# Lookout + VMware Workspace ONE UEM

## VMware Workspace ONE 生産性アプリの継続的な条件付きアクセスを使用

モバイルで企業データを受信する際に、統合エンドポイント管理ソリューションとクラウド ベースのモバイル脅威検知ソリューションを統合することによって、従来のペリメター セキュリティの範囲を超えて端末を保護および制御できます。

### VMware Workspace ONE UEM

- コンテナ化されたアプリと企業データ
- 個人データと企業データの分離
- 企業メールへのアクセス管理
- SSO による企業アプリへのシームレスなアクセス
- 統合ポリシー管理
- モバイル コンテンツ配信の保護
- メール、コンテンツ、およびアプリの高度な DLP

### Lookout Mobile Endpoint Security

- コンテナ化されたアプリに関するリスクの継続的評価
- フィッシング攻撃からの保護
- 高度なジェイルブレイク/ルートの検知
- 中間者攻撃の検知
- 準拠状態を確保するためのアプリ情報漏えいの制御
- サイドロード アプリケーションの可視化
- すべての脅威タイプに対応するカスタム修復ポリシー

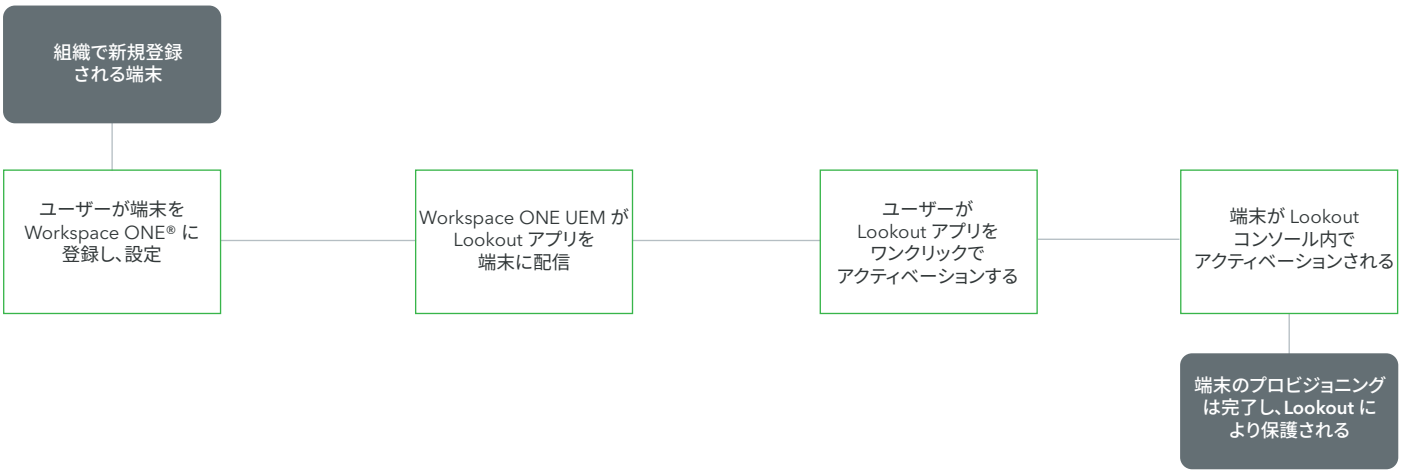
## 安全なモバイル環境を提供するシームレスな統合

| リスク | VMware Workspace ONE UEM | Lookout + VMware Workspace ONE UEM |
|---|---|---|
| アプリ配信 | 企業向けアプリを従業員に安全に配信します | Lookout エンドポイント アプリケーションを従業員端末に簡単に配信します |
| ポリシー違反 | 非準拠の端末が検知されると、自動化されたアクションによって端末が準拠状態に戻されます | Lookout によって検知された脅威またはリスクのあるアプリケーションの存在を考慮に入れて準拠した決定を下せます |
| アプリベースのリスク | コンテナ化されたアプリと企業データ (メールやコンテンツなど) | データを漏えいするアプリや、トロイの木馬およびスパイウェアなどのマルウェアを可視化します |
| 保護されていないネットワーク | トラフィック トンネリング機能を使用して、端末からのネットワーク アクセスを、端末上で管理されている企業向けアプリケーションにのみ分離します | 暗号化された企業データを転送している際に、中間者攻撃から保護します |
| 継続的な条件付きアクセス | 企業リソースへのアクセスは、準拠ポリシーに違反している場合は自動的に取り消すことができます | VMware® Workspace ONE 生産性アプリへのアクセスは、アプリ、ネットワーク、OS ベースの脅威が Lookout により検知された後に取り消すことができます |
| ジェイルブレイクとルート化 | ジェイルブレイクされた端末やルート化された端末を基本的に検知します | 何百もの OS 信号を分析して、基本的なジェイルブレイク/ルート検知をバイパスする試みを識別します |
| フィッシング攻撃 | なし | 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します |
| 紛失端末/盗難端末 | 紛失端末や盗難端末を検知するか、ビジネス データとアプリをリモートでワイプします | 紛失端末や盗難端末を検知するか、ビジネス データとアプリをリモートでワイプします |
| 安全でない認証 | Web、クラウド、モバイルのアプリにおけるワンタッチ モバイル シングル サインオン | Web、クラウド、モバイルのアプリにおけるワンタッチ モバイル シングル サインオン |

# 統合の仕組み

## 端末プロビジョニング

AirWatch® 搭載の Workspace ONE® 統合エンドポイント管理と統合することによって、Lookout エンドポイント アプリを管理されたモバイル端末で簡単に配信できるため、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。




## VMware Workspace ONE 生産性アプリに対する継続的な条件付きアクセス

Workspace ONE UEM との統合により、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。これには、Lookout のリスク ステータスに基づいて、管理されていない端末上の VMware Boxer のコンテナー化されたアプリへのアクセスをブロックする機能があります。Lookout が脅威を検知すると、端末は自社のセキュリティ ポリシー設定に応じて「高リスク」、「中リスク」、「低リスク」のいずれかに分類されます。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。