Lookout + BlackBerry UEM

Sichere Mobilität für Ihr Unternehmen

Unternehmen setzen heute zunehmend umfassende Mobilitätslösungen ein, um mobile Produktivität zu fördern. Angesichts zunehmender Datenmobilität schützt eine Unified-Endpoint-Management-Lösung in Kombination mit einer cloudbasierten Lösung für die Sicherheit mobiler Plattformen Ihre Unternehmensdaten auf allen Ebenen:

BlackBerry UEM

- 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 appbasierten Angriffen und Risiken
- Schutz vor Phishing-Angriffen
- Erkennung von netzwerkbasierten Angriffen
- Erkennung von gerätebasierten Angriffen und Risiken
- Benutzerdefinierte Beseitigungsrichtlinien nach Art der Bedrohung
- Einfache Bereitstellung und Support über BlackBerry UEM

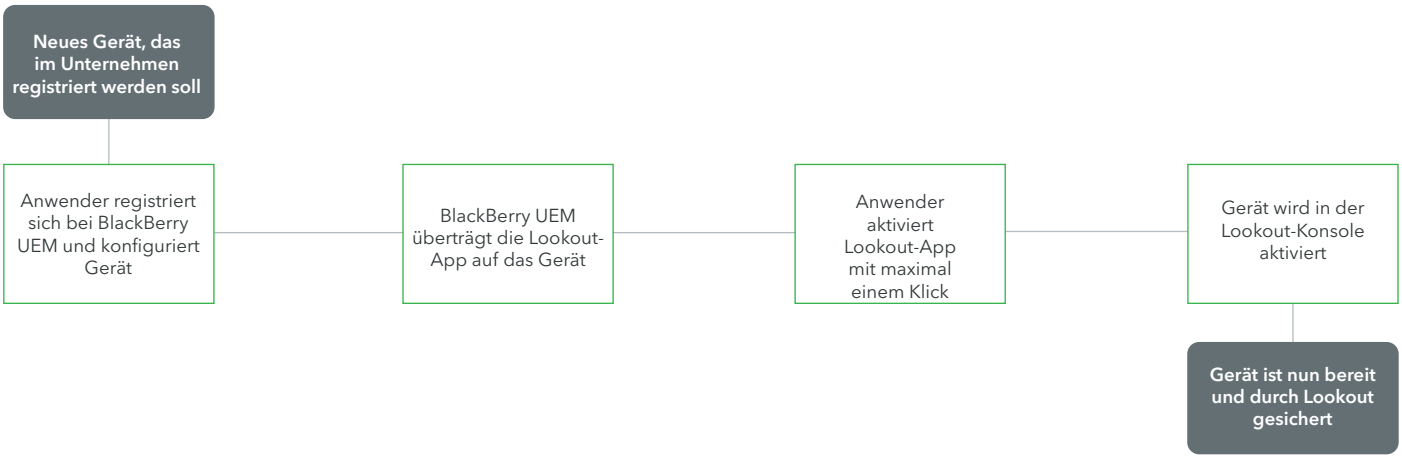
Nahtlose Integration für die Mobilgerätesicherheit

Risiken	Nur BlackBerry UEM	Lookout + BlackBerry UEM
Geräteverlust	Lokalisiert verlorenes Gerät und löscht die Gerätedaten per Remote-Verbindung	Lokalisiert verlorenes Gerät und löscht die Gerätedaten per Remote-Verbindung
Bereitstellung von Apps	Sichere Bereitstellung von Unternehmens-Apps	Stellt Lookout-App via BlackBerry UEM bereit
Richtlinienverstöße	Apps, die die Sicherheitsrichtlinien des Unternehmens verletzen, müssen manuell auf die „Black List“ gesetzt werden	Automatische Erkennung und Beseitigung von Apps, die Sicherheitsrichtlinien verletzen
Datenverlust	Kann mithilfe von Containern vor Datenverlust schützen	Vollständige Transparenz über Datenverlust, einschließlich Auffälligkeiten im Verhalten der Apps (wenn beispielsweise Kalenderdaten an externe Empfänger versendet werden)
Jailbreaking und Rooting	Bei gezielten Angriffen auf den Betriebssystemkern 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 risikobehaftete Konfigurationen, beispielsweise aktiviertes USB-Debugging
App-Schwachstellen		Erkennung von Apps, die unsichere Datenspeicher-/Datenübertragungsmethoden nutzen
Manipulierte Apps		Umfassende Erkennung bösartiger Apps, die von App-Reputation-Technologien nicht erfasst werden
Phishing-Attacken		Verhindert die Ausführung von URLs aus E-Mails, SMS, Messengern und Apps zu präparierten Websites
Container-Exploits		Erkennt Modifikationen an Zugriffsrechten, die einem Exploit zu Grunde liegen
Man-in-the-Middle-Angriffe		Schutz vor bösartigen Netzwerkangriffen auf verschlüsselte Unternehmensdaten während der Übertragung

So funktioniert die Integration

Gerätebereitstellung

Mithilfe Ihrer BlackBerry UEM-Lösung kann die Lookout-App auf Ihre Mobilgeräte übertragen werden. Dadurch wird eine schnelle und skalierbare Bereitstellung ermöglicht. Das folgende Diagramm zeigt den grundlegenden Bereitstellungsprozess für Geräte:



Beseitigung von Risiken

Durch unsere BlackBerry UEM-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: