Lookout for Google Chrome OS

Lookout protects organizations from cyberthreats targeting Chromebooks

Overview

Many organizations are now embracing the use of Google Chromebooks as a cost-effective method to connect to cloud resources and sustain productivity in the workplace. As more sensitive data goes to the cloud, your organization's security policies must extend to all endpoints including Chrome OS devices that are accessing business resources. Lookout makes it easy to get visibility into the entire spectrum of risk, apply policies to measurably reduce that risk, and integrate into your existing security and endpoint management solutions.

Protection against threats

As more sensitive data is accessed by Chromebook laptops and tablets, they are increasingly becoming a target for attackers. Lookout identifies threats targeting these primary attack vectors on Chrome OS:

- **Phishing and web content threats:** Protection against phishing attacks and website sites that when visited can execute malicious code to infect the connected Chromebook
- **Network-based threats:** Detection of man-in-the-middle attacks ensures cyber attackers do not intercept your network traffic.
- **App-based threats:** Detection of malicious Android apps used on Chromebooks is essential for protecting enterprise data.

Lookout shows phishing encounter rates exceeding 21% in 1Q2020.

Lookout is protecting users as they increasingly encounter phishing attacks at dangerous rate of more than 21%. Malicious URLs include ad fraud, botnets, command and control centers, links to malware, malware call-home, malware distribution points, phishing/fraud, spam URLs, and spyware.

chromebook

Benefits

Measurable reduction of risk

Close a large security gap and measure your risk reduction with analysis and reporting features

Seamless interoperability

Lookout integrates with all SIEM systems via our Mobile Risk API, including **Splunk, Defender ATP, Micro Focus, ArcSight, and QRadar**

Visibility into incidents

Get real-time visibility into incidents on Chrome OS devices, so you can respond effectively

Securely enable mobility

Embrace more flexible mobility programs, including BYOD, to increase employee productivity and stay competitive

Privacy by design

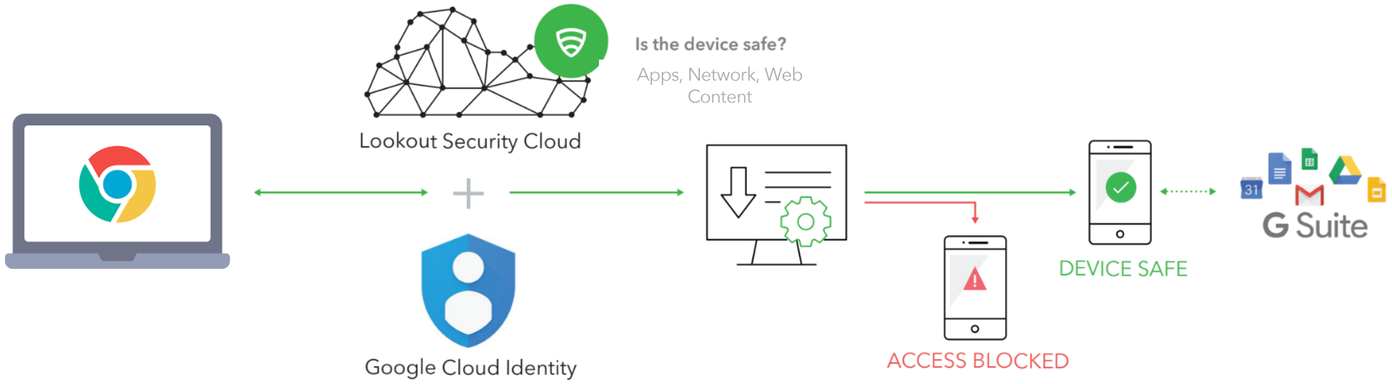
Ensure data sovereignty and employee privacy policies are upheld using our privacy controls

Easy to deploy and maintain

We integrate with any EMM (such as **VMware Workspace ONE® UEM, Microsoft Endpoint Manager, BlackBerry® UEM, IBM MaaS360®, MobileIron**)

How it works

Lookout leverages a lightweight endpoint app on employee Chrome OS devices, a cloud-based admin console that provides real time visibility into risk, and a tight integration with the Google Cloud. By monitoring the health of the Chrome OS device, Lookout assigns a risk-level and passes this information to Google Cloud Identity to apply access policies based on this information. Depending on the policy, access may be blocked until the threat on the device is removed.



Employee uses G-Suite from a Chromebook to connect to corporate data.

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.

Why Lookout

- Lookout has amassed one of the world's largest security datasets due to our global scale. Lookout has collected security data from over 180M devices worldwide and over 100M apps, with up to 100K new apps analyzed daily.
- This global sensor network enables our platform to be predictive by letting machine intelligence identify complex patterns that indicate risk. These patterns would otherwise escape human analysts.
- Lookout has a strong partnership with Google and has developed endpoint security applications for Android and Chrome devices. As a Google Cloud Partner and member of the Google App Defense Alliance, Lookout works closely with Google to share threat intelligence.