MATRIX42

Ist Ihre Firma bereit für Mobilität?

Erleben Sie die Produktivität und Flexibilität der Mobilität und bewahren Sie gleichzeitig Ihre Daten und Geräte sicher und in Übereinstimmung mit den Vorschriften auf.

INHALTSVERZEICHNIS

Das dynamische mobile Unternehmen

Das heutige Arbeitsumfeld unterscheidet sich stark von dem früherer Jahre. Heute kann ein Großunternehmen nur wettbewerbsfähig bleiben, wenn es dafür sorgt, dass die richtigen Mitarbeiter Zugang zu den richtigen Ressourcen, Hilfsmitteln, Daten und Informationen haben - und das auf sicherem Weg. Diese vielschichtige Aufgabe wird noch durch eine sehr dynamische Belegschaft erschwert; Mitarbeiter befinden sich im Laufe eines Tages an mehreren Orten und arbeiten mit mehreren Geräten - sowohl mit persönlichen als auch betriebseigenen. Zudem stellt die heutige Belegschaft Erwartungen hinsichtlich Konnektivität und Flexibilität, die es zuvor nicht gegeben hat.

- Lieferungen von Tablet-Computern an Unternehmen sollen erwartungsgemäß von 13,6 Millionen Geräten im Jahr 2011 auf 96,3 Millionen Geräten für 2016 ansteigen.[1]
- Die durchschnittliche Anzahl der Mobilgeräte, die ein Mitarbeiter mit sich trägt, ist von 2,7 im Jahr 2011 auf 3,5 angestiegen. 92 Prozent der mobilen Mitarbeiter glauben, dass ihre Smartphones sowohl für den geschäftlichen als auch den persönlichen Gebrauch aktiviert werden sollten. [2]
- 86 Prozent der Unternehmen erlauben entweder den Gebrauch privater, an das Netzwerk angeschlossene Geräte oder bewegen sich in diese Richtung. [3]
- Eine Umfrage von Harris Interactive und CareerBuilder vom Juni 2012 stellte fest, dass 69 Prozent der Mitarbeiter im Alter von 25 bis 34 auch außerhalb der Bürostunden arbeiten. [4]
- Dem Bericht „Q3 iPass Mobile Workforce“ vom September 2012 zufolge arbeiten mobile Mitarbeiter bis zu 20 Stunden pro Woche zusätzlich außerhalb des Büros.

Diese wachsende Verbreitung von Mobilgeräte, die mit dem Unternehmensnetzwerk verbunden sind, zwingt Leiter der Informationstechnologie dazu, einen Ausgleich zwischen ihrer Verantwortung für die Sicherheit und Integrität der Unternehmensdaten und den Erwartungen der Arbeitskräfte zu schaffen. Die neue Generation von Mitarbeitern erwartet, dass IT die Verwendung beliebiger Geräte - persönlicher und vom Unternehmen bereitgestellter - für den Zugriff auf Unternehmensnetzwerke zulässt.

Unternehmen, die sich an strikte Sicherheits- und Zugriffsvorschriften gewöhnt haben, stehen vor neuen Situationen, die sich nicht einfach und problemlos lösen lassen, vor allem, wenn die erforderlichen Richtlinien nicht vorhanden sind oder ihnen die Mittel fehlen, diese durchzusetzen:

- Ein Mitarbeiter kauft ein iPhone und fordert die IT-Abteilung auf, es für den Empfang von E-Mails aus dem Büro und den Zugriff auf das firmeneigene Intranet zu konfigurieren. *Haben Sie dafür eine IT-Richtlinie in Ihrem Unternehmen?*
- Ein Geschäftsleiter der Firma kauft iPads für das ganze Team, um die Produktivität zu steigern. Er holte dafür keine Erlaubnis ein. Nun laden Teammitglieder Dutzende von Anwendungen herunter und verwenden sie zur Erledigung ihrer Arbeit am Arbeitsplatz und unterwegs. *Verfügen Sie über Unternehmensrichtlinien für die IT-Lizenz-Compliance?*
- Der Leiter des Finanzwesens einer Firma verliert sein neues Android-Gerät auf einer Geschäftsreise. Es enthält Finanzdaten der Firma sowie eine Liste der 500 wichtigsten Kunden des Unternehmens mit detaillierten Kontaktdaten. *Hat Ihr Unternehmen IT-Sicherheitsrichtlinien für einen solchen Fall?*

[1] „Worldwide Enterprise Tablet Market Forecast Report (Prognose zum weltweiten Markt für Tablet-PCs in Unternehmen)“, Infinite Research, Januar 2012
[2] „iPass Global Mobile Workforce Report - Q1. Quartal 2012 (iPass Bericht zur globalen weltweiten Belegschaft - 1. Quartal 2012)“
[3] „2012 State of Mobile Security (Stand der mobilen Sicherheit)“, Information Week, Mai 2012
[4] „How Millennials Work Differently From Everyone Else (Warum Millennials anders arbeiten als andere Arbeitskräfte)“ Forbes, 13. Sept. 2012.

Wie Tabelle 1 zeigt, haben Firmen, Endanwender und IT-Abteilungen verschiedene Fragen und Bedenken zur Verwendung von Smartphones und Tablets im Unternehmen. Gemäß einer kürzlichen Umfrage des CIO Magazine bezeichneten 87 Prozent der Teilnehmer die Produktivitätsvorteile - vor allen anderen Faktoren - als treibende Kraft für die Investitionen ihrer Firma in die Mobiltechnologie. Die Umfrage lieferte weitere Beweise, dass die steigende Produktivität sowie andere Vorteile von Mobillösungen in einem Unternehmen hoch geschätzt werden.

Die Rolle der IT-Abteilung besteht darin, einen Ausgleich zu schaffen zwischen den Forderungen der immer anspruchsvolleren, technisch versierten Anwendern, den Ansprüchen der Geschäftsführer in Bezug auf das unternehmenskritische Wachstum und die Entwicklung des Geschäfts einerseits und dem Bedarf an Sicherheit und Kontrolle der Unternehmensdaten und Vermögenswerte andererseits. Dies wird noch erschwert durch die Kombination der ständig wachsenden Menge an Daten und Vermögenswerten.

Tabelle 1: Firmenweite Fragen zum Thema Mobilgeräte im Unternehmen

Geschäft	Endanwender	Endanwender
Wie können Smart-Geräte unseren Mitarbeitern helfen, produktiver zur arbeiten?	Habe ich überall und jederzeit Zugang zu den Informationen und Ressourcen, die ich für die effiziente Erledigung meiner Arbeit brauche?	Wie kann ich den Zugriff auf vertrauliche Unternehmensdaten auf einem abhanden gekommenen Gerät oder von einem früheren Mitarbeiter verhindern?
Verbessert die Flexibilität der Smart-Geräte die Arbeitsmoral und Arbeitszufriedenheit der Mitarbeiter?	Kann ich mein persönliches Gerät für den Zugriff auf das Unternehmensnetzwerk und meine E-Mail verwenden? Oder kann ich persönliche Anwendungen auf meinem Firmengerät verwenden?	Halten wir uns an die Vorschriften in Bezug auf die Anwendungen, die unsere Mitarbeiter auf ihren Geräten ausführen?
Können wir Kosten sparen, wenn wir unseren Mitarbeitern erlauben, ihre persönlichen Geräte für die Arbeit zu verwenden?	Gibt es eine schnellere Methode, meinem Gerät Apps hinzuzufügen oder bereitzustellen, ohne auf die Antwort von IT auf mein Helpdesk-Ticket warten zu müssen?	Wie verhindere ich, dass Endanwender IT-Vorgänge umgehen und die Firma in Gefahr bringen?

Dieses Dokument beschreibt die größten Herausforderungen, denen Firmen im Zusammenhang mit ihrer Mobilitätsstrategie gegenüber stehen. Es zeigt, wie Unternehmen effektive BYOD-Richtlinien (BYOD = bring-your-own-device; „bring dein eigenes Gerät“) implementieren können sowie fünf wichtige Schritte, die eine unternehmensweite Lösung für die Verwaltung mobiler Geräte beinhalten sollte.

Die wichtigsten Herausforderungen der Mobilität

Intelligente Geräte (bzw. ‘Smart Devices’) verbreiten sich zusehends in Unternehmen und an virtuellen Arbeitsplätzen und Mitarbeiter greifen mit mehreren Geräten von verschiedenen Orten auf Firmenressourcen zu. All dies bewirkt, dass Arbeit nicht mehr ortsgebunden ist, sondern zu einer Tätigkeit wird, die überall stattfinden kann. Dies bietet einem Unternehmen viele Möglichkeiten, schafft aber auch neue Herausforderungen.

Mobilität ist eine der größten Gefahren für die Sicherheit von Unternehmensdaten.
Firmen bemühen sich, ihre Mobilgeräte sicher zu verwalten, was höhere Investitions- und Betriebskosten verursachen kann und das Sicherheitsrisiko eines Unternehmens stark erhöht. Eine Lösung muss implementiert werden, die einen Sicherheitsstandard für alle (firmeneigene und persönliche) Mobilgeräte erstellt, vertrauliche Unternehmensdaten schützt und regulatorischen Anforderungen nachkommt.

Eine getrennte Verwaltung von Mobilgeräte ist ineffizient und teuer
Der Einsatz von Tools, die von einem Mobilfunkbetreiber oder Geräteheresteller bereit gestellt werden und jedes Gerät einzeln verwalten, oder das Erstellen von proprietären Infrastrukturen und Tools zur Unterstützung einer Managementinitiative für Mobilgeräte ist zeitaufwändig und teuer. Zudem ist die Integration mit Infrastrukturen von Drittherstellern kompliziert und schwierig.

Die Verbreitung und Vielseitigkeit der Geräte innerhalb des Unternehmens erschwert die Arbeit der IT-Abteilung
Heutzutage muss ein Unternehmen mehrere mobile Plattformen verwalten. Für die Firmen war es einfacher, Desktop-PCs und Laptops mit einem einzigen Betriebssystem standardmäßig zu verwalten, einige Hardwareoptionen festzulegen und Standardkonfigurationen für eine einfachere Verwaltung zu erstellen. Mit Mobilgeräten verwenden Mitarbeiter ihr bevorzugtes Gerät, unabhängig davon, ob das Betriebssystem iOS, Android, Windows oder ein anderes ist. Zudem gibt es mit Android und Windows viele verschiedene, einzigartige Geräte. Die IT-Abteilung muss nicht nur alle Mobilgeräte innerhalb eines Unternehmens identifizieren können, sondern sie muss auch wissen, wie jedes einzelne Gerät und das betreffende Betriebssystem verwaltet werden muss.

Die Bereitstellung, Konfiguration und Sicherung der Mobilgeräte kann zeitaufwändig und teuer sein
Die Komplexität der Mobilgeräteverwaltung führt zu einem Mangel an Standardisierung und Sicherheit. Die Konfiguration des Zugriffs auf HVD (Hosted Virtual Desktops) oder Cloud-Diensten über Saas (Software As A Service) und VDI (Virtual Desktop Infrastructure) auf Mobilgeräte ist ebenfalls komplex und eine Herausforderung, wenn eine Management-Lösung diese Bereiche nicht unterstützen kann.

Ist Ihre Firma bereit für Mobilität?

Die gleiche Studie in Information Week, die festgestellt hat, dass 86 Prozent der Unternehmen die Verwendung von persönlichen Geräten entweder bereits erlauben oder dies vorhaben, hat ebenfalls gezeigt, dass nur 40 Prozent der Firmen die Palette unterstützter Geräte einschränkt und verlangt, dass Anwender sie mit einem Mobilgeräte-Management (MDM)-System verbinden. Viele scheinen sich darauf zu verlassen, dass Anwender den Vorschriften zustimmen und diese auch einhalten. Wenn man bedenkt, wie viele Ressourcen die Firmen über die Jahre hinweg in die Sicherheit ihrer Daten investiert haben, scheint dies ein sehr unnötiges Risiko zu sein. Das ist vergleichbar mit einem Hausbesitzer, der alle Fenster und Türen verriegelt und dann doch das Garagentor weit offen lässt.

Vernachlässigt oder verzögert Ihre Firma die Einführung einer ganzheitlichen Mobilverwaltungsstrategie und -lösung für all Ihre Unternehmensgeräte und Tablets, kann dies leicht zu Ausfallzeiten für Anwender, einem erhöhten Sicherheitsrisiko und steigenden IT-Kosten führen. IT-Administratoren müssen vollständige Kontrolle über den Gerätezugriff und andere Compliance-bezogene Verwaltungsaktivitäten sowie über Änderungen an der Konfiguration im Zusammenhang mit dem Zugriff auf geschäftlichen Diensten haben (z. B. Sicherheitsanwendungen, Firewalls, Netzwerkzugriff, Patches, Richtlinien usw.). Dazu gehört auch die Fähigkeit, persönliche Anwenderdaten von den Unternehmensdaten unterscheiden zu können, um BYOD-Initiativen zu unterstützen und gleichzeitig den Datenschutz zu gewährleisten.

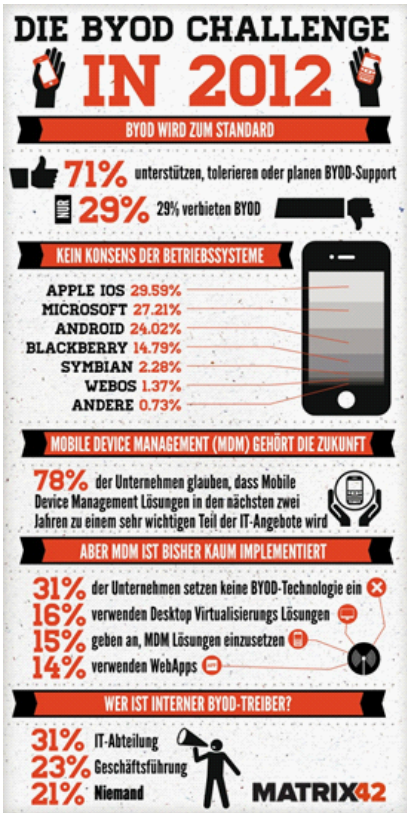
BYOD zu Ihren Konditionen

Die meisten Unternehmen haben nun eine BYOD-Richtlinie (‘Bring your own Device’) übernommen bzw. planen, eine zu übernehmen. Unternehmen können somit Geld sparen, indem sie einige der Hardwarekosten auf die Mitarbeiter abwälzen, die Zufriedenheit und Produktivität der Mitarbeiter steigern und mit dem Ziel der Sicherheit eine Partnerschaft mit Mitarbeitern aufbauen, damit kein Grund mehr besteht, den IT-Prozess zu umgehen.

Eine Umfrage unter beinahe 600 IT-Experten auf dre CeBIT 2012 zeigte, dass BYOD zum Standard wird. 71 Prozent unterstützen, tolerieren oder planen BYOD-Support. Siehe die Infografik >>>

Beinahe zwei Drittel der Umfrageteilnehmer gibt an, dass ihre IT-Abteilung eine gewisse Akzeptanz für BYOD zeigt, und 78 Prozent glaubt, dass Mobile Device Management (MDM) in den nächsten zwei Jahren eine bedeutende Rolle in ihrem IT-Angebot spielen wird.

Damit Firmen heutzutage wettbewerbsfähig bleiben können, ist es unerlässlich, dass sie Endanwendern über alle Handheld-Geräte und Tablets überall und jederzeit Zugriff auf die Firmenressourcen und



Daten gewähren. Für Firmen wird BYOD immer mehr zu einem Mandat statt zu einer Option. Mit technisch erfahrenen Anwendern, die ihre eigenen Geräte konfigurieren können, wenn sie nicht schnell genug Zugriff erhalten, haben Firmen keine andere Wahl als einen Weg zu finden, diese Anwender zufrieden zu stellen.

Glücklicherweise können IT-Experten mithilfe von MDM-Lösungen ihren Anwendern die gewünschte Flexibilität geben, während sie gleichzeitig die nötige Kontrolle behalten. Wesentlich für eine erfolgreiche BYOD-Richtlinie ist die Nutzung der richtigen Tools, die Mitarbeitern eine größere Auswahl geben und gleichzeitig mithilfe durchsetzbarer Unternehmensrichtlinien die Sicherheit wahren.

Fünf wichtige Schritte für die Verwaltung der Mobilität bei reduziertem Risiko

Hochdifferenzierte Mobilgeräte und Anwendungen sind für den Erfolg eines Unternehmens von entscheidender Bedeutung. Die Verwaltung der aktuellen Mobiltechnologie, die von Mitarbeitern verwendet wird und die Sicherstellung künftiger Bereitstellungen, kann eine echte Herausforderung sein. Unternehmen benötigen eine umfassende Management-Lösung für Smartphones und Mobilgeräte, die die Bereitstellung, Sicherheit, Überwachung, Verwaltung und Unterstützung beinhaltet. Eine solche Lösung muss über die Technologie verfügen, die diese Prozesse über mehrere Gerätetypen und Mobilbetriebssysteme hinweg vereinfacht. Im Folgenden sind fünf Schritte aufgeführt, die Teil einer ganzheitlichen MDM-Lösung sind, zusammen mit wichtigen Funktionen, die untersucht werden sollten:

Schritt 1: Automatisierte Bereitstellung der Geräte

- Automatisieren aller Aufgaben, die ein Gerät für den Geschäftsgebrauch vorbereiten, unter anderem E-Mail-Einrichtung, Anwendungszugriffe, Kennwortrichtlinien usw.
- Aktivieren der Geräte mithilfe von SMS, E-Mail, URL und anderer flexibler Optionen
- Anmelden von Unternehmens- und Mitarbeitergeräten, entweder einzeln oder gebündelt
- Authentifizieren der Anwender und Geräte mithilfe grundlegender und Verzeichnisservices-basierter Authentifizierung
- Sofortige Remote-Konfiguration („Over-the-Air“) der Richtlinien, Einstellungen, Zertifikate und Zugriffe auf Unternehmenskonten
- Drahtlose Bereitstellung interner und empfohlener Apps über den Unternehmens-App-Katalog

Schritt 2: Sicherung der Geräte und Reduzierung des Risikos

- Sicherstellen, dass autorisierte und konforme Geräte sicheren Zugriff auf Geschäftsressourcen und -konten haben
- Schutz der persönlichen und unternehmenseigenen Daten sowie des gesamten Geräts mit Hilfe von Verschlüsselung und Kennwortrichtlinien
- Verhindern des Gebrauchs nicht autorisierter Geräte durch Sperren von Gerätefunktionen und verstärkte Einschränkungen

- Überprüfung der Geräte auf Einhaltung der Unternehmensrichtlinien, Einstellungen, Anwendungen, Drittanbietern und mehr
- Automatisieren der Geschäftsrichtlinien für nicht konforme oder gehackte (Jailbroken) Geräte
- Schützen verlorener oder gestohlener Geräte durch Sperr- und Löschfunktionen

Schritt 3: Überwachung der Geräte

- Überprüfen der Geräte, der Netzwerkgesundheit und der Statistiken auf Ausnahmen
- Verfolgen der Anwenderaktivitäten wie App-Downloads, Voice, SMS und Datennutzung und Vergleichen mit vordefinierten Schwellenwerten und White- oder Blacklists
- Überwachen des Systemzugriffs und der Konsolen-Anwenderaktivitäten mithilfe detaillierter Ereignisprotokolle
- Einrichten von Warnungen und automatisierten Geschäftsregeln für spezifische Geräte- oder Netzwerkaktionen, Anwenderaktionen oder für die Systemleistung
- Generieren umsetzbarer Berichte mit automatischer Verteilung an das gesamte IT-Team
- Erstellen automatisierter Prozesse, um auf Probleme proaktiv reagieren zu können

Schritt 4: Verwaltung von Anwendungen

- Effizientes Verwalten und Kontrollieren der Anwendungen über alle Geräte hinweg
- Bereitstellen von Self-Service-Zugriff für genehmigte Anwendungen unter Verwendung des Service-Katalogs der Firma
- Optimieren und Automatisieren der Verwaltung mobiler Vermögenswerte und des Inventars
- Aktualisieren und Bereitstellen neuer Richtlinien, Einstellungen, Zertifikate, Apps, Software und Zugriff auf die Unternehmenskonten - Exchange Active Sync, Wi-Fi, VPN, CA, LDAP und mehr - remote „Over-the-Air“
- Weitergeben von Konfigurationsprofilen, Apps, Software oder Remote-Sperr-/Löschbefehlen auf Verlangen, zu einer geplanten Zeit oder bei der nächsten Anmeldung einer Gerätegruppe bzw. eines Geräts

Schritt 5: Unterstützung von Anwendern und Geräten

- Mobile Arbeitskräfte produktiv halten, indem Probleme mit Geräten schnell und effizient diagnostiziert und in Echtzeit behoben werden
- Remote-Diagnose der Geräte zur Identifizierung von Problemen
- Bereitstellen von Remote-Support für mobile Anwender und Kommunikation per SMS von der Konsole aus
- Remote-Kontrolle eines Geräts für leistungsfähigere Fehlerbehebung
- Bereitstellen von Remote-Verwaltungsmöglichkeiten für Anwender über ein Self-Service-Portal
- Fehlerbehebungen und Behandeln von Systemproblemen über ein integriertes Fallmanagement-System

Der Vorteil von Matrix42

Das Matrix42 Mobile Workplace Management erleichtert den Start eines BYOD-Programms, das gleichzeitig die Anforderungen der Mitarbeiter und der IT-Abteilung erfüllt, entweder über ein Cloud-basiertes Angebot oder mithilfe einer Plattform vor Ort. Mitarbeiter können mithilfe ihrer bevorzugten Mobilgeräte das Netzwerk aufrufen, Support anfordern und Services erhalten, während die IT-Abteilung die Kontrolle über alle Mobilgeräte des Unternehmens behält, besseren Service anbieten und Kosten reduzieren kann.

Matrix42 ist das erste Unternehmen, das das MDM-Management mit dem ITSM (IT Service Management) integriert und Anwendern ermöglicht, im Rahmen von BYOD-Richtlinien über ihren eigenen oder einen von Matrix42 bereitgestellten ServiceNow-Katalog jederzeit und überall Dienste und Geräte anzufordern und bereitzustellen. Durch diese automatischen Prozesse werden gängige, sich wiederholende IT-Aufgaben vom Helpdesk verlagert; die Endanwender lösen ihre IT-Probleme auf Abfrage und die Supportkosten werden um 70 Prozent reduziert.

Die Einbeziehung von Lizenz- und Asset-Management zusätzlich zur Aufzeichnung der Software-Lizenzen, Assets und Verträge ermöglicht die Analyse der Arbeitsprofile des Endanwenders, um dessen bevorzugten Geräte, Apps und Services zu bewerten. IT-Administratoren können sicherstellen, dass alle an das Netzwerk angeschlossenen Mobilgeräte in den Bestand aufgenommen, gesichert und im Rahmen der Unternehmensrichtlinien verwaltet werden, ganz gleich, ob sie BYOD für die Mitarbeiter unterstützen oder ob die Geräte dem Unternehmen gehören

Zusammenfassung

Die Entwicklung einer mobilen Strategie ist für den Erfolg von Initiativen zur Mobilität von Unternehmen von großer Bedeutung. Noch wichtiger ist, dass sich CIOs und IT-Direktoren die Zeit nehmen, die Strategien, Lösungen und Produkte zu überdenken - denn Entscheidungen, die auf den ersten Blick klar und leicht erscheinen, sind es oft nicht. IT-Abteilungen sollten sich auch eine Umstrukturierung ihrer Unternehmen überlegen, die dem täglichen und weit verbreiteten Bedarf an Verwaltung von Mobilgeräten gerecht wird. Wenn sich Mobilgeräteexperten in Ihrer IT-Abteilung hauptsächlich auf die Infrastruktur konzentrieren, dann werden ihre Kompetenzen nicht voll ausgeschöpft. Eine Möglichkeit, die Verwaltung der Mobilgeräte in den Mainstream der IT-Funktionen zu bringen, ist z. B. die Aufnahme der Experten in das Team zur Anwendungsentwicklung (so Forrester).

Die letzte und zugleich wichtigste Aufgabe ist jedoch, dass IT-Organisationen eine umfassende und ganzheitliche Management-Lösung für Mobilgeräte in Betracht ziehen, die die früher aufgeführten fünf Schritte beinhaltet: Bereitstellung, Sicherheit, Überwachung, Management und Support. Eine Lösung, die diese Prozesse über mehrere Gerätetypen und mobile Betriebssysteme hinweg vereinfacht und die Automatisierung und Self-Service-Optionen für die Erledigung alltäglicher Aufgaben bereitstellt. Eine solche Lösung erhöht die Flexibilität und Produktivität der Mitarbeiter, gewährleistet die Sicherheit der Unternehmensdaten und reduziert die Verwaltungskosten.

Matrix42 Software verwaltet mehr als 2,5 Millionen Kunden und stellt seit 20 Jahren Workplace Management-Lösungen bereit. Besuchen Sie uns auf www.matrix42.de oder kontaktieren Sie uns über info@matrix42.de oder per Telefon unter +49.0.6102/816.0, um herauszufinden, wie 2.500 Kunden weltweit die Kontrolle über ihren Arbeitsplatz übernehmen und die Produktivität der Mitarbeiter, die Effizienz von IT, die Anwenderzufriedenheit steigern und dabei Kosten sparen.

MATRIX42
MEMBER OF asseco GROUP

Deutsche Niederlassung
Dornhofstraße 44-46
63263 Neu-Isenburg, Deutschland
Tel: +49.0.6102/816.0
email: info@matrix42.de

U.S. Office
3400 North Ashton Blvd. Suite 110
Lehi, Utah 84043, USA
Tel: +1.801.653.3700
email: info@matrix42.com