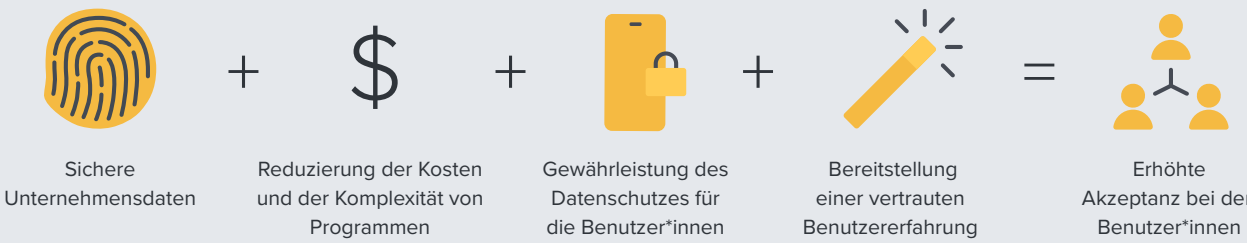
jamf

Jamf Mobile BYOD: **Datenschutz** und **Benutzerfreundlichkeit**

Steigern Sie mobiles BYOD, indem Sie die IT-Sicherheit mit dem Datenschutz und der Benutzererfahrung in Einklang bringen.

Der Aufstieg von iPhone und iPad als unübertroffener persönlicher Produktivitäts-Champion hat zu einer ständig verbundenen, modernen, mobilen Belegschaft geführt — und zu einer großen Herausforderung für das IT-Management.

Kritische Elemente für erfolgreiche mobile BYOD-Lösungen



Der Besitz von Mobilgeräten ist allgegenwärtig, und die meisten Mitarbeiter*innen nehmen ihre persönlichen Geräte mit an den Arbeitsplatz. In den letzten Jahren war es jedoch nicht einfach, dieses Potenzial der Geräte zu erschließen. Viele BYOD (Bring Your Own Device)-Lösungen sind vom Konzept her großartig, aber in der Praxis mangelhaft. Mitarbeiter*innen stellen die Hardware bereit, Organisationen den Zugang. Aber viel zu oft werden Geräte zu sehr verwaltet oder der Mitarbeiter wird nicht ausreichend bedient.

Auf der einen Seite ist ein vollständiges Gerätemanagement-Framework zu invasiv, da die IT-Abteilung jede App auf dem Gerät sehen kann — sowohl beruflich als auch privat. Die IT-Abteilung hat auch die Möglichkeit, das gesamte Gerät zu sperren, zu entsperren oder zu löschen. Die Besitzer*innen mobiler Geräte geben nur ungern die Kontrolle über ihre Geräte ab oder lassen sich in ihrer Privatsphäre einschränken — oder haben sogar das Gefühl, dass ihre Privatsphäre beeinträchtigt wird.

Eine weitere Methode zur Verwaltung von BYOD-Geräten ist die Verwaltung mobiler Apps, die es der IT-Abteilung ermöglicht, Unternehmensrichtlinien auf bestimmte Apps anzuwenden, die auf dem Gerät bereitgestellt werden. Diese Technik sichert die Apps, nicht den Teil des Geräts, der für die Arbeit verwendet wird. Durch die Implementierung von MAM erhalten Administrator*innen nicht die Möglichkeit, Unternehmensdienste wie die Konfiguration von WiFi, E-Mail oder die automatische Installation von Apps - auch nicht von gekauften - bereitzustellen, was mehr Interaktion mit dem Endbenutzer/der Endbenutzerin erfordert. Das Fehlen grundlegender Unternehmensrichtlinien führt dazu, dass sich diese Mitarbeiter*innen unterversorgt fühlen und die IT-Abteilung das Gefühl hat, Sicherheitslücken zu haben.

Die Realität ist, dass der Erfolg — oder Misserfolg — eines BYOD-Programms davon abhängt, ob die Technologie nutzbar ist, die Daten sicher sind und die Privatsphäre geschützt ist. **In diesem Beitrag wird dargelegt, wie Jamf und Apple BYOD-Lösungen anbieten, die dieses Gleichgewicht herstellen.**

Datenschutz zuerst

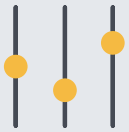
Auf unseren persönlichen Geräten befinden sich die privatesten Daten: persönliche Korrespondenz, Fotos, Kontakte und Dokumente. Selbst die Auswahl der auf dem Gerät installierten Apps kann sehr private Informationen über unsere Hobbys, Gewohnheiten und unseren Lebensstil preisgeben. Es überrascht nicht, dass die meisten Mitarbeiter*innen nur ungern Zugang zu diesen Informationen gewähren, indem sie ihr persönliches Gerät in einem MDM-System (Mobile Device Management) anmelden, das von der IT-Abteilung ihres Unternehmens kontrolliert wird.

Ein häufiger Grund für das Scheitern von BYOD-Programmen ist der Widerwille der Benutzer*innen, einem IT-Administrator/einer IT-Administratorin freiwillig Zugang zu diesen persönlichen Daten zu gewähren. Die Privatsphäre ist wichtig, und die Nutzer reagieren zunehmend empfindlich auf jeden Versuch, die Privatsphäre im Namen der IT-Kontrolle zu verletzen.

Sicherheit ist für die IT wichtig

Für IT-Manager*innen ist die Vorstellung eines ungehinderten Zugriffs auf interne Ressourcen von persönlichen Geräten mit unbekannter Konfiguration und Sicherheitskontrolle ein Alptraum. **Mobile Geräte sind ein häufiges Ziel für Malware- oder Phishing-Angriffe** und stellen eine potenzielle Angriffsfläche dar, wenn sie mit dem Netzwerk eines Unternehmens verbunden sind.

Ohne Sichtbarkeit und Kontrolle der Endgeräte ist eine wirksame IT-Sicherheit eine unmögliche Aufgabe. Das Sicherheitsbedürfnis ist der Grund, warum Unternehmen MDM für ihr BYOD-Programm einsetzen und daher von ihren Mitarbeitern verlangen, dass sie ihr persönliches Gerät registrieren, um Zugang zum internen Netzwerk, zu E-Mails, Kalendern, VPN und mehr zu erhalten.



IT-Administrator*innen können:

- Einsatz von Kontrollen zur Vermeidung von Datenverlusten
- Benutzerverwalteter Self-Service App-Katalog
- Unternehmensspezifischen Einstellungen, wie WLAN, VPN und Passcodes anwenden
- Installieren und Entfernen von Apps und Büchern des Unternehmens sowie der zugehörigen Daten
- Sammeln von Sicherheitsinformationen aus dem Arbeitskonto
- Hinzufügen/Entfernen von Einschränkungen zum Schutz von Daten- des Unternehmens

IT-Administrator*innen können nicht:

- Private Daten- wie Fotos, persönliche Post oder Kontakte löschen
- Alle personalisierten Apps entfernen
- Einsicht in alle privaten Daten, einschließlich der Namen der persönlichen Apps
- Die Nutzung des Geräts einschränken oder die Anzahl der installierbaren persönlichen Apps begrenzen
- Verfolgen Sie den Standort des Geräts
- Alle vom Benutzer*innen installierten Komponenten entfernen
- Sammeln Sie die Informationen der Benutzer*innen vom Gerät

Das richtige Gleichgewicht finden

Sowohl die Nutzer*innen als auch die IT-Abteilung haben durchaus berechtigte Bedenken. Der Mitarbeiter möchte nur ein Gerät verwenden, aber nicht auf den Zugriff und die Kontrolle über seine privaten Daten verzichten. Die IT-Abteilung möchte die Kosten für die Geräte senken und die Erfahrung der Mitarbeiter*innen verbessern, benötigt aber dennoch grundlegende organisatorische Sicherheit. Für viele Unternehmen bedeuteten diese Scheidewege ein Scheitern ihres BYOD-Programms.

Eine Lösung, um beiden Bedenken gerecht zu werden, besteht darin, die Rolle von MDM im Zusammenhang mit BYOD zu überdenken. Anstelle eines Einheitsansatzes können Administrator*innen ein Tool wählen, das für BYOD ausgelegt ist, mit einem Datenschutz, der die Mitarbeiter*innen zufriedenstellt, und mit starken Sicherheitskontrollen, die die Anforderungen von InfoSec-Teams erfüllen.

BYOD für die moderne Belegschaft

Führende Unternehmen entscheiden sich für einen Funktionssatz, der speziell für BYOD entwickelt wurde, um die Anforderungen beider Seiten zu erfüllen, ohne unnötige Komplexität und zusätzliche Kosten. Es ist wichtig, dass sowohl die IT-Abteilung als auch die Endbenutzer*innen die Vorteile eines für sie konzipierten BYOD-Programms genau kennen. Entscheidend für den Erfolg des Programms ist auch die Kommunikation und Transparenz gegenüber den Mitarbeitern über die Vorteile eines BYOD-Programms, da dies dazu beiträgt, etwaige Spannungen über die Verwendung eines persönlichen Geräts am Arbeitsplatz abzubauen. Im Folgenden finden Sie einige Beispiele dafür, was Unternehmen und Mitarbeiter*innen von einem gut konzipierten BYOD-Programm profitieren können.

Erfolg ist, wenn alle gewinnen

Vorteile für die Mitarbeiter*innen

Das native Apple Erlebnis, sowohl privat als auch beruflich, alles in einem Gerät:

- Transparenz der IT-Verwaltungsfunktionen für ein persönliches Gerät vor der Registrierung, um den Schutz der persönlichen Daten des Nutzers zu gewährleisten.
- Sicherer Zugriff auf Unternehmensressourcen wie E-Mails, Kalender, WLAN und Apps, um produktives Arbeiten zu erleichtern.

Organisatorische Vorteile

Ein Gleichgewicht zwischen Sicherheit und Benutzerdatenschutz, alles in einem Gerät:

- Gewährleistung der Sicherheit des Geräts und des Zugriffs auf Unternehmensdaten und -ressourcen, damit die Mitarbeiter geschützt und produktiv bleiben.
- Kostensenkung durch den Kauf von weniger Geräten

Wie Apple und Jamf die Privatsphäre der Nutzer*innen schützen

Wie in diesem Papier hervorgehoben wird, besteht das Ziel darin, einen Sweet Spot für persönliche Geräte zu finden, der nicht zu viel Verwaltung erfordert, aber es der IT-Abteilung dennoch ermöglicht, ihre Benutzer und ihr Unternehmen durch einfachen, sicheren Zugriff auf die Software und Apps, die die Benutzer*innen für ihre Arbeit benötigen, angemessen zu unterstützen. In diesem Sinne hat Jamf Apple genutzt, um die Vorteile und Möglichkeiten von Bring Your Own Device-Programmen zu erweitern.

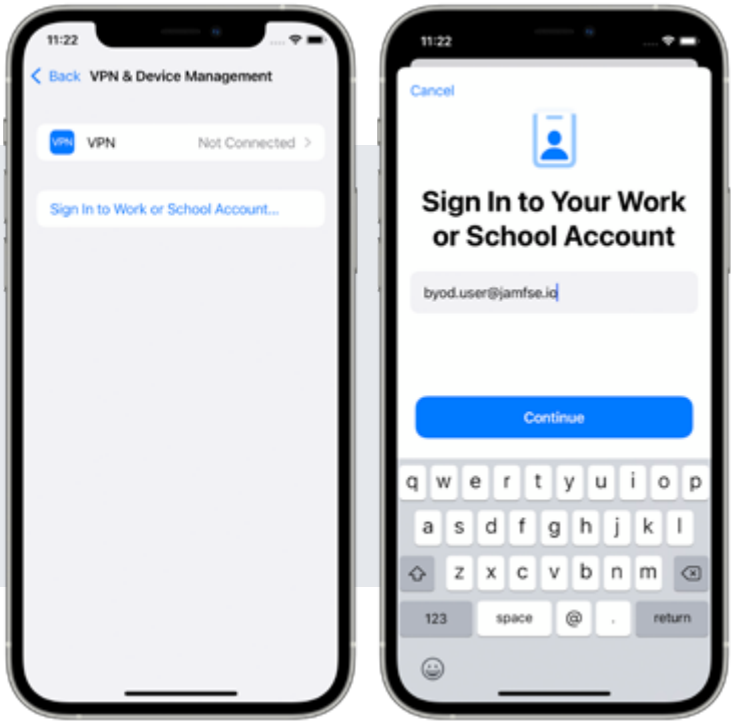
Die **kontobasierte Benutzerregistrierung** von Apple ist eine BYOD-Methode für iOS und iPadOS Geräte, die den Onboarding-Prozess der Benutzerregistrierung rationalisiert und sich darauf konzentriert, BYO-Benutzer*innen Unternehmenszugriff zu gewähren, während die Privatsphäre der Benutzer*innen auf ihrem persönlichen Gerät gewahrt bleibt. Unternehmen können diesen neuen Workflow nutzen, um persönliche mobile Geräte mit iOS und iPadOS 15 oder höher mit Jamf Pro 10.33 oder höher zu registrieren. Jamf Pro unterstützt die Apple eigenen Workflows für die **Benutzerregistrierung**, um getrennte Arbeits- und Privatkonten einzurichten und so die Privatsphäre der Mitarbeiter*innen zu schützen. Es gibt zwei Optionen für die Registrierung: Kontobasierte Benutzerregistrierung und profilbasierte Benutzerregistrierung. Jamf bevorzugt die kontobasierte Benutzeranmeldung, bei der sich ein Mitarbeiter/eine Mitarbeiterin über die App Einstellungen anmeldet.

Bei der Benutzerregistrierung werden persönliche und institutionelle Daten getrennt, indem eine persönliche Apple ID mit persönlichen Daten und eine verwaltete Apple ID mit Unternehmensdaten verknüpft wird. Jamf Pro unterstützt Apples Service Discovery-Funktion und ermöglicht die Verwendung einer Reihe von Konfigurationen, die die Verwaltung mit dem Mitarbeiter und der Art und Weise, wie er das Gerät für die Arbeit nutzt, in Verbindung bringen, und nicht mit dem Gerät selbst. Die Mitarbeiter*innen haben die Möglichkeit, auf sichere Weise auf ihre Unternehmensdaten zuzugreifen, ohne dass die IT-Abteilung das Gerät berühren oder ihnen einen Anmeldelink schicken muss, wodurch die Gefahr von Phishing-Angriffen sinkt. Die Mitarbeiter*innen erhalten sogar einen Jamf Self Service, mit dem sie Unternehmensanwendungen installieren können. Die Anmeldung ist eine vertraute und vertrauenswürdige Erfahrung, die es den Mitarbeiter*innen leicht macht und für Administrator*innen eine Art Zero-Touch-Deployment mit den Vorteilen eines sicheren Zugangs zu den Ressourcen ihres Unternehmens darstellt.

Wie sich ein Arbeitnehmer/eine Arbeitnehmerin anmeldet

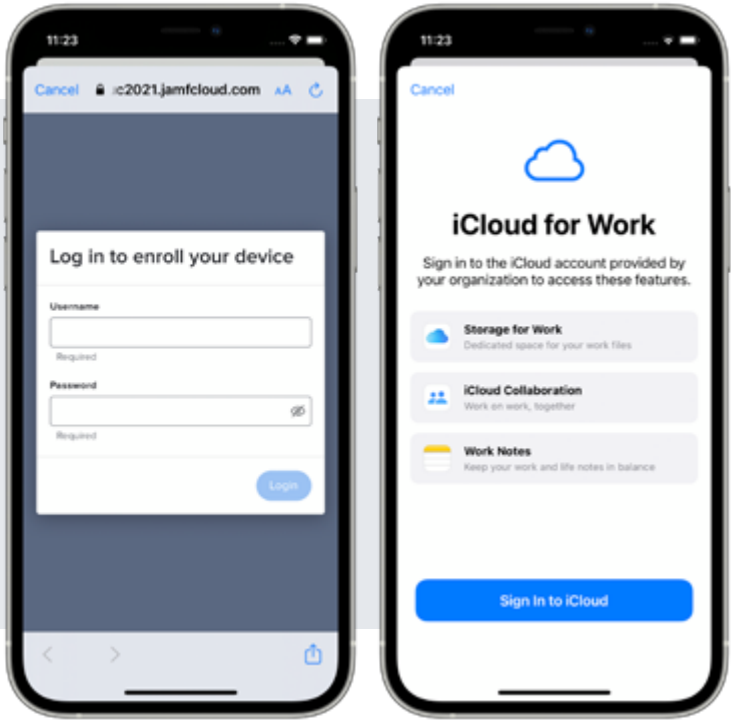
1

Der Benutzer authentifiziert sich am Gerät mit einer verwalteten Apple ID, indem er zu Einstellungen > Allgemein > VPN & Gerätemanagement navigiert und sich dann mit seiner verwalteten Apple ID bei seinem Arbeits- oder Schulkonto anmeldet. Nachdem der Benutzer*innen die verwaltete Apple ID eingegeben hat, muss er auf Weiter tippen.



2

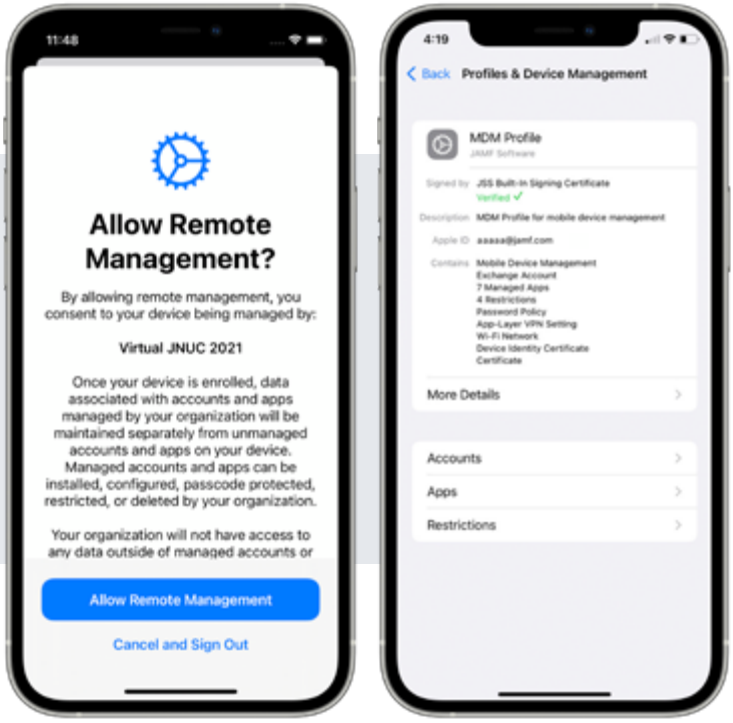
Das Anmeldeportal wird angezeigt und fordert den Benutzer auf, sein Jamf Pro-Benutzerkonto oder seine Verzeichnisanmeldeinformationen (z. B. LDAP oder Azure AD) einzugeben. Nach Eingabe der Anmeldedaten muss der Benutzer auf Anmelden tippen. Der Benutzer muss sich dann bei iCloud mit seiner verwalteten Apple ID-E-Mail-Adresse und seinem Passwort anmelden, wenn er dazu aufgefordert wird.



3

Der Benutzer wird aufgefordert, die Fernverwaltung zuzulassen, und das MDM-Profil wird auf das Gerät heruntergeladen.

Und das war's! Für den Endbenutzer ist es eine einfache Erfahrung, für die Organisation ein sicheres Unternehmen.



Zugangs- und Sicherheitslösungen für BYOD

Jamf Connect und Jamf Protect bieten zusätzliche und sichere Lösungen.

Die ZTNA-Funktionen (Zero Trust Network Access) von Jamf Connect stellen sicher, dass nur vertrauenswürdige Benutzer*innen auf sanktionierten, sicheren Geräten auf Arbeitsapps und Daten zugreifen können. Jamf Protect verbessert die starke Sicherheit von Apple zum Schutz von Unternehmensdaten.

Damit Jamf Connect und Jamf Protect funktionieren, müssen die Administrator*innen Jamf Trust auf den Geräten der Mitarbeiter*innen installieren: eine einzige App, die die Zugriffs- und Sicherheitsfunktionen von Jamf Connect und Jamf Protect auf mobilen Geräten bereitstellt. Jamf Trust arbeitet nur mit dem Arbeitskonto des Geräts, das persönliche Konto bleibt privat.

Schlussfolgerung

Ein erfolgreiches BYOD-Programm ist für Mitarbeiter und IT-Administratoren gleichermaßen von Vorteil. Mit der richtigen Lösung kann sich die IT-Abteilung auf die Erfüllung wichtiger Unternehmensanforderungen konzentrieren, ohne dass die Technologie selbst oder die Nutzer*innen davon betroffen sind. Und die Benutzer erhalten Komfort und Vertrautheit mit ihrem eigenen Gerät, ohne dass die IT-Abteilung eingreifen muss.

Erfahren Sie mehr über die Registrierung von **BYOD-Benutzern** oder sehen Sie, wie Jamf mit Apple Ihre BYOD-Pläne zum Leben erwecken kann, indem Sie eine **Testversion anfordern.**