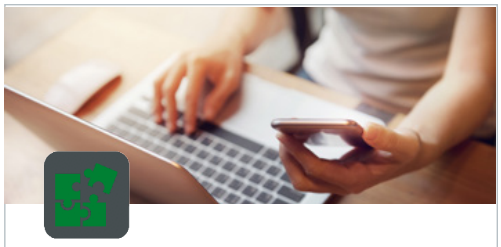
Gemeinsam noch sinnvoller: MTD und EMM

In nur wenigen Klicks zu mehr Schutz vor mobilen Bedrohungen

Cybersicherheit gewährleisten beim mobilen Arbeiten

Viele Unternehmen lassen ihre Mitarbeiter immer mehr Aufgaben per Mobilgerät erledigen. Dies erfordert jedoch einen sicheren, flexiblen Zugriff über solche Mobilgeräte auf Unternehmensdaten in der Cloud. Um diese Endgerätesicherheit zu gewährleisten, setzen Unternehmen seit Längerem auf EMM-Lösungen (Enterprise Mobility Management). Allerdings sorgen EMM-Lösungen allein nicht für Transparenz über mobile Cybersicherheitsbedrohungen und auch nicht für den passenden Schutz. Ihre Kernfunktion ist stattdessen die Verwaltung der Geräte, beispielsweise das Löschen von Daten auf verloren gegangenen oder gestohlenen Geräten und das Bereitstellen von Unternehmensanwendungen. Umfassende mobile Sicherheit bietet nur eine MTD-Lösung (Mobile Threat Defense) mit EMM.



Das Wichtigste in Kürze

1. EMM-Lösungen bieten keinen Einblick in mobile Bedrohungen.
2. MTD schützt vor Phishing auf Mobilgeräten sowie app-, geräte- und netzwerkbasierten Risiken.
3. Die Integration von EMM und MTD stärkt die Sicherheitslage beim mobilen Arbeiten.

Anwendungsfall aus der Praxis: mobile Mitarbeiter – aber sicher

Ein branchenführender Anbieter für Lösungen des Energiemanagements erhielt von einem namhaften EMM-Anbieter den Tipp, Lookout Mobile Endpoint Security in sein EMM-Deployment aufzunehmen. Mit der Empfehlung des EMM-Anbieters, Lookout zum Schutz vor mobilen Bedrohungen einzusetzen, und dem Hinweis, die EMM-Bereitstellung würde dadurch nicht komplexer, entschied sich das Unternehmen für Lookout. Angesichts einer überlasteten IT-Abteilung war es zudem froh über den minimalen Schulungsaufwand und die nahtlose Bereitstellung der Cybersicherheitslösung auf seinen iOS- und Android-Geräten. Die Integration von Lookout erfüllte nicht nur die Anforderungen des Informationssicherheitsteams, sondern ermöglichte auch gleich die Ausweitung der Strategie für mobile Sicherheit. Sie umfasst nun weitreichende Transparenz über Phishing auf Mobilgeräten sowie app-, geräte- und netzwerkbasierte Bedrohungen.

Unternehmenswichtige Lookout-Funktion

Lookout Mobile Endpoint Security bietet die umfassende und kontinuierliche Beurteilung von Risiken für iOS- und Android-Geräte, zum Schutz vor app-, geräte- und netzwerkbasierten Bedrohungen. Kontinuierlich überwacht Lookout den Zustand von Mobilgeräten und weist ihnen ein Risikoniveau zu – hoch, mittel oder gering. Diese Information wird an das EMM-System weitergegeben, das dann spezielle Richtlinien umsetzt, um bei einer Gefahrenlage den Zugriff auf Unternehmensressourcen zu unterbinden. Dadurch ist nicht nur gewährleistet, dass nur autorisierte Benutzer Zugriff auf für sie bestimmte Daten haben, sondern dass sich das Risikoniveau ihrer Geräte in einem akzeptablen Rahmen bewegt.

Warum Lookout?

Lookout Mobile Endpoint Security stellt die kontinuierliche Sicherheit und Compliance auf jedem Gerät sicher und nutzt dazu einen großen Datensatz, der aus mehr als 180 Millionen Geräten und der Analyse von über 100 Millionen mobilen Anwendungen gespeist wird. Die Lookout Security Cloud vereinfacht die Bereitstellung von Lookout und die Anwendung von Sicherheitsrichtlinien für verwaltete wie nicht verwaltete Geräte im gesamten Unternehmen. Gewarnt wird vor bösartigen Apps und Netzwerkverbindungen sowie Systemanomalien auf Betriebssystemebene. Die Warnungen erfolgen in Echtzeit und enthalten einfache Beseitigungsmaßnahmen zur direkten Problembehebung auf dem Gerät. Unternehmen sämtlicher Branchen bietet Lookout die erforderliche Transparenz und Sicherheit, um sensible Informationen vor dem Spektrum mobiler Risiken zu schützen.