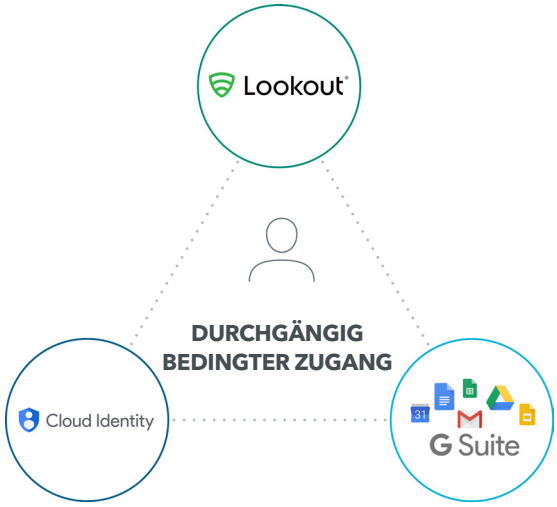
Lookout + Google Cloud

Lookout und Cloud Identity schützen in der Post-Perimeter Ära

Immer mehr Unternehmen setzen auf mobiles Arbeiten, um die Produktivität ihrer Mitarbeiter zu steigern, doch diese Netzwerküberschreitungen erfordern ein Umdenken bei der Sicherheit. Beim neuen Ansatz der Sicherheit über Netzwerkgrenzen hinaus (Post Perimeter Security) geht es um den Schutz von Unternehmensdaten, auf die Anwender und Geräte abseits des organisationseigenen Netzwerks zugreifen. Zum Schutz von Anwendern und Daten werden sowohl der Internetzugang als auch der Zugang zu Firmendaten je nach kontinuierlich überwachter Risikolage eingeschränkt oder freigegeben.

Gemeinsam sorgen Lookout Mobile Endpoint Security und Cloud Identity dafür, dass nur vertrauenswürdige Mobilgeräte auf G Suite-Angebote wie Google Docs und Google Präsentationen zugreifen können. Für diesen durchgängig bedingten Zugang überwacht Lookout dynamisch den Zustand von Endgeräten, die mit dem Unternehmensnetzwerk verbunden sind. So können sich nur vertrauenswürdige Geräte mit Plattformen vernetzen, in denen sensible Daten gespeichert sind. Lookout, eine Lösung, die sich bereits bei Hunderten Millionen Anwendern/Unternehmen und Behörden bewährt hat.

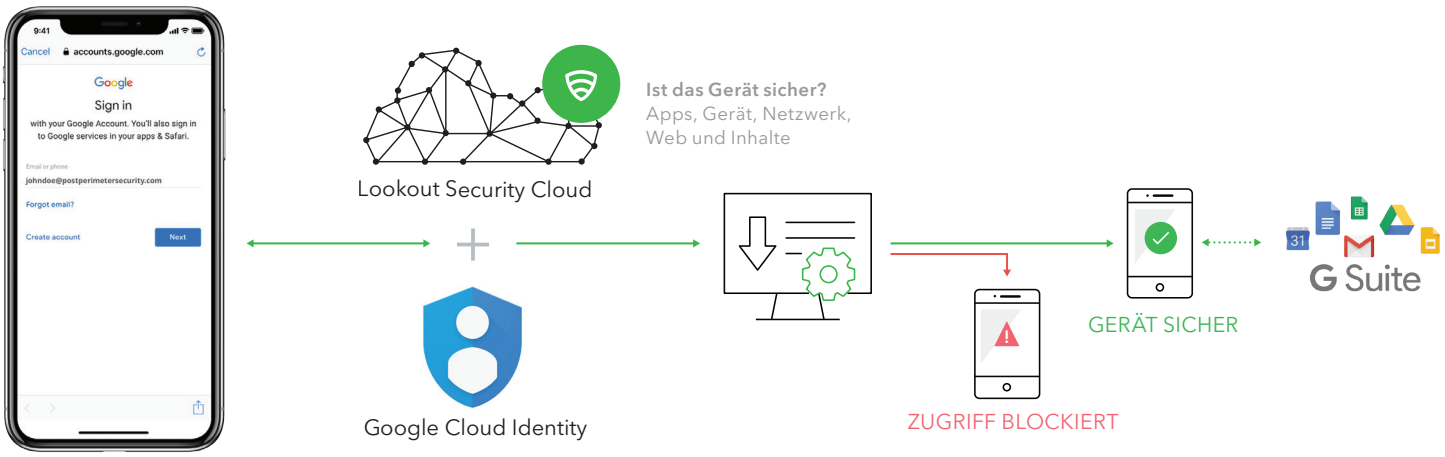


Sicherer Zugriff über Mobilgeräte dank Lookout und Cloud Identity

Nur mithilfe einer Lösung wie Cloud Identity lässt sich die Sicherheit über Netzwerkgrenzen hinaus durch IAM, SSO, ein einheitliches Endgerätemanagement und andere notwendige Funktionen sicherstellen. Lookout ergänzt diese Funktionen noch um Schutz vor Phishing-Versuchen, präparierten Apps und Geräterisiken. Hierfür tragen Cloud Identity und Continuous Conditional Access gemeinsam zur Gerätesicherheit und -integrität bei. Zusammen schützen Cloud Identity und Lookout Unternehmensdaten in G Suite vor bekannten und unbekannten Bedrohungen.

Risiken	Lookout + Cloud Identity
Unsichere Authentifizierung	Mehrfaktorauthentifizierung und Prüfung des Gerätezustands vor dem Zugriff auf die SSO-Plattform und Unternehmens-Apps
Unsichere Bereitstellung von Apps	Sichere Bereitstellung von zulässigen Apps; automatische Erkennung/Beseitigung von Apps, die gegen Sicherheitsrichtlinien verstoßen
Verstöße gegen Anwendungsrichtlinien	Funktion zum Erstellen von Unternehmensrichtlinien, sowie Abtrennung nichtkonformer Geräte vom Unternehmensnetzwerk
Präparierte und mit Schwachstellen behaftete Apps	Erkennung von Apps, die unsichere Datenspeicher-/Datenübertragungsmethoden nutzen, und von App-Verhalten, das zum Ausschleusen von Daten führen könnte
Grundlegende Schwachstellen und Fehlkonfigurationen des Betriebssystems	Voller Einblick in veraltete Betriebssysteme und 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

So gelingt der durchgängig bedingte Zugang



Ein Mitarbeiter greift über sein Gerät auf Unternehmensressourcen wie G Suite zu.

Lookout und – je nach Administratorrichtlinie – andere Quellen informieren Cloud Identity über den aktuellen Gerätezustand.

Erlaubt dem Administrator, Zugangsrichtlinien in Cloud Identity aufgrund von Lookout-Informationen zum Gerätezustand und Richtlinien zu konfigurieren.

Über die Post-Perimeter Security Alliance™

Die „Post-Perimeter Security Alliance" (Allianz für Sicherheit in der Post-Perimeter Ära) vereint führende Enterprise-Anbieter wie Google und Lookout, die eine gemeinsame Vision haben: die Gewährleistung von Sicherheit und Produktivität für eine moderne, cloud- und datenschutzorientierte Welt ohne klare Netzwerkgrenzen. Heute ist es besonders schwierig, mit nur einer einzigen Lösung umfassenden Schutz über die Netzwerkgrenzen hinaus zu erreichen. Dank integrierter Sicherheitsfunktionen, die Endgeräte, Cloud und Identitäten umspannen, sorgt diese Allianz für Sicherheit ohne Produktivitätseinschränkungen. Gemeinsam ermöglichen diese Lösungen die kontinuierliche Prüfung des Risikos für Unternehmensdaten sowie geeignete Gegenmaßnahmen.

Über die BeyondCorp-Allianz

In der BeyondCorp-Allianz haben sich Partner aus der Endgerätesicherheit und -verwaltung zusammengeschlossen, um mithilfe der Google Cloud Gerätezustandsdaten für dessen kontextsensible Zugriffslösung zu erheben. Im Rahmen des kontextabhängigen Zugriffs können Unternehmen Zugangsberechtigungen zu Apps und Infrastrukturen detailliert auf Basis der Anwenderidentität und des Zugriffsgrunds festlegen und umsetzen. Lookout engagiert sich bei BeyondCorp, um Unternehmen die Möglichkeit zu bieten, den Zustand mobiler Endgeräte im Unternehmensnetzwerk dynamisch zu überwachen. Hierfür werden die erfassten Daten der kontextsensiblen Zugriffs-Engine der Google Cloud zur Verfügung gestellt.

Über Lookout

Lookout sorgt für Cybersicherheit in einer mobilen, cloudorientierten Welt, in der die Netzwerkgrenzen zusehends verschwimmen. Dank des derzeit größten Datensatzes an Mobilgeräteinformationen bietet die Lookout Security Cloud einen tiefen Einblick in die gesamte Bandbreite mobiler Risiken. Lookout wird von Hunderten Millionen Anwendern, Hunderten Unternehmen und Behörden sowie Partnern wie AT&T, Verizon, Vodafone, Microsoft und Apple genutzt. Lookout hat seinen Hauptsitz in San Francisco und verfügt über Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, D.C.

Weitere Informationen erhalten Sie von Ihrem Ansprechpartner.

Lookout

lookout.com/de