Lookout + BlackBerry UEM

企業向けモバイル セキュリティ対策

モバイル端末を活用し、生産性向上を図る企業が増えています。モバイル端末で扱うデータが増加する今、統合エンドポイント管理ソリューションとクラウド ベースのモバイル セキュリティ ソリューションを組み合わせることで、より包括的なセキュリティ対策を実現し、企業データを保護することができます。

EMM

- デバイス管理とデータ ワイプ
- 個人データと企業データの分離
- 企業アプリケーションへのアクセス管理
- 認証とシングル サインオン
- モバイル端末でのコンテンツ アクセス管理

Lookout Mobile Endpoint Security

- アプリベースのリスクに対する保護
- フィッシング攻撃からの保護
- ネットワーク攻撃に対する保護
- 端末ベースのリスク検知
- すべての脅威タイプに対応するカスタム修復ポリシー
- EMM と連携させた容易な導入/運用

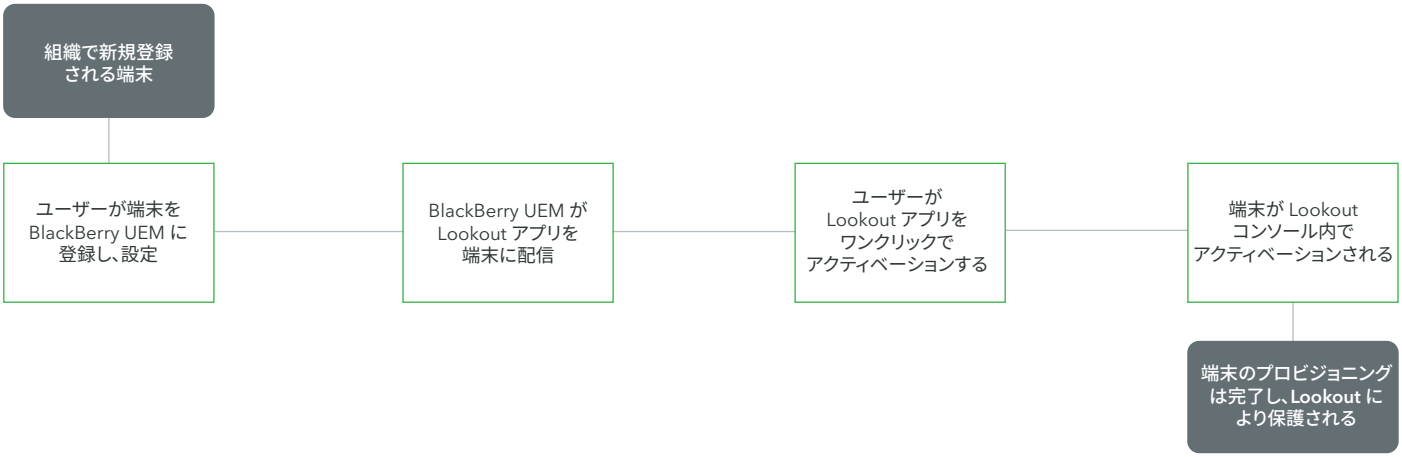
安全なモバイル環境を提供するシームレスな統合

リスク	BlackBerry UEM のみ	Lookout + BlackBerry UEM
端末紛失	紛失端末の捜索とリモートでのワイプ	紛失端末の捜索とリモートでのワイプ
アプリ配信	企業向けアプリの安全な配信	BlackBerry UEM 経由の Lookout アプリの配信
ポリシー違反	企業ポリシーに違反するアプリを手動でブラックリストに追加	セキュリティ ポリシーに違反するアプリを自動的に検知し修復
情報漏えい	モバイル端末内にコンテナー領域を作成し、情報漏えいを防止	アプリの挙動を詳細に把握し、カレンダー データを外部送信するなどアプリの危険な動作も含め、情報漏えいの状況を完全に可視化
ジェイルブレイクとルート化	OS のカーネル レベルが標的にされた場合、必ずしも効果的とは言えない	さまざまな OS 信号を分析することで、高度なジェイルブレイク/ルート化を検知可能
最新ではないオペレーティング システム	OS バージョンの必須条件を手動で指定	古いオペレーティング システムを使っている端末と Android のセキュリティ パッチ レベルを完全に可視化
危険な端末設定	端末のパスコードを強制的に設定	USB デバッグの有効化など、リスクの高い端末設定を可視化
アプリ脆弱性		安全でないデータ保存方式や通信方法を利用しているアプリを検知
悪意のあるアプリ		レピュテーション技術では検知することができない悪意あるモバイル アプリを包括的に検知
フィッシング攻撃		メール、SMS、メッセージング アプリ内の悪意のある URL、およびそれらが組み込まれたアプリへの接続を防止
コンテナー エクスプロイト		エクスプロイトにつながるようなアクセス権限の改ざんを検知
中間者攻撃		暗号化された企業データを転送している際に、悪意のあるネットワーク攻撃から保護

統合の仕組み

端末プロビジョニング

BlackBerry UEM ソリューションを使って、Lookout のエンドポイント アプリをモバイル端末に簡単に配信することができます。迅速でスケーラブルな端末プロビジョニングが可能になります。プロビジョニングは、以下の基本フローに従って実行されます。



脅威修復

BlackBerry UEM 統合により、カスタマイズされた修復ポリシーを使って、リスクに晒されている端末をリアルタイムで隔離できます。Lookout がリスクを検知した場合、端末は、セキュリティ ポリシー設定に従って「高リスク」、「中リスク」、「低リスク」に分類されます。脅威修復プロセスは、以下の基本フローに従って実行されます。