Lookout + Google Cloud Identity

Sichere Mobilität für produktivere Mitarbeiter im Unternehmen

Mit Google Cloud Identity können Administratoren Anwender, Geräte und Anwendungen sicher über eine zentrale Plattform verwalten. Dazu stehen eine native Mehrfaktorauthentifizierung (MFA), Single Sign-on (SSO) und Funktionen zur Mobilgeräteverwaltung zur Verfügung. Cloud Identity ist eine Hauptkomponente von Googles BeyondCorp-Modell für Unternehmenssicherheit und ermöglicht Mitarbeitern den sicheren Zugriff auf Anwendungen und Ressourcen ihrer Organisation – und zwar überall und mit jedem Gerät, wie es in der modernen Arbeitswelt verschwimmender Netzwerkgrenzen unabdingbar ist.

Viele Unternehmen setzen heute formale Mobility-Initiativen ein, um die mobile Produktivität ihrer Mitarbeiter zu fördern. Angesichts zunehmend unscharfer Netzwerkgrenzen ist Cloud Identity mittlerweile eine gängige Methode für Mitarbeiter, über ihre Mobilgeräte auf Unternehmensanwendungen zuzugreifen. Lookout schützt Hunderte Millionen Anwender sowie Unternehmen und Behörden vor netzwerk-, anwendungs- und gerätebasierten Risiken. Gemeinsam sorgen Lookout und Google Cloud dafür, dass nur vertrauenswürdige Mobilgeräte über Cloud Identity Zugang zu Unternehmensdaten und -anwendungen erhalten. Lookout Continuous Conditional Access überwacht dynamisch den Zustand des Endgeräts, während der Nutzer mit dem Unternehmen verbunden ist. Dadurch werden unautorisierte Zugriffe auf Infrastruktur und Daten der Organisation effektiv unterbunden.

Cloud Identity

- Identitäts- und Zugriffsmanagement
- Single Sign-on für Unternehmensanwendungen
- Verbesserte Kontosicherheit dank maschinellem Lernen
- Unified Endpoint Management
- Mobiler Zugriff auf Inhalte
- Mehrfaktorauthentifizierung (MFA)

Lookout Mobile Endpoint Security

- Continuous Conditional Access zu Unternehmensdaten
- Schutz vor app-, geräte- und netzwerkbasierten Risiken
- Phishing- und Content-Schutz vor webbasierten Bedrohungen
- Benutzerdefinierte Beseitigungsrichtlinien nach Art der Bedrohung
- Handlungsorientierte Warnungen und Beseitigung von Bedrohungen in Echtzeit

Nahtlose Integration für die Mobilgerätesicherheit

Risiken	Nur Google Cloud Identity	Lookout + Google Cloud Identity
Unsichere Authentifizierung	Erfordert MFA für den Zugriff auf die SSO-Plattform	Prüfung des Gerätezustands vor dem Zugriff auf die SSO-Plattform und Apps
Unsichere Bereitstellung von Apps	Sichere Bereitstellung von white-listed Apps aus Google Play und dem Apple App Store	Automatische Erkennung und Beseitigung von Apps, die Sicherheitsrichtlinien verletzen
Verstöße gegen Anwendungsrichtlinien	Apps, die die Sicherheitsrichtlinien des Unternehmens verletzen, müssen manuell auf die „Black List" gesetzt werden	Bei nicht richtlinienkonformen Geräten wird der Zugriff auf das Unternehmensnetzwerk unterbunden
Bösartige und mit Schwachstellen behaftete Apps	Sicherstellung der Richtlinieneinhaltung mittels Whitelisting für Anwendungen	• Erkennung von Apps, die unsichere Datenspeicher-/Datenübertragungsmethoden nutzen • Erkennung von App-Verhalten, das zum Stehlen von Daten führen könnte
Grundlegende Schwachstellen und Fehlkonfigurationen des Betriebssystems		• Voller Einblick in veraltete Betriebssysteme • Einblick in riskante Gerätekonfigurationen; Erkennung von Jailbreaking/Rooting
Netzwerkbasierte Angriffe		Schutz vor bösartigen Netzwerkangriffen auf verschlüsselte Unternehmensdaten während der Übertragung
Web- und contentbasierte Bedrohungen		Überwachung und Blockade von Phishing-Versuchen auf Mobilgeräten, bei denen Web- und andere Inhalte eingesetzt werden

Continuous Conditional Access mit Cloud Identity

Durch unsere Cloud Identity-Integration können gefährdete Geräte mittels benutzerdefinierter Beseitigungsrichtlinien in Echtzeit unter Quarantäne gestellt werden. Dies ermöglicht auch Zugangssperren für G Suite und andere Unternehmensanwendungen auf nicht verwalteten Geräten, je nach Risikoeinstufung durch Lookout. Sobald Lookout eine Bedrohung erkennt, wird abhängig von Ihren Sicherheitseinstellungen das Geräterisiko als „hoch", „mittel" oder „gering" eingestuft. Das folgende Diagramm zeigt, wie Bedrohungen generell beseitigt werden: