Secure BYOD for Office 365 users with Lookout

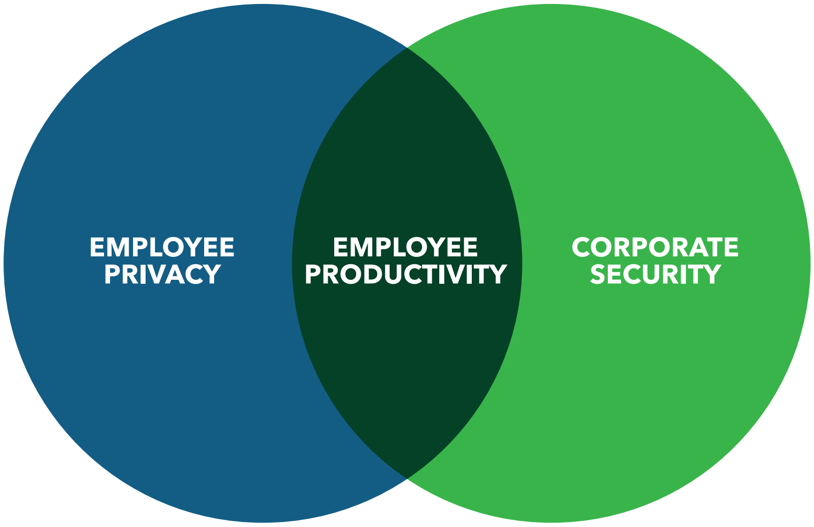
Continuous Conditional Access for Microsoft Intune-protected apps

Work has fundamentally changed

Critical data has moved to the cloud, and employees demand access to that data from any network, from any location. Always connected, personal mobile devices are increasingly used for work. At the intersection of personal and business use, firms need mobile security strategies that support productivity, safeguard corporate data, and address employee resistance to corporate oversight of personal devices.

Users do not want MDM on their mobile device

Employees increasingly demand to use their own mobile phone or tablet for both personal and professional use and do not want Mobile Device Management (MDM) on their device. This challenges security teams to balance employee privacy and security to enhance employee productivity.



Microsoft Office 365 is driving productivity of BYOD

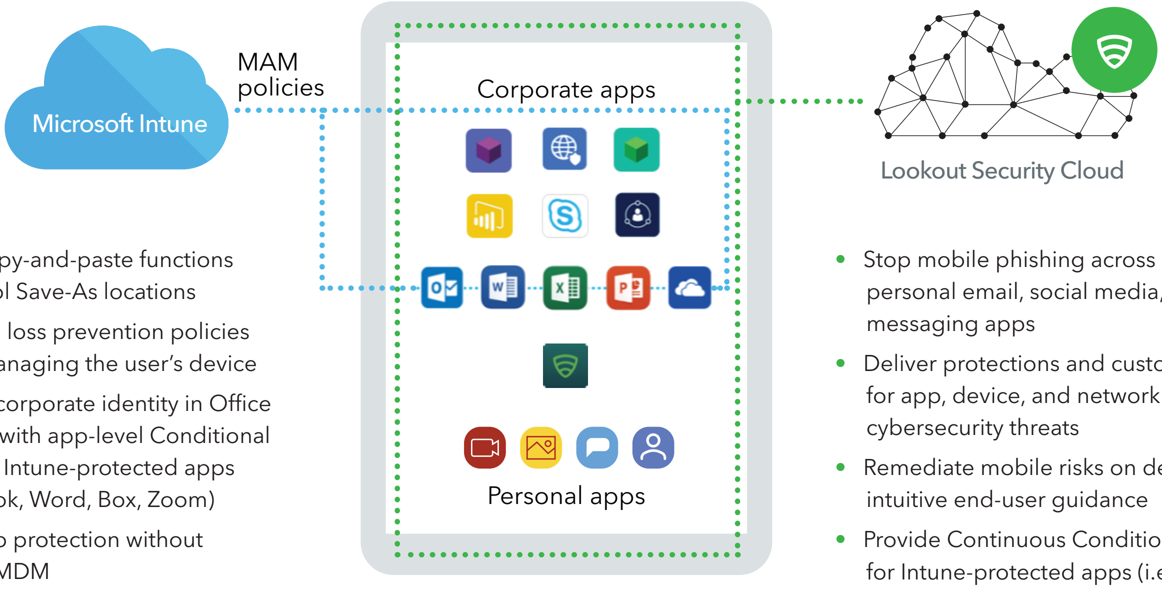
With over 200 million Office 365 business users, Microsoft is heavily influencing employee productivity across all platforms including mobile. Office 365 enables users to launch familiar productivity apps, such as Outlook, Teams, and Excel from their mobile device for fast reliable access to corporate data. Organizations, however, must take further steps to secure their BYOD workforce and the mobile applications accessing corporate data. **With Lookout Continuous Conditional Access for Microsoft Intune-protected apps, organizations can provide security for BYOD users without managing devices.**

Lookout secures Intune-protected apps from mobile threats without MDM

Lookout is a mobile threat defense (MTD) solution that protects your enterprise data from cybersecurity attacks targeting mobile devices. Through an integration with Microsoft Intune-protected apps such as Office 365, Lookout Continuous Conditional Access takes the following steps to safeguard your organization's sensitive data:

1. Continuously monitors device health
2. Assigns a risk level of 'low', 'medium', or 'high' to the device
3. Passes the risk level to Intune in real-time as the user attempts access
4. Denies access to the application if device risk level is unacceptable
5. Provides remediation guidance to the end-user to remove the threat
6. Grants access to the application once the threat has been remediated

Together, Microsoft and Lookout provide comprehensive mobile security for Office 365 BYOD users.



- Restrict copy-and-paste functions and control Save-As locations
- Apply data loss prevention policies without managing the user's device
- Authorize corporate identity in Office 365 apps, with app-level Conditional Access for Intune-protected apps (i.e. Outlook, Word, Box, Zoom)
- Enable app protection without requiring MDM

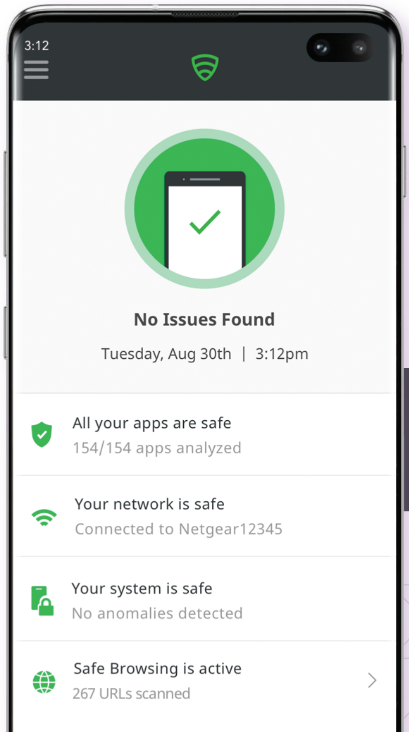
- Stop mobile phishing across work and personal email, social media, and text messaging apps
- Deliver protections and custom policies for app, device, and network cybersecurity threats
- Remediate mobile risks on devices with intuitive end-user guidance
- Provide Continuous Conditional Access for Intune-protected apps (i.e. Outlook, Word, Excel, PowerPoint, OneDrive, Adobe, Box, Zoom)

Lookout Is the best approach for securing Microsoft Office 365

Microsoft and Lookout have partnered to enable organizations to securely embrace smartphones in the workplace.

Lookout was the first to...

- **integrate mobile threat defense** with Microsoft Intune.
- **deliver mobile threat intelligence** to Windows Defender ATP.
- **provide mobile threat telemetry** to Microsoft Security Graph.
- **offer Continuous Conditional Access** for Office 365 for BYOD users.


3:12

No Issues Found

Tuesday, Aug 30th | 3:12pm

All your apps are safe
154/154 apps analyzed

Your network is safe
Connected to Netgear12345

Your system is safe
No anomalies detected

Safe Browsing is active
267 URLs scanned

About Lookout

Lookout is a cybersecurity company for the post-perimeter, cloud-first, mobile-first world. Powered by the largest dataset of mobile code in existence, the Lookout Security Cloud provides visibility into the entire spectrum of mobile risk. Lookout is trusted by hundreds of millions of individual users, enterprises and government agencies and partners such as AT&T, Verizon, Vodafone, Microsoft, Apple and others. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more, visit **www.lookout.com** and follow Lookout on its blog, Facebook, LinkedIn, and Twitter.

Security capability	Microsoft Intune MAM	Lookout	Microsoft MAM + Lookout
Restrict copy-and-paste functions and control Save-As locations	●		●
Apply data loss prevention policies without managing the user's device	●		●
Authorize corporate identity in Office 365 apps, with app-level Conditional Access	●		●
Enable app protection without requiring MDM	●		●
Stop mobile phishing across work and personal email, social media, and text messaging apps		●	●
Deliver protections and custom policies for app, device, and network cybersecurity threats		●	●
Remediate mobile risks on devices with intuitive end-user guidance		●	●
Provide Continuous Conditional Access for corporate apps based on device health		●	●

To learn more, visit **www.lookout.com** and follow Lookout on its blog, Facebook, LinkedIn, Twitter.

blog.lookout.com lookoutinc lookout lookout

Lookout®

Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ and DAY OF SHECURITY™ are trademarks of Lookout, Inc.

All other brand and product names are trademarks or registered trademarks of their respective holders.