CORTADO

PRAXISGUIDE MOBILE SICHERHEIT

Sicher mobil.
Von Device bis KI.

Der Praxisguide für den sicheren mobilen Arbeitsplatz

- **40 Checkpunkte in 5 Bereichen**
  vom Gerät bis zur KI, zum direkten Abhaken
- **Selbstcheck mit Ampel**
  sehen, wo Ihr Unternehmen heute steht
- **Praxis-Tipps und nächste Schritte**
  konkret umsetzbar, ohne Fachchinesisch



ISO 27001
GUTcert · AFNOR Group

Software Bundesverband IT-Mittelstand Made in Germany
100% Service Qualität Zukunft 2026

OMR REVIEWS LEADER MOBILE DEVICE MANAGEMENT Q4/26

Capterra 5

DAS WICHTIGSTE IN KÜRZE

Fünf Sätze für Entscheider.
Alles Weitere zum Abhaken.

- **Mobile Geräte sind heute Arbeitsplätze.** Wer E-Mails, Dateien und KI auf dem Smartphone nutzt, braucht dort dieselbe Sicherheit wie am Rechner.
- **Sicherheit beginnt mit Übersicht.** Nur bekannte und einheitlich eingerichtete Geräte lassen sich schützen.
- **Regeln wirken nur, wenn die Technik sie durchsetzt.** Code-Sperre, Updates und Löschen bei Verlust gehören ins Mobile Device Management, nicht in ein Rundschreiben.
- **Datenschutz und Compliance muss man belegen können.** Auch für Prüfer, Kunden und den Betriebsrat.
- **KI ist schon auf den Geräten.** Mit klaren Regeln und einer sicheren Alternative wird aus Schatten-KI ein Produktivitätsgewinn.

INHALT

→	**Mobiles Arbeiten braucht Sicherheit.** Warum das Thema jetzt drängt	3
1	**Mobile Device Management** Alle Geräte kennen und steuern	4
2	**Endpoint Security** Geräte härten und schnell reagieren	6
3	**Compliance** Vorgaben kennen, Maßnahmen belegen	8
4	**Datenschutz** Firma und Privat sauber trennen	10
5	**KI auf dem Diensthandy** Regeln festlegen und durchsetzen	12
✓	**Selbstcheck und Fahrplan** Ihre Ampel und die nächsten 3 Schritte	14

SO NUTZEN SIE DEN GUIDE

Abhaken, zählen, loslegen.

Jedes Kapitel endet mit 8 Checkpunkten. Haken Sie ab, was bei Ihnen schon gilt.

Auf Seite 14 tragen Sie Ihre Haken ein und sehen auf einen Blick, wo Sie stehen.

WARUM JETZT

Mobiles Arbeiten braucht Sicherheit.

Geräte, Apps, Daten und KI – zentral verwaltet und geschützt. Vier Entwicklungen machen das Thema dringend.

58 %
der Unternehmen ermöglichen mobiles Arbeiten.[1]

29 %
der KI-Nutzenden im Job verwenden Tools, die der Arbeitgeber nicht bereitstellt.[2]

119
neue Software-Schwachstellen werden im Schnitt pro Tag bekannt.[3]

Mehr Geräte, mehr Apps

Smartphones, Tablets und Laptops greifen von überall auf Firmendaten zu. Jedes ungeschützte Gerät ist ein offener Eingang.

KI im Arbeitsalltag

Mitarbeitende übersetzen, fassen zusammen und formulieren mit KI-Apps. Oft ohne Freigabe und ohne zu wissen, wohin die Daten gehen.

Neue Pflichten

NIS-2, BSI IT-Grundschutz und der EU AI Act machen Sicherheit und Nachweise für viele Unternehmen zur Pflicht.

Angriffe zielen aufs Smartphone

Phishing per SMS und Messenger, verlorene Geräte, veraltete Systeme: Der mobile Arbeitsplatz ist ein bevorzugtes Ziel.

DIE GUTE NACHRICHT

Mit klaren Regeln und dem richtigen Werkzeug ist mobiles Arbeiten sicher.

Die fünf Kapitel dieses Guides zeigen, worauf es ankommt, und mit den 40 Checkpunkten sehen Sie, wo Sie heute stehen.

[1] Bitkom Research, Befragung von 602 Unternehmen ab 20 Beschäftigten, Mai 2025 · [2] IW-Kurzbericht 63/2026 „Schatten-KI“, Befragung von knapp 5.000 Beschäftigten, September 2026 · [3] BSI, Die Lage der IT-Sicherheit in Deutschland 2025 (Juli 2024 bis Juni 2025)

KAPITEL 1 · MOBILE DEVICE MANAGEMENT

Was Sie nicht kennen, können Sie nicht schützen.

1

WORUM ES GEHT

In vielen Unternehmen wächst die Zahl mobiler Geräte schneller als die Übersicht. Smartphones und Tablets greifen täglich auf E-Mails, Dateien und Firmen-Apps zu. Mobile Device Management sorgt dafür, dass jedes Gerät bekannt ist, einheitlich eingerichtet wird und über seinen ganzen Lebenszyklus gesteuert werden kann: vom ersten Einschalten bis zur Rückgabe.

Typische Lücken aus der Praxis

- **Die Geräteliste lebt in einer Tabelle** und ist nie ganz aktuell.
- **Neue Geräte werden von Hand eingerichtet**, jedes ein bisschen anders.
- **WLAN- und E-Mail-Zugänge** werden per Zettel oder Chat weitergegeben.
- **Beim Austritt bleibt das Firmenkonto** noch Wochen auf dem Gerät.

PRAXIS-TIPP

Die Lücke sichtbar machen

Exportieren Sie alle Geräte, die sich in den letzten 30 Tagen an Ihrem E-Mail-System angemeldet haben, und vergleichen Sie sie mit Ihrer Inventarliste. Die Differenz zeigt, wie viele Geräte Sie heute nicht kennen.

Was davon gilt bei Ihnen schon?

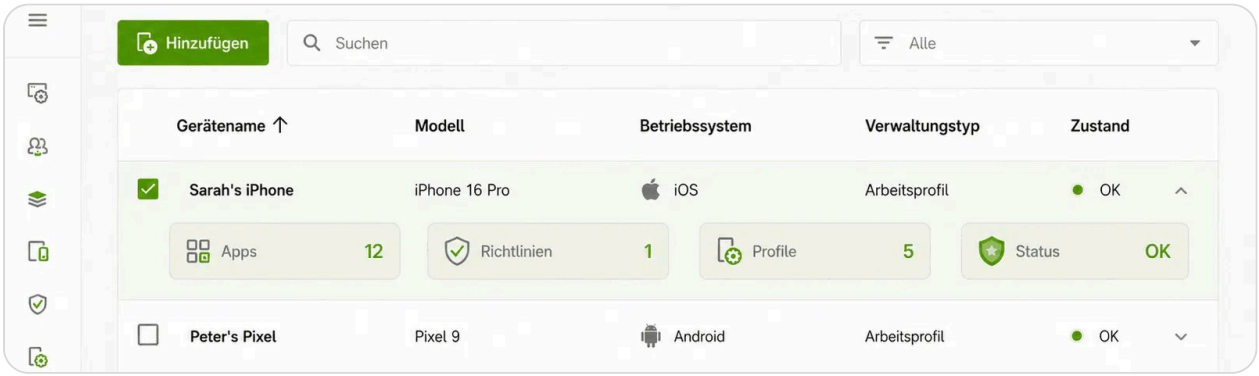
- [ ] 01 **Inventar:** Wir kennen alle iOS-, iPadOS-, macOS- und Android-Geräte mit Zugriff auf Firmendaten.
- [ ] 02 **Zuordnung:** Jedes Gerät ist einer Person oder einer Gruppe zugeordnet.
- [ ] 03 **Zero-Touch:** Neue Geräte richten sich beim ersten Einschalten automatisch ein.
- [ ] 04 **Zugänge:** WLAN, E-Mail, VPN und Zertifikate werden zentral verteilt.
- [ ] 05 **Apps:** Firmen-Apps werden zentral bereitgestellt und aktualisiert.
- [ ] 06 **Rollen:** Für unterschiedliche Rollen gibt es eigene Profile, z. B. Außendienst und Verwaltung.
- [ ] 07 **Lebenszyklus:** Ausgemusterte Geräte werden zurückgesetzt und aus dem Inventar entfernt.
- [ ] 08 **Offboarding:** Beim Austritt werden Zugänge und Firmendaten am selben Tag entfernt.

Ihre Haken in Kapitel 1: ___ von 8 · Übertrag auf Seite 14

SO GEHT'S MIT CORTADO MDM

Zero-Touch Enrollment für Apple und Android, App Management und Profile per Vorlage. Bis zu 5x schnellere Bereitstellung und bis zu 75 % weniger Verwaltungsaufwand.

Quelle: cortado.com/de/roi



Verwaltungsportal von Cortado MDM: Geräteübersicht mit Apps, Richtlinien, Profilen und Zustand je Gerät

KAPITEL 2 · ENDPOINT SECURITY

Jedes Gerät ist ein Eingang ins Firmennetz.

2

WORUM ES GEHT

Ein verlorenes Smartphone, ein veraltetes Betriebssystem oder eine App aus unbekannter Quelle genügen, damit Firmendaten in falsche Hände geraten. Endpoint Security auf mobilen Geräten heißt: Geräte härten, aktuell halten und im Ernstfall in Minuten reagieren statt in Tagen.

Typische Lücken aus der Praxis

- **Die Code-Sperre ist freiwillig** oder vierstellig.
- **Updates hängen Monate hinterher**, weil niemand sie einfordert.
- **Bei Verlust weiß niemand, wen man anruft.** Das Gerät bleibt tagelang offen.
- **Jailbreak und Root bleiben unbemerkt** und hebeln alle Schutzmechanismen aus.

PRAXIS-TIPP

Die Notfallkarte fürs Portemonnaie

Mit dem Handy ist unterwegs oft auch die Nummer der IT weg. Drucken Sie die Notfall-Nummer auf die Rückseite des Firmenausweises oder geben Sie eine kleine Karte fürs Portemonnaie aus. So meldet jede und jeder einen Verlust sofort, vom Hoteltelefon ebenso wie vom Handy einer Kollegin.

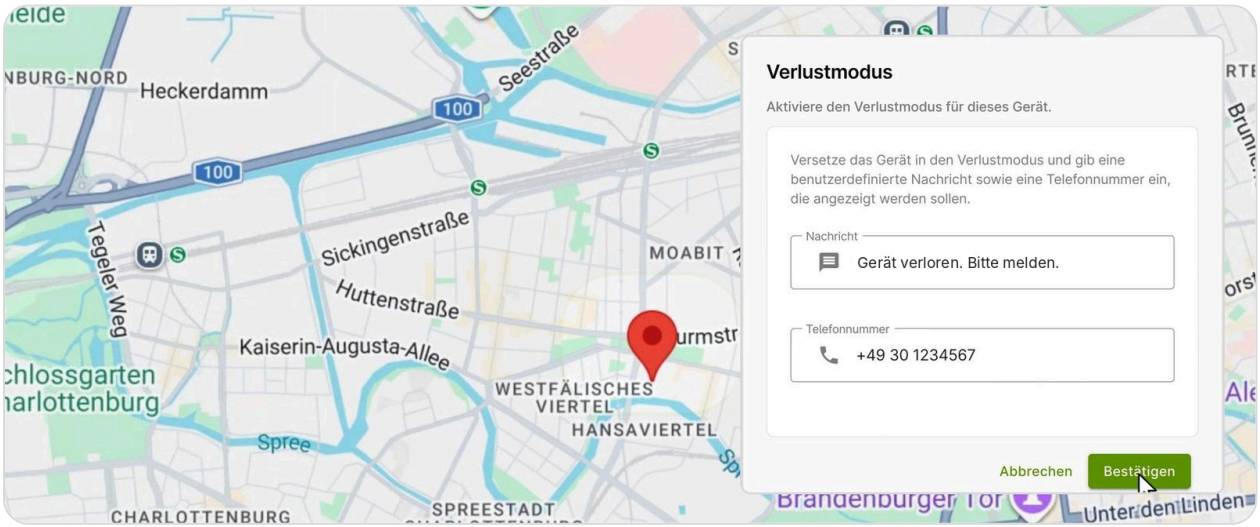
Was davon gilt bei Ihnen schon?

- [ ] 09 **Code-Sperre:** Eine sichere Code-Sperre und automatische Sperre sind auf allen Geräten Pflicht.
- [ ] 10 **Verschlüsselung:** Die Geräteverschlüsselung ist überall aktiv.
- [ ] 11 **Updates:** Betriebssystem-Updates werden innerhalb einer festen Frist eingespielt.
- [ ] 12 **Manipulation:** Geräte mit Jailbreak oder Root werden erkannt.
- [ ] 13 **App-Quellen:** Apps kommen nur aus freigegebenen Quellen.
- [ ] 14 **Fernzugriff:** Verlorene Geräte lassen sich aus der Ferne sperren, orten und löschen.
- [ ] 15 **Meldeweg:** Alle wissen, wo sie ein verlorenes Gerät sofort melden.
- [ ] 16 **Konsequenz:** Geräte, die die Regeln nicht erfüllen, verlieren den Zugriff auf Firmendaten.

Ihre Haken in Kapitel 2: ___ von 8 · Übertrag auf Seite 14

SO GEHT'S MIT CORTADO MDM

Sperren, Orten und Löschen der Firmendaten mit wenigen Klicks im Verwaltungsportal. Richtlinien für Code-Sperre, Verschlüsselung und Updates per Vorlage.



Verwaltungsportal von Cortado MDM: verlorenes Gerät orten und in den Verlustmodus versetzen

KAPITEL 3 · COMPLIANCE

Sicherheit muss man belegen können.

3

WORUM ES GEHT

Mobile Geräte sind längst Teil von Prüfungen: durch gesetzliche Vorgaben, Anforderungen von Kunden und Versicherern oder interne Audits. Es reicht nicht, sicher zu sein. Sie müssen zeigen können, welche Regeln gelten, wie sie umgesetzt sind und dass sie eingehalten werden.

WELCHE VORGABEN MOBILE GERÄTE BETREFFEN

- **NIS-2:** verpflichtet viele Unternehmen wichtiger Sektoren zu Risikomanagement, inklusive der Sicherheit von Endgeräten. In Deutschland umgesetzt durch das NIS-2-Umsetzungsgesetz.
- **BSI IT-Grundschutz:** eigene Bausteine für Smartphones und Tablets (SYS.3.2.1) und für Mobile Device Management (SYS.3.2.2).
- **DSGVO:** verlangt geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten (Art. 32).

Typische Lücken aus der Praxis

- **Regeln stehen in einer E-Mail** von vor drei Jahren.
- **Ob ein Gerät die Regeln erfüllt**, weiß nur, wer es in der Hand hält.
- **Vor dem Audit** werden Nachweise tagelang zusammengesucht.
- **Niemand weiß genau**, welche Vorgaben für das eigene Unternehmen gelten.

Was davon gilt bei Ihnen schon?

- [ ] 17 **Vorgaben:** Wir wissen, welche Vorgaben für uns gelten.
- [ ] 18 **Schriftlich:** Unsere Regeln für mobile Geräte sind schriftlich festgelegt.
- [ ] 19 **Technisch:** Die Regeln sind im MDM umgesetzt, nicht nur auf Papier.
- [ ] 20 **Status:** Der Compliance-Status jedes Geräts ist jederzeit abrufbar.
- [ ] 21 **Abweichungen:** Verstöße werden automatisch erkannt und gemeldet.
- [ ] 22 **Berichte:** Nachweise für Audits lassen sich schnell exportieren.
- [ ] 23 **Änderungen:** Anpassungen an Richtlinien werden dokumentiert.
- [ ] 24 **Überprüfung:** Die Regeln werden mindestens einmal im Jahr überprüft.

Ihre Haken in Kapitel 3: ___ von 8 · Übertrag auf Seite 14

PRAXIS-TIPP

Eine Tabelle, drei Spalten

Legen Sie eine einfache Übersicht an: Anforderung, Maßnahme, Nachweis. Sie zeigt Lücken sofort und erspart im nächsten Audit viel Sucherei.

SO GEHT'S MIT CORTADO MDM

Konfigurationsvorlagen für Geräterichtlinien, die sich an den Empfehlungen des BSI und den Anforderungen der DSGVO orientieren, ab dem ersten Tag einsatzbereit. So sind Ihre Regeln nicht nur beschlossen, sondern auf jedem Gerät umgesetzt.

KAPITEL 4 · DATENSCHUTZ

Firmendaten bleiben Firmendaten. Privates bleibt privat.

4

WORUM ES GEHT

Nutzen Mitarbeitende ihr Diensthandy auch privat oder ihr privates Gerät für die Arbeit (BYOD), treffen zwei Welten aufeinander. Datenschutz heißt hier: Firmendaten konsequent schützen, ohne in die Privatsphäre einzugreifen, und einen Anbieter wählen, dem Sie Ihre Daten anvertrauen können.

Typische Lücken aus der Praxis

- **Firmen-E-Mails landen in privaten Apps** und Cloud-Speichern.
- **Mitarbeitende fürchten,** dass die IT private Fotos und Nachrichten sieht.
- **Die MDM-Daten liegen** bei einem Anbieter außerhalb der EU.
- **Der Betriebsrat erfährt** erst nach der Einführung vom MDM.

PRAXIS-TIPP

Spielregeln schriftlich festhalten

Eine Nutzungsvereinbarung regelt, was auf dem Gerät erlaubt ist, welche Daten die IT sehen kann und was beim Austritt passiert. Das schafft Rechtssicherheit und Vertrauen. Cortado stellt Mustervereinbarungen für Firmengeräte und für BYOD bereit: Sprechen Sie uns einfach darauf an.

Was davon gilt bei Ihnen schon?

- [ ] 25 **BYOD-Regel:** Private Nutzung und private Geräte sind schriftlich geregelt.
- [ ] 26 **Trennung:** Arbeitsprofil bzw. verwaltete Apps trennen Firmen- und Privatdaten.
- [ ] 27 **Selektiv löschen:** Beim Austritt werden nur Firmendaten gelöscht, private bleiben.
- [ ] 28 **Privatsphäre:** Die IT sieht keine privaten Inhalte wie Fotos oder Nachrichten.
- [ ] 29 **Hosting:** Unser MDM-Anbieter hostet in der EU, am besten in Deutschland.
- [ ] 30 **Vertrag:** Ein Vertrag zur Auftragsverarbeitung liegt vor.
- [ ] 31 **Mitbestimmung:** Der Betriebsrat ist eingebunden, falls vorhanden.
- [ ] 32 **Transparenz:** Mitarbeitende wissen, welche Daten die IT sehen kann.

Ihre Haken in Kapitel 4: ___ von 8 · Übertrag auf Seite 14

SO GEHT'S MIT CORTADO MDM

Entwickelt in Berlin, betrieben im BSI-C5-zertifizierten Rechenzentrum in Frankfurt am Main. Firmendaten lassen sich gezielt entfernen, private Daten bleiben unberührt.

Firmendaten in der KI? Nur, wenn die Richtlinie es erlaubt.

5

WORUM ES GEHT

Mitarbeitende nutzen KI-Apps längst auf dem Smartphone: zum Übersetzen, Zusammenfassen und Formulieren. Oft ohne Freigabe und ohne zu wissen, wohin die Daten gehen. Ein Verbot hilft wenig, die Nutzung wandert dann ins Private. Besser sind klare Regeln, technische Leitplanken und eine sichere Alternative.

Typische Lücken aus der Praxis

- **Kundendaten werden in kostenlose KI-Chats** kopiert.
- **Jede Abteilung nutzt ein anderes Tool**, niemand hat den Überblick.
- **Es gibt keine Regel**, welche Daten in eine KI dürfen.
- **Niemand wurde geschult,** obwohl der EU AI Act KI-Kompetenz verlangt.

PRAXIS-TIPP

Erst erlauben, dann begrenzen

Starten Sie mit einer freigegebenen KI-Lösung für alle und regeln Sie dann, was nicht erlaubt ist. Wer eine gute Alternative hat, braucht keine Schatten-KI.

IHR BONUS

Aiverti AI 1 Monat kostenlos

Testen Sie die sichere KI-Alternative mit Ihrem Team. Einfach den Code bei Aiverti einlösen:

CMSAI-ITSA

aiverti.ai/de/ai

Aiverti

Was davon gilt bei Ihnen schon?

- [ ] 33 **Richtlinie:** Eine KI-Richtlinie regelt, welche Tools und welche Daten erlaubt sind.
- [ ] 34 **Verteilung:** Freigegebene KI-Apps werden zentral per MDM verteilt.
- [ ] 35 **Begrenzung:** Nicht freigegebene KI-Apps sind auf Firmengeräten gesperrt.
- [ ] 36 **Datenfluss:** Das Kopieren von Firmendaten in private Apps ist eingeschränkt.
- [ ] 37 **Anonymisierung:** Sensible Daten werden geschützt, bevor sie ein KI-Modell erreichen.
- [ ] 38 **Alternative:** Alle haben eine sichere KI-Lösung für den Arbeitsalltag.
- [ ] 39 **Schulung:** Mitarbeitende sind im Umgang mit KI geschult.
- [ ] 40 **Nachweis:** Die KI-Nutzung ist dokumentiert und für Audits nachvollziehbar.

Ihre Haken in Kapitel 5: ___ von 8 · Übertrag auf Seite 14

Aiverti + CORTADO

SO GEHT'S MIT AIVERTI UND CORTADO

Aiverti bringt sichere KI ins Unternehmen. Cortado bringt sie auf die mobilen Geräte.

- **Eine KI-Plattform statt Tool-Wildwuchs:** Aiverti bündelt KI-Modelle, Funktionen und Agenten auf einer Oberfläche. Admins legen fest, welche Gruppen was nutzen.
- **Rechtssicher von Anfang an:** Aiverti ist konsequent auf die Anforderungen von DSGVO und EU AI Act ausgerichtet, mit Sitz und Hosting in der EU.
- **Daten geschützt:** Sensible Daten werden anonymisiert, bevor sie ein KI-Modell erreichen. In Deutschland gehostete und lokale Modelle sind verfügbar.
- **Auf jedes Gerät per Cortado MDM:** Aiverti kommt als Web-App bzw. Web Clip zentral auf Smartphones und Tablets, ohne dass Mitarbeitende selbst etwas installieren.

SELBSTCHECK UND FAHRPLAN

Wie grün ist Ihre Ampel?

So geht’s: Haken pro Kapitel zählen, Zahl eintragen, Ampelfarbe markieren und die Kapitelnummer im passenden Feld notieren.

Grün · 7–8 Haken
Gut aufgestellt. Regelmäßig prüfen.
MEINE KAPITEL

Gelb · 4–6 Haken
Nachholbedarf. Lücken gezielt schließen.
MEINE KAPITEL

Rot · 0–3 Haken
Handlungsbedarf. Hier zuerst ansetzen.
MEINE KAPITEL

KAPITEL	IHRE HAKEN	AMPEL
1 · Mobile Device Management	☐ von 8	○ ○ ○
2 · Endpoint Security	☐ von 8	○ ○ ○
3 · Compliance	☐ von 8	○ ○ ○
4 · Datenschutz	☐ von 8	○ ○ ○
5 · KI auf dem Diensthandy	☐ von 8	○ ○ ○
Gesamt	☐ von 40	

Ihre nächsten 3 Schritte

1. **Übersicht schaffen.** Ohne vollständiges Inventar bleibt jede Maßnahme lückenhaft.
2. **Rote Kapitel zuerst.** Zwei Checkpunkte aus dem schwächsten Kapitel in den nächsten 30 Tagen umsetzen.
3. **Regeln festschreiben.** Festhalten, was gilt, und von der Technik durchsetzen lassen.

GELB ODER ROT?

Wir gehen die Liste mit Ihnen durch.

Kostenloser MDM-Sicherheitscheck mit den Expert.innen von Cortado.

Termin wählen

cortado.com/de/sicherheitscheck

ÜBER CORTADO

Mobile Device Management
Made in Germany.

Cortado Mobile Solutions ist der MDM-Spezialist für Apple und Android aus Berlin.

- **Alle Geräte, ein Portal.** iPhone, iPad, Mac, Apple TV und Android zentral verwalten, von der Zero-Touch-Einrichtung bis zum Offboarding.
- **Sicher von Anfang an.** Konfigurationsvorlagen für Geräterichtlinien, die sich an den Empfehlungen des BSI und den Anforderungen der DSGVO orientieren.
- **Daten in Deutschland.** Entwickelt in Berlin, betrieben im BSI-C5-zertifizierten Rechenzentrum in Frankfurt am Main.
- **Spürbar weniger Aufwand.** Bis zu 5x schnellere Bereitstellung und bis zu 75 % weniger Verwaltungsaufwand.

KOSTENLOSER MDM-SICHERHEITSCHECK

30 Minuten.
Ihre Checkliste. Unsere Expert.innen.

Wir gehen Ihre 40 Checkpunkte gemeinsam durch und zeigen Ihnen die nächsten Schritte. Unverbindlich und kostenlos.

Jetzt Termin wählen

cortado.com/de/sicherheitscheck

SELBST AUSPROBIEREN

Cortado MDM kostenlos testen

Richten Sie Ihre ersten Geräte selbst ein und erleben Sie, wie einfach zentrale Verwaltung sein kann. Kostenlos und unverbindlich.

cortado.com/de/testen

ERSPARNIS BERECHNEN

ROI-Rechner

Einfach Gerätezahl wählen und sehen, wie viel Zeit und Geld Cortado MDM in Ihrem Unternehmen spart.

cortado.com/de/roi

ISO 27001 GUTcert · AFNOR Group

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft 2026

OMR REVIEWS LEADER MOBILE DEVICE MANAGEMENT Q4/26

Capterra 5