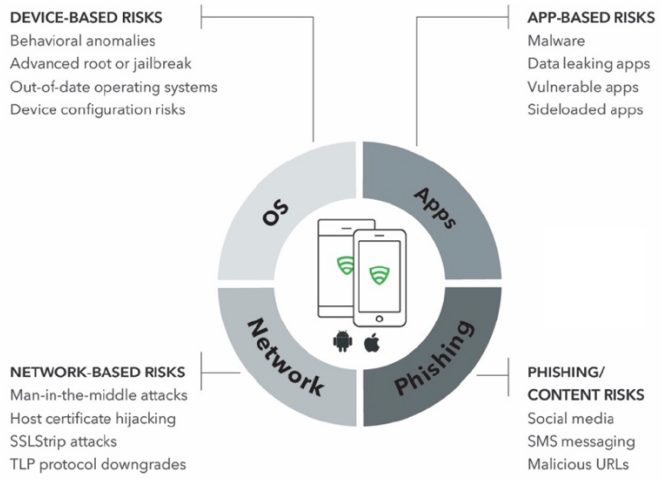
Lookout + Microsoft Partnership

Better together, Lookout + Microsoft secure enterprise mobility

Overview

Organizations are increasingly adopting mobile management strategies to empower mobile productivity, but in today's sophisticated threat landscape it's more challenging than ever to ensure corporate data and assets stay protected. With Lookout's mobile protection of iOS and Android devices combined with Microsoft mobile and security solutions, organizations are able to embrace a mobile first, cloud first approach to enable employee productivity while protecting sensitive data accessed by their mobile devices.



Comprehensive mobile security

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

- Phishing on email, SMS, messaging & apps
- Malicious and side loaded applications
- OS, config, and rooting/jailbreak risks
- Network and man-in-the-middle attacks

Lookout + Microsoft Azure Active Directory (AAD) and Intune

Risk-based conditional access

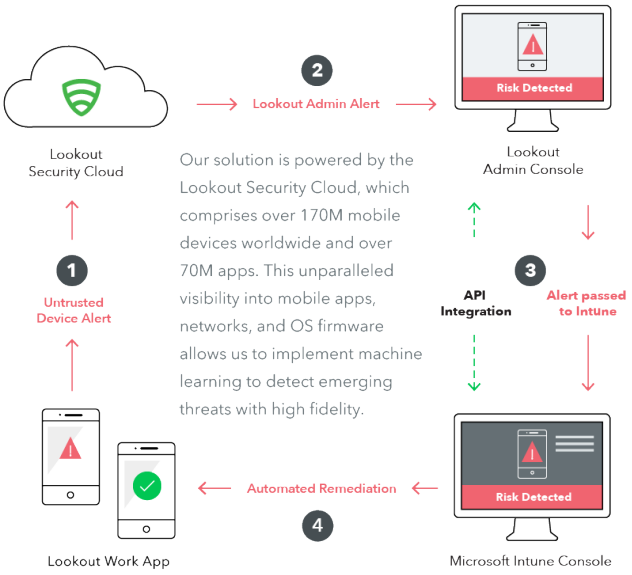
With the Microsoft EMS and Lookout integration, Lookout can inform Intune of device risks such as malicious applications, OS vulnerabilities, network attacks, phishing attempts or even applications that violate GDPR policies. These alerts are integrated into the Intune management console and can be used to inform conditional access policies that prevent risky devices from accessing corporate resources until the compliance violation is remediated.

Ease of use

The integration between Lookout and Azure Active Directory allows for seamless deployment and management of the Lookout client app via Microsoft Intune. This includes integrated policy management for users and groups as well as integrated identity with AAD for single sign-on for end users and administrators.

Security and compliance

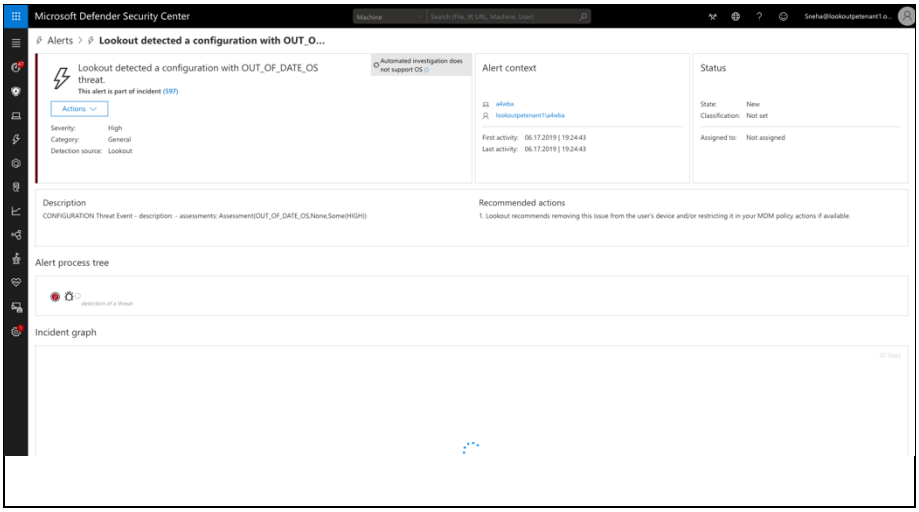
Lookout application compliance capability allows an organization to discover mobile applications that violate enterprise security, privacy or governance policies. For example, applications that expose the user's contact list or location can be blacklisted and usage information sent to Intune for reporting and conditional access policies.



Lookout + Microsoft Windows Defender ATP

Mobile security device alerts integrated with windows devices

Lookout's Mobile Endpoint Security solution is integrated with Microsoft's Windows Defender Advanced Threat Protection (ATP). This integration enables Microsoft customers to detect, view, investigate, and respond to advanced cyberattacks and data breaches on iOS and Android devices from within the Windows Defender ATP management console. The integrated console will expose Lookout device threat and health information to the main dashboard and throughout subsections for a fully integrated single pane of glass experience.



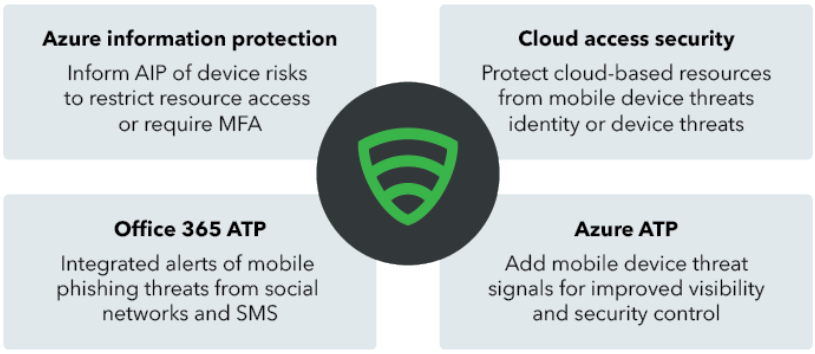
Enhanced visibility into mobile threats

- Integrated console for mobile alerts
- Dashboard with threat summaries
- Correlation across user devices
- Threat alert details and remediation
- Mobile device event history timelines

Lookout + Microsoft Graph Security API

Mobile device threat data for Microsoft advanced security workloads

Lookout integration with the Microsoft Graph Security API will allow customers to query, receive, correlate, and report on Lookout mobile threat telemetry from an ecosystem of Microsoft Graph-connected applications. Lookout telemetry can combine with other threat intelligence and security signals from across Microsoft products, services, and security solutions as well as signals from third party Microsoft Graph providers to identify and mitigate cyberthreats.



Uniquely powerful threat telemetry

- Ensure only health devices access corporate resources
- Leverage threat signals to inform conditional access
- Phishing alert signals broaden other ATP alerts

Why Lookout

Microsoft and Lookout have partnered to enable organizations to securely embrace smartphones and tablets in the workplace. Lookout shares Microsoft's vision of applying machine learning techniques to a large security dataset in order to rapidly detect and respond to new threats. Lookout has collected security data from over 170M devices worldwide, and has analyzed over 70 million iOS and Android apps using advanced machine learning techniques to identify risks on those platforms. As a distinguished Microsoft Partner, Lookout has pioneered a number of valuable Microsoft integrations:

- **Microsoft Intune and Enterprise Mobility + Security.** With seamless activation using Azure Active Directory, Lookout enforces Lookout Continuous Conditional Access based on real-time network, and device-based risks.
- **Microsoft Windows Defender ATP.** This integration enables Microsoft customers to detect, view, investigate, and respond to cyber-attacks and data breaches on iOS and Android devices within the WDATP Management Console.
- **Microsoft Intelligent Security Graph.** Seamless integration to share Lookout telemetry-based mobile threat events.
- **Microsoft Intune MAM:** Lookout assesses mobile device health and enforces Continuous Conditional Access to MAM-enabled apps.

To learn more about how Lookout + Microsoft can help protect your organization, go to lookout.com/microsoft.