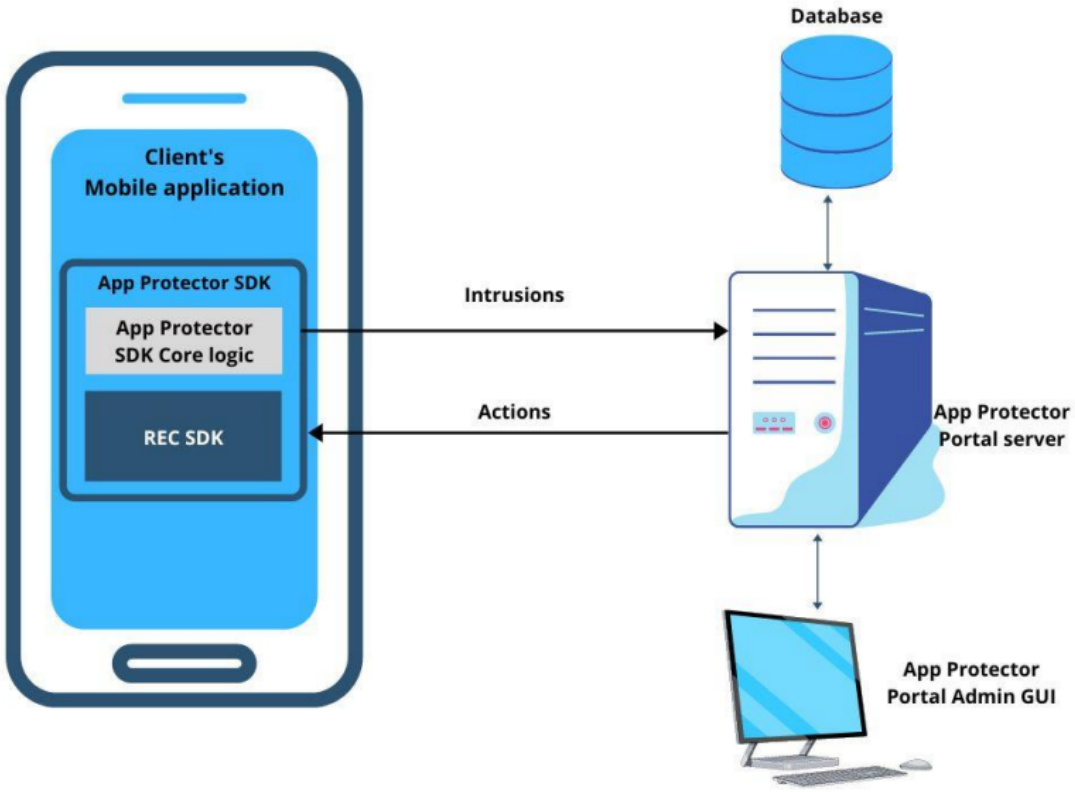
Portal solution

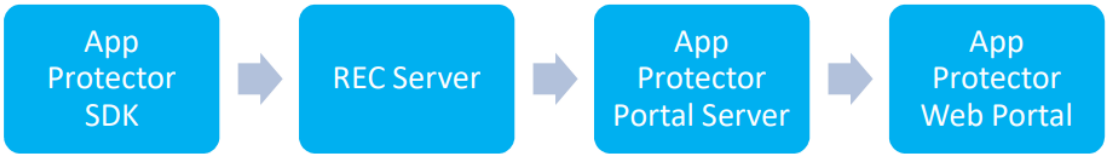
App Protector Portal

App Protector Portal is a solution that enables clients to create an App Protector configuration for each **user** and/or **mobile application**. The Portal could be used when App Protector SDK is implemented in online mode. Using this solution, clients will be able to set which attack App Protector SDK online should detect and choose which response will be created after the attack is detected. App Protector SDK online collects data of detected attacks and sends it to Portal. Based on the inputs from the SDK, the client will be able to see statistics for each platform, Android and iOS.

The figure below represents a high-level App Protector environment.



App Protector environment



App Protector attack detection flow

App Protector SDK online implementation consists of:

- **App Protector SDK** – detects threats on mobile applications;
- **REC Server** – collects data from App Protector SDK (part of which is REC SDK);
- **App Protector Web Portal** – allows to client to create new, update or delete existing applications and configurations. Also, the Portal displays statistics about detected attacks;
- **App Protector Portal Server** – receives all the data (identifiers, applications, and configurations) and saves it in a database.

App Protector SDK, integrated within mobile applications, detects attacks and periodically sends information about the detected threats to REC Server. REC Server collects all data from SDK and communicates with App Protector Portal Server. App Protector Portal Server fetches data from REC Server and passes it to App Protector Web Portal. Communication, between SDK and Servers, is authenticated using access tokens contained in HTTP headers.

App Protector Web Portal

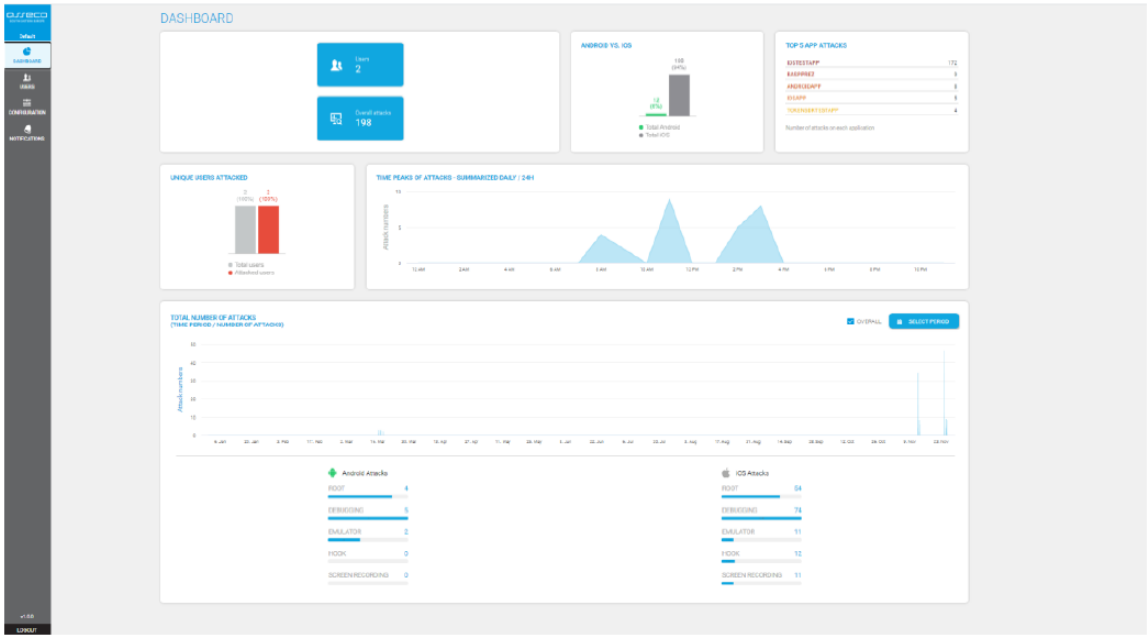
App Protector Web Portal is a web application used for the administration and configuration of App Protector functionality within mobile applications. App Protector Portal GUI allows clients to manage which attacks App Protector should detect and to define responses to detected attacks from a single point. App Protector Portal GUI contains a dashboard that displays current statistics and graphics based on detected attacks for each platform, Android and iOS.

After the Client logs in App Protector Portal web application, it can view statistics and reports displayed on the dashboard and view the list of users. Also, Portal allows the Client to add new or update, delete and configure existing applications. The Portal Web application has a notification inbox that contains a list of activities made by administrators.

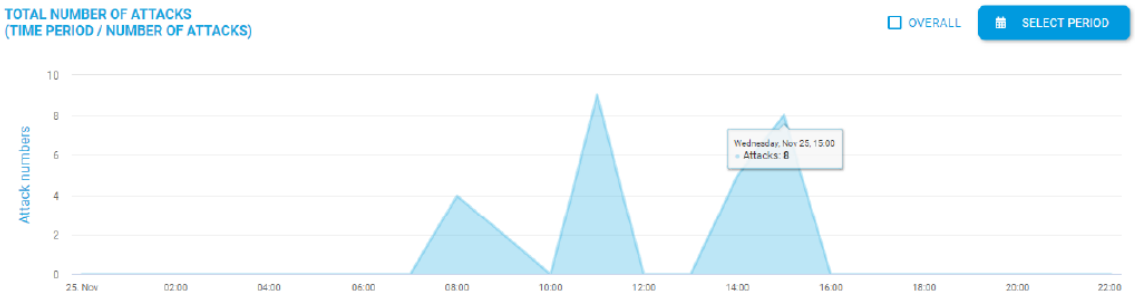
App Protector Web Portal Dashboard shows:

- Number of users;
- Number of overall attacks;
- 5 most attacked applications;
- Graphical representation of attacks – overall, over some period or last 24h;

- Number of performed attacks for each detected attack on iOS and Android platforms (Jailbreak/Root, Debugging, Emulator, Hook, Screen Recording).

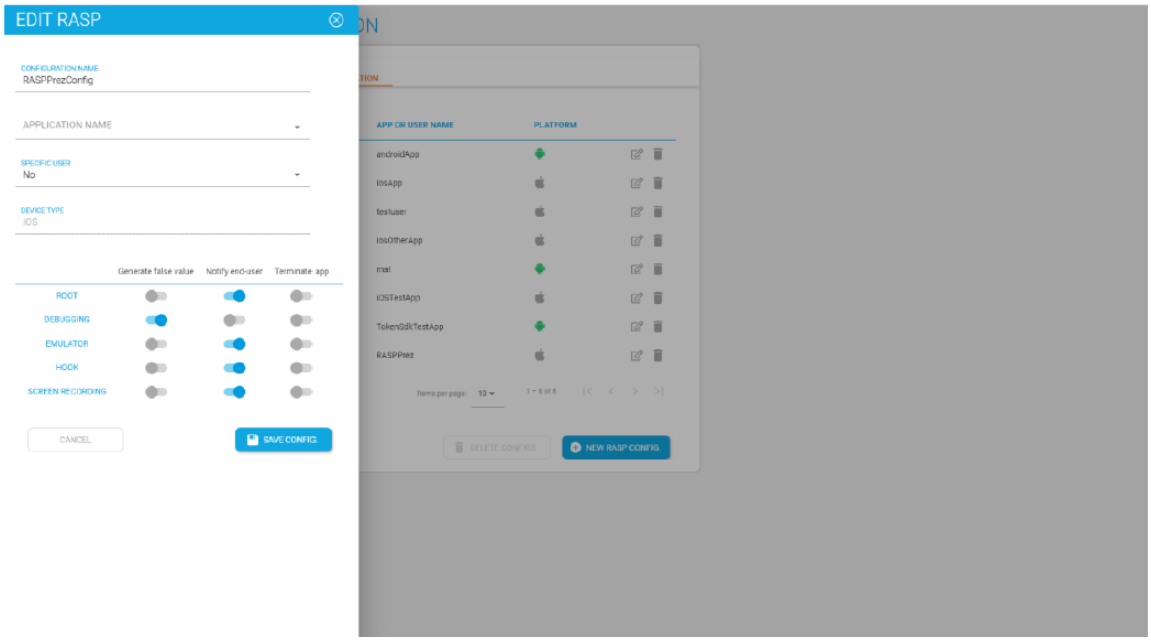


App Protector Web Portal Dashboard



Graphical representation for detected attacks

App Protector Web Portal allows the Client to change configuration and settings for all or specific users and for each mobile platform, Android and iOS. The Portal allows the Client to choose which attacks App Protector should detect and define a response for a detected response from one point of interaction.



App Protector Configuration

Generally, App Protector is a tool that can be integrated with, or within, a mobile application's runtime environment. The best security preventive environment is built in App Protector SDK which is implemented within the mobile application. Generally, App Protector is tracking device behavior, it analyses what is happening, and based on that it responds to the application. App Protector Portal enables monitoring and logging of detected attacks and changing App Protector configurations using App Protector Portal GUI.

REC SDK

When the App Protector SDK implementation type is online, then part of App Protector SDK is REC SDK as well.

REC, **R**isk **E**vent **C**ollector, is a component that receives risk indicators from the mobile application and sends them to the risk assessment system. For the purpose of the Risk assessment system to consume risk indicators from mobile applications and REC, the event bus (broker) component is used. REC's main purpose is to connect mobile devices and message queue which can forward the data to a 3rd party system (such as an anti-fraud system). It is a system responsible for collecting mobile device attack information which can later be used for evaluating risk indicators.