CORTADO
MOBILE SOLUTIONS

BYOD-Leitfaden, inkl. DSGVO-Checkliste

eBook

Inhalt

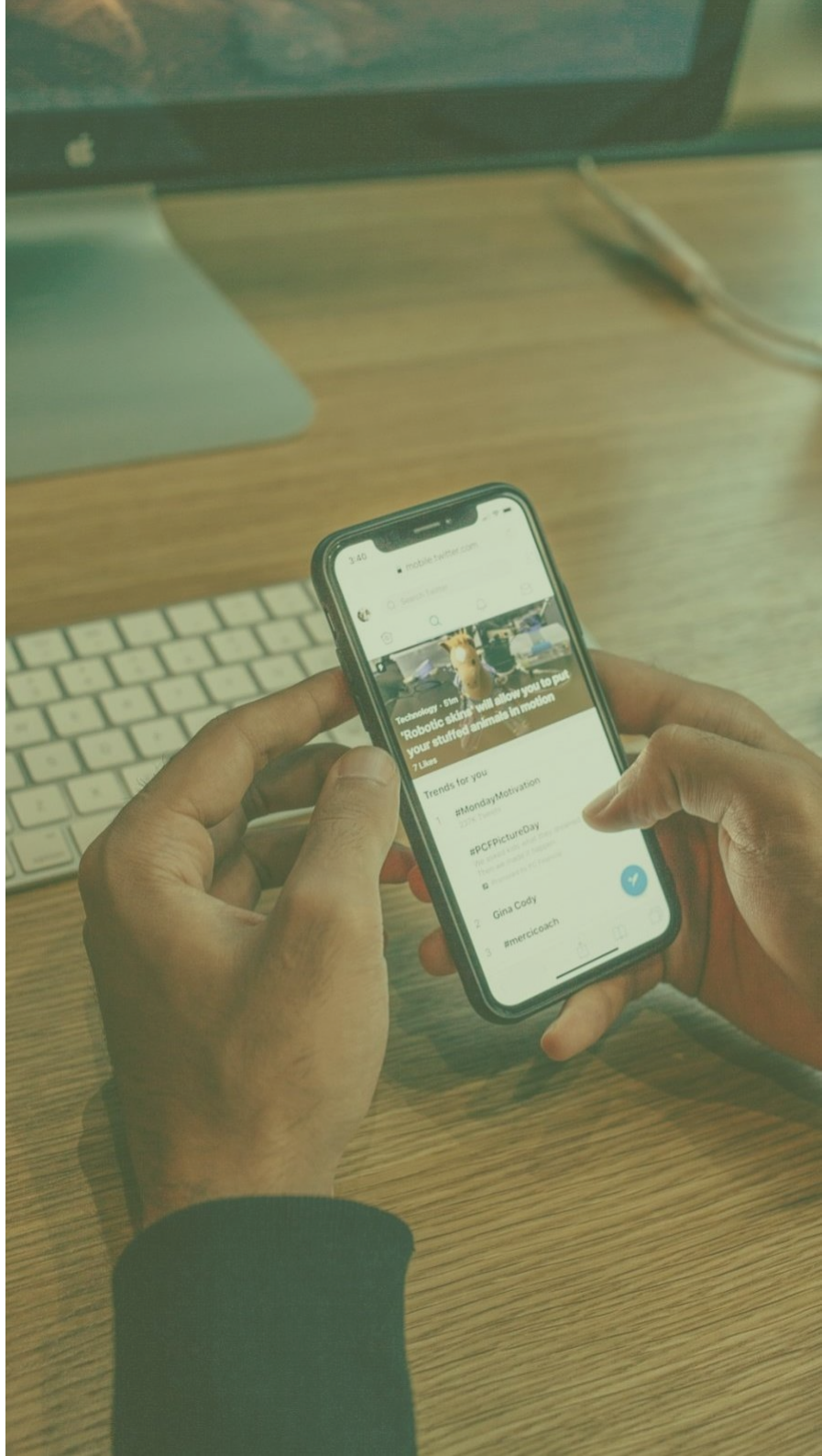
BYOD: Zurück im Rampenlicht

Aufgrund aktueller Entwicklungen unterscheidet sich Bring Your Own Device (BYOD) heute deutlich von seinem ursprünglichen Konzept.

Apple und Google haben BYOD für ihre Plattformen verbessert und neue Anmeldungsoptionen veröffentlicht. In der Zwischenzeit haben die Anbieter von Mobile Device Management (MDM) ihre Plattformen weiter optimiert, wodurch die Implementierung und Verwaltung von BYOD viel einfacher geworden ist. Für iPhone und iPads sind die jüngsten Änderungen (z.B. bei der Benutzerregistrierung) so einschneidend, dass sogar Organisationen mit bestehenden BYOD-Richtlinien dazu ermutigt werden, ihre Meinung zu überdenken.

All dies bedeutet, dass die Steigerung der Mitarbeiterproduktivität und -mobilität jetzt einfacher denn je ist. Leider sind die aktuellen Vorteile des BYOD-Modells immer noch nicht allgemein bekannt, und sowohl Unternehmen als auch viele Endbenutzer stehen dem Thema auf der Basis veralteter Informationen skeptisch gegenüber.

Angesichts der jüngsten Verbesserungen ist es das Ziel dieses eBooks, eine Neubewertung des BYOD-Konzepts vorzunehmen und einen Überblick darüber zu geben, was Organisationen erwarten können. Wir betrachten, welche Vorteile BYOD bietet, in welchen Bereichen das Modell am besten eingesetzt werden und welche organisatorischen Arbeitsprozesse es vereinfachen kann.



Was ist Bring Your Own Device?

Mobile Geräte, wie Smartphones, Tablets und Laptops, werden regelmäßig für die Arbeit benutzt, häufig auch im Home-Office oder unterwegs.

Wenn Unternehmen mobile Geräte zum Arbeiten bereitstellen, erfordert dies oft einen erheblichen Planungsaufwand und hohe Vorlaufkosten.

Wesentlich einfacher und günstiger ist es, den Mitarbeitern die sichere Nutzung ihrer eigenen Geräte mit Hilfe von Mobile Device Management-Software zu ermöglichen. Gleichzeitig müssen sich die Endbenutzer – aufgrund technischer Vorkehrungen - keine Sorgen machen, dass ihre Privatsphäre beeinträchtigt wird.

Dies wird allgemein als Bring Your Own Device (BYOD) bezeichnet.

In Wirklichkeit ist BYOD ein proaktiver Schritt in Richtung eines verbesserten Arbeitens aus der Ferne. Außerdem verringert BYOD das Risiko, dass Arbeitnehmer ihre persönlichen Smartphones ohne formelle Erlaubnis und damit auch ohne jegliche technischen Schutzmaßnahmen nutzen.

Quelle: **Microsoft Intelligence Security Association, 2020**

Um mobile Geräte korrekt in MDM-Lösungen zu integrieren, sollten die folgenden Aspekte berücksichtigt werden:

System-Zugriffsrechte & Apps

So wie jeder stationäre Desktop Zugriff auf Ressourcen und Anwendungen benötigt, so benötigen auch Mitarbeiter, die mobile Geräte verwenden, diesen Zugriff. MDM-Software ist hier nützlich, um den Geräten die richtigen Ressourcen zur Verfügung zu stellen und zu entscheiden, wer auf welche Daten zugreifen kann. Die Zugriffsrechte sollten hier – wie bei anderen Geräten - kontrolliert und nur zugeteilt werden, wenn sie vom Mitarbeiter wirklich benötigt werden.

Hardware mit Passwörtern sichern

Ein absolutes Muss, wenn es um die Integration von Smartphones und Tablets geht, ist die Absicherung des Gerätes selbst mit Hilfe von Passwörtern. Dies ist mit BYOD einfach zu realisieren. Bedenken Sie hierbei, dass die jüngste Entwicklung hin zu einer größeren Benutzerfreundlichkeit von BYOD dazu geführt hat, dass komplexe Passwörter, die die Benutzer oft frustrieren, nicht mehr standardmäßig durchgesetzt werden können (z.B. bei iOS-Geräten mit Benutzerregistrierung).

Schutz von Daten bei der Übertragung durch Verschlüsselung

Die verschlüsselte Datenübertragung ist die nächste obligatorische Sicherheitsmaßnahme, die für mobile Geräte erforderlich ist, um das unbefugte Lesen von Daten zu verhindern (Man-in-the-Middle-Angriffe). In der Regel ist eine State-of-the-Art-Verschlüsselung der Daten, die zwischen dem Gerät und dem Netzwerk übertragen werden, ausreichend. Wenn zusätzliche Sicherheit als notwendig erachtet wird, können die Daten in einen VPN-Tunnel oder andere proprietäre Tunnel, wie z.B. einen Mobile Data Service (MDS), eingebettet werden.

Herstellung der DSGVO-Konformität und Verhinderung von Datenverlusten

Wenn mobile Geräte Zugang zu Arbeitsplatzdaten erhalten, besteht die Gefahr, dass personenbezogene Daten, die ursprünglich für einen bestimmten Zweck gesammelt wurden (z.B. die E-Mail-Adresse oder Telefonnummer eines Kunden zum Zweck des Kundendienstes), für einen ganz anderen Zweck verwendet werden. Seit 2018 stellt dies einen Verstoß gegen die Allgemeine Datenschutzverordnung (DSGVO) der Europäischen Union dar und kann eine Geldstrafe von 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes einer Organisation nach sich ziehen. Organisationen sind daher verpflichtet, die unrechtmäßige Verarbeitung personenbezogener Daten zu verhindern. Ebenso ist es wichtig, dass sie auf Risiken hinweisen, die mit der Speicherung von Daten auf mobilen Geräten, USB-Sticks, CDs oder dem Verschieben von Daten auf private E-Mail-Konten oder Consumer-Cloud-Speicher verbunden sind.

Umgang mit von Malware ausgehenden Bedrohungen

Ein spezieller Malwareschutz ist für mobile Geräte mit Android oder iOS nicht unbedingt erforderlich - ihre Betriebssysteme sind mit einer Sandbox-Architektur konzipiert, die verhindert, dass Malware leicht gefährdete Bereiche des Geräts kompromittieren kann. Außerdem überprüfen Google Play und der App Store die Sicherheit der bei ihnen angebotenen Apps, was die Sicherheit ebenfalls erhöht. Es ist jedoch theoretisch möglich, dass Nutzer verseuchte Apps von nicht vertrauenswürdigen Quellen herunterladen. Dies stellt ein Risiko für das Unternehmensnetzwerk dar, und es ist wichtig, die Nutzer vorsorglich auf dieses Risiko hinzuweisen und zu überlegen, welche Abwehrmaßnahmen ergriffen werden können.

Was macht BYOD sicher?

Speziell entwickelte Mobile Device Management-Software, wie die von Cortado, ist in der Lage, die Probleme bei der Integration mobiler Geräte zu lösen, sei es für BYOD- oder firmeneigene Geräte. Ein weiterer entscheidender Aspekt, um BYOD sicher zu machen: Containerisierung.

Native Containerisierung auf mobilen Geräten bezieht sich auf die Trennung von arbeitsbezogenen Anwendungsdaten von den privaten Daten des Gerätebesitzers. Dadurch wird ein unsichtbarer "Container" speziell für arbeitsplatzbezogene Inhalte geschaffen.

Mit Hilfe der MDM-Software kann dieser Container mit allen Apps gefüllt werden, die für die produktive Arbeit erforderlich sind, unabhängig davon, ob sie intern entwickelt oder aus einem App-Store heruntergeladen wurden. Diese Apps werden vom Unternehmen verwaltet und per Fernzugriff auf die Geräte der Benutzer geschoben.

Wenn Geräte auf diese Weise verwaltet werden, ist es viel einfacher, sensible Daten zu schützen. Bei Bedarf – z.B. bei einem Geräteverlust - können der Container und alle unternehmensrelevanten Daten aus der Ferne vom Gerät entfernt werden.

Mit der Containerisierung ist es auch leichter, DSGVO-Verstöße zu verhindern. Wie bereits erwähnt, wurde diese weltweit relevante Datenschutzbestimmung von der EU im Jahr 2018 eingeführt und verlangt von den Organisationen die Einhaltung der Sorgfaltspflicht zum Schutz.

Einzigartige Stärken einer BYOD-Flotte

Geringere Anfangsinvestition = schnellere Rendite

Ein BYOD-Konzept ermöglicht es Ihnen, die Kapitalmenge zu reduzieren, die an die mobilen Geräte gebunden ist, die Ihre Mitarbeiter zur Arbeit benötigen. Unternehmen, die mit knappen Budgets arbeiten, können die Mitarbeiter dazu ermutigen, sich an den Kosten für neue Hardware zu beteiligen, so dass jeder aktuelle Geräte für wenig Geld nutzen kann.

Bequemer für Organisationen und Mitarbeiter

Für einige Arbeitsbereiche, in denen es auf Schnelligkeit und Flexibilität der Mitarbeiter ankommt, ist BYOD aufgrund seiner geringen Komplexität und schnellen Umsetzbarkeit am besten geeignet. Sie können per Fernzugriff schnell Zugriff auf Anwendungen und Ressourcen gewähren und sich dann nach Beendigung des Projekts oder der Beschäftigung leicht auflösen. Auch die Mitarbeiter profitieren, da die Funktionalität ihrer eigenen Geräte erweitert wird und sie keine Zeit damit verbringen müssen, den Umgang mit einem anderen Gerät zu erlernen.

Weniger Komplexität bedeutet auch weniger Management

Allgemeine Verwaltungsaufgaben oder gelegentliche Helpdesk-Anrufe treten unabhängig von der Art der Geräteverwaltung auf und verbrauchen Ressourcen. BYOD macht die Verwaltung so rationell wie möglich: Ein Vorteil: Die Benutzer verwenden die Geräte, mit denen sie bereits vertraut sind. Support-Tickets im Zusammenhang mit neuen Geräten sind daher seltener anzutreffen.

BYOD mit Android-Geräten

Wie BYOD implementiert wird, ist von Gerät zu Gerät unterschiedlich und hängt auch von den jeweiligen Betriebssystemen und Versionen ab. Android, Googles Betriebssystem für mobile Geräte, bietet seit mehreren Jahren ein sicheres und einfach zu implementierendes BYOD-System an. Dank der attraktiven Preise für Android-Geräte und der großen Auswahl an Geräten besitzen viele Mitarbeiter bereits Android-Geräte, die für BYOD geeignet sind. Mit nur wenigen Klicks können die Mitarbeiter die vorhandenen integrierten Unternehmensfunktionen nutzen und persönliche Geräte in Arbeitswerkzeuge verwandeln.

Sobald ein privates Gerät mit MDM-Software aktiviert ist, werden der Arbeitsbereich und die persönlichen Daten getrennt. Das Hauptmerkmal auf Android-Geräten ist das Arbeitsprofil, das auf der rechten Seite näher betrachtet wird. Dies ist die primäre Methode zur Datentrennung und unerlässlich für ein sicheres BYOD.

Für die richtige Balance zwischen Arbeit und Entspannung bietet Android eine Reihe nützlicher Features. Mit dem Fokusmodus können Mitarbeiter Apps ausblenden, die sie bei wichtigen Aufgaben ablenken. BYOD-Benutzer können auch eine spezielle "verwaltete" Version des Google Play-App-Stores verwenden, die von der Organisation kuratiert werden kann. Dadurch hat jeder Mitarbeiter die Freiheit, die von ihm benötigten Apps von einer sorgfältig ausgewählten "Whitelist" herunterzuladen.

Viele Bedenken hinsichtlich der Eignung von Android haben sich mittlerweile überholt. Inzwischen verfügt Android über viele selbsteingebaute Sicherheitsmaßnahmen. Eine Gartner-Studie aus dem Jahr 2017 bewertete Googles Betriebssystem sogar als sicherer als das damalige iOS. Obwohl beide Plattformen heute relativ gleichwertig sind, bietet Android wohl immer noch die benutzerfreundlichste und beste BYOD-Erfahrung.

Androids Work Profile

Androids Work Profile

Das Android- Arbeitsprofil ist die eingebaute Technologie, die arbeitsbezogene Daten von persönlichen Daten getrennt hält.

Obwohl das Grundkonzept und die Implementierung des Arbeitsprofils seit mehreren Jahren konstant geblieben sind, haben visuelle Veränderungen die Benutzerfreundlichkeit und Funktionalität von BYOD für die neuesten Geräte weiter verbessert.

Die vom Unternehmen verwalteten Apps sind durch einen blauen Koffer klar erkennbar und werden dupliziert, um eine persönliche "unmanaged" Version der gleichen App anzubieten. Getrennte Instanzen aller Anwendungen sind daher zulässig, und verwaltete Versionen von Anwendungen können Geschäftsdaten leicht isolieren und Datenverluste verhindern.

Mit diesem digitalen Arbeitsplatz können Anwender ihr Android- Gerät wie gewohnt nutzen – und trotzdem sind die Unternehmensdaten geschützt. Wichtig für die Benutzer ist, dass das Android- Arbeitsprofil klar abgrenzt, welche Bereiche auf dem Gerät des Mitarbeiters verwaltet werden und welche nicht. Sie wissen, dass ihre Aktionen von ihrem Arbeitgeber verwaltet werden, sobald sie auf die mit dem Koffer gekennzeichntet Version einer App klicken.

Schließlich können das gesamte Arbeitsprofil und alle Daten der Organisation aus der Ferne gelöscht werden, und der Benutzer sieht nur, dass sein Arbeitsprofil entfernt wurde.

BYOD mit iOS

Vor der Einführung der Benutzerregistrierung („User Enrollment“) im Jahr 2019 ging ein sicheres BYOD mit iOS-Geräten auf Kosten der Privatsphäre der Benutzer. Während es den Arbeitnehmern möglich war, ihre eigenen Geräte mit MDM zu verbinden und für die Arbeit zu nutzen, waren die Admins in der Lage, fast alle Benutzerdaten einzusehen, unabhängig davon, ob sie etwas mit der Arbeit zu tun hatten oder nicht.

Hinter den Kulissen fanden inzwischen viele Veränderungen statt, die auch private iPhones und iPads wirklich arbeitsplatztauglich machten. Seit iOS 13 bietet iOS bei BYOD eine größere Benutzerakzeptanz, mehr Privatsphäre für die Endbenutzer, eine einheitlichere Verwaltung und viele weitere Verbesserungen hinsichtlich der Sicherheit und der Performance. Mit der Benutzerregistrierung werden alle verwalteten Anwendungen und Konfigurationen mit einer neuen verwalteten Apple ID verknüpft, sobald ein Benutzer seine Geräte mit der MDM-Software des Unternehmens registriert. Wie bei Android wird damit die notwendige Datentrennung zwischen den beiden "Personas" auf dem Gerät hergestellt. Unternehmen können die arbeitsbezogenen Daten, auf die das Gerät Zugriff hat, sicher verwalten, während die Privatsphäre der Benutzer geschützt bleibt. Die Kommunikation mit dem Unternehmen kann über separate VPNs für jede Anwendung weiter abgesichert werden, wodurch die Notwendigkeit eines geräteweiten VPNs vermieden wird. Schließlich können die verwalteten Daten bei Bedarf einfach gelöscht werden.

Auf iOS- und Android-Geräten ist BYOD recht ähnlich - sicheres und benutzerfreundliches BYOD ist auf beiden Typen leicht zu implementieren. Eine bemerkenswerte Ausnahme ist jedoch das Fehlen von doppelten "Arbeits"-Anwendungen auf iOS. Wie die Benutzerregistrierung im Vergleich zu Apples anderem Verwaltungsmodus aussieht, ist auf der rechten Seite aufgeführt.

Benutzer- Registrierung:

Im Vergleich zu Android ist die Datentrennung nicht so deutlich erkennbar.

Für die IT- Abteilungen von Unternehmen ist jetzt nur die Wahl zwischen der Benutzerregistrierung („User Enrollment“) oder der überwachten betreuten Registrierung („Supervised“; die für firmeneigene Geräte gilt) von Bedeutung. Administratoren sollten sich für eines der beiden Modelle entscheiden und ihre vorhandene Geräteflotte entsprechend aktualisieren. Mit BYOD und Benutzerregistrierung sind die Kontrollen für Administratoren begrenzt:

Richtlinien und Befehle

Festlegung der Sperrcodelänge, Komplexität usw.

Sperren der die Geräte in Notfällen

Siri deaktivieren, wenn das Gerät gesperrt oder entsperrt ist

Ausblenden von Benachrichtigungen, Kontrollzentrum und Heute- Ansicht aus dem Sperrbildschirm

Passwort erzwingen beim Koppeln von AirPlay- Geräten

Backups verschlüsseln

Sicherungen und Synchronisierung von Enterprise Books ermöglichen

Angabe, ob unverwaltete Anwendungen auf verwaltete Anwendungskontakte zugreifen können

Angabe, ob verwaltete Apps Daten von persönlichen Apps herunterladen können (und umgekehrt)

Forcieren der Safari Betrugswarnung

Erlaubnis von AirDrop für nichtverwaltete Anwendungen

Aktivieren/Deaktivieren der iCloud- Synchronisierung für verwaltete Anwendungen

Abrufen von Geräteinformationen (z.B. Modell oder Akkustand) & Sicherheitsstatus

Profil- Management

Austausch (ActiveSync) > WLAN > Zertifikate > App- Layer- VPN > SCEP-Konfiguration

BYOD und DSGVO-Checkliste

Wie bereits erwähnt, sind alle Unternehmen, die Teil der Europäischen Union sind oder Daten europäischer Bürger verarbeiten, zur Einhaltung der Datenschutzgrundverordnung (DSGVO) verpflichtet. Es liegt in der Verantwortung des Arbeitgebers, selbst wenn es sich im Rahmen eines BYOD-Programms um Geräten in Privatbesitz handelt, angemessen nachzuweisen, dass sensible Daten durch klar dokumentierte Prozesse und Verfahren geschützt sind.

Unsere Website enthält weitere kostenlose White Papers und Blog-Posts, die sich eingehender mit dem Thema Datenschutz befassen. Den Rahmen dieses E-Books würde das Thema sprengen. Dennoch ist es wichtig, die Bedeutung dieses Themas hervorzuheben. Die folgende Checkliste gibt einen kurzen Überblick, was bei der Planung des BYOD-Konzepts zu berücksichtigen sind.

- Was: Bestimmen Sie die Arten von Daten, die Sie verarbeiten und die Sie gemäß DSGVO angemessen schützen sollen.
- Wer: Bestimmen Sie, welche Benutzer Zugang zu sensiblen persönlichen Daten haben sollen und kontrollieren Sie die Zugriffsrechte entsprechend, zum Beispiel mit Hilfe einer Verwaltungslösung für mobile Geräte.
- Wo: Stellen Sie fest, wo sensible Daten gespeichert sind. Stellen Sie sicher, dass sie angemessen geschützt sind, und ergreifen Sie Maßnahmen, damit sie nicht an anderer Stelle gespeichert werden können.
- Warum: Klären Sie Ihre Benutzer vor der Einführung von BYOD über den Datenschutz auf. Kommunizieren Sie, welche Anwendungen größere Risiken verhindern und legen Sie klare Verfahren für den Umgang mit sensiblen persönlichen Daten fest.

Fazit

Dank einer Fülle von aktuellen Änderungen unterscheidet sich Bring Your Own Device (BYOD) heute deutlich von seinem ursprünglichen Erscheinungsbild. Nach mehreren Jahren haben Apple und Google, die Unternehmen mit den beiden meistgenutzten Betriebssystemen für mobile Geräte, BYOD zu einem verfeinerten Konzept geformt. In dieser Form eignet es sich für eine große Zahl von Einsatzfällen.

Und auch die Anbieter von Mobile Device Management (MDM), deren Lösungen für die BYOD-Implementierung benötigt werden, haben ihre Hausaufgaben gemacht. Sie sprechen Empfehlungen aus, welche Änderungen vorgenommen werden sollten, und entwickeln immer einfachere Werkzeuge für die Zusammenarbeit mit den IT-Abteilungen.

Obwohl BYOD mit iOS und Android noch einige Schwachpunkte hat: BYOD hat sich insgesamt verbessert und hat sich zu einem homogeneren und einfacheren Gerätemanagement entwickelt.

Bei der BYOD ist es wichtig, dass den Benutzern die Grenzen der BYOD und die Rolle, die sie bei der Reduzierung von Risiken spielen, bewusst gemacht werden. Falls erforderlich, kann dies auch durch einen Vertrag zwischen Arbeitgeber und Arbeitnehmer geregelt werden.

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

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

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

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