Lookout + EMM

Securely enable mobility for your organization

Organizations are increasingly adopting formal mobility programs to empower mobile productivity. As data is becoming more mobile, coupling an enterprise mobility management solution with a cloud-based, mobile security solution provides the defensive layers needed to protect your enterprise data:

EMM

- Device management and data wipe
- Separation of personal and enterprise data
- Protection against phishing attacks
- Access to enterprise applications
- Authentication and single sign-on
- Mobile access to content

Lookout Mobile Endpoint Security

- Protection against app-based risks
- Protection against phishing attacks
- Detection of network-based risks
- Detection of device-based risks
- Custom remediation policy across threats types
- Easy to deploy and maintain with your EMM

Seamless integration to provide secure mobility

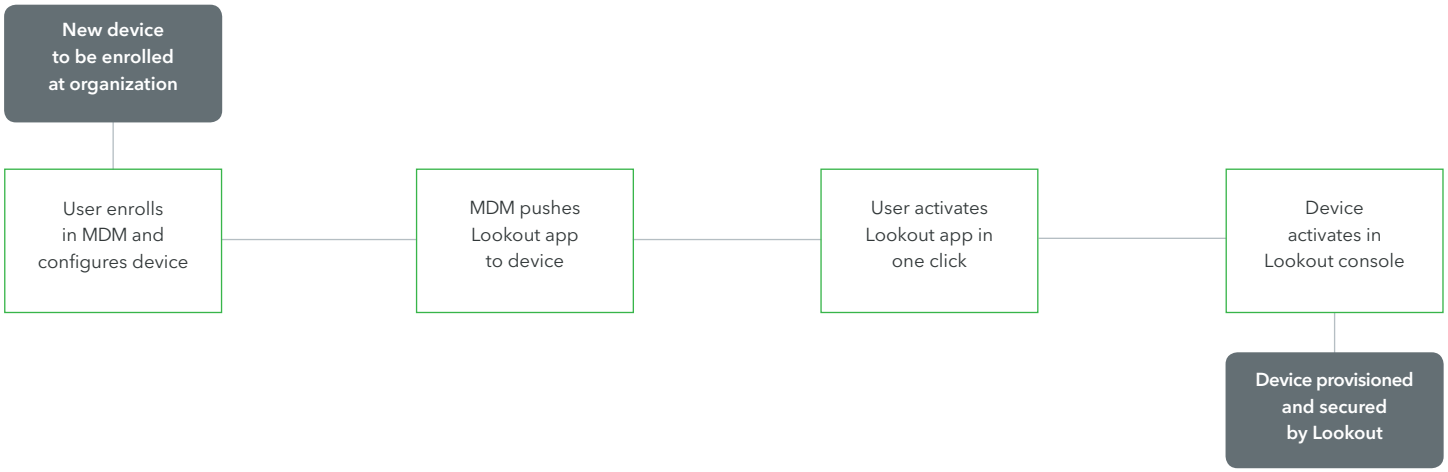
Risks	MDM only	Lookout + MDM
Lost device	✔ Locates and remotely wipes lost device	✔ Locates and remotely wipes lost device
App distribution	✔ Secure distribution of enterprise apps	✔ Distribute Lookout app via MDM
Policy violations	⚠ Manual blacklisting of apps determined to violate company policy	✔ Automated detection and remediation of apps that violate security policies
Data leakage	⚠ Can protect against employee data leakage using containers	✔ Full visibility into data leakage, including risky app behaviors such as apps that send calendar data externally
Jailbreaking and rooting	⚠ Not always effective due to the nature of the attack targeting the kernel of the OS	✔ Advanced jailbreak/root detection by analyzing hundreds of OS signals
Out-of-date operating systems	⚠ Can manually specify a minimum OS version	✔ Full visibility into devices with out-of-date operating systems and Android Security Patch levels
Risky device configurations	⚠ Can enforce a passcode on device	✔ Visibility into several risky configs, such as USB debugging enabled
App vulnerabilities	X None	✔ Detect apps using insecure data storage/transfer methods
Malicious apps	X None	✔ Comprehensive detection of malicious mobile apps that go unnoticed by app reputation technologies
Phishing attacks	X None	✔ Prevents connections via malicious URLs in email, SMS, messaging apps and those embedded into apps
Container exploits	X None	✔ Detects modifications to access privileges that indicate an exploit
Man-in-the-Middle Attacks	X None	✔ Protection against malicious network attacks on encrypted enterprise data in transit

X No Protection ⚠ Limited Protection ✔ Protected

How the Integration Works

Device Provisioning

Using your MDM solution, the Lookout endpoint app can be easily distributed across your mobile devices, allowing for rapid and scalable device provisioning. The device provisioning process follows these basic flows:



Risk Remediation

Through our MDM integration, at risk devices can be quarantined in real-time using custom remediation policies. When Lookout detects a risk, the device will be categorized as either "high risk", "moderate risk", or "low risk" depending on your security policy settings. The risk remediation process follows these basic flows: