# Android ist bereit für den Einsatz im Unternehmen

## Zusammenfassung für Entscheidungsträger

Android ermöglicht eine mobile, vernetzte Belegschaft mit mehreren Sicherheitsebenen, umfassender Verwaltung und diversen Geräten für jede Aufgabe. In den vergangenen Jahren hat die ständig wachsende Beliebtheit von Android bei den Benutzern dazu geführt, dass Android-Geräte in Unternehmen gelangten. Die IT musste daher einen skalierbaren Plan zur sicheren massenweisen Einführung dieser Geräte erarbeiten. In diesem Whitepaper sondiert MobileIron den Status der Android-Sicherheit und Android-Verwaltung und zeigt, wie Google Schritt für Schritt Bedenken und Hindernisse für die Akzeptanz von Android im Unternehmen beseitigt. Die zunehmende Konzentration von Google auf Sicherheit und Flexibilität sowie das wachsende Interesse an Android für Unternehmen – einer neuen und effektiveren Android-Verwaltungslösung – unterstreichen, dass Android jetzt für Unternehmen verfügbar und einsetzbar ist. Durch die leistungsstarke Kombination von Android mit einer Enterprise Mobility Management Plattform (EMM) können Unternehmen all die neuen Funktionen für Android-Geräte in großem Maßstab sicher einführen.

**In diesem Whitepaper werden folgende Themen diskutiert:**

- Wachsende Akzeptanz von Android in Unternehmen
- Verbesserungen der Sicherheitsfunktionen
- Geringere Fragmentierung der Verwaltung
- Strikte Trennung von betrieblichen und privaten Daten und besserer Datenschutz für den Endbenutzer
- Drastisch verbesserte Registrierungsprozesse zur Entlastung des Supports

Informieren Sie sich über diese und weitere Themen und erfahren Sie, warum MobileIron von Android für Unternehmen überzeugt ist.

MobileIron

MKT DE-A4 v1.1

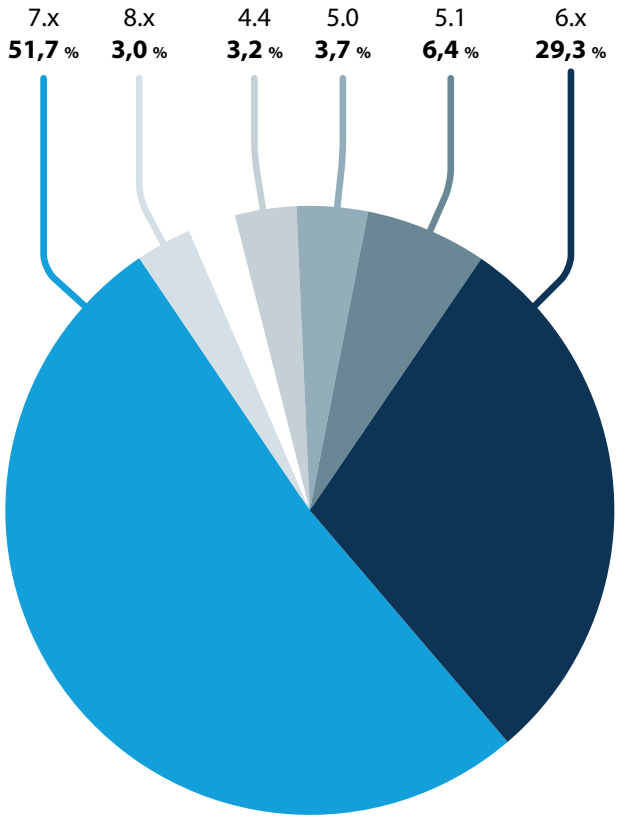
# Einführung: Das Potenzial von Android und EMM

Die extreme Beliebtheit von Android bei Verbrauchern führte unvermeidlich dazu, dass viele dieser Geräte auch zur Arbeit mitgenommen wurden. Angesichts dieses Trends fällte Google die strategische Entscheidung, sich auf Android als effektives Gerät für Unternehmen zu konzentrieren, der IT die Verwaltung zu erleichtern und eine hohe Datensicherheit in einer Arbeitsumgebung sicherzustellen. Die Einführung von Android 5.0 Lollipop vor einigen Jahren stellte einen Wendepunkt dar. Seitdem unterstrich jede Freigabe einer größeren Android-Version diesen neuen Trend.

Über 77 % der an Unternehmen ausgelieferten Geräte liefen 2016 unter Android (Quelle: ICD März 2017); Unternehmen in aller Welt nutzen somit Android eindeutig für geschäftliche Zwecke. Mit der zunehmenden Akzeptanz von Android in Unternehmen kommen viele neue Geräte an den Arbeitsplatz. Nach Angaben von Google verwenden etwa 50 % der Android-Geräte in Unternehmen Android 6.0 oder höher. Die von MobileIron erstellten, verdichteten Kundendaten lassen den Schluss zu, dass etwa 83 % der Unternehmen Geräte mit den Android-Versionen 6.0 oder höher verwenden.[1] Mit der Einführung neuer, kostspieligerer Android-Handgeräte bei den Mitarbeitern stehen für die Android-Plattform auch modernere Sicherheits- und Verwaltungsfunktionen zur Verfügung als für die älteren und billigeren Angebote auf dem Markt.

Mit anderen Worten, die drei großen Android-Versionen, die bereits auf den Markt kamen – Marshmallow, Nougat und Oreo – zeigen deutlich, dass Android sich nach wie vor auf die Anforderungen in Unternehmen konzentriert. Trotz der Verbesserungen von Android wurden jedoch im Dezember 2017 nur 35 % der Geräte verwaltet (Google, Dezember 2017). Das heißt, nur ein deutlich kleinerer Teil der Unternehmen hat bisher verstanden, welches Potenzial eine Enterprise Mobility Management-Plattform (EMM) zur Absicherung der Android-Geräte bietet. Es sei darauf hingewiesen, dass alle diese neuen Sicherheits- und Verwaltungsfunktionen der Android-Plattform nur mit einer EMM-Lösung genutzt werden können. Mit der wachsenden Gefahr potenzieller Datenverluste, einer Schatten-IT sowie der zunehmenden Nutzung von Malware und Sicherheitslücken ist der ungesicherte Zugriff der Mitarbeiter mit ihren Android-Geräten auf sensitive Unternehmensdaten ohne den Schutz einer EMM-Plattform eine riesige Sicherheitslücke im Unternehmen. Durch die Registrierung eines Android-Geräts auf einer EMM-Plattform wird die Datensicherheit gewährleistet, zugleich bleibt diese Sicherheitsmaßnahme für den Endbenutzer unsichtbar.

*Über MobileIron verwaltete Android-Distribution, Stand Januar 2018*




1 Nach allgemeinen Statistiken der Android-Versionen verwenden 50 % der Kunden Android 6.0 oder höher

# Evolution von Android: Systematische Berücksichtigung der Kundenerwartungen erfordert höhere Sicherheit

Eine hartnäckige, aber falsche Einschätzung überschattet den Einsatz von Android in Unternehmen bis heute: Android sei unsicher. Diese Einschätzung mag in der Zeit bis Android 4.4 berechtigt gewesen sein. Seitdem hat Android jedoch die Sicherheitsfunktionen drastisch verbessert und ist jetzt eine der sichersten Betriebssystemplattformen, wenn das Betriebssystem über eine EMM-Lösung ordnungsgemäß verwaltet wird.

Tatsächlich hielt die Gartner Group 2016 und 2017 die mobilen Gerätesicherheitskontrollen von Android für besser als die von iOS, wie aus dem Gartner Report zur mobilen Betriebssystem- und Gerätesicherheit und dem Vergleich der einzelnen Plattformen hervorgeht.

## Wesentliche Meilensteine der Versionen

In Version 5.0 führte Android das Arbeitsprofil für Android für Unternehmen und die vom Unternehmen verwalteten Bereitstellungsarten ein. Das Arbeitsprofil ist für BYOD-Initiativen gedacht, bei denen der Datenschutz der Benutzer respektiert werden muss.

Vom Unternehmen verwaltete Geräte dagegen sind Bereitstellungen, für die das Unternehmen allein haftet und das komplette Gerät kontrolliert. Mit diesen Optionen verfügt die IT über alle Tools und Optionen zur Verwaltung von Android-Bereitstellungen für segmentierte Populationen. In der gleichen Version wurde auch eine standardmäßige Verschlüsselung der gesamten Festplatte eingeführt.

In Android 6.0 wurden die Fernverwaltung der Anwendungsberechtigungen ergänzt, die Zertifikatverwaltung für die passwortlose Registrierung und Integration verbessert und die COSU-Kiosk-Implementierung (für unternehmenseigene Einzweckgeräte) von Android eingeführt. Android 6.0 hat somit die möglichen Bereitstellungsoptionen (mit COSU) erweitert und die Sicherheitskonfigurationen verbessert, so dass in Android wichtige Anwendungsfälle sicher implementiert werden konnten.

In Android 7.0 wurde dann die Authentifizierung für das Arbeitsprofil eingeführt, damit Administratoren vor dem Zugriff auf Unternehmensanwendungen eine separate Work Challenge erzwingen konnten. Darüber hinaus führte Google Always-on-VPN ein und verbesserte die Verschlüsselung, so dass jetzt standardmäßig einzelne Dateien statt der kompletten Festplatte verschlüsselt werden können. Durch die Dateiverschlüsselung können die Unternehmensdateien mit einem anderen

Schlüsselsatz geschützt werden als das Gerät. Bei der Komplettverschlüsselung der Festplatte lagen nach Entsperrung des Geräts sowohl die privaten als auch die betrieblichen Daten unverschlüsselt vor. Bei dateiabhängiger Verschlüsselung bleiben die Unternehmensdaten jetzt verschlüsselt, bis mit der Work Challenge das Arbeitsprofil entsperrt wird. In Android 7.0 ist die Sicherheit der Unternehmensdaten somit besser gewährleistet.

Mit Version 8.0 führte Android die Zero-Touch-Registrierung ein, d. h. alle Android-Geräte sind durch die Registrierung über die EMM-Plattform geschützt. Darüber hinaus können Unternehmen mit Arbeitsprofilen auf voll verwalteten Geräten das Gerät verwalten und die benötigten Anwendungen in einem separaten Profil kapseln. Schließlich nutzen das Muttergeräteprofil und das Arbeitsprofil jetzt eineindeutige Verschlüsselungsschlüssel, um die Daten noch besser zu schützen.

## Monatliche Sicherheitsupdates

Seit Android 5.0 verteilt Google monatlich Sicherheitsupdates unabhängig von Android Framework. Viele Android-OEMs hielten die Implementierung dieser Forderung ursprünglich für problematisch; heute folgt jedoch eine signifikante Zahl von OEMs genau den Google-Standards und führt monatlich Patches ihrer Geräte durch. Dies verbessert die Konsistenz und Sicherheit für die Kunden weltweit.

Durch diese Sicherheitsupdates sind selbst Geräte mit älteren Android-Versionen gegen Bedrohungen geschützt, die erst heute erkannt werden. Dank des Open-Source-Konzepts von Android lassen sich Sicherheitsprobleme schnell identifizieren, die dann nicht nur von Google, sondern von beliebigen Partnern, OEMs oder der Community beseitigt werden und wesentlich zur heutigen Sicherheit von Android beitragen.

Wie schnell diese Sicherheitsupdates übernommen werden, hängt von den Mobilfunkbetreibern und OEMs ab. Die Geräte, die ins Unternehmen mitgebracht werden, sollten daher die hohen Standards für die Akzeptanz im Unternehmen erfüllen.

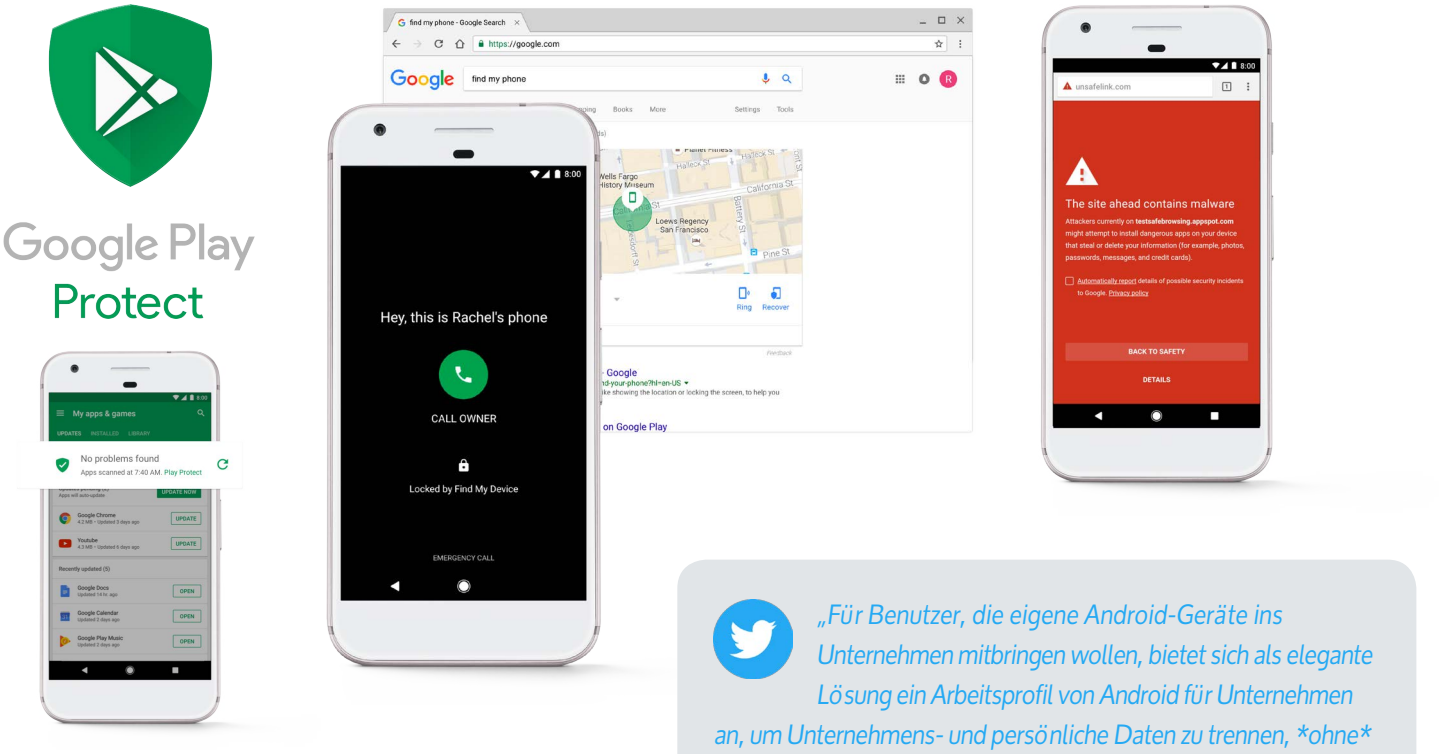
## Google Play Protect

Google Play Protect ist ein Paket von Sicherheitstools von Google zum Schutz der Benutzer und Geräte vor Bedrohungen. Es scannt pro Tag über 50 Milliarden Anwendungen im und außerhalb des Google Play Store. Google Play Protect wird auf allen für Google Mobile Services (GMS) zertifizierten Geräten vorinstalliert und scannt Bedrohungen lokal auf dem Gerät Tag und Nacht.

Play Protect enthält außerdem Erkennungsfunktionen wie Find My Device und Google Chrome Safe Browsing Protection. Damit werden sowohl die Geräte als auch der Play Store überwacht, und die Administratoren können darauf vertrauen, dass die Geräte geschützt sind.


## GMS-Zertifizierung

Ein GMS-zertifiziertes Gerät ist ein Gerät, das den OEM-Zertifizierungsprozess von Google bestanden hat, so dass die OEMs Google-Anwendungen wie Play Store, Gmail und Chrome vorinstallieren dürfen.




Play Protect verhindert allerdings nicht die Installation aus unbekannten Quellen, zweifellos heute eine der größten Bedrohungen für Android-Geräte, da damit Android-Anwendungsdateien (APKs) installiert werden können, die nicht aus dem Google Play Store stammen. Standardmäßig sind unbekannte Quellen jedoch für Geräte mit Android für Unternehmen deaktiviert und unabhängig von den gewählten Bereitstellungsarten voll über die EMM-Plattform kontrollierbar.

Wenn die Installation aus unbekannten Quellen deaktiviert ist, sinkt die Infektionsrate mit Malware, wie kürzlich von Nokia für Android gemeldet, weltweit von 68 % auf 0,05 % (Quelle: Nokia). Sollten unsauber programmierte Anwendungen ihren Weg auf die Geräte finden, wird das Schadenspotenzial durch die sichere Installation minimiert. Die Apps laufen in Sandboxen und sind damit von anderen Anwendungen getrennt. Mit dem Arbeitsprofil für Android für Unternehmen können die Apps mit spezifisch verschlüsselten Profilen gestartet werden, wobei die auf dem Gerät gesicherten Daten von außen nur zugänglich sind, wenn Berechtigungen eingeräumt wurden.

*„Für Benutzer, die eigene Android-Geräte ins Unternehmen mitbringen wollen, bietet sich als elegante Lösung ein Arbeitsprofil von Android für Unternehmen an, um Unternehmens- und persönliche Daten zu trennen, *ohne* dass das Unternehmen die vollständige Kontrolle über das Gerät übernimmt."*

@Jason Bayton, Jason Bayton

## Private und Unternehmensdaten trennen

Mit der Registrierung eines Geräteadministrators ist das Unternehmen voll verantwortlich für das verwaltete Gerät, unabhängig davon, ob es im Rahmen einer BYOD- oder COBO-Initiative (für unternehmenseigene, nur für geschäftliche Zwecke verwendbare Geräte) verwaltet wird. Wenn Unternehmensanwendungen in Containern gekapselt oder integriert sind, können EMM-Administratoren Richtlinien sowie Konfigurationen erzwingen, Details der installierten Anwendungen anzeigen und sogar Geräte komplett nach Belieben löschen, da umfassende Administratorrechte zur Verwaltung des Geräts vorhanden sind. Dies kann natürlich bei einer BYOD-Initiative Bedenken der Benutzer provozieren, die möglicherweise auf Datenschutz verzichten müssen, wenn sie eigene Geräte verwenden.

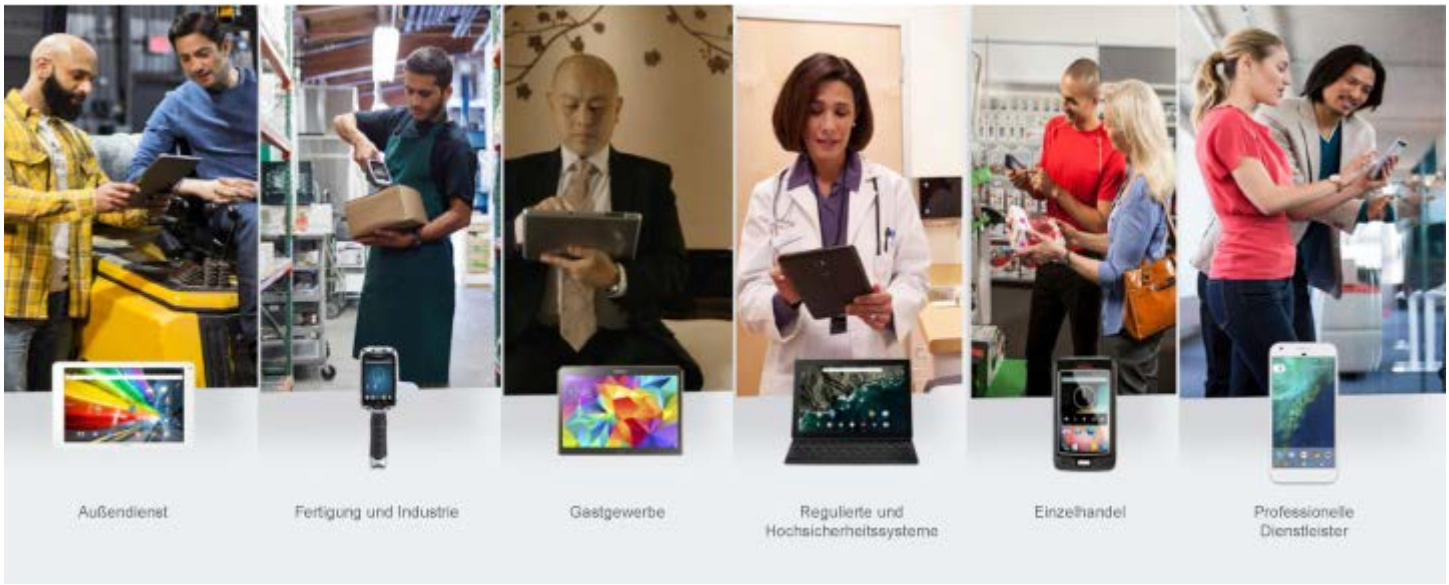
Mit dem Arbeitsprofil von Android für Unternehmen kann das Unternehmen jedoch nur eine sichere dedizierte Arbeitsumgebung auf dem Gerät einsehen und kontrollieren. Die ersten Schritte ähneln sich, da ein Unternehmensbenutzer zunächst den EMM Agent aus dem Play Store herunterlädt; sobald der Unternehmensbenutzer sich authentifiziert, erstellt die EMM-Lösung ein zweites verschlüsseltes Arbeitsprofil ähnlich einem Container auf dem Gerät und übergibt vor dem Abschluss der Registrierung den EMM Agent des Geräts an das neue Profil.

Das heißt, nach der Registrierung können Administratoren nur die Anwendungen und Einstellungen im Arbeitsprofil sehen und verwalten, nicht die Einstellungen und Anwendungen des Geräts selbst. Es gibt hierbei einige Ausnahmen, beispielsweise kann geräteweit ein Passcode erzwungen oder ein kompromittiertes Gerät erkannt werden, Datenschutz und Datenkontrolle werden jedoch in vollem Umfang durchgesetzt und respektiert.

Bei den Anwendungen selbst wird jede Anwendung, die das Unternehmen per Push überträgt, im Gerät wie jede andere Anwendung auf dem Start-Bildschirm bzw. im App-Drawer angezeigt, allerdings mit einem Work Badge markiert. Wenn eine App bereits auf dem Gerät existiert, wird eine zweite Arbeitskopie erstellt und mit einem Badge als Hinweis versehen, dass die Anwendung auf Unternehmens-Content zugreift und Informationen separat von der privaten Seite speichern kann.

Nach Ende des Arbeitstages können Benutzer das Arbeitsprofil mit einer einfachen Umschaltung in den Schnelleinstellungen deaktivieren, indem sie von oben nach unten über den Bildschirm wischen. Die Arbeitsanwendungen werden dann grau dargestellt und alle Synchronisationen von E-Mails und anderen Unternehmensdaten gestoppt; damit kann ein Gleichgewicht zwischen Privatleben und Arbeit hergestellt werden. Zusammen mit der Arbeitszeitfunktion von MobileIron lässt sich damit das lokale Arbeitsrecht in Ländern wie Frankreich und Deutschland durchsetzen.

Das Arbeitsprofil bietet darüber hinaus die erforderliche Kontrolle über Unternehmensdaten mit granularen Einstellungen für den Schutz gegen Datenverlust (DLP). Hierbei kann beispielsweise der Austausch von Kontakten und Daten zwischen Arbeitsprofil und Gerät begrenzt werden, so dass ohne ausdrückliche Zustimmung keine Daten in das Arbeitsprofil übernommen oder von dort kopiert werden können.



## Geringere Fragmentierung, bessere Konsistenz

Die meisten Unternehmen, die heute Android-Geräte verwalten, nutzen diverse Geräte verschiedener OEMs. Viele dieser OEMs haben etwas abweichende Android-Implementierungen, die sich in der Ausführung bestimmter Funktionen unterscheiden. Das Verwaltungsmodell mit dem Geräteadministrator überlässt beispielsweise dem OEM die Integration der Verwaltungs-APIs in ihre Android-Images. Einige OEMs haben diese Integration übernommen, andere nicht. Aufgrund der Autonomie der OEMs kam es in der Android-Welt im Laufe der Zeit nicht nur wie oft erwähnt zu einer starken Fragmentierung der unterschiedlichen Android-Versionen, sondern auch der Verwaltung.

Unternehmen, die viele Geräte von verschiedenen OEMs kauften, stellten fest, dass sie weder über eine übersichtliche, konsistente Verwaltungsumgebung verfügen noch sicher sein können, dass Optionen, die sich auf einem Geräte verwalten lassen, auch auf anderen Android-Geräten repliziert werden können. Dies galt selbst für OEM-Standardanwendungen. Beispielsweise konnte die E-Mail bei einem OEM-Android-Gerät eines bestimmten Typs fernkonfigurierbar sein, bei einem anderen OEM aber nicht, usw. Erfahrene EMM-Administratoren werden sich noch an Zeiten erinnern können, als sie Android-Geräte nach deren Verwaltungsfunktionen auswählten. Wenn ein Unternehmen bestimmte Geräte von verschiedenen OEMs kaufte, musste es fast immer damit rechnen, dass Funktionen eines Geräts auf anderen Geräten nicht unterstützt wurden. Zum Teil betraf dies selbst Geräte, die vom gleichen OEM gefertigt wurden! Dies führte letztendlich zu enormer Frustration, und die Unternehmen favorisierten zunehmend andere Mobilgeräte, deren Verwaltungsfunktionen zuverlässig und konsistent waren.

Google brachte 2014 Android für Unternehmen unter der Bezeichnung Android for Work auf den Markt, um den fragmentierten Markt zu konsolidieren und die OEMs weitgehend vom Support für Unternehmen zu entlasten. Dieses Konzept garantierte eine stabile, zuverlässige und reproduzierbare Verwaltung unabhängig davon, für welche Geräte ein Unternehmen sich entschieden hatte. Mit der zunehmenden Reife von Android entwickelt sich auch Android für Unternehmen weiter, so dass Google vertraulich die Außerdienststellung der spezifischen Geräte-Administrator-APIs zugunsten von Android für Unternehmen ankündigte.

Google kontrolliert die APIs für Android für Unternehmen jedoch nicht in vollem Umfang. Zebra hat bereits eigene APIs integriert, Samsung wird dies in Kürze tun. Google erlaubt es OEMs nach wie vor, eigene Zusatzprodukte auf das von Google gelieferte Basissystem aufzusetzen, so dass beispielsweise Lösungen wie Knox Mobile Enrollment auch funktionieren, wenn bestimmte APIs für den Geräteadministrator nicht mehr unterstützt werden.

Letztendlich geht es immer darum, für Administratoren und Endbenutzer gleichermaßen ein Benutzererlebnis zu schaffen, das trotz der vielen verschiedenen OEMs vertraut wirkt; diese Geräte haben möglicherweise ein anderes Look & Feel, die Prozesse zur Verwaltung der Geräte sind jedoch identisch, unabhängig davon, ob Sie ein Huawei- oder Pixel-Gerät benutzen.

## OEMs legen viel Wert auf die Anforderungen der Unternehmen

Immer mehr OEMs, die Android unterstützen, konzentrieren sich darauf, die Erwartungen der Unternehmen zu erfüllen. Zahlreiche OEMs, darunter auch die in der Liste „für Android für Unternehmen empfohlen" genannten OEMs, verpflichten sich jetzt, 3 Jahre lang Patches anzubieten. Ein Beispiel dafür ist die Freigabe von Note 8 für Unternehmen von Samsung Ende 2017. Samsung verpflichtete sich, für dieses Gerät 3 Jahre lang Software und Sicherheits-Patches sowie 2 Jahre lang die Geräte-Hardware anzubieten; dies ist deutlich länger als bei normaler Verbraucher-Hardware.

Mit diesem unternehmensfreundlichen Konzept zur Hardwareverfügbarkeit und Softwarepflege unterstreichen OEMs, dass sie sich enger dem typischen Hardware-Lebenszyklus in vielen Unternehmen anpassen können. Dies ist eine bessere Lösung für die ewige Trennung von Verbrauchern und Unternehmen.

**Für Android für Unternehmen empfohlen**

Bezieht sich auf eine Liste empfohlener Geräte, die die Mindestanforderungen für Massenregistrierung, Hardware, Sicherheits-aktualisierungen und Benutzererlebnis erfüllen und zu den spezifischen Bedürfnissen und dem Budget jedes Unternehmens passen. Die Liste finden Sie unter:

https://androidenterprisepartners.withgoogle.com/#!/results/browse-all/2

## Verzicht auf den Geräteadministrator

Im Dezember 2017 veröffentlichte Google eine signifikante Mitteilung mit weitreichenden Konsequenzen: Die Geräteadministrator-APIs, die seit Android 2.2 zur Android-Verwaltung genutzt werden, werden nur noch zwei Jahre mit lang bis zur Markteinführung von Android Q unterstützt.

Dies war seit langer Zeit erwarten worden, da Android für Unternehmen sich schnell weiterentwickelt, macht es wenig Sinn, zwei miteinander konkurrierende Verwaltungslösungen weiterzuführen, insbesondere weil der Geräteadministrator eine Reihe von Nachteilen und Einschränkungen besitzt, nicht nur im Vergleich mit Android für Unternehmen, sondern auch im Vergleich mit anderen mobilen Betriebssystemen.


MobileIron

# Verwaltung ganz einfach

## Gerätebereitstellung ohne Probleme

Mit Android für Unternehmen sind umständliche Registrierungen zur Geräteverwaltung im eigenen Netzwerk Vergangenheit. Viele EMM-Administratoren haben für die verschiedenen mobilen Betriebssysteme im Unternehmen eine Registrierungsdokumentation erstellt. Die Android-Registrierung für die Benutzer umfasst in der Regel Dutzende Seiten zur Erstkonfiguration mit dem Assistenten, zur Verwaltung der Google-Konten, zur Suche nach verteilten öffentlichen Anwendungen im Play Store usw.

Die Endbenutzer können einzelne Schritte nach Belieben überspringen, zudem ist der Prozess zeitaufwendig und verwirrend, so dass die EMM-Administratoren oft die Vorbereitung (oder Vorregistrierung) übernehmen, um den Support zu entlasten.

Mit Android für Unternehmen soll der Zeit- und Arbeitsaufwand zur Bereitstellung neuer Optionen signifikant sinken, beispielsweise NFC (5.0+), DPC-Identifikator (ab 6.0+), QR-Code (7.0+) und Zero-Touch-Bereitstellung (8.0+). Dies bedeutet sowohl für die Administratoren als auch für die Benutzer eine Entlastung, da die 30–40 Schritte einer bisherigen Registrierung entfallen.

**NFC:** Ein Bereitstellungsgerät überträgt durch Nahfeldkommunikation die NFC-Nutzdaten auf das neue Gerät. Die NFC-Nutzdaten enthalten Anweisungen, wie die Bereitstellung bei durch das Unternehmen verwalteten Geräten erfolgen soll.

**QR-Code:** Ein manuell oder über die EMM-Lösung erstellter QR-Code wird mitgeliefert. Er enthält die Nutzdaten zur Bereitstellung eines vom Unternehmen verwalteten Geräts. Das Gerät ruft das QR-Code-Setup mit 6 Tippaktionen auf dem Begründungsbildschirm auf.

**DPC-Identifikator:** Bei der normalen Konfiguration des Geräts gibt der Endbenutzer einen eindeutigen Identifikator für jede EMM-Plattform anstelle des normalen Google-Kontos ein, sobald er dazu aufgefordert wird. Auf diese Weise wird ein Server-Aufruf an Google gesendet und die Bereitstellung des vom Unternehmen verwalteten Geräts eingeleitet.

Einige Bereitstellungsoptionen funktionieren am besten, wenn die Geräte vor Ort vorbereitet werden, beispielsweise NFC Bump, andere sind für eine zuverlässige Fernbereitstellung mit QR und DPC-Identifikator vorgesehen.

**Zero-Touch:** Diese Funktion setzt ganz neue Maßstäbe. Unterstützt wird sie ab Android 7.0 mit Google Pixel-Geräten sowie Android 8.0 und höher. Zero-Touch ermöglicht – ähnlich wie das Geräteregistrierungsprogramm DEP von Apple – die automatische Bereitstellung eines Geräts ohne jegliche Handarbeit für die Registrierung! Die EMM-Administratoren erstellen und übernehmen eine Zero-Touch-Konfiguration im Zero-Touch-Portal und können die für Zero-Touch vorbereiteten Geräte dann direkt an die Endbenutzer ausliefern, damit ein neues oder auf die Werkeinstellungen zurückgesetztes Gerät mit Zero-Touch so schnell wie möglich aktiviert und die Konfiguration nicht umgangen werden kann.

## Einheitliches Verwaltungserlebnis

Android für Unternehmen nutzt einen Satz APIs im Betriebssystem selbst für alle OEMs. Android für Unternehmen verspricht eine schnellere, sichere und einfachere Verwaltung als je zuvor. Unternehmen können darauf vertrauen, dass jedes für das Unternehmen ausgewählte GMS-zertifizierte Gerät zuverlässig und reproduzierbar funktioniert.

Da sich Android für Unternehmen weiter entwickelt, werden die OEMs in zunehmendem Maße ähnlich wie Zebra und Samsung eigene Software und eigene Lösungen auf der Basisumgebung von Android für Unternehmen aufsetzen, d. h. Tools, die die Unternehmen in der Vergangenheit gern genutzt haben, werden auch in Zukunft funktionieren.

## Automatische Kontoverwaltung

Wie bei iOS- und iTunes-Konten verursachen EMM-Administratoren die zweifellos größten Kopfschmerzen Google-Konten, die im Unternehmen oder von den Benutzern selbst verwaltet werden.

Um den Aufwand zur Verwaltung vieler Google-Konten zu verringern, nutzen manche Unternehmen Konten für mehrere Geräte oder versuchen, per Push Anwendungsinstallationsdateien (APKs) direkt von der EMM-Konsole statt über Google Play zu übertragen. Beide Konzepte haben Sicherheitslücken, verletzen die Distributionsrechte und sind potenzielle Datenschutz-Alpträume!

Darüber hinaus wurden seit der Einführung des Schutzes vor dem Reset auf die Werkeinstellungen (Factory Reset Protection - FRP) in Android 5.0 immer mehr Unternehmens-Geräte gesperrt, die die Geräteadministrator-APIs zur Android-Verwaltung verwenden, und mussten zur kostspieligen Reparatur in ein OEM-Servicezentrum vor Ort gebracht werden.

Android für Unternehmen verlangt keine vom Benutzer bzw. vom Unternehmen verwalteten Google-Konten mehr, dies gilt auch für die von Android für Unternehmen ursprünglich geforderte Verifizierung der G Suite-Domain. Heute können Unternehmen entweder weiterhin G Suite und Google zur ganzheitlichen Kontoverwaltung im Unternehmen einsetzen, oder mit verwalteten Google-Play-Konten ohne G Suite problemlos, vollautomatisch und unabhängig von den Benutzern Konten ohne Eingriff des Administrators sehr schnell konfigurieren.

Darüber hinaus verlinken verwaltete Google Play-Konten nicht zu weiteren Google-Diensten und werden nicht zur Sicherung der Gerätedaten verwendet - eindeutig ein Vorteil für Unternehmen, die Wert auf Datenschutz und Vermeidung von Datenverlusten Wert legen und deshalb keine privaten Google-Konten akzeptieren.

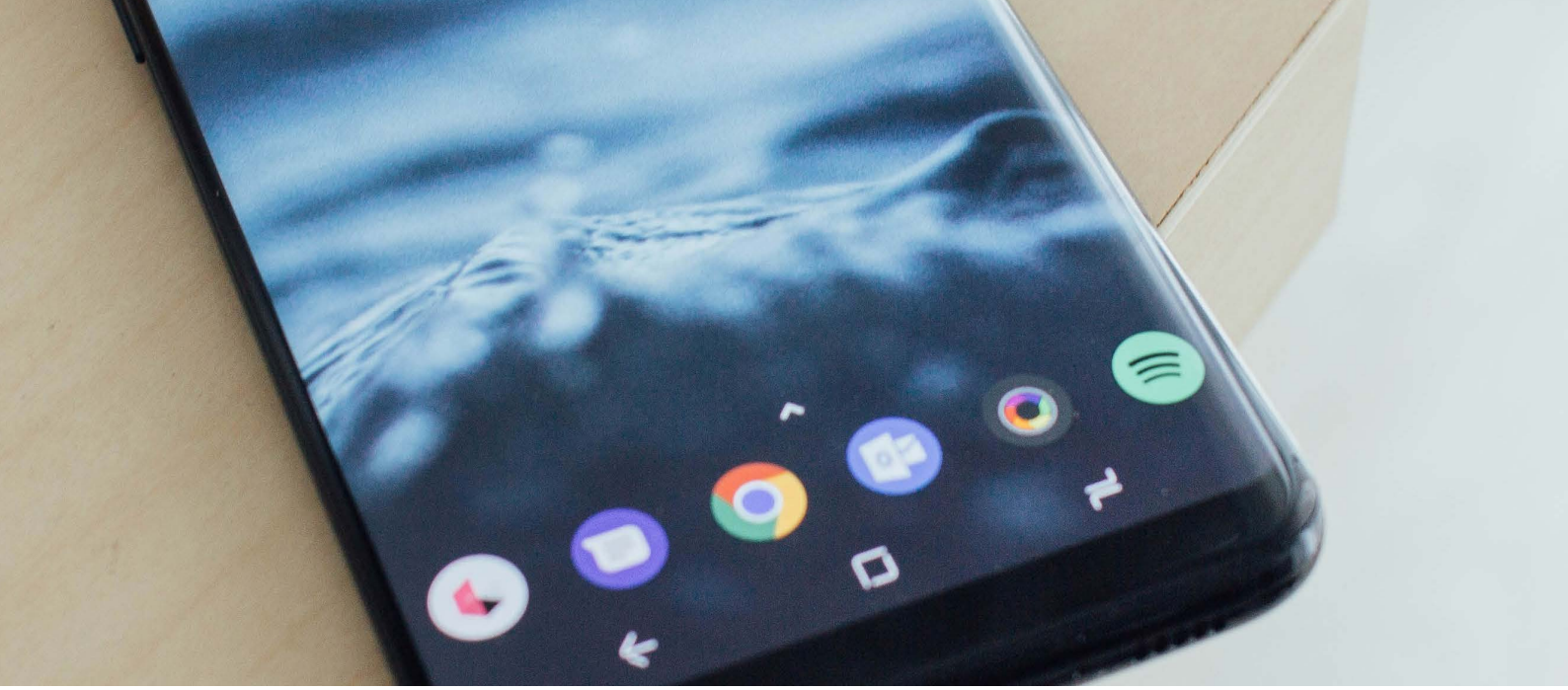
MobileIron

**APP**-KONFIGURATION COMMUNITY

## Die Rolle der AppConfig-Community

Die AppConfig-Community ist ein Verbund branchenführender EMM-Lösungsanbieter und App-Entwickler, die gemeinsam die Mobilität in Unternehmen für Kunden und Entwickler beschleunigen und vereinfachen wollen. Die Community will die Akzeptanz von mobilen Unternehmensanwendungen erhöhen und deren Bereitstellung rationalisieren. Dazu bietet sie ein Standardkonzept zur App-Konfiguration und App-Verwaltung, aufbauend auf den umfangreichen App-Sicherheits- und Konfigurationsregeln des Betriebssystems. Weitere Informationen finden Sie unter AppConfig.org/Android

Durch ihre Zusammenarbeit vereinfachen die Mitglieder der AppConfig-Community für Entwickler die Implementierung eines konsistenten Satzes von Kontrollen, so dass die IT-Administratoren im Unternehmen Apps bequem entsprechend ihren Unternehmensrichtlinien und Unternehmensanforderungen konfigurieren und verwalten können. Mit den Tools der AppConfig-Community und bewährten Verfahren können die Entwickler bei vielen Anwendungsfällen im Unternehmen auf EMM-spezifische Integrationen verzichten. Die Endbenutzer profitieren von den automatisierten Funktionen, beispielsweise dem ohne weitere Konfiguration verfügbaren Standardumfeld, mit dem die Benutzer sofort Zugriff auf ihre Apps erhalten. Umständliche Konfigurationen oder Anmeldeinformationen entfallen.



## Verwaltete Anwendungen

Bei Android für Unternehmen müssen die Benutzer nicht mehr den Play Store besuchen, um ihre Anwendungen zu installieren. Stattdessen kann das Unternehmen per Push öffentliche und private Apps im Hintergrund auf den Geräten ohne Eingriff des Endbenutzers installieren. Es nutzt dazu die oben erwähnte automatische Kontoverwaltung und die Google Play APIs, die direkt in die EMM-Plattform integriert sind.

Alte Registrierungen mit weiteren Schritten zur Konfiguration von Anwendungen während des Registrierungsprozesses unterstützt Android für Unternehmen durch verwaltete Anwendungskonfigurationen, mit denen Unternehmen die App-Details in der EMM-Lösung vor der Installation vorkonfigurieren können.

Mit dieser Funktion lassen sich Anwendungen wie Chrome so konfigurieren, dass unerwünschte Websites blockiert oder Popup-Fenster standardmäßig deaktiviert werden. Gmail kann bereits für die Abholung von E-Mails konfiguriert werden. Manche Apps unterstützen über die Kerberos-Integration eine Integration in die Unternehmensdienste und eine vollständige App-Konfiguration ganz ohne Passworte. Per-App-VPN-Lösungen funktionieren nun ohne kompliziertes Setup.

Verwaltete Anwendungen mit Android für Unternehmen können entweder über den Play Store bezogen oder vom Unternehmen als interne Whitelist des für Android für Unternehmen erlaubten App-Bestandes gehostet werden und bei der Bereitstellung von Geräten in großen und kleinen Netzwerken viel Zeit sparen. Weitere Kontrollen wie die Rechteverwaltung stellen sicher, dass ein Benutzer eine Berechtigung nicht verweigern bzw. gewähren kann, die nach Ansicht des Unternehmens für die zu installierende Anwendung notwendig oder unerwünscht ist.

Schließlich können Unternehmen mit der Möglichkeit zur Sperrung der Deinstallation, zur Akzeptanz der Geschäftsbedingungen von Anwendungen im Namen der Benutzer und zur Verhinderung einer Deinstallation ein perfektes Ökosystem für Unternehmensanwendungen entsprechend ihren Wünschen gestalten. All dies ist ohne ein privates Google-Konto auf dem Gerät möglich.

# Fazit

Android hat sich im Laufe der Jahre deutlich verbessert und zu einem ausgereiften und stabilen mobilen Betriebssystem entwickelt, das selbst strengste Unternehmensanforderungen erfüllen kann.

Aufgrund der Android-eigenen Flexibilität und der offenen Plattform können OEMs damit Geräte für alle gewünschten Formfaktoren, Funktionsumfänge und Budgets kreieren, die zugleich eine hohe Sicherheit sowie die Gewissheit bieten, dass Unternehmensdaten ohne Kompromisse für den Endbenutzer von Anfang bis Ende abgesichert sind.

Android für Unternehmen bietet für Initiativen wie BYOD, COPE, COBO usw. Komplettlösungen zur strikten Trennung zwischen privaten und Unternehmensdaten, zur universellen und zuverlässigen OEM-Verwaltung sowie Bereitstellungsprozesse, die die Registrierung der Geräte in Unternehmen deutlich beschleunigen und den Aufwand an Zeit, Geld und Support drastisch reduzieren.

Da sich Android in den kommenden Jahren weiterentwickeln wird, gehen wir davon aus, dass noch weitere Verbesserungen zu erwarten sind.

## Weitere Informationen finden Sie hier ...

Ob Ihr Unternehmen nun bereits heute auf Android setzt, Lösungen evaluiert, die Migration bereits in vollem Gang ist oder Sie Support suchen: MobileIron kann Sie unterstützen. Unsere Kunden mit zehntausenden Geräten nutzen die Skalierungsvorteile und Flexibilität von Android. Weitere Informationen zu Anwendungsfällen finden Sie auf unserer Webseite unter Case Studies. Alle Sicherheits- und Verwaltungsfunktionen der neuesten Android-Plattformen können nur über eine EMM-Lösung verwaltet werden. Mit 15.000 Kunden ist die ausgezeichnete MobileIron EMM-Plattform eine sichere Basis, welche sowohl die Benutzererwartungen als auch die IT-Sicherheitsanforderungen für jede Android-Implementierung erfüllt.

Unser oben zitierter, langjähriger MobileIron-Partner und Freund Jason Bayton bietet umfangreichen, lösungsoffenen Content zur Funktionalität und vergleicht diese auf seiner Website mit der Registrierung in firmeneigenen Systemen.

Weitere Informationen bzw. einen Ansprechpartner finden Sie bei MobileIron

MobileIron

401 East Middlefield Road

Mountain View, CA 94043, USA

globalsales@mobileiron.com

www.mobileiron.com

Tel.: +1 877 819 3451

Fax: +1.650.919.8006