Lookout for Small Business + Microsoft Office 365

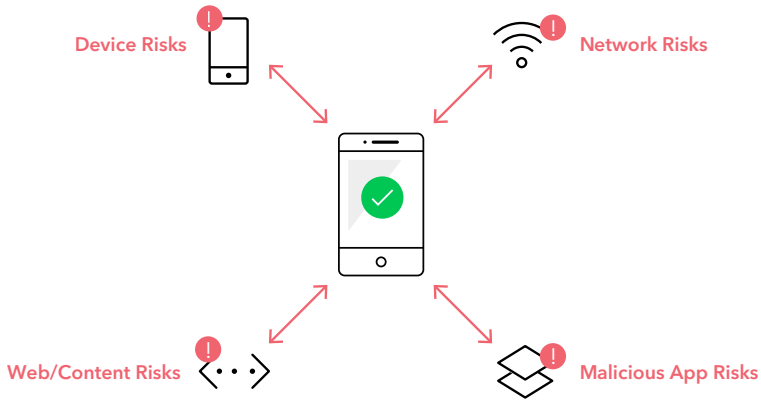
Enabling secure productivity of your mobile workforce

Overview

Small businesses are increasingly relying on Microsoft Office 365 to enable their employees to work how they want with trusted applications like Outlook, Word, Excel, and Powerpoint on multiple devices. On-the-go access to company resources from mobile devices is now expected by users and boosts productivity as employees connect from nearly anywhere. However, such convenience can present a cybersecurity risk to businesses, which if not mitigated, can result in a breach of sensitive information.

Lookout provides visibility into the spectrum of mobile risk enabling secure access to company resources from mobile devices. With Lookout, you can access sensitive business and personal data knowing you have full protection against the following mobile threats:

- App-based threats: Malware, rootkits, and spyware
- Network-based threats: Man-in-the-middle attacks
- Device-based threats: Hijacked admin control, out-of-date software, or risky device setup
- Web & Content-based threats: Phishing attacks or malicious websites & files



Benefits of Lookout + Microsoft Office 365

Measurable reduction of risk

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

Visibility into mobile incidents

Get real-time visibility into incidents on mobile devices, so you can respond quickly and effectively

Securely enable mobility

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

Privacy by design

Ensure your data sovereignty and employee privacy are upheld using our privacy controls features

Self-remediation

Save time and stay safe by enabling users to remediate without the need for assistance from IT

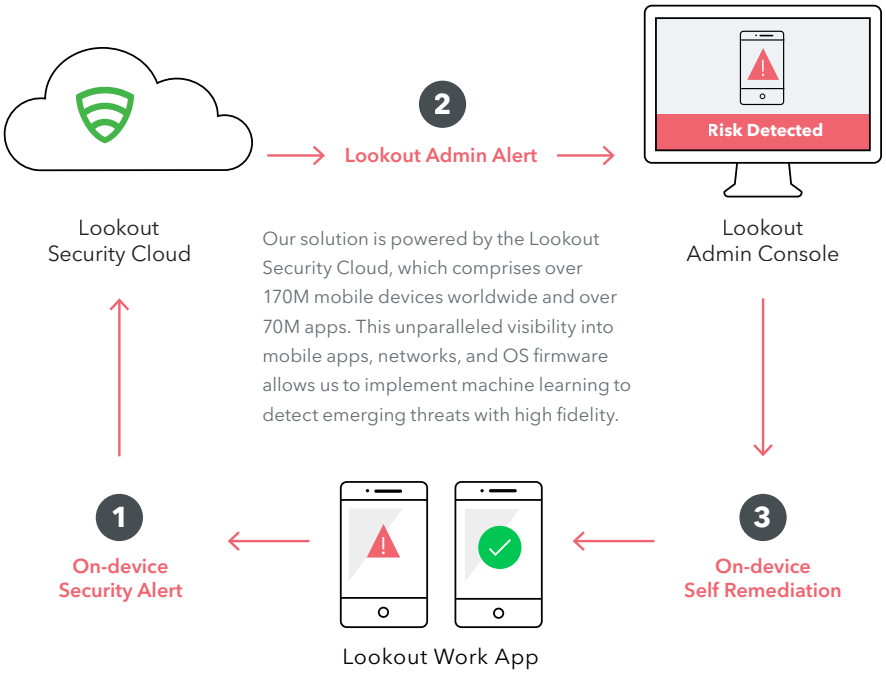
"Gartner predicts that 80% of worker tasks will take place on a mobile device by 2020."

Gartner, *Prepare for Unified Endpoint Management to Displace MDM and CMT,* June 2018

How It Works

Lookout leverages a lightweight endpoint app on employee devices, a cloud-based admin console that provides real time visibility into mobile risk, and the vast security intelligence data of the Lookout Security Cloud.

Lookout continuously monitors the health of the mobile device and immediately sends alerts to both the device and Lookout Admin Console upon detection of a threat. Based upon the severity of the threat, Lookout will either require and provide steps for remediation by the user or allow the user to continue after acknowledgment.



1. Lookout detects a threat
2. Alert window pops up on users device and admin console
3. Based on severity, Lookout blocks access to either the internet or the domain (i.e. microsoft.com)
4. Lookout requests remediation
5. User self-remediates threat
6. Lookout restores access to the internet or the domain
7. User continues to access Office 365 applications

Lookout users experience a 95% self-remediation rate for threats.

The Lookout Difference

- Mobile is a new era of computing and requires a new era of security solution designed exclusively for this platform.
- Lookout has been securing mobility since 2007 and has amassed one of the world's largest mobile security datasets due to our global scale and mobile focus. Lookout has collected security data from over 170M devices worldwide and over 70M apps, with up to 90K new apps added daily.
- Driven by artificial intelligence leveraging our massive dataset, combined with industry leading AI and a rich patent portfolio, Lookout is the leader in detecting and remediating zero-day and known threats in a post-perimeter world.

To learn how you can secure your mobile fleet today, contact us at info@lookout.com.