

Android Enterprise – Einrichtung und Best Practices

White Paper



Inhalt

Einleitung	3
Was ist Android Enterprise?	3
Geeignete Hardware verwenden.....	4
Android-Enterprise-Features auswählen.....	4
Android-Arbeitsprofil	5
Fully Managed Device (Vollständige Geräteverwaltung).....	6
Empfohlene Richtlinien für Android Enterprise	7
Arbeitsprofil	7
Vollständig verwaltete Geräte.....	8
Passwort-Richtlinien	10
Empfohlenes App-Management	11
Importieren von Apps & App-Updates.....	12
Konfigurieren von Anwendungen	13
Fazit	13

Einleitung

In diesem White Paper geben wir Tipps und Empfehlungen, die Ihnen bei der Auswahl, Einrichtung und Verwaltung von Geräten mit **Android Enterprise** helfen. Zudem haben wir verschiedene Geräte-Richtlinien für Sie zusammengestellt, die ein unterschiedliches Maß an Benutzerfreundlichkeit und Sicherheit bieten.

Wir zeigen Ihnen, wie Sie mit Hardware, die nicht auf der Android Recommended Liste steht, umgehen können, nennen Ihnen die Vor- und Nachteile der Android-Enterprise-Funktionen und haben eine Auswahl von Konfigurationen für Best-Practices zum Thema Anwendungsmanagement zusammengestellt. All diese Empfehlungen, die auf unseren Erfahrungen im Enterprise Mobility Management basieren, können mit einer kompatiblen MDM/MAM-Lösung wie Cortado MDM problemlos umgesetzt werden.

Was ist Android Enterprise?

Der Anteil der Geräte weltweit mit einem Android-Betriebssystem belief sich 2018 auf 85 %¹. Auch wenn es gegensätzliche Studien gibt, die zeigen, dass 82 % der mobilen Unternehmensnutzung iOS vorbehalten ist², ist davon auszugehen, dass die Verwendung von Android-Geräten in Unternehmen zukünftig noch zunehmen wird.

Android Enterprise – früher „Android for Work“ – wird wahrscheinlich zu dieser Entwicklung beitragen. Googles Plattform umfasst MDM-Tools und APIs (Application Programming Interfaces), die nach 2014 schrittweise freigegeben wurden. Alle Geräte, die die Android-Kompatibilitätsanforderungen von Google erfüllen – also als Google Mobile Services (GMS) zertifiziert sind – unterstützen Android Enterprise. Mit Android Enterprise haben IT-Administratoren eine größere Kontrolle über Unternehmensgeräte, da die Lösung u.a. die einfache Trennung von persönlichen und arbeitsbezogenen Daten ermöglicht.

Ursprünglich waren Android-APIs nicht im Betriebssystem enthalten. Android-Geräte ließen sich daher kaum mit EMM-Lösungen, die den Anforderungen von Unternehmen entsprachen, verwalten. Die MDM-Funktionalität von Android Enterprise umfasst derzeit Device Management APIs und ergänzt bestehende EMM-Lösungen in Unternehmen. Dadurch ist das Auswählen von Android-Unternehmensgeräten einfacher geworden. Zwei Hauptfunktionen – „Android Work Profile“ und „Fully Managed Device“ – werden im Folgenden näher erläutert.

1 International Data Corporation (IDC). (2018). Smartphone Market Share. Abgerufen von International Data Corporation: <https://www.idc.com/promo/smartphone-market-share/os> (08.02.2019)

2 Evans, J. (2017, August 30). Apple's iOS dominates enterprise mobility, data shows. Abgerufen von Computerworld: <https://www.computerworld.com/article/3220988/apple-ios/apples-ios-dominates-enterprise-mobility-data-shows.html> (08.02.2019)

Geeignete Hardware verwenden

Soll Android in Ihrem Unternehmen das Betriebssystem der Wahl sein, müssen Sie zunächst die entsprechende Hardware auswählen. Sicherlich haben Sie Vorlieben, aber man sollte nicht voreingenommen an die Auswahl herangehen. Im Gegensatz zum iOS-Ökosystem modifizieren die OEM-Partner von Google in ihren Hardware-Produktlinien bestimmte Aspekte des Android-Betriebssystems, was zu einer Fragmentierung und möglichen Inkompatibilität mit MDM-Systemen führen kann. Daher muss bei der Auswahl neuer Android-Hardware einiges beachtet werden.

Glücklicherweise bietet Google mit **Android Enterprise Recommended** eine Entscheidungshilfe. Auf dieser Website finden Sie eine vollständige Liste der Android-Hardware mit einer Kompatibilitätsgarantie für Android Enterprise. Außerdem erfahren Sie, welche Android-Enterprise-Features Sie mit welcher Hardware nutzen können.

Allerdings wissen wir, dass einige Geräte kompatibel sind, obwohl sie nicht in der Liste aufgeführt werden. Wenn Sie ein Gerät implementieren möchten, das nicht auf der Liste der empfohlenen Android-Enterprise-Geräte genannt wird, können Sie uns kontaktieren. Wir teilen Ihnen gern mit, welche Erfahrung wir mit dieser speziellen Hardware gemacht haben. Haben Sie jedoch Verständnis dafür, dass wir nur aus Erfahrung sprechen können und das Geräteverhalten bei Betriebssystem-Updates nicht vorhersagen (oder garantieren) können. Daher ist es am besten, sich nach Möglichkeit an die Enterprise Recommended Liste zu halten.

Android-Enterprise-Features auswählen

Wie bereits erwähnt, gibt es derzeit zwei Hauptfeatures von Android Enterprise: „Android-Arbeitsprofil“ und „Fully Managed Device“ (vollständig verwaltetes Gerät). Diese beiden Features schließen einander aus, d.h. Sie können auf jedem Gerät nur eines dieser Features verwenden.

Mittels unterschiedlicher Formen der Geräteregistrierung werden „Android-Arbeitsprofil“ und „Fully Managed Device“ aktiviert. Im Folgenden sehen wir uns die Aktivierung genauer an, wägen Vor- und Nachteile ab und geben Empfehlungen für den Einsatz in typischen Anwendungsfällen.

Android-Arbeitsprofil

Das Arbeitsprofil von Android wird aktiviert, indem ein kompatibles Android-Gerät ohne weitere Vorbereitung über die Schnellregistrierungsfunktion (via QR-Code, Self Service Link, etc.) registriert wird. Was diese Funktion einzigartig macht, ist, dass ein mit dem Arbeitsprofil konfiguriertes Gerät über einen privaten und einen Business-Container verfügt. Diese Container sind voneinander getrennt, werden dem Benutzer jedoch in einer Benutzeroberfläche angezeigt.

Als Administrator können Sie:

- › Konfigurationen (wie Exchange-Mail-Konfigurationen) pushen
- › Anwendungen aus dem Play Store pushen
- › APKs (Android Packages wie Microsoft Word oder unternehmensspezifische Anwendungen) über den Managed Google Play Store verteilen
- › Sicherheitsrichtlinien auf den Business-Container übertragen

Um dem Endbenutzer die Unterscheidung zwischen geschäftlichen und privaten Anwendungen zu erleichtern, werden Anwendungen, die Sie in den Business-Container geschoben haben, mit einem Aktenkoffer-Icon versehen (siehe Abb.1). Einige Sicherheitsrichtlinien, wie z.B. Passwortbeschränkungen (also die Festlegung einer Mindestlänge für den Sperrbildschirm-PIN eines Geräts), werden für das gesamte Gerät verwendet. Generell beschränkt sich Ihr Grad an Kontrolle jedoch auf den Business-Container.

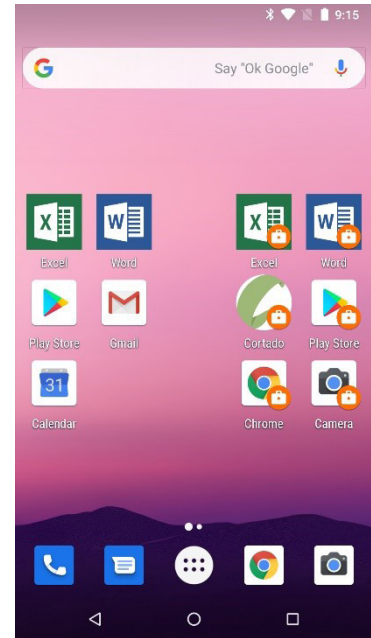


Abb. 1 Android-Arbeitsprofil

Vorteile des Arbeitsprofils:

- › Keine weitere Vorbereitung auf dem Gerät erforderlich
- › Gute Kompatibilität mit Android-Geräten ab Android 5.1.1.
- › Unternehmensdaten werden sicher im Business-Container abgelegt (warum dies wichtig ist, erläutern wir **in unserem Whitepaper** zur EU-Datenschutz-Grundverordnung).
- › Endbenutzer können mit ihren privaten Geräten sicher und ohne Änderung ihrer privaten Anwendungen oder Einstellungen mit Geschäftsdaten arbeiten, was das On/Offboarding von Geräten einfach macht.
- › Endbenutzer können WhatsApp weiterhin im privaten Container nutzen, ohne die Geschäftskontakte zu gefährden

Nachteile:

- › Die Kontrolle durch den Administrator ist auf den Business-Container beschränkt.
- › Keine Möglichkeit, die Installation von Drittanbieter-Applikationen im privaten Container zu deaktivieren, was ein Sicherheitsrisiko darstellen kann muss durch eine Sensibilisierung der Nutzer verhindert werden. Obwohl die Risiken einer Beeinträchtigung des Arbeitsprofils durch betrügerische Apps im privaten Container sehr gering sind, muss dieser Aspekt berücksichtigt werden.
- › Endbenutzer können das Arbeitsprofil löschen und die Verbindungseinstellungen für WLAN/VPN ändern, was die Arbeitsbelastung des Helpdesk erhöhen könnte.

Das Arbeitsprofil kann für folgenden Szenarien empfohlen werden:

- Ihre Endbenutzer sind sich der Risiken bewusst, die mit der manuellen Aktivierung von Entwickleroptionen und der Installation von Anwendungen aus nicht-offiziellen Appstores verbunden sind.
- Sie wissen, welche Android-Geräte Ihre Endbenutzer verwenden und sind sich sicher, dass diese kompatibel sind.
- Ihre Endbenutzer bevorzugen BYOD, also wollen ihre persönlichen Geräte für Arbeitszwecke verwenden.
- Ihre Endbenutzer verwenden WhatsApp oder andere Messenger, die normalerweise Kontaktdaten mit unbefugten Cloud-Anbietern synchronisieren.

Fully Managed Device (Vollständige Geräteverwaltung)

Um die zweite Hauptfunktion von Android Enterprise, die vollständige Geräteverwaltung, aktivieren zu können, sind einige Vorbereitungen erforderlich. So müssen Sie jedes Gerät, das Sie in diesem Modus einrichten möchten, auf Werkeinstellungen zurücksetzen. In **unserem Handbuch** erfahren Sie, welche Enrollment-Varianten Cortado unterstützt.

Diese Funktion unterscheidet sich vom Arbeitsprofil dadurch, dass auf dem Gerät kein privater Bereich mehr vorhanden ist. Das gesamte Gerät und seine zu verwaltenden Funktionen werden vom MDM-Administrator gesteuert, daher der Name „Fully Managed Device“.

Vorteile:

- Sie haben die erweiterte, detaillierte Kontrolle über das mobile Gerät.
- Viele Sicherheitsfunktionen sind verfügbar, um das Gerät gegen Angriffe zu schützen (z.B. keine manuelle Installation von nicht-marktüblichen Anwendungen auf dem Gerät).
- Manuelle (Fehl-)Konfiguration von Einstellungen (wie WLAN etc.) kann vom Administrator deaktiviert werden.

Nachteile:

- Vollständig verwaltete Geräte sind nicht für BYOD-Szenarien geeignet.
- Da es keine Trennung durch Container gibt, ist die Verwendung von Apps wie WhatsApp nicht zu empfehlen.

Die vollständige Geräteverwaltung wird in folgenden Fällen empfohlen:

- Die Anwender nutzen erst seit kurzem Android-Geräte und es fehlt ihnen an der erforderlichen Erfahrung in puncto Gerätesicherheit.
- Sie haben hohe Sicherheitsanforderungen. Daher muss in Kauf genommen werden, dass die Freiheit der Endbenutzer in gewissem Maße eingeschränkt wird.
- Sie verwalten diverse firmeneigene Geräte oder sind im Begriff, zweckgebundene Geräte einzuführen. Eine private Nutzung ist nicht oder nur sehr eingeschränkt gestattet.
- Anwendungen wie Facebook oder WhatsApp werden im Unternehmenskontext nicht verwendet.

Empfohlene Richtlinien für Android Enterprise

Nach der Auswahl Ihrer Geräte, der Android-Enterprise-Funktion und der Registrierungsmethode muss festgelegt werden, welche Richtlinien Sie durchsetzen möchten. Die Entscheidung über die passenden Richtlinien für Ihre Android-Geräte sollte sehr sorgfältig getroffen werden. Werden mobile Geräte ausschließlich für optimale Sicherheit konfiguriert, besteht die Gefahr, dass unzufriedene Endbenutzer Ihre Maßnahmen zu umgehen versuchen. Die daraus resultierende Schatten-IT stellt für viele Unternehmen ein echtes Problem dar.

Wir haben drei Android-Richtlinien-Sets zusammengestellt, die in verschiedenen Szenarien sinnvoll sind. Der erste Satz von Richtlinien begünstigt die Benutzerfreundlichkeit gegenüber der maximalen Geräteverriegelung (Tabellenspalte: Fokus Usability), der zweite Satz favorisiert einen ausgewogenen Ansatz (Tabellenspalte: Ausgewogen) und der letzte ist ein kompromissloses Sicherheitsset, das alle verfügbaren Maßnahmen nutzt, um die Sicherheit eines Android-Geräts zu erhöhen (Tabellenspalte: Fokus Sicherheit). Da sich die verfügbaren Richtlinien-APIs bei den Android-Enterprise-Funktionen Arbeitsprofil und Fully Managed Device unterscheiden, haben wir sie entsprechend gruppiert.

Arbeitsprofil

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
Kamera	Ein	Ein	Ein
Konten ändern	Ein	Aus	Aus
Chrome	Ein	Ein	Aus
Profilübergreifendes Kopieren und Einfügen	Aus	Aus	Aus
Google Play Store	Ein	Ein	Ein
Installation von nicht marktgängigen Apps	Aus	Aus	Aus
Bildschirmaufnahme	Ein	Aus	Aus
Erstmalige Benutzerhinweise überspringen	Aus	Aus	Aus
Anzeige der Anrufer-ID-Informationen	Ein	Ein	Ein

Android Enterprise Einrichtung und Best Practices

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
Die Verknüpfung von Apps im übergeordneten Profil zulassen	Aus	Aus	Aus
Bluetooth Kontaktfreigabe	Ein	Ein	Aus
Systemverhalten für App-Berechtigungen	Automatische Zuteilung	Automatische Zuteilung	Eingabeaufforderung
Kontaktsuche anzeigen	Ein	Ein	Ein
Fingerabdruck	Ein	Ein	Ein
„Trust Agents“	Aus	Aus	Aus
Nicht bearbeitete Benachrichtigungen	Ein	Aus	Aus

Vollständig verwaltete Geräte

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
ADB	Aus	Aus	Aus
Automatisch Datum und Uhrzeit	Ein	Ein	Aus
Automatische Zeitzone	Ein	Ein	Aus
Daten-Roaming	Ein	Aus	Aus
USB-Massenspeicher	Ein	Aus	Aus
Standortmodus	Aus	Aus	Aus
Wi-Fi-Schlafrichtlinie	Standard	Standard	Standard
Bluetooth konfigurieren	Ein	Ein	Aus
Konfigurieren von „Cell-Broadcasts“	Ein	Aus	Aus

Android Enterprise Einrichtung und Best Practices

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
Konfiguration von „Credentials“	Ein	Aus	Aus
Konfiguration von „Tethering“	Ein	Aus	Aus
VPN konfigurieren	Ein	Ein	Aus
WLAN-Konfiguration	Ein	Ein	Aus
App-Steuerung	Ein	Ein	Aus
„Verify Apps“	Ein	Ein	Ein
Apps installieren	Ein	Ein	Ein
Unbekannte Quellen installieren	Aus	Aus	Aus
Apps deinstallieren	Aus	Aus	Aus
Sperrbildschirm Alle Funktionen deaktivieren	Aus	Aus	Ein
Bildschirm sperren Sichere Kamera	Ein	Aus	Aus
Sperrbildschirm Sichere Benachrichtigungen	Ein	Aus	Aus
Lautstärke anpassen	Ein	Ein	Ein
Debugging-Funktionen	Aus	Aus	Aus
„Factory reset“	Ein	Aus	Aus
Master-Volumen	Ein	Ein	Ein
Mikrofon	Ein	Ein	Ein (Aus)
Einbinden von physischen Medien	Ein	Ein (Aus)	Ein (Aus)
Android Beam	Ein	Aus	Aus

Android Enterprise Einrichtung und Best Practices

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
Ausgehende Anrufe	Ein	Ein (aus)	Ein (Aus)
Standort teilen	Ein	Ein	Ein
SMS	Ein	Ein (aus)	Ein (aus)
USB-Dateiübertragung	Ein	Aus	Aus
„Stay On“			Niemals
Änderungen am WLAN	Ein	Ein	Aus
Netzwerk-Reset	Ein	Aus	Aus
„Safe Boot“	Aus	Aus	Aus
„Status bar“ deaktiviert	Aus	Aus	Aus
Benutzer hinzufügen	Aus	Aus	Aus
Benutzer entfernen	Aus	Aus	Aus

Passwort-Richtlinien

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
Passwort erzwingen	Ein	Ein	Ein
Passworttyp	Gerät	Arbeitsprofil	Arbeitsprofil
Passwortstärke	Einfaches Passwort	Einfaches Passwort	Komplexes Passwort
Minimale Passwortlänge	4	6	8
Mindestbuchstabenanzahl	N/A	N/A	1
Mindestanzahl Kleinbuchstaben	N/A	N/A	1
Mindestanzahl numerische Zeichen	N/A	N/A	1

Richtlinie	Fokus Usability	Ausgewogen	Fokus Sicherheit
Mindestanzahl Sonderzeichen	N/A	N/A	1
Mindestanzahl Großbuchstaben	N/A	N/A	1
Ablauf des Passworts	Keine	365	180
Maximal fehlgeschlagene Anmeldungen	10	10	10
Passwortverlauf	N/A	5	10
Automatische Sperrzeit (min)	5	1	1

Empfohlenes App-Management

Android Enterprise macht die Verwaltung von Geschäftsanwendungen einfach. In Kombination mit den App-Management-Funktionen von **Cortado MDM** wird die Integration neuer Anwendungen in Ihren Anwendungspool, aus dem Sie Software den Endgeräten zuordnen und ausrollen können, weiter vereinfacht.

Android Enterprise ermöglicht es MDM-Lösungen, diesen Prozess weiter anzupassen, so dass die Aktualisierung von Anwendungen noch komfortabler, zuverlässiger und sicherer wird.

Empfohlene Apps

Bevor Sie dem App-Pool neue Anwendungen hinzufügen, sollten Sie jedoch einige Dinge bedenken: Wir empfehlen, wann immer möglich, Anwendungen von vertrauenswürdigen, bekannten Entwicklern zu verwenden. Einige Texteditoren oder Open-Source-Office-Programme können kostenlos heruntergeladen werden, werden aber oft mit Anzeigen oder In-App-Käufen geliefert, die der Benutzerfreundlichkeit und der Sicherheit des Geräts abträglich sind.

Diese Einrichtung hat sich für die täglichen Aufgaben einer mobilen Belegschaft als ausreichend erwiesen:

Zweck	Empfohlene App
E-Mail	Gmail or Nine Work or IBM Verse
Kontakte	Google Contacts or Stock-Contacts-App
Kalender	Google Kalender oder Stock-Kalender-App
Textbearbeitung	Google Docs oder Microsoft Word
Präsentationen	Google Slides oder Microsoft PowerPoint
Arbeitsblätter	Google Sheets oder Microsoft Excel
Browser	Google Chrome
PDF	Google PDF Viewer oder Adobe Acrobat Reader
Camera	Open Camera

Bitte beachten Sie:

Wenn Sie vorinstallierte Apps auf dem Gerät verwenden möchten, müssen Sie sicherstellen, dass diese vorinstallierten Apps in der Lage sind, das zu tun, was Sie wollen. So erlaubt beispielsweise nicht jede Standard-PIM-App eine bidirektionale Synchronisation.

Einige Google-Anwendungen sind möglicherweise nicht mit jedem Gerät kompatibel. Daher können Sie diese Anwendungen nicht ausrollen und müssen entweder auf Standardanwendungen oder Alternativen zurückgreifen. Wenn Sie Beratung benötigen, zögern Sie nicht, uns zu kontaktieren.

Importieren von Apps & App-Updates

Wenn Sie Android-Anwendungen genehmigen, können Sie einstellen, wie sich die Anwendung und Cortado MDM verhalten sollen, falls es ein Update der Anwendung gibt, das nach einer neuen App-Berechtigung fragt. In diesem Fall ist es am besten, wenn die App genehmigt bleibt. Wenn Sie eine sehr kontrollierte Umgebung haben, können Sie sich jedoch für den Widerruf der Genehmigung entscheiden. Dies kann ein schlechter Kompromiss sein und erfordert, dass Sie die App regelmäßig und manuell erneut genehmigen müssen.

In jedem Fall empfehlen wir, E-Mail-Benachrichtigungen an einen überwachten Admin-Posteingang senden zu lassen, wenn es ein Update für eine Anwendung gibt, das zusätzliche Berechtigungen benötigt.

Konfigurieren von Anwendungen

Android Enterprise bietet eine granulare Konfiguration für MDM-Administratoren. Wenn Sie eine Anwendung importiert haben, können Sie deren Kontrollkästchen im linken Rahmen aktivieren und im rechten Rahmen auf „Konfigurieren“ klicken.

Hier können Sie:

- › den Status der Berechtigungen festlegen, die die Anwendung bei der Installation anfordert
- › Berechtigungen global über die Richtlinie „Systemverhalten für App-Berechtigungen“ steuern oder auf App-Ebene anpassen

Standardmäßig werden diese Berechtigungen nicht vom MDM verwaltet, sondern der Benutzer wird aufgefordert, bei der Installation Berechtigungen zu vergeben oder zu verweigern. Sofern Ihre Benutzer nicht besonders technisch versiert sind, empfehlen wir, die Berechtigungen nur für die von uns empfohlenen Anwendungen zu vergeben. Der Vorteil ist, dass Endbenutzer bei der Einrichtung keine Fehler machen können, wie z.B. eine wichtige Berechtigung zu verweigern.

Wir empfehlen, gar keine Berechtigungen zu verweigern oder nur, wenn Sie wirklich wissen, welche Folgen dies für das Verhalten der App hat. So kann es beispielsweise bei einigen Anwendungen vorkommen, dass, wenn der Zugriff auf den Speicher verweigert wird, sie nicht mehr funktionieren, nicht starten oder Fehler erzeugen, die der Endbenutzer nicht nachvollziehen kann.



Fazit

Insgesamt stellt Android Enterprise einen Fortschritt in Richtung optimales Management von Android-Geräten für den Unternehmenseinsatz dar. Die Integration in EMM-Lösungen wurde vereinfacht, so dass immer mehr Unternehmen die Vorteile der auf dem Markt erhältlichen erschwinglichen Android-Geräte nutzen können.

..... Headquarters

Cortado Mobile Solutions GmbH

Alt-Moabit 91a/b
10559 Berlin, Germany
Tel.: +49 (0)30 408 198 500
Fax: +49 (0)30 408 198 501
E-Mail: info@cortado.de
www.cortado.de

..... USA (Colorado)

Cortado, Inc.

3858 Walnut Street, Suite 130
Denver, CO 80205, USA
Tel.: +1-303-487-1302
E-mail: info@cortado.com
www.cortado.com

Cortado Pty Ltd.

Australia

Level 12, Plaza Building,
Australia Square, 95 Pitt Street
NSW 2000 Sydney, Australia
Tel.: +61-(0)2-8079 2989

Cortado Japan

Japan

5F Yaesu Dori Building,
3-4-15 Nihonbashi,
Chuo-ku Tokyo
Tokyo 103-0027
Tel.: +81-(0)3-6870 3467



Alle Namen und Warenzeichen sind Namen und Warenzeichen der jeweiligen Hersteller.

Folgen Sie Cortado auf:



facebook



twitter



youtube



linkedin