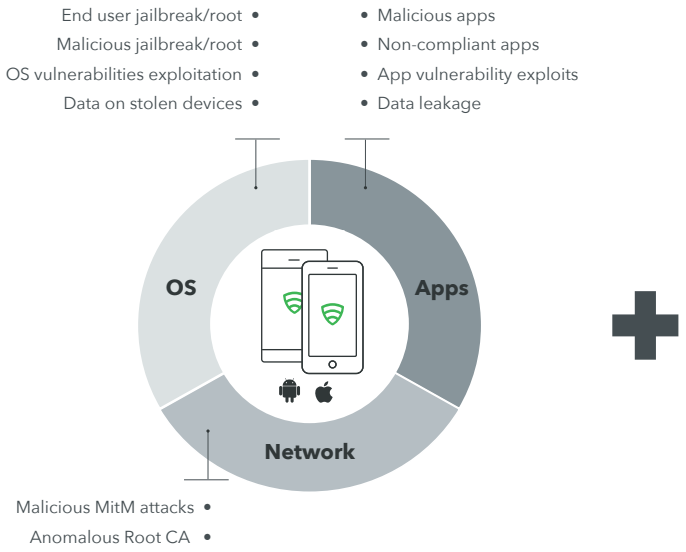
Lookout + Microsoft

Partnering to enable secure mobility in the enterprise

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 and Microsoft Enterprise Mobility + Security (EMS), organizations are able to embrace a mobilefirst, cloudfirst approach to enable their employees while protecting sensitive data accessed by their mobile devices.



Microsoft

Microsoft Enterprise Mobility + Security

Identity and Access Management
Azure Active Directory Premium

Managed Mobile Productivity
Microsoft Intune

Information Protection
Azure Information Protection

Identity Driven Security
Microsoft Advanced Threat Analytics
Microsoft Cloud App Security

Key Benefits of Lookout + Microsoft EMS

Comprehensive mobile security to enable productivity

Microsoft EMS provides an identity-driven security solution that offers a holistic approach to the security challenges in this mobile-first, cloud-first era. Lookout complements EMS' identity-based security with its rich mobile threat intelligence by continuously monitoring the device for threats, passing that information directly to EMS to inform conditional access policies. Lookout protects against threats against three attack vectors:

1. App-based threats: Trojans, spyware, rootkits, as well as non-compliant apps that leak sensitive data
2. Network-based threats: Man-in-the-middle and SSL attacks that can steal encrypted data-in-transit
3. OS-based threats: Advanced jailbreaking of iOS devices and rooting of Android devices

Risk-based conditional access

Conditional access policies within Intune allow you to protect corporate email, files and other resources from unauthorized access, based on customizable factors that ensure security and compliance, such as location, device and user state, application sensitivity and risk. With the Microsoft EMS and Lookout integration, you have the ability to include Lookout threat intelligence into the conditional access policies that you've defined within Intune to manage and secure access to your apps, such as Office mobile apps, as well as take action to selectively wipe data from devices.

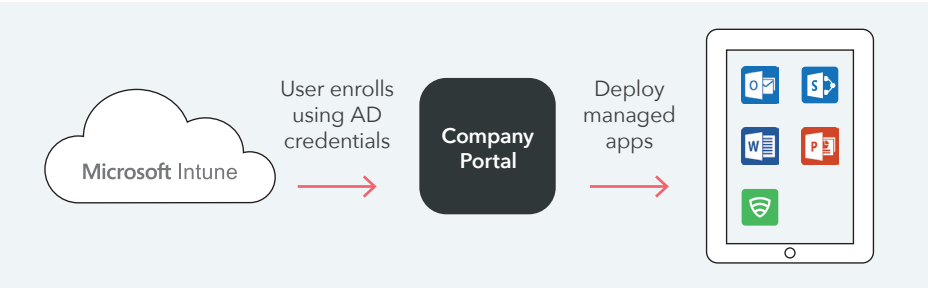
Ease of use

The integration between Lookout and EMS allows for seamless deployment and management of the Lookout client app via Microsoft Intune, integrated policy management for users and groups, and integrated identity with Azure Active Directory for single signon for both end users and administrators.

How the Integration Works

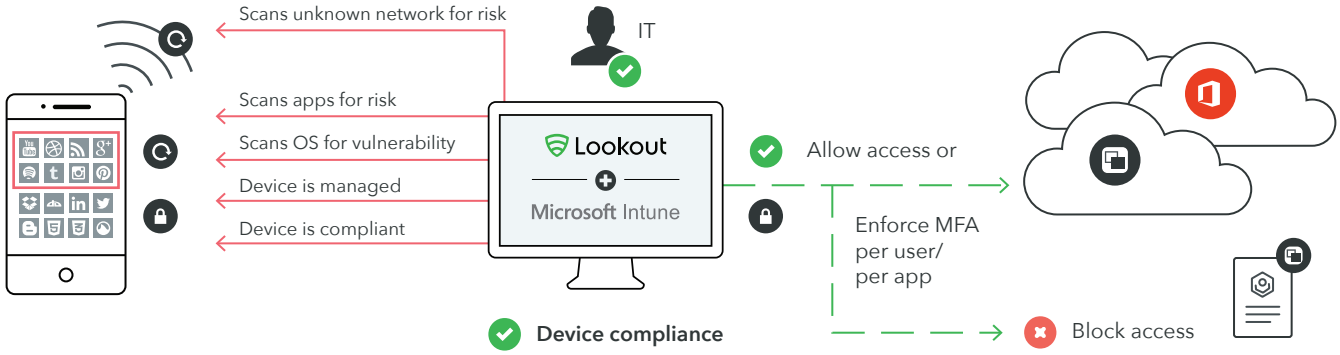
Device provisioning

Using Microsoft Intune, the Lookout endpoint app can be easily distributed across your mobile devices, allowing for rapid and scalable device provisioning.



Risk-based conditional access

Lookout provides visibility into malicious threats or the presence of apps that leak sensitive data, informing Intune's assessment of the device's compliance state. For example, if an employee in the Finance department unknowingly downloads a malicious mobile application, Lookout will identify this threat and trigger Intune's conditional access policies to restrict access to your corporate data until that threat is remediated.



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