

Lookout + VMware

Empowering security insights with Lookout and VMware Workspace ONE Intelligence

Embrace a secure mobile first, cloud first approach to productivity

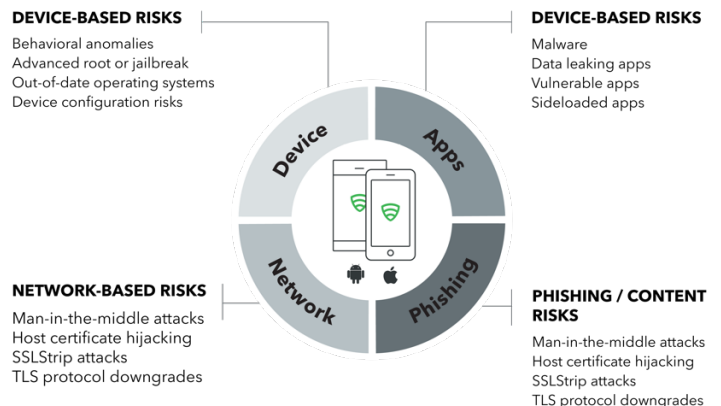
Organizations are increasingly adopting mobile management strategies to empower mobile productivity, but in today’s sophisticated threat landscape it’s more challenging than ever to ensure corporate data and assets stay protected. With Lookout’s mobile protection of iOS and Android devices combined with VMware’s productivity and device management 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.

Lookout enhances Workspace ONE Intelligence

Lookout Mobile Endpoint Security solution is integrated with VMware Workspace ONE Intelligence. This integration enables VMware Workspace ONE customers to detect, view, investigate, and respond to advanced cyber-attacks and data breaches on iOS and Android mobile devices from within the VMware Workspace ONE platform. The integrated console exposes Lookout device threat and health information to the main dashboard and throughout subsections for a fully integrated single pane of glass experience.

“This partnership will allow today’s organizations to get visibility into the entire spectrum of mobile risk provided by Lookout, apply policies to measurably reduce that risk, and do it all from a cohesive and integrated platform.”

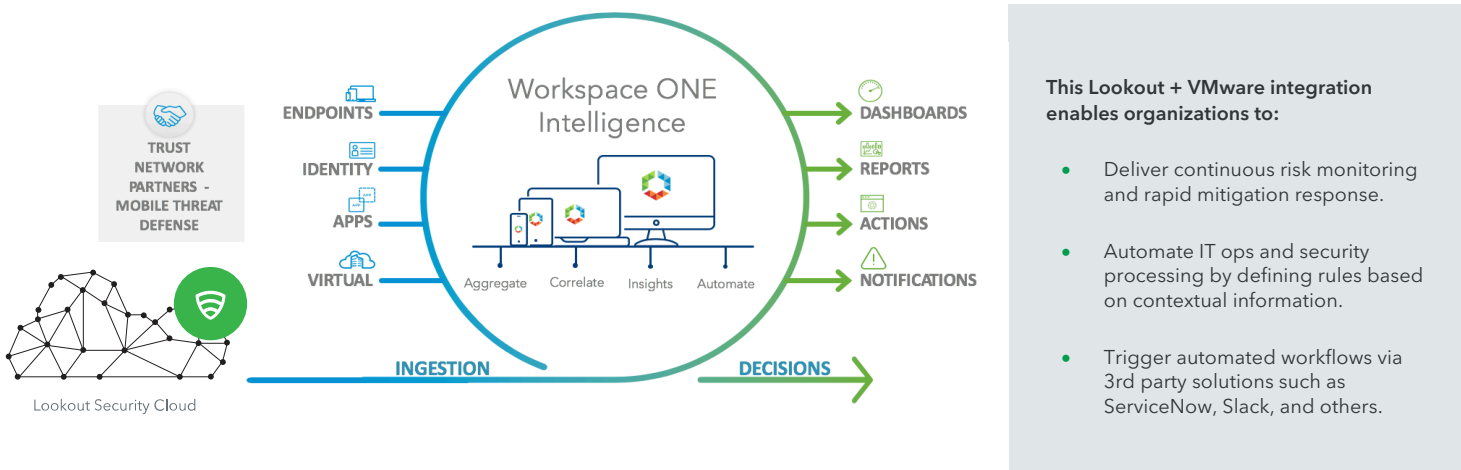
Mark Jaffan Vice President of Business and Corporate Development at Lookout



Lookout and VMware leverage predictive analytics and a massive data

Lookout has the world’s largest mobile security dataset due to its global scale and mobile focus and has collected security data from over 170M devices worldwide and over 70M apps, with up to 90K new apps added daily. This global sensor network enables the Lookout platform to be predictive by letting machine intelligence identify complex patterns that indicate risk. These patterns would otherwise escape human analysis.

Lookout captures threat type, threat description, assigns a threat severity of low, medium, and high and provides recommended 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 VMware Workspace ONE Intelligence console.



Why Lookout

Lookout Mobile Endpoint Security ensures continuous security and compliance on every device, leveraging a large data set fed by over 170 million devices, and the analysis of over 70 million mobile apps. With the Lookout Security Cloud, it’s easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts on malicious apps, network connections, and system anomalies at the OS level in real time; accompanied by simple on-device remediation capabilities.

To learn more about how Lookout and VMware Workspace ONE Intelligence enable a secure mobile-first, cloud-first approach to employee productivity, download a free trial at [Lookout + VMware](#) or contact [Lookout](#) or VMware partner or sales representative.