# Lookout + VMware Workspace ONE UEM

## Mit Continuous Conditional Access für VMware Workspace ONE-Produktivitäts-Apps

Unternehmensdaten werden immer häufiger über Mobilgeräte abgerufen und gespeichert. Die Integration einer Unified-Endpoint-Management-Lösung in eine cloudbasierte Lösung zur Erkennung von Mobilgeräte-Bedrohungen kann daher Geräte und Apps schützen, die sich außerhalb des geschützten Netzwerks befinden:

### VMware Workspace ONE UEM

- Containerisierte Anwendungen und Unternehmensdaten
- Trennung von persönlichen und geschäftlichen Daten
- Zugriff auf E-Mails des Unternehmens
- Nahtloser Zugriff auf Unternehmens-Apps dank Single-Sign-On
- Einheitliches Richtlinienmanagement
- Sichere Verteilung mobiler Inhalte
- Erweiterte Datenabsicherungslösung für E-Mails, Inhalte und Apps

### Lookout Mobile Endpoint Security

- Fortlaufende Risikobewertung für containerisierte Apps
- Schutz vor Phishing-Angriffen
- Erkennung von erweiterten Jailbreak/Root-Bedrohungen
- Erkennung von Man-in-the-Middle-Angriffen
- Compliance dank Kontrolle über ungewollten Datenabfluss aus Apps
- Volle Transparenz für „sideloaded" Apps
- Benutzerdefinierte Maßnahmen je nach Art der Bedrohung

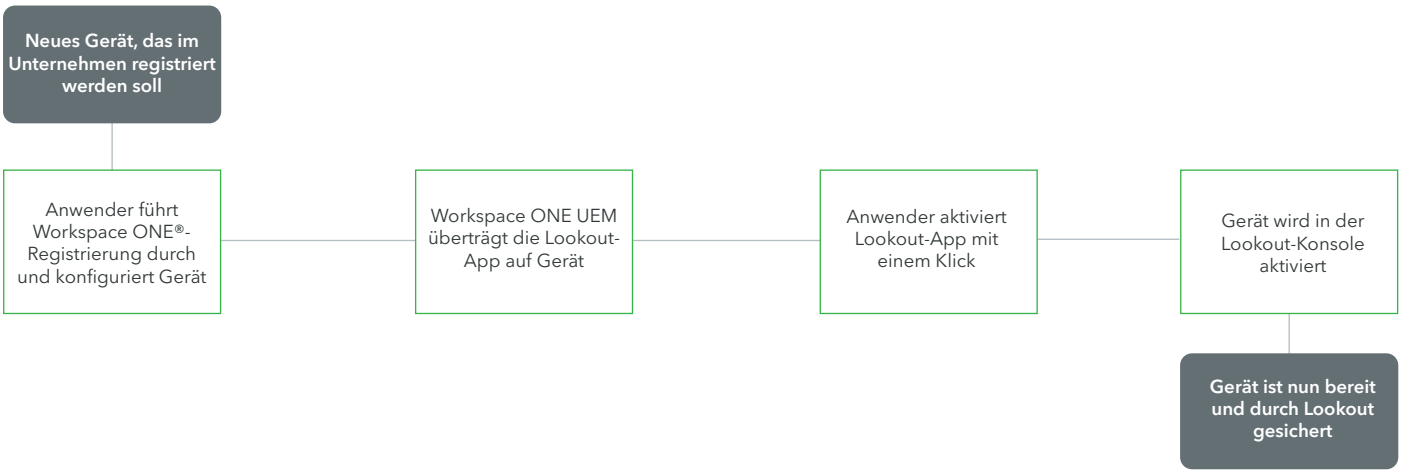
### Nahtlose Integration für die Mobilgerätesicherheit

| Risiken | VMware Workspace ONE UEM | Workspace ONE UEM + Lookout |
|---|---|---|
| App-Verteilung | Sichere Bereitstellung von Unternehmens-Apps für Mitarbeiter | Einfaches Bereitstellen der Lookout App auf Mitarbeitergeräten |
| Verletzung der Sicherheitsrichtlinien | Wird ein nicht konformes Gerät erkannt, wird der Fehler durch automatisierte Maßnahmen behoben | Compliance-Entscheidungen berücksichtigen jetzt auch Bedrohungen oder riskante Anwendungen, die Lookout findet |
| Appbasierte Risiken | Containerisiert Anwendungen und Unternehmensdaten wie E-Mails oder andere Inhalte | Bietet Visibilität in Apps, die Daten ausschleusen, sowie in Malware, Trojaner und Spyware |
| Ungeschützte Netzwerke | Das Tunneling des Datenverkehrs beschränkt den Netzwerkzugriff durch Geräte auf ausschließlich verwaltete Unternehmensanwendungen auf dem jeweiligen Gerät | Schützt vor Man-in-the-Middle-Angriffen auf verschlüsselte Unternehmensdaten während der Übertragung |
| Continuous Conditional Access | Der Zugang zu Unternehmensressourcen lässt sich bei Verstößen gegen Compliance-Richtlinien automatisch widerrufen | Widerruf des Zugriffs auf VMware® Workspace ONE-Produktivitäts-Apps, wenn Lookout Bedrohungen auf App-, Netzwerk- oder Betriebssystembasis erkennt |
| Jailbreaking und Rooting | Basiserkennung von manipulierten Geräten (Jailbreaking und Rooting) | Analyse von hunderten Betriebssystemsignalen zur Identifizierung von Versuchen, die grundlegende Jailbreaking-/Rooting-Erkennung zu umgehen |
| Phishing-Attacken | --- | Verhindert Verbindungen über URLs in E-Mails, SMS, Messaging Apps und bösartigen Websites |
| Geräteverlust/-diebstahl | Erkennung verloren gegangener/gestohlener Geräte oder Fernlöschung von Unternehmensdaten und -anwendungen | Erkennung verloren gegangener/gestohlener Geräte oder Fernlöschung von Unternehmensdaten und -anwendungen |
| Unsichere Authentifizierung | Mobile Einmalanmeldung bei Web-, Cloud- und mobilen Anwendungen | Mobile Einmalanmeldung mit nur einem Fingertipp bei Web-, Cloud- und mobilen Anwendungen |

# So funktioniert die Integration

## Gerätebereitstellung

Mithilfe von Workspace ONE® Unified Endpoint Management, unterstützt durch AirWatch®, kann die Lookout App mühelos auf Ihre Mobilgeräte aufgespielt werden. Dies ermöglicht eine schnelle und skalierbare Bereitstellung. Das folgende Diagramm zeigt den grundlegenden Bereitstellungsprozess:




## Continuous Conditional Access für VMware Workspace ONE-Produktivitäts-Apps

Durch unsere Workspace ONE UEM-Integration können gefährdete Geräte durch benutzerdefinierte Maßnahmen in Echtzeit unter Quarantäne gestellt werden. Dies ermöglicht auch Zugangssperren für containerisierte VMware Boxer-Apps auf nicht verwalteten Geräten, je nach Risikoeinstufung durch Lookout.  Sobald Lookout eine Bedrohung erkennt, wird abhängig von Ihren Sicherheitseinstellungen das Geräterisiko als „hoch", „mittel" oder „gering" eingestuft. Das folgende Diagramm zeigt, wie Bedrohungen generell beseitigt werden: