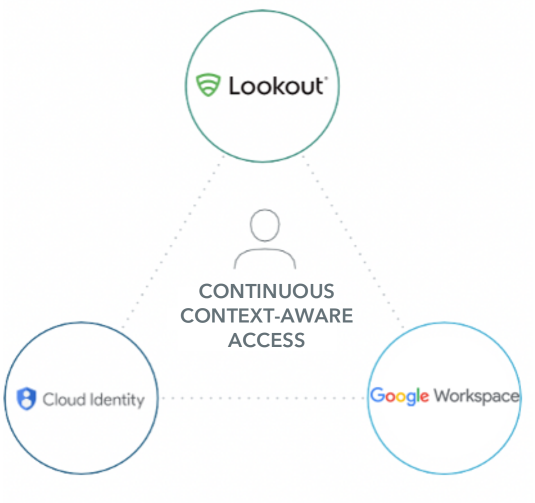
Lookout + Google BeyondCorp

Enable Zero Trust for your organization with Lookout and BeyondCorp



Global reliance on cloud-based infrastructure and services that are accessible from any device is causing security teams to rethink the way they protect their organizations. Employees use Android, ChromeOS and iOS devices to access productivity apps like Google Workspace to be productive outside the office, but this renders an organization's perimeter-based security obsolete. Therefore, security needs to be extended to every endpoint, including those running Android, ChromeOS and iOS. Organizations need a modern approach that delivers a Zero Trust strategy by only permitting access to corporate resources from mobile devices with a permitted risk level, and then need to continuously monitor the risk level to modify access privileges to protect your data and applications.

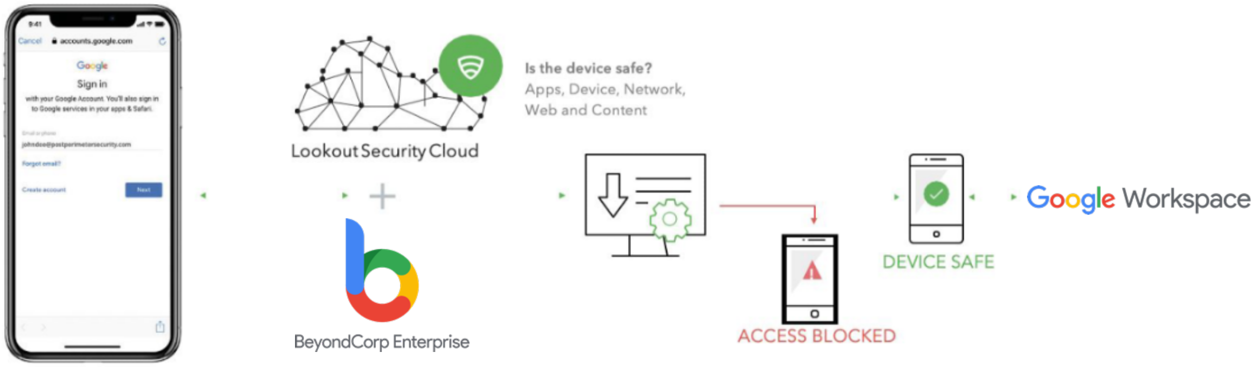
Lookout and Google ensure that you only provide access to mobile devices with acceptable levels of risk (as determined by organizational policies). With a platform built for mobile from the ground up, Lookout can detect threats even if they've never seen them before. Lookout provides continuous security telemetry to Google Cloud, ensuring that your data and infrastructure stay secure.

Lookout and BeyondCorp Provide Secure Mobile Access

Integrating Lookout with a scalable platform like Google Cloud is paramount to building a strong modern endpoint protection strategy. Together, Lookout Continuous Context-Aware Access and Google BeyondCorp protect your Google Workspaces from malicious threats delivered via mobile phishing scams, malicious apps, and device-level exploits.

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 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 Context-Aware Access Works



Employee accessing Workspace from their mobile device

BeyondCorp will receive the latest device risk data from Lookout and other sources based on policies set by admin

Access is allowed or blocked based on policies set in the Google Admin console that feed on security signals from Lookout

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 an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.