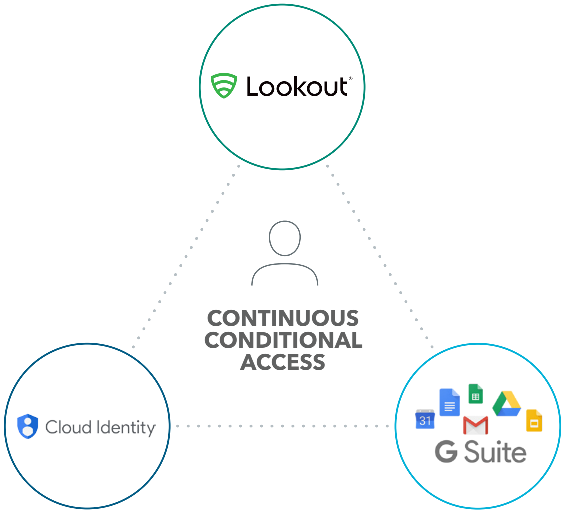
Lookout + Google Cloud

Securely Enable Your Post-Perimeter World with Lookout and Cloud Identity

As organizations adopt mobility to empower employee productivity, post-perimeter security is becoming a priority. Post-perimeter security is a new approach to enterprise security centered on the protection of corporate data when accessed by users and devices outside the corporate perimeter. It controls access to both the Internet and corporate data based on continuous assessment of risk, then modifies access to protect data and users if risk levels are exceeded.

Together, Lookout and Cloud Identity ensure only trusted mobile devices are accessing G Suite tools like Docs and Slides with the integration of Cloud Identity and Mobile Endpoint Security. Trusted by hundreds of millions of individuals, enterprises, and government agencies, Lookout Continuous Conditional Access dynamically monitors the health of an endpoint while a user is connected to the enterprise, allowing only trusted devices to connect to platforms storing sensitive data without being compromised by device, application, or network risks.

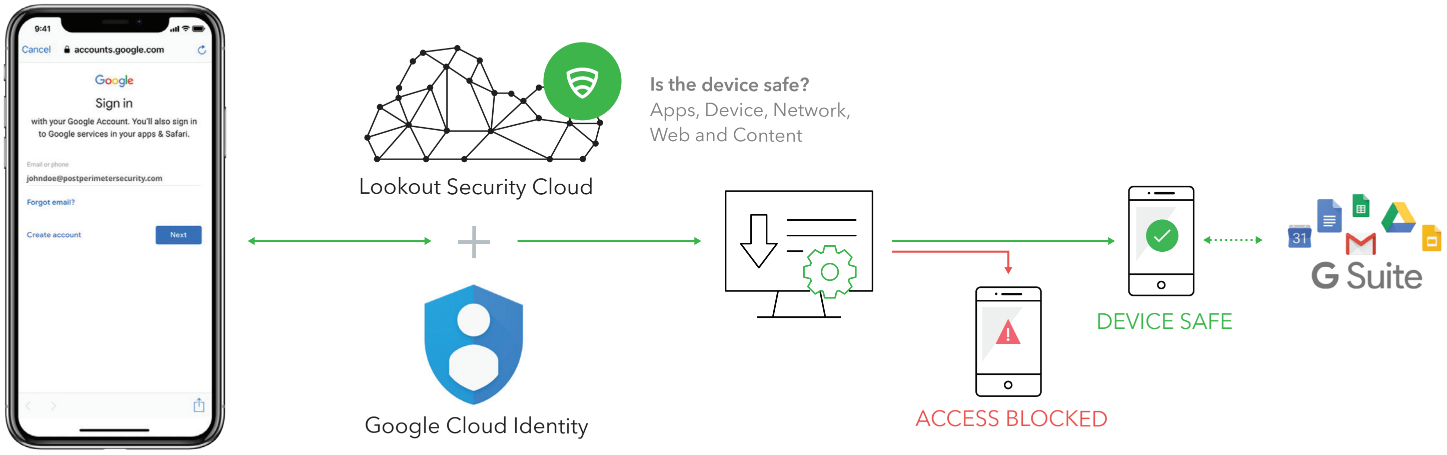


Lookout and Cloud Identity Provide Secure Mobile Access

Leveraging a solution like Cloud Identity is paramount in building a strong post-perimeter security posture by enabling IAM, SSO, unified endpoint management, and other necessary security capabilities. Lookout adds additional functionality to those capabilities by ensuring the security and health of the actual device by leveraging Cloud Identity with Continuous Conditional Access and protecting against phishing attempts, malicious app, and device-level risks. Together, Cloud Identity and Lookout protect access to corporate data stored in G Suite from known and unknown malicious threats.

Risks	Lookout + Cloud Identity
Insecure authentication	Requires MFA and ensures device is healthy enough to access SSO platform and corporate apps
Insecure app distribution	Enables secure distribution of white-listed apps and automated detection/remediation of apps that violate security policies
Application policy violations	Create app blacklisting policies and isolate the device from the corporate network if it violates implemented policies
Vulnerable and malicious apps	Detect apps using insecure data storage/transfer methods and risky app behavior that could cause data leakage
Underlying OS vulnerabilities and misconfigurations	Gain full visibility into out-of-date operating systems, risky device configurations, and jailbreak/root detections
Network-based attacks	Be protected against malicious network attacks on encrypted enterprise data in transit
Web and content based threats	Monitor and block mobile phishing attempts that leverage web and content

How Continuous Conditional Access Works



Employee accessing corporate resource like G Suite from device.

Cloud Identity will get the latest device health state from Lookout and other sources based on policies set by admin.

Allows admin to configure access policies in Cloud Identity based on Lookout device state and policies.

About The Post-Perimeter Security Alliance™

The Post-Perimeter Security Alliance includes leading enterprise vendors like Google and Lookout with a common vision to provide security and productivity for the modern, perimeter-less, cloud-delivered, and privacy-focused world. Today, it is difficult to achieve end-to-end post-perimeter security from a one-stop shop. With integrated security capabilities across endpoint, cloud, and identity, the Post-Perimeter Security Alliance delivers security without sacrificing productivity. Together, these solutions provide continuous assessment of risk to corporate data, and remediation and controls in the presence of such risks.

About BeyondCorp Alliance

The BeyondCorp Alliance is a group of endpoint security and management partners with whom Google Cloud is working with to feed device posture data for Google Cloud's context-aware access solution. Context-aware access allows organizations to define and enforce granular access to apps and infrastructure based on a user's identity and the context of their request. Lookout is a member of the Beyond Corp Alliance - giving organizations the ability to dynamically monitor the health of mobile endpoints connected to the enterprise and feed that data to Google Cloud's context-aware access engine.

About Lookout

Lookout is a cybersecurity company for the post-perimeter, cloud-first, mobile-first world. Powered by the largest dataset of mobile code in existence, the Lookout Security Cloud provides visibility into the entire spectrum of mobile risk. Lookout is trusted by hundreds of millions of individual users, enterprises and government agencies and partners such as AT&T, Verizon, Vodafone, Microsoft, Apple and others. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

Please contact your partner for more information.

Lookout®

lookout.com