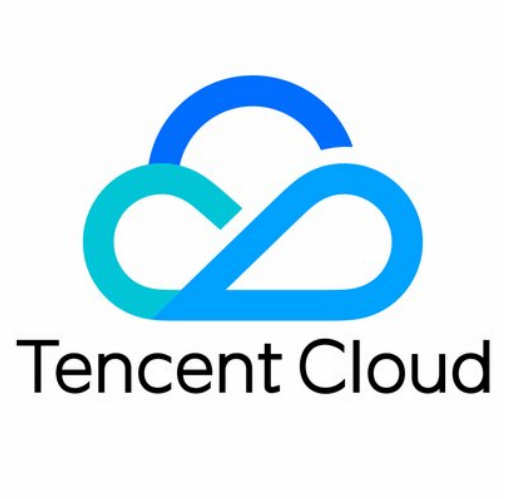
Mobile Security

Product Introduction

Product Documentation



Contents

Product Introduction
Product Overview

Last updated：2023-05-26 15:56:59

Product Overview

Mobile Security provides one-stop security solutions for mobile apps. You can enjoy a range of features such as security detection, application reinforcement, channel monitoring and security SDK by uploading signed installer packages. Mobile Security can help you prevent apps from being pirated or cracked, identify application vulnerabilities in time, and monitor the distribution of copyrighted and pirated apps to effectively safeguard the interests of mobile app owners.

Notes

Please note the following when using Mobile Security:

- Apps should be re-signed after reinforcement, otherwise they cannot be properly installed.
- To generate multi-channel packages, reinforce the app, use the multi-channel package tool and re-sign the channel packages.

Usage Restrictions

Mobile Security Usage Restrictions:

- Apps must be signed before upload.

Product Strengths

Last updated：2019-01-30 10:11:56

Mobile Security boasts the following product strengths:

Industry-leading Security Detection Engine

Mobile Security adopts Tencent's security detection engine which is also adopted by multiple Tencent apps with hundreds of millions of users. This market-proven engine can help developers identify security risks in apps as early as possible.

Excellent Reinforcement Performance

Mobile Security strictly controls the influence of reinforcement on app installer packages so that the size and performance of apps do not change significantly after reinforcement.

Outstanding Compatibility

Over a thousand types of physical machines are used to verify the stability of reinforcement to ensure the compatibility of reinforcement solutions on mainstream models.

Comprehensive Channel Monitoring

Mobile Security integrates the data of two major Tencent products: MyApp, with which the distribution through mainstream channels can be obtained, and Tencent Mobile Manager, with which the latest malware trends and solutions can be learned. In addition, Mobile Security constantly monitors multiple channels in China to help developers stay updated on the piracy situation in distribution channels.

Product Features

Last updated：2019-01-30 10:12:00

Mobile Security provides users with one-stop service covering features such as application reinforcement, security evaluation, channel monitoring, security SDK, compatibility test, and quality tracking.

Application Reinforcement

- DEX file reinforcement: It reinforces DEX files via digital encoding to prevent apps from being reverse engineered through debuggers.
- Resource file protection: Apps cannot run normally if resource files were illegally tampered or deleted.
- Anti-repackage protection: Apps cannot run normally once any file in the apps has been modified or replaced.
- Anti-debugger protection: This prevents apps from being affected by various static and dynamic debugging tools.
- Anti-memory dump protection: This prevents app code from being stolen through dynamic debugging and dump.
- Advanced memory protection: This provides strong protection for memory data to effectively prevent the source code from being stolen through memory debugging and memory dump.
- .so file protection: This protects specified .so files from being reverse engineered, so that core sensitive logic are not exposed.

Security Evaluation

- Data security evaluation: Audit of sensitive log information leakage, audit of file storage permission, audit of sensitive database data, and audit of sensitive system component data, etc.
- Network communication security evaluation: Audit of encrypted transmission security, and audit of HTTPS communication security, etc.
- Application security evaluation: Audit of remote command execution vulnerability, audit of insecure app configuration, audit of DoS vulnerability, audit of unauthorized logical access vulnerability, and audit of common

Web vulnerability, etc.

- Third-party database security evaluation: High-risk third-party databases scan audit, and third-party database vulnerability alerts, etc.

Channel Monitoring

- Real-time monitoring: Continuous monitoring on a 24/7 basis is provided to effectively observe the distribution channels's piracy situation.
- Precise channel source and download capacity: We can trace the precise channel source of copyrighted and pirated apps and their download capacities. We can even provide the specific link to the download page.
- Massive resources and comprehensive monitoring: In addition to real-time monitoring of nearly a 100 channels, MyApp and Tencent Mobile Manager resources are also integrated to quickly perceive the distribution of copyrighted apps and the interception of malicious apps. With our massive and industry leading resources, we can comprehensively monitor the distribution of copyrighted and pirated apps without missing a single detail.

Security SDK

- Database security protection: Secure database SDK is provided to effectively ensure the security of core data and prevent information leakage.
- Keyboard input protection: Secure keyboard SDK is provided to ensure the security of input data, and effectively prevent threats such as screen capture and theft of input information.
- Anti Game Botting: Anti Game Botting SDK is provided to effectively prevent botting from modifying and ruining the game.

Compatibility Analysis

- Automatic compatibility test: We provide 50 random types of physical machines for automatic compatibility and adaptability testing. This will effectively reflect the compatibility and adaptability of the app on physical machines.

- Specific tests for less compatible models: We provide 30 random types of less compatible physical machines for automatic compatibility and adaptability testing. This will effectively reflect the compatibility and adaptability of the app on models with especially poor compatibility.

Quality Tracking

- App crash tracking: Various real-time crash information will be provided, including the information reported by Android Native. In addition to the error stacks, detailed operation information for every error occurrence will also be collected for further analysis.

Usage Scenarios

Last updated：2019-01-30 10:12:03

Mobile Security can be applied in the following scenarios:

During App Development

Mobile Security provides various SDKs such as secure keyboard SDK for developers to integrate.

Post App Development

Mobile Security's security detection can be used to detect security vulnerabilities in the app in time.

Pre App Release

Mobile Security's application reinforcement can be used to prevent the app from being pirated or cracked after release.

Post App Release

Mobile Security's channel monitoring enables app developers to have a firm grasp on the copyrighted and pirated apps distribution situation.