DATASHEET

BrightCloud®
Threat Intelligence

BrightCloud®
Mobile Security SDK

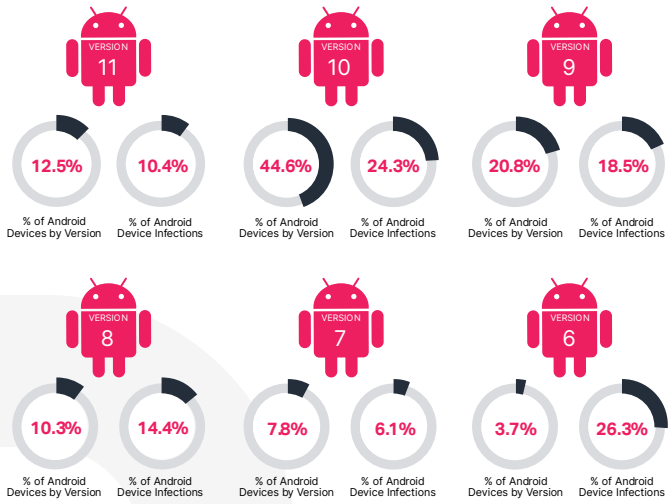
Simple, flexible, powerful detection and protection for Android® devices

Overview

- Malicious apps and PUAs are a threat to personal and corporate data and can compromise financial transactions
- Of the threats detected on Android devices in 2020, Trojans and malware accounted for 95.9% of it, an increase from their 92.2% share in 2019.[1]
- The BrightCloud® Mobile Security SDK offers enhanced mobile security, including antivirus, antimalware, application scanning and interrogation, device root detection and device risk scoring

Polymorphic malware hides from traditional detection. Individuals using smartphones and tablets tend to engage in activities that increase the risk of attacks on themselves and networks. For instance, using unsecured public WiFi or downloading apps from untrustworthy third-party sites can infect a device with mobile malware. These could lead to unwanted consequences, including data exfiltration, camera and microphone hijacking, financial extortion or acting as a Trojan horse into the WiFi network it connects to.

Android Infections by Version[1]



Mobile Security SDK benefits:

1) Industry-leading mobile threat protection

2) Simple, flexible development options for partners

3) Does not slow devices or hinder user productivity

BrightCloud detects a variety of malicious apps, including malware, spyware and trojans. PUAs include commercial rooting tools, hacking tools, aggressive advertising and data leakage apps. Security administrators may consider eliminating PUAs, as they have the potential to impact data loss or incur unwanted mobile usage fees.

The BrightCloud® Mobile Security SDK addresses mobile device threats by enabling technology partners to offer enhanced mobile security for their customers within their solutions. It features antivirus, antimalware, application scanning and interrogation, device root detection and device risk scoring, all while utilizing very little memory, bandwidth or battery life. As a fully functional mobile security solution, it offers significantly better protection than a simple, static block list approach and is designed to stay ahead of today's mobile threats.

Partner Benefits

1. **Block/address** the malware at the network edge preventing the lateral spread
2. **Faster (policy-based) response** to potential malware without network bandwidth or user experience impact
3. **Enhanced protection** with AI-based intelligence combining historical insights and real-time insights

BrightCloud® Mobile Security SDK in Action

The BrightCloud Mobile Security SDK enables our technology partners to monitor Android devices, check for malicious apps, act on threats and check overall device status.

Device Scanning

The SDK scans the device to detect threats when either initiated by the user or triggered by events occurring on the device. Additionally, the SDK proactively scans at set intervals to ensure changes do not go unnoticed. This multi-pronged approach offers optimal protection from viruses and malware without compromising the user experience. Results can be integrated into the host application for visibility of overall protection status and extended detection details can be requested for suggested remediation actions.

Root Detection

Rooted devices can try to bypass security and may be more vulnerable to malicious apps. The SDK uses a multitude of detections to determine the status of the device and checks for root management applications, potentially dangerous applications and root cloaking applications.

Device Risk Score

The service provides a simple, flexible and powerful risk scoring mechanism to ensure BrightCloud partners and end users are secure. When calculating a device score that partners can use to make a simple go/no-go decision, various attributes including whether the device is rooted, contains high-risk malware and other criteria are taken into consideration.

Runtime Permissions

When using the mobile SDK in Android OS API level 23 (Marshmallow) or higher, runtime permissions must be accepted by a user. With this feature, partners can retrieve a list of required permissions and present any permissions that have not yet been accepted by the user.

Partners have access to all of these features, with the flexibility to adjust their configuration based on their unique needs.

This flexibility allows partners to leverage the SDK in various scenarios, such as:

- Mobile device management providers can bolster their customers' mobile security through enhanced protection
- Smartphone manufacturers, mobile network operators and communications service providers can differentiate through pre-loaded security for their users, featuring their own brand
- Financial institutions and anti-fraud providers can protect their customers' mobile transactions by ensuring that devices transacting with their systems are within acceptable risk levels

Partner Integration Options

BrightCloud follows established Android app development standards to help make SDK implementation simple in partners' solutions. BrightCloud partners are responsible for developing all UI components (both client and management interface) using the SDK and leveraging only the functionality needed for their use case.

The SDK solution consists of access to an online Gradle repository and actively maintained documentation that includes details all of the classes and interfaces in the library. In addition to Android-native integration into the apps, developers can quickly access the latest changes and choose whether to accept cutting-edge features or stay with well-established components. BrightCloud follows a lifecycle model in alignment with Google to ensure actively supported Android OS versions remain compatible as Android continues to tighten compliance and security requirements.

APIs allow for full management of all of the SDK security functions. For example, the partner can configure:

- Scan settings
- Real-time protection settings
- Quarantine

[1]2021 Webroot BrightCloud® Threat Report

Contact us to learn more
BrightCloud.com
Phone: +1 800 870 8102

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.