Lookout + Google Cloud Identity

企業のモバイルの生産性向上を安全に実現する

Google Cloud Identity を使用すると、管理者は、ネイティブの多要素認証、シングル サインオン、モバイル端末管理を使用して、1 つのコンソールから安全にユーザー、端末、アプリケーションを簡単に管理することができます。Google の BeyondCorp 企業セキュリティ モデルの主要コンポーネントである Cloud Identity によって、社員は場所や端末を問わず企業アプリやリソースに安全にアクセスできます。

企業は、社員の生産性を強化する方法として、正規のモバイル活用プログラムを採用しています。このポストペリメターの世界において、Cloud Identity は、社員がモバイル端末から企業アプリケーションにアクセスするための主要な方法の 1 つになりました。Lookout は、ネットワーク、アプリケーション、端末ベースのそれぞれリスクから保護する点で、数億人の個人ユーザー、企業、政府機関から信頼されています。Lookout と Google Cloud を組み合わせることで、信頼できるモバイル端末だけが Cloud Identity 経由で企業データとアプリにアクセスできるようになります。Lookout Continuous Conditional Access は、ユーザーが企業に接続している間、エンドポイントの正常性を動的に監視し、信頼できる端末だけが企業のインフラとデータに接続できるようにします。

Cloud Identity

- ID とアクセスの管理
- 企業アプリのシングル サインオン
- 機械学習によるアカウント セキュリティの強化
- 統合エンドポイント管理
- モバイルからのコンテンツ アクセス
- 多要素認証

Lookout Mobile Endpoint Security

- 企業への継続的な条件付きアクセス
- アプリ、端末、ネットワークベースのリスクに対する保護
- ウェブベースの脅威からの Phishing and Content Protection
- すべての脅威タイプに対応するカスタム修復ポリシー
- 対応可能なアラートとリアルタイムの脅威修復

安全なモバイル活用を提供する シームレスなインテグレーション

リスク	Google Cloud Identity のみ	Lookout + Google Cloud Identity
安全でない認証	SSO プラットフォームにアクセスするには MFA が必要	SSO プラットフォームやアプリにアクセスする際に端末の正常性を確認
安全ではないアプリの配信	Google Play と Apple App Store の両方でホワイトリスト登録されているアプリの安全な配布	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
アプリケーション ポリシーの違反	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	ポリシーに違反する端末をエンタープライズ ネットワークから隔離
脆弱なアプリと悪意のあるアプリ	社員が活用できるアプリケーションをホワイトリスト登録してコンプライアンスを確保	• 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 • 情報漏えいにつながる可能性のある危険なアプリ動作を検知
OS の脆弱性と適切でない構成		• 古い OS を完全に可視化 • 危険な端末構成とジェイルブレイク / ルート検知の可視化
ネットワークベースの攻撃		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
Web およびコンテンツベースの脅威		Web やコンテンツ経由のモバイルフィッシング行為を監視し、ブロック

Continuous Conditional Access と Cloud Identity

Cloud Identity Integration では、カスタム修復ポリシーを使用して、リスクのあ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 G Suite や他の企業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。