Globales Pharmaunternehmen schützt geistiges Eigentum durch bedingte Zugangsberechtigungen mit Lookout und Microsoft

Die Herausforderung

Der CISO eines führenden Pharmaunternehmens wollte die Datenverlusts- und Compliance-Risiken reduzieren, die durch Mobilgeräte entstehen, wenn sie auf Daten aus der pharmazeutischen Forschung zugreifen. Um die weltweite Organisation vor Angriffen auf mobile Geräte und vor unternehmensweiten Datenlecks zu schützen, entschied er sich dafür, ein Projekt zur mobilen Sicherheit zu initiieren.

Obwohl dem CISO ein Budget für eine Lösung zur mobilen Endgerätesicherheit zur Verfügung stand, war es die Aufgabe des IT-Teams, das Rollout einer neuen Lösung zu managen. Es war also entscheidend, dass sich jede neue Technologie in kurzer Zeit und ohne einen komplexen Registrierungs- und Aktivierungsprozess für die zwanzigtausend weltweit verteilten Mitarbeiter bereitstellen lassen würde.

Nach dem Deployment erwartete der CISO, dass diese Mobile-Endpoint-Security-Lösung Schutz für die folgenden Szenarien bietet:

- iOS- und Android-Malware in BYOD-Umgebungen
- Netzwerkangriffe über ein infiziertes oder ungeschütztes WLAN
- Apps, die ein Datenleck haben und das Potenzial besitzen, dass das Unternehmen seine Branchen-Compliance verliert

Kundenprofil

Branche: Gesundheitswesen

Mobilgeräte: 20.000

Mobilitätsrichtlinie: BYOD

EMM-Lösung: Microsoft Enterprise Mobility + Security

Mobile-Security-Lösung: Lookout Mobile Endpoint Security

Die Lösung

- Integration von Microsoft Enterprise Mobility + Security und Lookout Mobile Endpoint Security

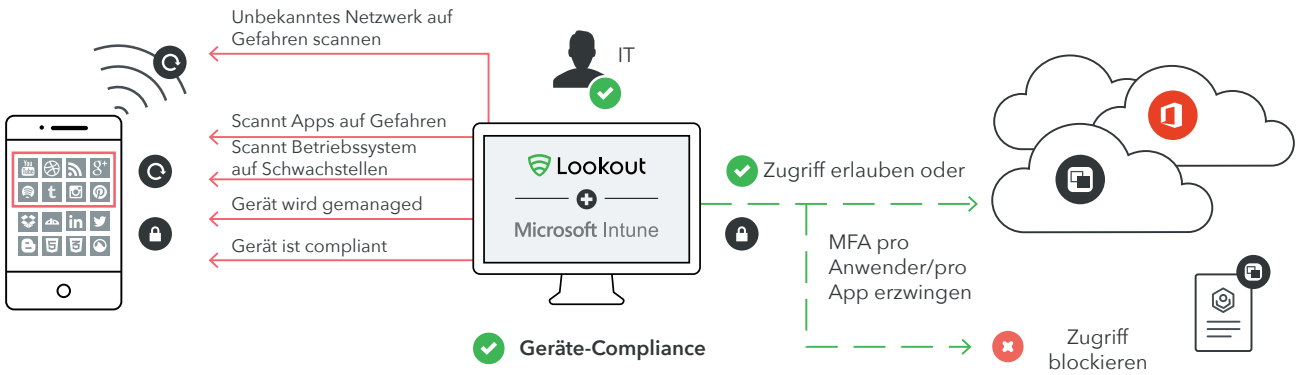
Das Ergebnis

- Echtzeit-Transparenz über Risiken von Mobilgeräten
- Einführung von Richtlinien für bedingte Zugangsberechtigungen, mit denen der Zugriff auf Unternehmensdaten so lange eingeschränkt werden kann, bis die mobilen Bedrohungen beseitigt worden sind
- Mobilgerätesicherheit durch einen ganzheitlichen Management-Ansatz für diese End-to-End-Lösung

Die Lösung

Nachdem er eine engere Auswahl von Mobile-Security-Lösungen unter die Lupe genommen hatte, stand für den CISO fest, dass die Integration zwischen Microsoft Intune, der Lösung zur Verwaltung mobiler Geräte in der Microsoft Enterprise Mobility + Security Suite, und Lookout Mobile Endpoint Security die bestmögliche Lösung darstellte. Der Grund dafür war, dass die Integration eine einzigartige, aber ganz wesentliche Funktion bietet: bedingte Zugangsberechtigungen.

Lookout Mobile Endpoint Security macht mobile Risiken in Echtzeit sichtbar, z. B. hoch entwickelte mobile Bedrohungen, Datenverluste durch Apps sowie infizierte WLAN-Netzwerke. Über Lookout wird die Sicherheitsanalyse von Intune zum Compliance-Status des Geräts informiert. Wenn ein Mitarbeiter in der Abteilung F&E z. B. unbeabsichtigt eine bösartige mobile Anwendung herunterlädt, identifiziert Lookout diese Bedrohung und aktiviert die Richtlinien für bedingte Zugangsberechtigungen in Intune, um den Zugriff auf Unternehmensdaten so lange einzuschränken, bis die Bedrohung beseitigt wurde.



Der CISO und der CIO dieses führenden Pharmaunternehmens waren sich einig, dass die kombinierte Lösung aus Microsoft und Lookout einen deutlichen Mehrwert liefert, den eine Enterprise-Mobility-Management-Lösung allein nicht bieten kann. Denn Mobile Endpoint Security unterstützt die Richtlinien für bedingte Zugangsberechtigungen, indem in Echtzeit mobile Bedrohungen erkannt werden.

Insbesondere der CIO profitiert von einem integrierten Richtlinienmanagement für Benutzer und Gruppen sowie von dem integrierten Identitätsmanagement mit Azure Active Directory, das den Single Sign-on (SSO) für Endanwender und Administratoren erlaubt.

Das Ergebnis

Dieser Pharmakonzern ist jetzt in der Lage, eine globale Sicherheitsrichtlinie für sämtliche Mitarbeiter einzurichten: Sollte Lookout ein mobiles Risiko identifizieren und ein Mobilgerät eines Mitarbeiters daher als nicht compliant einstufen, wird der Zugriff auf Unternehmensressourcen durch Microsoft Intune geblockt und der Benutzer wird aufgefordert, das Problem anhand einer Schritt-für-Schritt-Anleitung durch Lookout zu beheben. Erst dann kann er wieder Zugriff erhalten.

Mit den kombinierten Möglichkeiten der Lösungen von Lookout und Microsoft wurden die Erwartungen der Sicherheits- und Technologieteams übertroffen. Da Lookout Mobile Endpoint Security direkt in die Intune-Konsole integriert ist, kann diese End-to-End-Lösung über eine einzige Oberfläche verwaltet werden.

Der CISO und der CIO dieses Weltmarktführers können die integrierte Lösung aus Lookout Mobile Endpoint Security und Microsoft Enterprise Mobility + Security jetzt dem CEO und dem Aufsichtsrat präsentieren und dabei den Beleg erbringen, dass die Lösung mobile Risiken, mit denen das Unternehmen weltweit konfrontiert ist, messbar reduziert.