Lookout Integrations and Alliances

Lookout integrates with leading enterprise tools to deliver unified security, visibility, and remediation of mobile threats

Overview

As the leading provider of mobile security, it's important for Lookout to integrate with tools that help organizations benefit from unified security, visibility, and management of endpoints. As such, Lookout has built a number of native integrations and alliances with other mobility and security tools in order to make sure customers get the most out of every tool and can build the strongest security posture possible.

The shift away from traditional perimeter-based security into a post-perimeter world means that employees are accessing the same data from their mobile devices that they can from their computers in the office. For that reason, it's necessary for security teams to integrate mobile security solutions into their existing stack in order to make sure the devices accessing data out in the world are secure and, by association, the data itself that they access is secure.

By securing users and organizations against phishing, application, device, and network threats, Lookout plays a key role in making sure the entire employee base is operating in a secure fashion and can do so from anywhere.

Lookout®

Lookout protects against the spectrum of mobile risk by leveraging our cloud-based threat intelligence to detect and protect against:

- Phishing attacks targeting a user's mobile device across email, SMS, messaging, and other apps
- Malicious and side loaded applications that could pose serious threats to the greater organization
- OS, configuration, and rooting or jailbreaking risks that could cause the device to fall out of compliance
- Network-based attacks such as man-in-the-middle that can silently view and filter device traffic

Integration and Alliance Overview

As a long-standing member of the Apple Developer program, Lookout has developed iOS mobile endpoint security applications for both personal and Enterprise-level protection. The Lookout security research teams work closely with Apple to share threat intelligence and ensure security on iOS devices.

Lookout compliments and enhances the iOS platform by enabling Enterprises to be able to embrace mobility and drive digital business transformation. Lookout provides unparalleled visibility into:

App review to vet in-house developed apps to ensure corporate compliance. This ensures compliance with both internal and external policies and standards.

App behaviour and risk for corporate compliance grants visibility into app behaviour to prevent exfiltration of corporate data. Ex: Blacklist apps that send data to external cloud services.

Network protections secure devices from being leveraged for Man-in-the-Middle attacks

Phishing and Content Protection protects employees from mobile phishing attacks that come through any channel from email to text to third-party apps.

BlackBerry is a technology and resell partner of Lookout with worldwide capability to resell Lookout MES. With its acquisition of Cylance, they can now protect Windows, MacOS, and Linux servers, desktops, and laptops. Lookout compliments this by providing a full range of protections for iOS and Android devices. Together, Lookout and BlackBerry Cylance provide comprehensive security for all endpoints in the post-perimeter world.

BlackBerry UEM Connector for both managed and unmanaged endpoints provides an integrated solution that enables Continuous Conditional Access to protect corporate data. Ex: Unhealthy devices can be quarantined in real time with custom policies

Over the course of Lookout's long-standing partnership with Google, we have developed both a personal and Enterprise mobile endpoint security application for Android devices. Lookout's security research team works closely with Google to share threat intelligence, and most recently discovered the BeiTaAd plug-in in multiple applications on the Play Store. Google has since banned the developer of those applications from adding apps to the Play Store.

Google Cloud Identity Integration (aka BeyondCorp API) integrates with Lookout, which is the first mobile threat detection platform to do so, to provide Continuous Conditional Access to GSuite and other corporate apps.

Lookout was the first MTD to integrate with Microsoft for Intune, Windows Defender ATP, and the Microsoft Graph Security API. Lookout protects millions of Office 365 users around the world.

Intune integration provides Continuous Conditional Access to corporate resources based on risk assessment conducted by Lookout. Ex: If the device is found to be noncompliant, access to resources like Exchange Online and SharePoint Online can be blocked.

Windows Defender ATP with AAD Authentication provides a single pane of glass for threats across devices to drive more intelligent correlation and remediation tactics.

Lookout is the only VMware partner to have three Workspace ONE digital workspace integrated solutions available. Lookout offers integrations with Workspace ONE UEM for managed mobile devices, Workspace ONE Boxer for unmanaged mobile devices and Workspace ONE Intelligence as part of VMware's TrustNetwork partnership program as VMware's only Mobile Threat Defense partner.

Workspace ONE UEM (AirWatch) integration provides Continuous Conditional Access for managed environments based on device health. Ex: At-risk devices can be quarantined in real time using custom remediation policies.

Workspace ONE Boxer integration enables Bring You Own Device (BYOD) mobile application management based on the health of the device

Workspace ONE Intelligence Integration provides a Single pane of glass for threats across devise to drive more intelligent correlation and remediation tactics.

Citrix Endpoint Management (XenMobile) integration provides Continuous Conditional Access for managed environments based on device health. Ex: At-risk devices can be quarantined in real time using custom remediation policies.

ArcSight integration Arcsight integration enables admins to leverage their SIEM and feed both mobile alerts and device health risks into one central location

Our co-marketing and co-selling partnership brings together two solutions to provide a comprehensive endpoint protection posture across all devices. Ex: Leverage Sentinel One to protect all desktops, laptops, and servers while Lookout protects all mobile devices

Lookout mobile risk information Splunk integration enables admins to leverage their SIEM and feed both mobile alerts and device health risks into one central location