

企業におけるAndroid

Google AndroidデバイスとMcAfee Enterprise Mobility Managementの併用

Androidが企業内に浸透しつつあり、ITリーダーにはAndroidを管理するための戦略が必要となっています。既に利用可能な基本機能に加えて、マカフィーはAndroidの使用に対するサポートを拡大しており、リモート管理、暗号化、他の重要な最小要件などの基本プラットフォームにおける、エンタープライズ向け機能の成熟と歩調を合わせています。



すべての企業ユーザーも一人の個人ユーザーです。パーソナルデバイスを職場に持参し、そのデバイスでも仕事をしたいと思っています。昨年までそれはiPadでした。しかし今年は、Androidです。ユーザーが企業アプリケーションにアクセスするためにAndroidの使用を要求しているなら、これらのデバイスのセキュリティ保護と管理について、そしてMcAfee® Enterprise Mobility Management (McAfee EMM®) がいかに役立つかを知っていただく必要があるかもしれません。

主なポイント

McAfee Enterprise Mobility Management ソリューションは、以下を含むライフサイクルタスクに焦点を当てることによって、Androidの企業導入における成功を保証します

- 管理 – モバイルデバイスライフサイクルの追跡と管理
- プロビジョニング – スマートフォンやタブレットの導入と使用中
- セキュリティ保護 – スマートフォンやタブレット、企業データ、およびアクセスするITネットワークの透過的なセキュリティ保護
- サポート – ITサポート費の最小化とユーザー生産性の最大化
- 監査 – 企業ITおよびポリシーコンプライアンスレポート要件のサポート

コアプラットフォームとデバイス機能を活用して、必要なセキュリティ、管理、スケール、制御、そしてユーザーが望むオープンなユーザー体験を提供します。

基本から始める

Androidのようなオープンソース指向のプラットフォームは、開発者に想像力を発揮させることを奨励していますが、そのような独立性には制御が必要です。また、セキュリティやコンプライアンスの維持、管理のために絶え間ない努力が強いられています。Googleはデバイスのオペレーティングシステム(OS)を出荷し、個々のデバイスメーカーは、Googleのブループリントにおおまかに従って個々のデバイスを構築し、ターゲット市場向けにカスタマイズしています。そのため、商用生産のデバイスOSのいくつかのリリースが同時に発生し、各リリースを使用した複数のデバイス構成を持つ可能性があります。このことが私たちにわかるのは、消費者のデバイスを企業に安全に接続するための取り組みをリードしてきたからです。McAfee EMMプラットフォームは、企業ネットワーク内のスマートフォン、PDA、およびタブレットをノートPCやデスクトップPCと同レベルのセキュリティ保護で統合します。

通常、デバイスメーカーやプラットフォームベンダーが、企業のITおよびコンプライアンスリーダーが必要とするセキュリティと管理性が備わった製品を提供できるようになるのは、複数回にわたるリリース後です。たとえば、営業がデバイスを紛失してしまった場合、そのデバイスの顧客窓口はどうするでしょうか？ Android 2.2は、最初のGoogleリリースでパスワード画面を提供していますが、これではデータ保護に対する最低限のセキュリティ制御機能しかありません。多くの企業が、暗号化がなく、窃盗者がその気になれば顧客データベースを攻撃する可能性があることを依然として懸念しています。Microsoft Exchangeのサポートはどうでしょうか？多くのAndroidデバイスはこのサポートを提供していません。多くの企業ユーザーには、Microsoftのメールがサポートされるまでは不要なものにすぎないのです。

McAfee EMMプラットフォームは、Androidユーザーに重要なコアセキュリティ機能(パスワードやPINのロック解除、リモートワイプの要件)を提供しています。現在では、ネットワークに接続しようとしているAndroidデバイスを信頼できない場合は、パスワードを無効にしてロックしてから、機密データを削除する(工場出荷時の設定に戻す)ことができます。ただし、すべてのAndroidデバイスがサポートされているわけではありません。これらの機能は、「パスワード有効画面」や「リモートワイプの開始」などのポリシーを理解して実施する、特定のAndroidデバイスの機能に基づいています。

ActiveSyncとその後

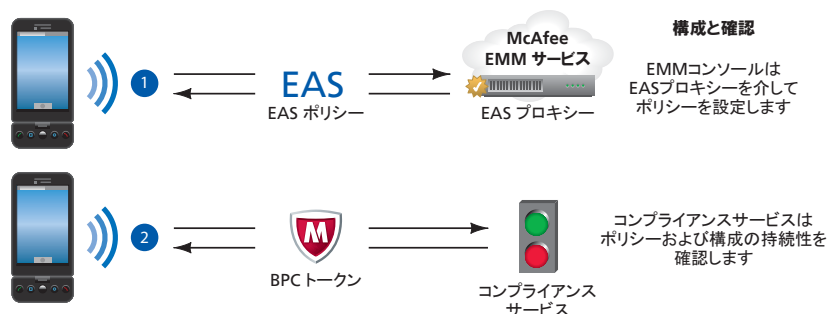
Android 2.2プラットフォーム以前は、ActiveSyncプロトコルにより、McAfee EMMがこれらのネイティブなポリシー実施機能を管理できました。ポリシーは、Webベースのコンソールを使用して作成され、Androidプラットフォームにプッシュされます。ポリシープッシュはネイティブクライアントによって認識され、McAfee EMM Compliance Serviceを介して継続的に実施されます。追加のエージェントによってではなく、デバイス上でネイティブに実行される操作として、ポリシー実施はリアルタイム、低レイテンシ、および低電力で行われます。

スポットライト：保管中のデータの暗号化

マカフィーの調査では、企業がAndroidの採用を阻む最大の要因は、保管中のデータ暗号化に対するネイティブサポートです。

Googleまたはハンドセットメーカーがこの機能を提供するまで、SDカードへの証明書の設定やデバイスの取り付けなど、手動の対応策が必要です。

なお、手動の方法では、多くの企業IT組織の規模、利便性、またレポートの要件を満たすことができません。



GoogleがAndroid 2.2をリリースしたときには、ActiveSyncに負担のない、これらの最低限のポリシー管理機能が有効でした。現在はAndroid 2.2以降を実行しているさまざまなAndroidデバイスをサポートするためにこのインフラストラクチャーを活用しており、より頑強な最小機能を実装するための方法を模索しています。

企業からの期待を実現

McAfee EMMプラットフォームは、モバイルデバイス管理とポリシー管理されたエンドポイントセキュリティ、ネットワークアクセス制御、およびコンプライアンスレポート機能をシームレスなシステムで融合します。これを実現するには、ネイティブデバイスのプラットフォーム内に、強力な認証、ハードウェアベースの暗号化、ポリシーベースのリソース制御、レポートなどの特定のコア機能が必要です。Googleは、これらの機能の一部をネイティブに有効にしているように思われますが、デバイスメーカーがプラットフォームを差別化するために一部の機能を最初に実装している場合があります。これらの機能のどれもAndroid V2.2では利用できません。

詳細情報

デバイスの状況はすばやく変化します。市場で最も成功しているデバイスプラットフォームの1つであるAndroidは、私たちの開発チームが細心の注意を払っています。マカフィーのAndroidサポートは、組み込まれたセキュリティ機能で企業のセキュリティに対する期待に応えるプラットフォーム機能によってのみ制御します。熱烈的な消費者やモバイル企業によってもたらされる市場機会に向けたGoogle Android機能とMcAfee EMM機能の拡張に今後ご注目ください。