Lookout + Google Cloud Identity

Développez la productivité mobile de votre organisation en toute sécurité

Google Cloud Identity permet aux administrateurs de gérer les utilisateurs, les appareils et les applications en toute sécurité et en un clin d'œil depuis une seule et même console à l'aide de l'authentification multifacteur native, de l'authentification unique et de la gestion des appareils mobiles. En tant que composant clé du modèle de sécurité pour entreprise BeyondCorp de Google, Cloud Identity permet aux employés de bénéficier d'un accès sécurisé aux applications et aux ressources de leur entreprise, quels que soient leur localisation et l'appareil utilisé, ce qui est un facteur déterminant dans le monde extra-périmétrique actuel.

Les entreprises adoptent des programmes de mobilité pour développer la productivité de leurs employés. Dans le monde extra-périmétrique d'aujourd'hui, la solution Cloud Identity est devenue incontournable, car elle permet aux employés d'accéder aux applications de leur entreprise depuis leurs appareils mobiles. Des centaines de millions de personnes, d'entreprises et d'organismes publics font confiance à Lookout pour les protéger de tout risque émanant du réseau, des applications et des terminaux. Ensemble, Lookout et Google Cloud veillent à ce que seuls les appareils mobiles de confiance puissent accéder aux données et applications d'entreprise via Cloud Identity. L'accès conditionnel continu de Lookout surveille de manière dynamique la santé d'un terminal pendant qu'un utilisateur est connecté à l'entreprise, ainsi seuls les appareils de confiance seront autorisés à se connecter à l'infrastructure et aux données de l'entreprise.

Cloud Identity

- Gestion des identités et des accès
- Authentification unique pour les applications d'entreprise
- Sécurité des comptes améliorée via le machine learning
- Gestion unifiée des terminaux
- Accès mobile au contenu
- Authentification multifacteur

Lookout Mobile Endpoint Security

- Utilisation de l'accès conditionnel continu dans l'entreprise
- Protection contre les risques basés sur les applications, les appareils et les réseaux
- Protection contre les contenus et le phishing émanant de menaces Web
- Politique personnalisée de correction selon les types de menaces
- Alertes exploitables et correction des menaces en temps réel

Intégration transparente pour assurer une mobilité sécurisée

Risques	Google Cloud Identity uniquement	Lookout + Google Cloud Identity
Authentification non sécurisée	Nécessite l'authentification multifacteur pour accéder à la plate-forme d'authentification unique	Garantit que l'appareil est suffisamment en bonne santé pour accéder à la plate-forme d'authentification unique et aux applications de l'entreprise
Distribution des applications non sécurisées	Distribution sécurisée des applications placées en liste blanche par Google Play et l'App Store d'Apple	Détection et correction automatique des applications violant des politiques de sécurité
Violations de politiques d'application	Possibilité de créer manuellement une liste noire des applications identifiées comme contraires à la politique de l'entreprise	Isolation de l'appareil du réseau de l'entreprise en cas de violation des politiques mises en œuvre
Applications vulnérables et malveillantes	Garantir le respect de la conformité en créant une liste blanche des applications que les employés peuvent utiliser	• Détection des applications utilisant des méthodes de stockage/transfert de données non sécurisées • Détection des comportements d'applications à risque susceptibles de dévoiler des données
Vulnérabilités et défauts de configuration sous-jacents du système d'exploitation		• Visibilité totale dans les systèmes d'exploitation obsolètes • Visibilité dans les configurations d'appareils à risque et détections des jailbreaks/roots
Attaques basées sur le réseau		Protection contre les attaques réseau malveillantes ciblant des données d'entreprise chiffrées en cours de transfert
Menaces pesant sur le Web et les contenus		Surveillance et blocage des tentatives de phishing mobile via le Web et les contenus

Utilisation de l’accès conditionnel continu avec Cloud Identity

Grâce à notre intégration Cloud Identity, les terminaux à risque peuvent être mis en quarantaine en temps réel grâce à des politiques de correction personnalisées. Elles permettent notamment de bloquer tout accès à G Suite et à d’autres applications d’entreprise sur des appareils non gérés, conformément au statut de risque indiqué par Lookout. Lorsque Lookout détecte une menace, il classe l’appareil dans la catégorie « à haut risque », « à risque modéré » ou « à faible risque » selon les paramètres de votre politique de sécurité. Le processus de correction des menaces suit les étapes de base suivantes :