Lookout + EMM

Sichere Mobilität für Ihr Unternehmen

Unternehmen setzen zunehmend auf offizielle Mobilitätskonzepte, um die Produktivität ihrer mobilen Mitarbeiter zu fördern. Die Datenmobilität nimmt immer weiter zu. Eine Enterprise Mobility-Management-Lösung in Kombination mit einer cloudbasierten Lösung für die Sicherheit mobiler Plattformen schützt Ihre Unternehmensdaten auf allen Ebenen.

EMM

- Geräteverwaltung und Datenlöschung
- Trennung von persönlichen und Unternehmensdaten
- Zugriff auf Anwendungen des Unternehmens
- Authentifizierung und einmaliges Anmelden
- Mobiler Zugriff auf Inhalte

Lookout Mobile Endpoint Security

- Schutz vor App-basierten Risiken
- Erkennung von netzwerkbasierten Risiken
- Erkennung von gerätebasierten Risiken
- Benutzerdefinierte Beseitigungsrichtlinien nach Art der Bedrohung
- Einfache Bereitstellung und Wartung mit Ihrem EMM

Nahtlose Integration für die Mobilgerätesicherheit

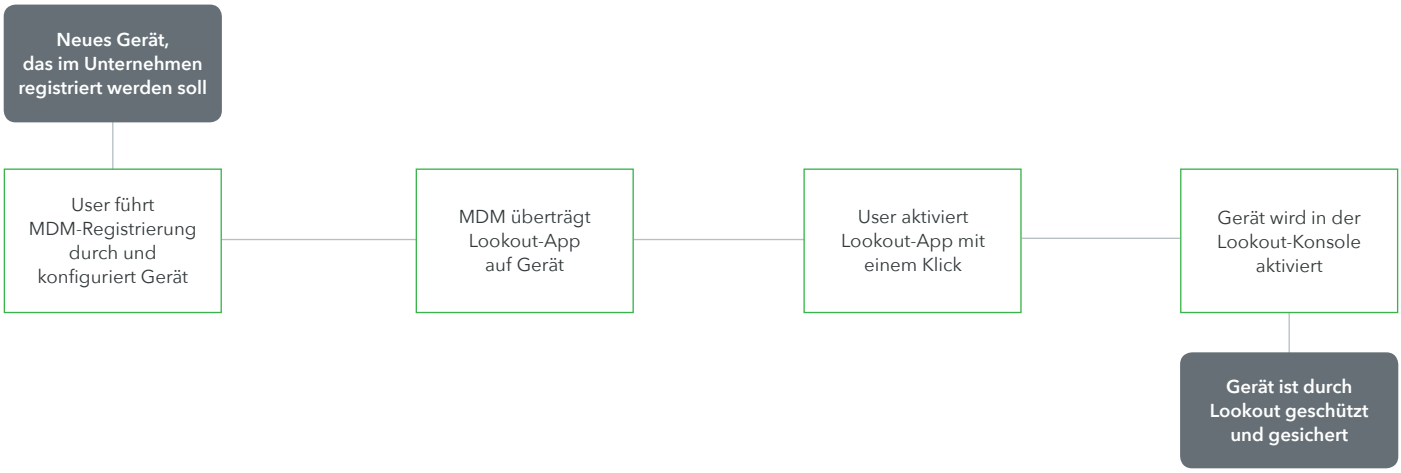
Risiken	Nur MDM	Lookout + MDM
Geräteverlust	✔ Lokalisiert verlorenes Gerät und löscht die Gerätedaten per Remote-Verbindung	✔ Lokalisiert verlorenes Gerät und löscht die Gerätedaten per Remote-Verbindung
Bereitstellung von Apps	✔ Stellt Unternehmens-Apps auf sichere Weise bereit	✔ Stellt Lookout-App via MDM bereit
Richtlinienverstöße	⚠ Apps, welche die Sicherheitsrichtlinien des Unternehmens verletzen, müssen manuell auf die „Blacklist" gesetzt werden	✔ Apps, die Sicherheitsrichtlinien verletzen, werden automatisch erkannt und beseitigt
Datenverlust	⚠ Kann mithilfe von Containern vor Datenverlust schützen	✔ Vollständige Transparenz über Datenverlust, einschließlich Auffälligkeiten im Verhalten der App, wenn beispielsweise Kalenderdaten an externe Empfänger versendet werden
Jailbreaking und Rooting	⚠ Bei gezielten Angriffen auf den OS-Kernel nicht immer wirksam	✔ Erweiterte Jailbreaking-/Rooting-Erkennung durch die Analyse von hunderten Betriebssystemsignalen
Veraltete Betriebssysteme	⚠ Manuelle Definition einer Mindest-Betriebssystemversion	✔ Vollständige Transparenz über Geräte mit veralteten Betriebssystemen und Android-Sicherheitspatches
Riskante Gerätekonfigurationen	⚠ Festlegung eines obligatorischen Geräte-Passcodes	✔ Transparenz über verschiedene risikoreiche Konfigurationen, etwa aktiviertes USB-Debugging
App-Schwachstellen	X Kein Schutz	✔ Erkennt Apps, die unsichere Datenspeicher-/Datenübertragungsmethoden nutzen
Bösartige Apps	X Kein Schutz	✔ Umfassende Erkennung bösartiger Apps, die von App-Reputation-Technologien nicht erfasst werden
Container-Exploits	X Kein Schutz	✔ Erkennt Modifikationen an Zugriffsrechten, die einen Exploit anzeigen
Man-in-the-Middle-Angriffe	X Kein Schutz	✔ Schützt vor bösartigen Netzwerkangriffen auf verschlüsselte Unternehmensdaten während der Übertragung

X Kein Schutz ⚠ Begrenzter Schutz ✔ Geschützt

So funktioniert die Integration

Device Provisioning

Mithilfe Ihrer MDM-Lösung kann die Lookout-Endpoint-App mühelos auf Ihre Mobilgeräte ausgespielt werden. Dadurch wird ein schnelles und skalierbares Deployment ermöglicht. Das folgende Diagramm zeigt den grundlegenden Bereitstellungsprozess für Geräte:



Beseitigung von Risiken

Durch unsere MDM-Integration können gefährdete Geräte durch benutzerdefinierte Beseitigungsrichtlinien in Echtzeit unter Quarantäne gestellt werden. Sobald Lookout ein Risiko erkennt, wird abhängig von Ihren Sicherheitseinstellungen das vom Gerät ausgehende Risiko als „hoch", „mittel" oder „gering" eingestuft. Das folgende Diagramm zeigt, wie Bedrohungen in der Regel beseitigt werden: