Why deploying MTD and EMM together makes sense

Add protection for mobile threats with only a few more clicks

Cybersecurity Challenges for Mobile Management

In business today, employees are frequently working from mobile devices. This challenges organizations to provide mobile employees secure and flexible access to cloud-based enterprise data. In an attempt to secure their mobile fleet, organizations have traditionally deployed enterprise mobility management (EMM) solutions as the answer for securing mobile endpoints. However, EMM solutions, alone, provide no visibility and protection against mobile cybersecurity threats. Instead, they enable organizations to perform device management tasks such wiping a lost/stolen device and distributing enterprise apps. For comprehensive mobile security, organizations should implement mobile threat defense (MTD) with EMM.

Real World Use Case for Secure Mobility within Organizations

An industry leader in providing energy management solutions was encouraged by a top EMM provider to integrate Lookout Mobile Endpoint Security at the same time as their EMM deployment. After the EMM vendor recommended Lookout for protection against mobile threats and that it would be a minor incremental effort during the EMM implementation, the organization moved forward with Lookout. Facing IT resource constraints, the organization was pleased with the need for minimal user training and the seamless cybersecurity deployment to iOS and Android devices. Not only did the Lookout implementation meet requirements set out by the information security team, it also enabled an advanced mobile security strategy with comprehensive visibility into mobile phishing, application, device, and network-based threats.

Key points…

1. EMMs do not have visibility into mobile threats
2. MTD provides protection against mobile phishing, app, device, and network threats
3. EMM and MTD integration provide an advance mobile security posture

Lookout Critical Capability

Lookout Mobile Endpoint Security provides comprehensive and continuous assessment of risk across iOS and Android devices to secure against app, device, and network-based threats. By continuously monitoring the health of mobile devices, Lookout is able to assign a risk-levels of ‘high, medium, and low’, and pass this information to an EMM, which can action custom policies to deny access to corporate resources based on device risk tolerance. This not only ensures that an authorized user is accessing appropriate data, but also that the risk levels of their device are within acceptable limits.

Why Lookout?

Lookout Mobile Endpoint Security ensures continuous security and compliance on every device, leveraging a large data set fed by over 180 million devices, and the analysis of over 100 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. For organizations across all industries, Lookout delivers the visibility and security required to safeguard sensitive information against the spectrum of mobile risk.