Lookout + Google Cloud Identity

Securely enable mobile productivity for your organization

Google Cloud Identity enables admins to easily manage users, devices, and applications securely from one console with native multifactor authentication, single sign-on and mobile device management. As a key component of Google's BeyondCorp enterprise security model, Cloud Identity enables employees to have secure access to enterprise apps and resources from anywhere and any device, which is critical in a post-perimeter world.

Organizations are adopting formal mobility programs as a way to empower employee productivity. In this post-perimeter world, Cloud Identity has become one of the main ways for employees to access enterprise applications from mobile devices. Lookout is trusted by hundreds of millions of individual users, enterprises and government agencies to protect against network, application, and device-based risks. Together Lookout and Google Cloud ensure only trusted mobile devices are accessing enterprise data and apps via Cloud Identity. 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 enterprise infrastructure and data..

Cloud Identity

- Identity and access management
- Single sign-on for enterprise apps
- Enhanced account security through Machine Learning
- Unified Endpoint Management
- Mobile access to content
- Multi-factor authentication

Lookout Mobile Endpoint Security

- Continuous Conditional Access to the enterprise
- Protection against app, device, and network based risks
- Phishing and Content Protection from web-based threats
- Custom remediation policy across threats types
- Actionable alerts and real-time threat remediation

Seamless integration to provide secure mobility

Risks	Google Cloud Identity only	Lookout + Google Cloud Identity
Insecure authentication	Requires MFA to access SSO platform	Ensures device is healthy enough to access SSO platform and apps
Insecure app distribution	Secure distribution of white-listed apps from both Google Play and the Apple App Store	Automated detection and remediation of apps that violate security policies
Application policy violations	Manual blacklisting of apps determined to violate company policy	Isolate the device from the corporate network if it violates implemented policies
Vulnerable and malicious apps	Ensure compliance by whitelisting which applications employees can leverage	• Detect apps using insecure data storage/transfer methods • Detect risky app behavior that could cause data leakage
Underlying OS vulnerabilities and misconfigurations		• Full visibility into out-of-date operating systems • Visibility into risky device configurations and jailbreak/root detections
Network-based attacks		Protection against malicious network attacks on encrypted enterprise data in transit
Web and content based threats		Monitor and block mobile phishing attempts via web and content

Continuous Conditional Access with Cloud Identity

With our Cloud Identity Integration, at-risk devices can be quarantined in real time using custom remediation policies. This includes the ability to block access to G Suite and other enterprise apps on unmanaged devices based on Lookout risk status. When Lookout detects a threat, the device will be categorized as either "high risk", "moderate risk", or "low risk" depending on your security policy settings. The threat remediation process follows these basic flows: