BrightCloud® モバイル セキュリティ SDK

for Android™ and iOS®

概要

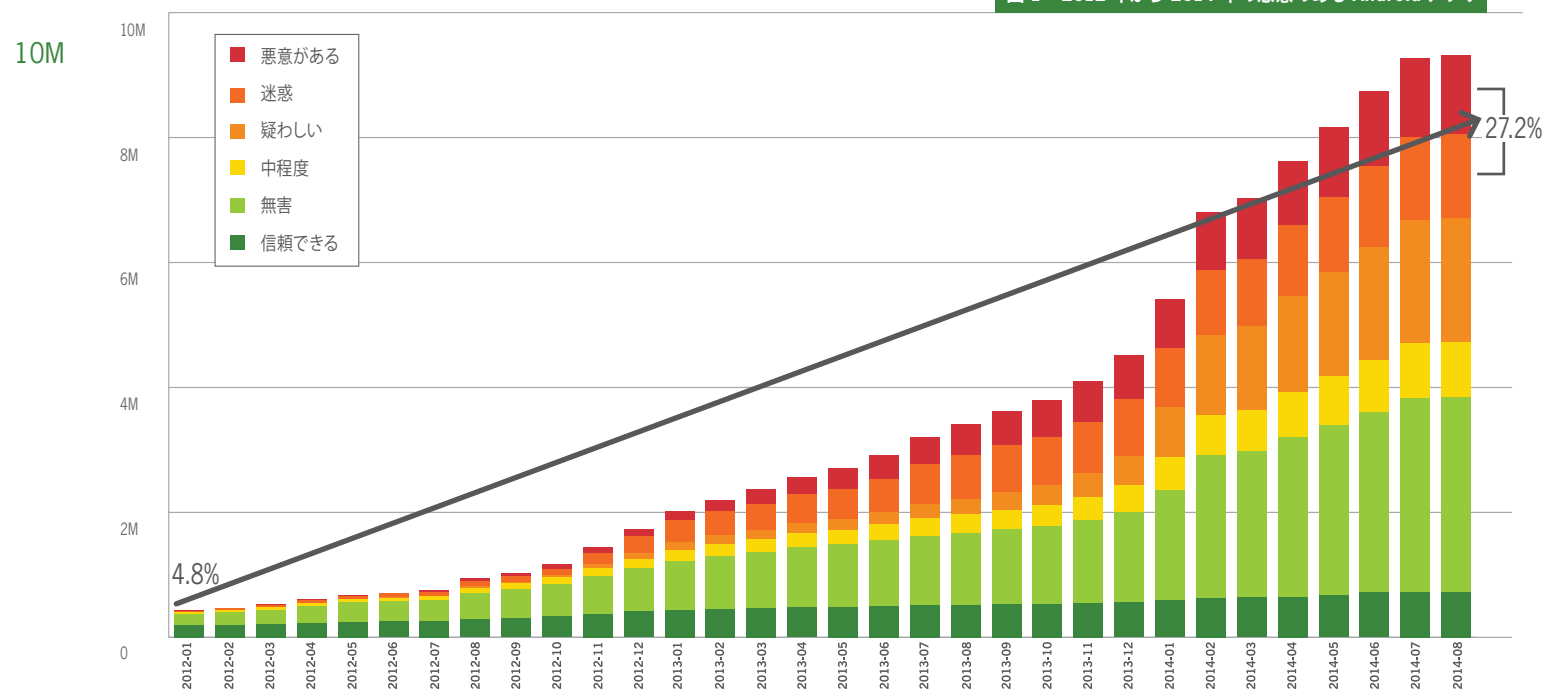
» 2011 年 6 月から、悪意のある Android アプリは 5000% 近く増加しています
» モバイル マルウェアをホストしているサイト、悪意のあるアプリ、およびデバイスの紛失や盗難により、企業データは脅威に晒されます
» BrightCloud® Mobile Security SDK は、ウイルス対策、マルウェア対策、デバイスおよびアプリの調査、安全な Web 閲覧と Web 分類、全体的なデバイス リスク スコアなどの強化されたモバイル セキュリティを提供します

Webroot 脅威調査チームは、2011 年 6 月から 2014 年 6 月までの間に、Android ™ デバイスでのモバイル マルウェアが 5,564% 増加していると指摘しています (図 1)。同じ期間に、潜在的に迷惑なアプリ (PUA) は 764% 増加しました。PUA には、商用ルーティング ツール、ハッキング ツール、強引な広告、およびデータ流出アプリなどがあります。PUA によってデータを損失したり、不要なモバイル使用料金が生じたりする可能性があるため、セキュリティ管理者が PUA の排除を検討する場合もあります。

また、スマートフォンやタブレットを使用しているユーザーは、ソーシャル メディア サイトを頻繁に使用したり、脆弱性が増す可能性があるサイト (ギャンブルやポルノのサイトなど) にアクセスするなど、攻撃のリスクが増加する操作を行う傾向にあります。また、モバイル デバイスは物理的な紛失や盗難も脅威になります。組織外の人物が企業データへのアクセス権を得る可能性があるためです。

BrightCloud Mobile Security SDK では、モバイル管理パートナーがユーザーに強化されたセキュリティを提供できるようにすることで、モバイル デバイスの脆弱性に対処します。ウイルス対策、マルウェア対策、デバイスおよびアプリの調査、安全な Web 閲覧および分類に加え、全体的なデバイス スコア付け機能が備わっており、管理者はネットワーク上のデバイスのリスク レベルを評価できます。SDK は軽量で効率的であり、メモリ、帯域幅、バッテリーはわずかしか使用しません。完全に機能するモバイル セキュリティ SDK は、単純な静的ブラックリストによる手法に比べ、大幅に優れた保護を提供します。

図 1 » 2012 年から 2014 年の悪意のある Android アプリ



モバイル セキュリティ SDK の利点

» 業界最先端のモバイル脅威保護機能

» デバイスの速度低下や生産性の妨げにならない

» 安全な Web 閲覧により、悪意のある URL やフィッシング攻撃をブロック

» パートナーはシンプルで柔軟な導入オプションを使用できる

BRIGHTCLOUD モバイル セキュリティ SDK によるパートナーの利点

» **競合会社との差別化**
モバイル脅威に対する業界最先端の保護をユーザーに提供できる

» **ウェブルート インテリジェンス ネットワーク (Webroot® Intelligence Network, WIN) の利用**
世界で最も強力なクラウド セキュリティ ネットワークを介して、数百万ものソースから得られるインテリジェンスを利用

» **簡単な統合で完全な制御を実現**
UI を使用しない簡単な統合により、自社ブランドをユーザーに印象付けることができる

» **ユーザー エクスペリエンスへの影響なし**
フットプリントおよびバッテリー消費を最小限に抑えつつ、強力な保護を提供することでユーザーの満足度を向上する

BRIGHTCLOUD® モバイル セキュリティ SDK の実行

BrightCloud® モバイル セキュリティ SDK には、いくつかのモジュールがあります。モバイル管理パートナーは、アクティブ プロテクション サービス、スキャナ サービス、アプリ情報モジュール、デバイス情報モジュール、SecureWeb™ ブラウザ、およびデバイス リスク スコアから選択できます。パートナーは、固有のニーズに基づいて、これらのサービスを柔軟に組み合わせて使用できます。これにより、パートナーは次のようなさまざまなケースで SDK を活用できます。

» MDM プロバイダは、強化された保護機能を特別料金で提供することで、ユーザーのモバイル セキュリティを強化できます。

» スマートフォン メーカーは、組み込みのセキュリティ機能に自社ブランドを付けることで差別化を図れます。

» 金融機関は、ネットワークに接続しているデバイスが確実に許容できるリスク レベルに保たれるようにすることで、お客様のモバイル取引を保護できます。

アクティブ プロテクション サービス (モニター サービス)

このサービスでは、デバイスのイベントを追跡します。サービスは常時実行状態にすることも、ホスト アプリの実行中は有効にして、ホスト アプリが終了したら無効にすることもできます。ホスト アプリはモニター サービスを完全に制御できます。たとえば、リモート サーバーへの接続中はサービスを有効にし、その後、ホスト アプリによってサービスが終了されるように設定できます。

アクティブ プロテクション サービスを使用して、ホスト アプリに、ダウンロード中のファイル、インストール中のアプリ、および実行中のアプリを通知することもできます。ホスト アプリはこれらのイベントをログに記録し、通知を表示して、これらのイベントに基づいて他のカスタム アクションを実行できます。

スキャナ サービス

ホスト アプリはこのサービスを使用して、システム全体にわたってファイルとアプリのウイルス対策およびマルウェア対策のスキャンを実行できます。スキャンはバックグラウンドでサイレントで実行することも、ホスト アプリでスキャナにリスナーをセットアップして、ユーザーにフィードバックを提供することもできます。スキャン結果は単一の永続的なリストに保存されます。ホスト アプリはこのリストを使用して、対話式で検疫したり、個々のファイルやアプリを削除したりすることができます。

アプリ情報モジュール

このモジュールはデバイスにインストールされ、実行されているアプリに関する詳細情報を提供します。調査されたアプリのデータ ポイントは、ホスト マシンで構成できます。たとえば、各種パッケージ属性、証明書およびマニフェスト情報、さまざまなネットワークおよびプロセスなどに関連するデータ ポイントを構成できます。

デバイス情報モジュール

このモジュールは、Android™ と iOS® の両方に関して、デバイスおよびオペレーティング システムの詳細情報を提供します。BrightCloud SDK は、デバイスがルート指定された状態であるか、エミュレータで実行されているかをチェックできます。また、さまざまなハードウェア統計を収集し、デバイスを一意に特定できます。

URL 評価および IP 分類による安全な Web 閲覧

モバイル管理ベンダーは、独自の BrightCloud Web 分類および評価情報を使用する SecureWeb ブラウザを利用することで、ユーザーが悪意のあるサイトに接続したり、フィッシング攻撃に遭ったりしないようにすることができます。安全な閲覧を有効にすると、URL に有害なコンテンツが含まれていないか自動的にスキャンされ、その結果に基づいてブロックされます。パートナーも、ギャンブル、ポルノ、およびソーシャル ネットワーク サイトなど、83 を超えるカテゴリに基づいてコンテンツをフィルタに掛けることができます。この機能は標準的な Android ブラウザで実行することも、パートナーのブラウザに組み込むこともできます。

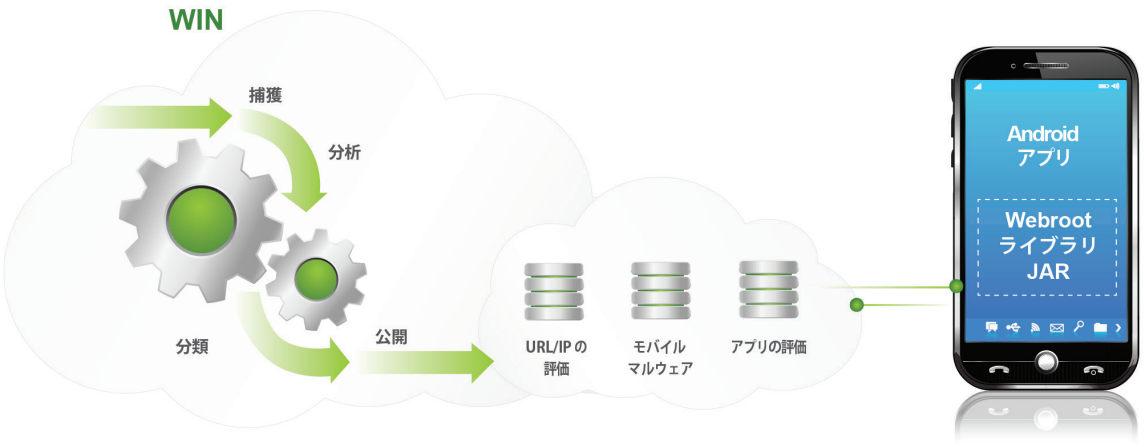


図 2 » セキュリティ SDK 実装

デバイス リスク スコア

シンプルで柔軟性があり、強力なリスク スコアメカニズムを提供し、Webroot® のパートナーとエンド ユーザーの情報を保護します。デバイス スコアの計算では、ユーザー、デバイス、およびパートナーのアプリのすべてが考慮されます。システムではエンドポイントが保護され、デバイスがルート指定されているかジェイルブレイクか、リスクの高いマルウェアが含まれているか、最新の定義を使用しているかなどのリスク基準に基づいたシンプルな「許可 / 不許可」の決定が行われます。さまざまなカテゴリに重み付けが行われ、パートナーのリスクの許容度に基づいて、パートナーの裁量でスコアを調整できます。

パートナーの統合オプション

Webroot® では、パートナーがソリューションにシンプルな SDK 実装を行うために必要なすべてのツールを提供しています。Webroot のパートナーは SDK を使用してすべての UI コンポーネント (クライアントと管理インターフェイスの両方) を導入する必要があります。BrightCloud® モバイル セキュリティ SDK ライブラリはモジュラー設計であり、メモリ使用量を非常に少量に抑えることができます。選択した構成に応じて、必要なモジュールのみがメモリにロードされます。

SDK ソリューションは、Java Library for Android ™、または iOS® のヘッダー ファイル、サンプル アプリ、およびドキュメントで構成されています。コンパイルされた Java Library (JAR) またはヘッダー ファイルがパートナーのアプリに組み込まれます。サンプル アプリを使用して、パートナーはライブラリの統合がどのように実行されるかを確認できます。ドキュメントには、管理を行えるようにするライブラリ内のすべてのクラスやインターフェイスの詳細が含まれています。

API によって、すべての SDK セキュリティ機能を完全に管理できます。たとえば、パートナーは次を構成できます。

- スキャン設定
- 定義の更新頻度
- リアルタイム保護設定
- 検疫
- 脅威および URL 無視リスト
- URL カテゴリ ブロック / 無視リスト
- ライセンスおよびインストール トラッキング

導入が完了すると、セキュリティ定義と Web フィルタリング データベースが WIN によってホストされます。定義の更新と Web 参照が、Webroot サーバーに対して照会されます (図 2)。

ウェブルートについて

ウェブルートは、サイバー セキュリティに焦点を当て、個人および企業向けのソリューションである Webroot SecureAnywhere® の一連の製品群および、テクノロジー パートナー向けの BrightCloud® セキュリティ インテリジェンス ソリューションを通じて Software-as-a-service(SaaS) がもつパワーをインターネット セキュリティの世界にもたらしています。その結果、Net PromoterScore による顧客満足度ではナンバー 1 を誇っています。詳細については、http://www.webroot.co.jp をご覧くださ い。

ウェブルート株式会社
〒 107-0062
東京都港区南青山 3-13-18
313 南青山 8F
+81 3 4588 6500