Lookout Google Cloud

4 Ways Lookout and Google Cloud Empower Mobile Workers While Protecting Enterprise Data

Lookout and Google have partnered up to give your employees seamless access to what they need without risking your enterprise data.

The trend toward remote work, already well underway before 2020, was accelerated by the pandemic. Now, organizations need to support their employees as they work from any location and device of their choosing, whether they're Android- or iOS-based. This poses a significant challenge for IT leaders: How can they ensure the security and privacy of data no matter what device an employee uses to access it? How can they guard against insecure apps, rogue malware, and malicious content that might find its way onto unmanaged devices? How can they protect the organization from phishing and other social engineering attacks?

The answer is **a modern, Zero Trust strategy that lets employees use their device of choice while ensuring that only healthy devices can access enterprise data.** You must be able to continuously monitor the risk level of both the user and device in order to ensure ongoing protection of data, users, and applications. You should also educate users by providing them the information they need to remove any threat that may arise.

> Organizations need to support their employees as they work from any location and device of their choosing, whether they're Android- or iOS-based.

Lookout Google Cloud

Cybersecurity company Lookout has partnered with Google Cloud to enable organizations to secure their mobile devices, even if those endpoints aren't managed. This partnership enables employees to securely access Google Workspace and other enterprise apps without the fear of mobile threats compromising corporate data. The integration of Lookout Continuous Conditional Access and Google BeyondCorp protects valuable intellectual property such as confidential presentations built in Slides, financial reports and analysis calculated in Sheets, and research reports residing in Docs by ensuring only healthy devices have access to that highly sensitive data.

The integration between Lookout and Google Cloud helps make BeyondCorp — the Google Zero Trust model — a reality. Lookout integrates with Google Workspace and BeyondCorp Enterprise to deliver Zero Trust security from endpoint to cloud. **Here are four ways in which this partnership works to protect your organization's valuable data.**

1 Control access to corporate data and apps.

2 Meet privacy and compliance standards.

3 Protect data at the device level.

4 Gain the benefits of BYOD without the risks.

1 Control access to corporate data and apps.

Lookout protects your data from known and unknown threats through the Lookout Security Graph, which leverages machine intelligence and telemetry data from tens of millions of devices, apps, and phishing URLs. **Lookout continuously assesses the risk profile of mobile devices and delivers it dynamically via the Google BeyondCorp devices API.** Should a device become compromised or pose a security risk, the system can quarantine it in real time using predefined remediation policies. This includes the ability to block access to Google Workspace and other enterprise apps. Together, Lookout and Google Cloud enable employees to use Android- and iOS-based devices securely without violating their privacy and trust.

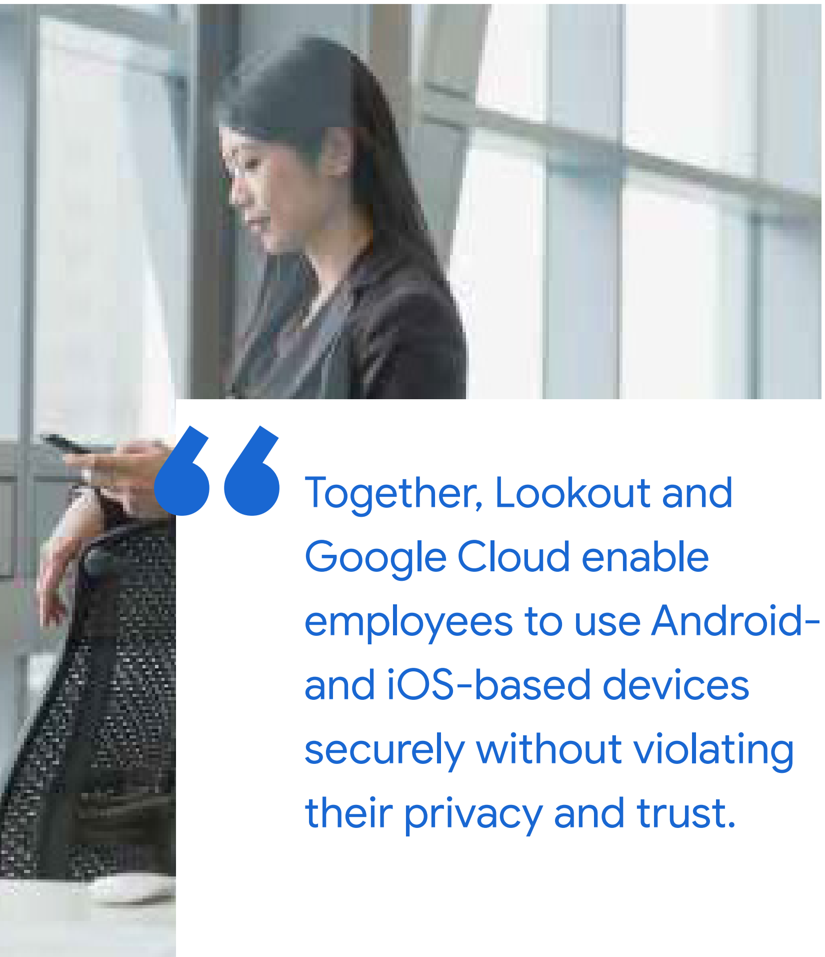
2 Meet privacy and compliance standards.

Privacy and compliance standards continue to evolve and now encompass mobile devices and apps in their parameters. Mobile makes it difficult for risk and compliance teams to know which apps are accessing sensitive compliance-related data. In addition, some app permissions could seem innocuous but still violate corporate privacy standards. Lookout provides full risk and compliance capabilities to give complete visibility into the data access and transfer practices of all mobile apps, in addition to alerting when malware is present on a device. **Based on the organization's risk policies, Lookout flags access or transfer practices that increase risk, violate compliance, or unintentionally exfiltrate corporate data.** Lookout passes this information onto Google Cloud Identity, which limits access to Google Workspace until the issue is resolved.

3

Protect data at the device level.

Employees using phones and tablets for work expect to have the freedom to use their devices as they wish. However, they could mistakenly compromise corporate data by downloading malicious apps whether for work or personal reasons. These days, attackers can deliver mobile malware, device vulnerability exploits, and phishing attacks through almost any app on mobile devices. Lookout protects your employees and your data from these threats. It also enables protection against mobile phishing campaigns, which use social engineering techniques to fraudulently acquire login information or trick users into installing malware. **By silently protecting users in the background until a threat is detected, Lookout enables employees to use their devices as they wish within the bounds of your corporate acceptable use policies.**



> “Together, Lookout and Google Cloud enable employees to use Android- and iOS-based devices securely without violating their privacy and trust.

4

Gain the benefits of BYOD without the risks.

A bring-your-own-device (BYOD) approach benefits employees and organizations alike. Employees don’t need separate work and personal devices. They can use their device of choice to get their work done. Your company, meanwhile, doesn’t have to purchase and manage dozens, hundreds, or thousands of devices. **The continuous risk assessment that Lookout provides protects the user, device, and organization from mobile threats on any Android or iOS device, no matter whether it’s managed, unmanaged, personal or corporate-owned.** It does all this with end-user privacy in mind, which ensures that IT and security teams can provide the necessary protections without invading the personal privacy of their employees.

Lookout and Google Cloud enable modern work with security from endpoint to cloud

Lookout and Google Cloud work together to enable customers to work productively and securely from anywhere and on any device. Their integration ensures that you only provide access to mobile devices that meet risk thresholds determined by your company’s 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.

To learn more ways in which Lookout integrates with Google Cloud to deliver Zero Trust security from device to cloud, visit bit.ly/3wYDsnM.