Fallstudie

Führendes Pharmaunternehmen schützt wichtige Forschungsarbeiten mit Lookout

Die Herausforderung

Eines der weltweit führenden Pharmaunternehmen wollte verhindern, dass sensible Daten durch Datenlecks öffentlich gemacht werden. Außerdem sollten Compliance-Anforderungen für mobile Geräte, die für den Zugriff auf Forschungsdaten des Unternehmens verwendet werden, umgesetzt werden. Der CISO erkannte eine Lücke im Schutz vor mobilen Phishing-Angriffen und App-Risiken, die bei mehr als 20.000 mobilen Nutzern zu Datenverlusten führen könnten.

Während der CISO über das Budget für mobile Sicherheitslösungen verfügte, war es Aufgabe des IT-Teams, die Einführung einer neuen Lösung zu verwalten. Um Auswirkungen auf die laufende Impfstoffforschung möglichst einzuschränken, mussten Störungen während des Einführungsprozesses in der gesamten mobilen Flotte reduziert werden.

Die Nutzung privater Geräte für die Arbeit ist in allen Branchen, auch in der Pharmaindustrie, weit verbreitet. Dies stellt ein erhebliches Risiko dar, wenn private Geräte auf Forschungsdaten zugreifen. Der CISO erkannte, dass das Unternehmen bei der Absicherung privater Geräte verstärkt auf einen Zero-Trust-Ansatz setzen musste. Nur private Geräte, welche die Einhaltung der wichtigsten Compliance- und Sicherheitsanforderungen erfüllen, können auf Daten zugreifen. Die Herausforderung bestand darin, ein Zero-Trust-Modell auf diese Endgeräte anzuwenden und Sicherheitsanforderungen kontinuierlich durchzusetzen.

Kundenprofil

Industrie: Pharmaindustrie

Mobile Geräte: 20.000

Mobile Strategie: Bring-your-own-device (BYOD)

Enterprise Mobility Management Lösung:
Microsoft Endpoint Manager

Sicherheitslösung:
Lookout Cloud Security Platform

Integrierte Lösung

Integrierter Microsoft Endpoint Manager

Lookout Mobile Endpoint Security

Lookout Phishing- und Content Protection

Ergebnisse

- Schutz vor mobilen Phishing-Angriffen auf dienstlichen und privaten Apps
- Sichtbarkeit von Risiken auf mobilen Geräten in Echtzeit
- Aktivierung von Zugriffsrichtlinien, um den Zugang zu Daten einzuschränken, bis mobile Bedrohungen beseitigt sind
- Gesicherte mobile Endgeräte mit zentraler Verwaltung
- Umsetzung der BYOD-Richtlinie mit Lookout zur Sicherung aller nicht verwalteten Geräte

Die ausgewählte Lösung zum Schutz mobiler Endgeräte muss nach der Implementierung vor diesen Risiken schützen:

- Mobile Phishing-Angriffe über alle Apps hinweg, nicht nur E-Maill
- iOS- und Android-Malware auf Geräten von Mitarbeitern
- Angriffe über kompromittierte oder ungesicherte Wi-Fi-Netzwerke
- Apps, die Datenlecks verursachen und möglicherweise zu Compliance Verstößen führen

Die Lösung

Nach der Evaluierung einer Reihe von mobilen Sicherheitslösungen kam der CISO zu dem Schluss, dass die Integration von Microsoft Endpoint Manager und Lookout Mobile Endpoint Security die bestmögliche Wahl darstellt. Die Integration ermöglicht eine kontinuierliche Anpassung der Zugriffskontrolle für ein mobiles BYOD-Gerät basierend auf Echtzeit-Änderungen der Risikostufe des Geräts. Wenn das Risikoniveau zu hoch wurde, konnte der Zugriff automatisch geändert werden, um sensible Unternehmensdaten zu schützen.

Lookout ermöglicht einen risikobasierten Zugriff, indem es dem Enterprise Mobility Management Transparenz über mobile Risiken bietet, was wiederum eine Zero-Trust-Strategie für Benutzer auf mobilen Geräten ermöglicht. Durch die kontinuierliche Überwachung von Risiken wie mobilen Bedrohungen, App-Datenlecks und kompromittierten Wi-Fi-Netzwerken beschränkt Lookout den Zugriff auf Daten von kompromittierten mobilen Geräten. Wenn beispielsweise ein Mitarbeiter der Forschungsabteilung unwissentlich eine bösartige mobile Anwendung herunterlädt, identifiziert Lookout die Bedrohung und löst Conditional Access Richtlinien aus, um den Zugriff auf Unternehmensdaten zu beschränken, bis die Bedrohung vom Endgerät entfernt ist.

Sowohl der CISO als auch der CIO dieses führenden Pharmaunternehmens waren sich einig, dass die Lösung von Lookout und Microsoft eine Kombination aus mobiler Sicherheit und mobilem Zero Trust bietet, um geistiges Eigentum zu schützen. Darüber hinaus erkannten sie, dass Enterprise Mobility Management (EMM) allein nicht ausreicht.

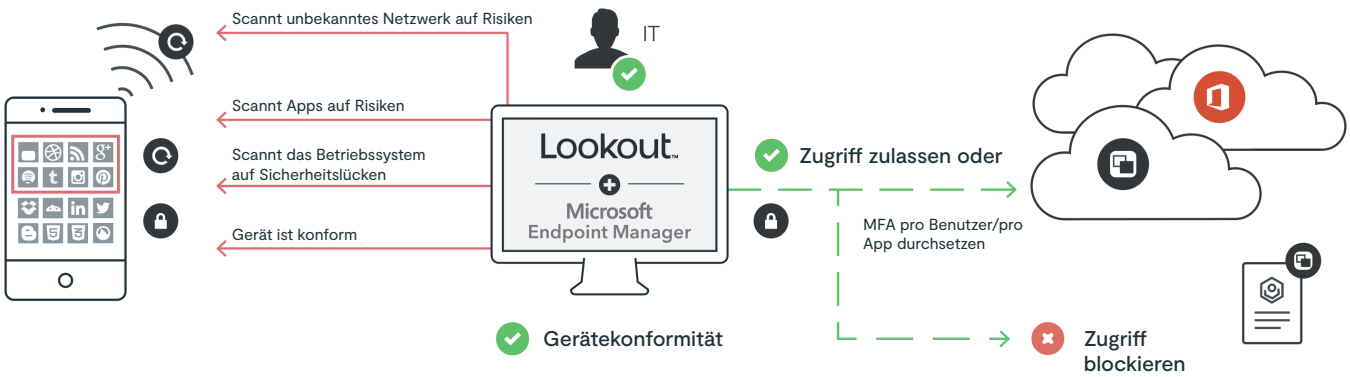
Lookout-Richtlinien bieten Echtzeit-Erkennung von mobilen Bedrohungen und eine Risikobewertung, während EMM die Geräte nur alle paar Stunden überprüft. Mit Lookout war der CIO in der Lage, eine integrierte Richtlinienverwaltung für Benutzer durchzusetzen. Der CISO hat mit einem Klick Zugriff auf Risiko- und Compliance-Berichte für alle Benutzer und Apps, die auf deren Geräten installiert sind.

Die Ergebnisse

Durch die nahtlose Implementierung von Lookout ist dieses Pharmaunternehmen in der Lage, eine globale Sicherheitsrichtlinie für seine Mitarbeiter zu erstellen. Wird ein mobiles Gerät aufgrund eines Risikos als nicht konform befunden, wird der Zugriff des Benutzers auf Unternehmensressourcen gesperrt. Er erhält erst dann wieder Zugang, wenn er das Problem durch Befolgung der Anweisungen von Lookout behebt.

Seit Lookout Mobile Endpoint Security mit Phishing- und Content Protection nahtlos in die Microsoft EMM-Lösung integriert ist, kann das Unternehmen alles über eine zentrale Ansicht verwalten.

Der CISO und der CIO sind in der Lage, die Anforderungen an den Schutz aller Endgeräte vor Cybersecurity-Angriffen zu erfüllen und eine messbare Reduzierung der mobilen Risiken für die gesamte globale Belegschaft zu erreichen.



Über Lookout

Lookout ist der Anbieter für Cybersicherheit vom Endgerät bis in die Cloud, der Zero Trust Sicherheit bietet, um Risiken zu reduzieren und Unternehmensdaten zu schützen. Unsere zentrale, Cloud-native Plattform schützt digitale Informationen über Geräte, Anwendungen, Netzwerke und Clouds hinweg und passt sich modernen Arbeitsplatz-Anforderungen an. Unternehmen und Behörden jeder Größe vertrauen auf Lookout, um sensible Daten zu schützen, sowie frei und sicher arbeiten und sich vernetzen zu können. Um mehr über die Lookout Cloud Security Platform zu erfahren, besuchen Sie www.de.lookout.com und folgen Sie Lookout auf unserem Blog, LinkedIn und Twitter.

Weitere Informationen finden Sie unter
de.lookout.com

Fordern Sie eine Demo an unter
de.lookout.com/demo-anfragen