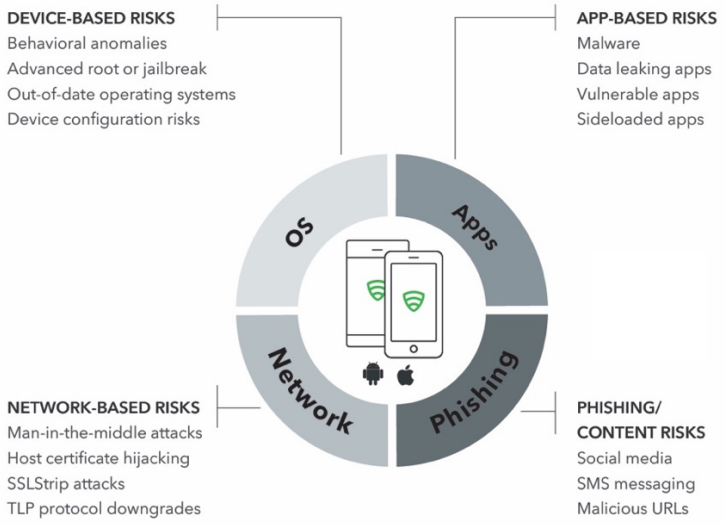
Lookout + Microsoft Windows Defender ATP

Partnering to enable secure mobility in the enterprise

Protecting enterprise data from mobile threats

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 mobile protection of iOS and Android devices combined with Microsoft mobile and security solutions, organizations can 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

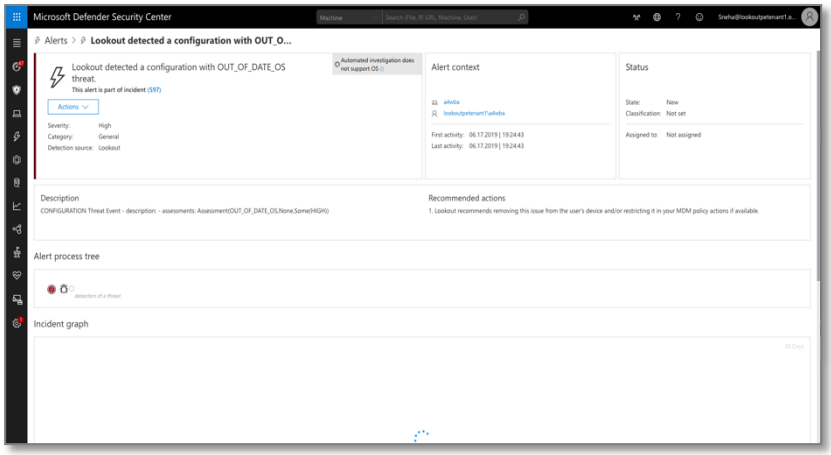
Lookout and Microsoft Windows Defender ATP

Lookout Mobile Endpoint Security solution is integrated with Microsoft 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 portal. The integrated portal will expose Lookout device threat and health information to the main dashboard and throughout subsections for a fully integrated single pane of glass experience.

Information includes the threat type, threat description, threat severity of low/medium/high, and remediation steps for the threat. Threats identified include malicious applications, mobile phishing attacks, network attacks and operating system vulnerabilities. These threat notifications are immediately sent to the user as well as the Windows Defender ATP portal. Integrating a user's mobile device threat information with that of the user's Windows devices provides an improved security picture of an enterprise environment and the security threats users are facing.

How the integration works

The Lookout Windows Defender ATP integration uses a Lookout ATP connector to pass mobile device and threat information from the Lookout Mobile Risk API to the Windows Defender ATP API. This integration does not require Intune or other MDMs because the Lookout cloud service communicates directly to the Windows Defender cloud service. The mobile device and threat information exposed by Lookout is specific to the customer's environment and will be integrated throughout the Windows Defender ATP portal, including the main operator dashboard, analytics dashboard, alerts and machine screens for a fully integrated experience.



Features Snapshot

- Integrated console for mobile alerts
- Dashboard threat summary
- Device correlation with user's other devices
- Alert details including threat description, severity, and remediation recommendations
- Mobile device history event timelines

"The integration between Lookout's mobile threat defense and Microsoft's Windows Defender ATP service will provide an unprecedented level of visibility and response capability across the different device types enterprise customers must secure"

Moti Gindi

General Manager Windows Cyber Defense, Microsoft

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 Microsoft Partner, Lookout has also pioneered other valuable Microsoft integrations including **Microsoft Intune and Enterprise Mobility + Security, Microsoft Intelligent Security Graph**, and **Microsoft Intune MAM.**