Mobiles BYOD mit Jamf und Apple

Arbeitsgeräte können *alle* Geräte sein.

Und sie sind nicht auf die von der Firma herausgegebenen beschränkt.

Das Arbeitsgerät eines Mitarbeiters/einer Mitarbeiterin ist nicht nur ein vom Unternehmen zur Verfügung gestellter Laptop, sondern jedes Gerät, das auf Arbeitsressourcen zugreift - einschließlich privater Smartphones oder Tablets. Das ist Bring Your Own Device (BYOD), unabhängig davon, ob Sie ein formelles Programm für BYOD haben oder nicht.

Eine kürzlich durchgeführte ZIPPIA-Studie hat gezeigt, dass **17 % der Mitarbeiter*innen** ihre privaten Geräte für die Arbeit nutzen, ohne die IT-Abteilung darüber zu informieren.

Die Nutzer*innen bringen bereits ihre eigenen Geräte mit zur Arbeit; Sie haben keine andere Wahl.

Dies stellt ein ernsthaftes Sicherheitsproblem dar. Die IT-Abteilung kann keine Geräte schützen, von denen sie nichts weiß. Der jüngste **Security 360-Bericht** von Jamf hat beispielsweise ergeben, dass „21 % der Mitarbeiter*innen falsch konfigurierte Geräte verwenden, was sie einem Risiko aussetzt."

Sie haben die Wahl, ein formelles und umfassendes BYOD-Programm anzubieten, das Daten und Netzwerke schützt. Eine Lösung, mit der die Benutzer*innen zufrieden sind und produktiv arbeiten können, während gleichzeitig ihre Privatsphäre und Ihre Daten geschützt werden.

Was braucht ein persönliches Arbeitsgerät?

BYOD muss nutzbar, sicher und privat sein.

Bessere Sicherheit muss auch mit einer hervorragenden Benutzerfreundlichkeit einhergehen. Sie möchten, dass Ihre Mitarbeiter*innen so produktiv wie möglich sind und die Geräte so sicher wie möglich nutzen. Man muss es ihnen also leicht machen.

Unternehmen müssen den Arbeitsbereich der Geräte konfigurieren und sichern und gleichzeitig eine nahtlose Nutzung von Arbeits- und Privatapps ermöglichen. Und es muss klar sein, dass für diese Geräte der gleiche Grad an Privatsphäre gilt wie für nicht registrierte Geräte.

Historische BYOD-Optionen

Unternehmen und Mitarbeiter*innen haben Bedenken bei der Einführung und Umsetzung historischer BYOD-Lösungen. Solche Herausforderungen wie der Schutz der Privatsphäre der Mitarbeiter*innen, die Erfahrung der Mitarbeiter*innen und die organisatorische Sicherheit können BYOD-Einsätze behindern.

Was ist mit Mobile Application Management (MAM)?

Allein mit MAM:

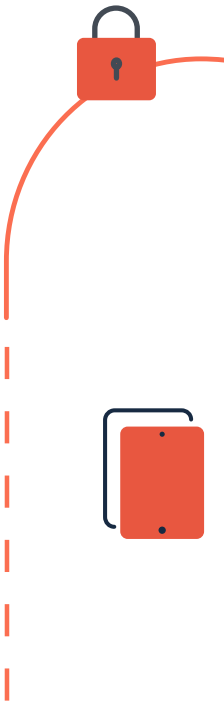
- Die IT-Abteilung kann weder Wi-Fi noch E-Mail konfigurieren und nicht automatisch installieren - nicht einmal die gekauften Apps
- Die Nutzer*innen müssen die Apps selbst herunterladen und haben möglicherweise nur eine begrenzte Anzahl zur Auswahl
- Unternehmen haben höhere Entwicklungskosten - Apps müssen speziell für MAM entwickelt werden

Vollständige Geräteverwaltung:

- Durch die Verwaltung des gesamten Geräts führt eine vollständige Geräteverwaltung zu Verletzungen der Privatsphäre und ist viel zu invasiv. Kein Arbeitnehmer/keine Arbeitnehmerin möchte diese Art der BYOD-Einführung.

Keine Lösung oder nicht verwaltete Geräte:

- Wenn Mitarbeiter*innen persönliche Geräte verwenden, um auf Unternehmensressourcen zuzugreifen, ohne dass die Sicherheit im Unternehmen oder das Bewusstsein für IT oder InfoSec gegeben ist



Ein erfolgreiches BYOD-Programm setzt Jamf und Apple ein.

Die Apple Funktionen, die die Unternehmensdaten schützen, schützen auch die persönlichen Inhalte eines Nutzers/einer Nutzerin vor der Einsicht oder Interaktion durch das Unternehmen. Es sind zwei Geräte in einem.

Wie unterstützt Jamf BYOD?

Durch die Verwendung der Apple eigenen Arbeitsabläufe **zur Benutzerregistrierung** und einer verwalteten Apple ID (MAID) werden getrennte berufliche und private Konten eingerichtet, wodurch die Privatsphäre der Mitarbeiter*innen geschützt wird. Jamf unterstützt Unternehmen dann bei der Sicherung und Konfiguration des Arbeitskontos des Geräts. Die IT-Abteilung kann sicherstellen, dass die Geräte den Unternehmensstandards entsprechen, und den Zugriff und die App-Berechtigungen entsprechend den individuellen oder abteilungsspezifischen Anforderungen erlauben.

Jamf stützt sich auf die starken Sicherheitsvorkehrungen von Apple und den unübertroffenen Schutz der Privatsphäre:

- Rigoroser Schutz der Privatsphäre der Mitarbeiter*innen
- Bereitstellung eines Unternehmenszugangs ohne Unterbrechung der Benutzererfahrung
- Schutz vor Bedrohungen für Apps und Unternehmensdaten
- Sichere Verbindungen zu Geschäftsapps

Apple nimmt den Schutz der Privatsphäre ernst.

Apples Benutzerregistrierung und der eingebaute Datenschutz erlauben es nur Apple Administrator*innen, das Arbeitskonto eines Geräts zu konfigurieren; es ist ihnen nicht möglich, auf das persönliche Konto zuzugreifen.

Den Möglichkeiten, die Unternehmen mit einem Mobile Device Management (Mobilgeräteverwaltung, MDM) haben, sind eiserne Grenzen gesetzt.

Mit einem MDM

Unternehmens-IT kann:

- Konten konfigurieren
- Auf den Bestand an verwalteten Apps zugreifen
- Nur verwaltete Daten entfernen
- Apps installieren und konfigurieren
- Erfordert einen Passcode mit sechs Zeichen
- Bestimmter Beschränkungen durchsetzen
- VPN pro Anwendung konfigurieren

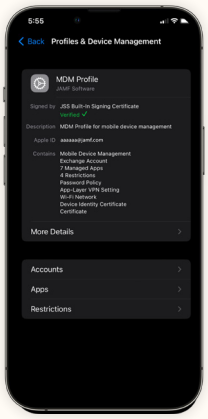
Die Unternehmens-IT kann das nicht:

- Persönliche Informationen, Nutzungsdaten oder Protokolle einsehen
- Auf den Bestand an persönlichen Apps zugreifen
- Alle personenbezogenen Daten entfernen
- Übernahme der Verwaltung einer persönlichen App
- Einen komplexen Passcode oder ein Passwort verlangen
- Auf den Standort des Zugangsgeräts zugreifen
- Auf eindeutige Gerätekennungen zugreifen
- Das gesamte Gerät aus der Ferne löschen
- Aktivierungssperre verwalten
- Auf Roaming-Status zugreifen
- Modus „Verloren“ aktivieren

QUELLE: APPLE. „BENUTZERREGISTRIERUNG UND MDM”

Wie Jamf BYOD ermöglicht

Unsere Lösungen arbeiten zusammen, um Apps, Daten und Geschäftsverbindungen zu verwalten und zu schützen und einen **Trusted Access** zu ermöglichen. Außerdem versichern sie den

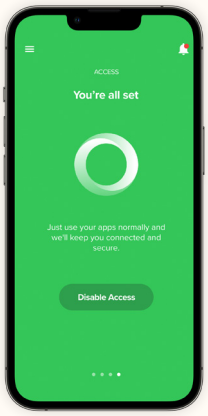


Nutzer*innen, dass ihre Privatsphäre unangetatet bleibt.

Geräteregistrierung zum Schutz der Privatsphäre

Jamf Pro trennt Arbeits- und Privatkonten mit der Apple Benutzeranmeldung. Dadurch wird verhindert, dass Organisationen persönliche Daten einsehen oder kontrollieren können.

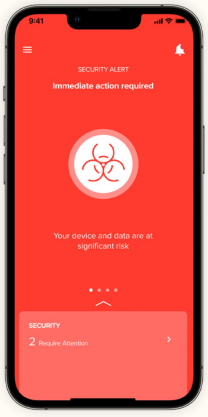
- Konfigurieren Sie den Zugang zu Unternehmensdiensten, einschließlich WiFi, E-Mail und Kontakte
- Verteilen und Verwalten der gesamten Bibliothek von iOS oder iPadOS Apps für die Arbeit
- Einsatz von Richtlinien zum Schutz vor Datenverlust, die den Datenfluss von verwalteten zu nicht verwalteten Apps verhindern
- Bieten Sie das native Apple Erlebnis, das iOS Nutzer*innen von der Anmeldung bis zur täglichen Nutzung wünschen



Sicherer Zugang und Konnektivität

Jamf Connect stellt sicher, dass nur autorisierte Benutzer*innen auf verwalteten Geräten auf Arbeitsapps und Daten zugreifen können. Jamf Trust ist die Endbenutzer-App für Jamf Connect.

- Bieten Sie sichere, verschlüsselte Verbindungen zu Geschäftsapps mit Zero Trust Network Access (ZTNA)
- Verwalten Sie den Netzwerkverkehr auf App Ebene und schützen Sie die Privatsphäre, indem Sie ZTNA über Per-App-VPN konfigurieren



Mobile Endpoint-Schutz

Jamf Protect verbessert die starke Sicherheit von Apple zum Schutz von Unternehmens daten. Jamf Trust ist die Endbenutzer-App für Jamf Protect.

- Verwalten Sie App-Risiken mit Workflows, die Apps überprüfen, um anfällige oder undichte Apps zu entfernen
- Erkennen und Abfangen von Man-in-the-Middle-Angriffen (MitM)
- Sicherheitsprüfungen durchführen, z. B. auf veraltete oder anfällige Betriebssystemversionen achten

Die Erfahrung der Mitarbeiter*innen

Wenn Mitarbeiter*innen auf Arbeitsressourcen zugreifen, sollten Sie ihnen das Erlebnis bieten, das Apple Benutzer*innen erwarten.

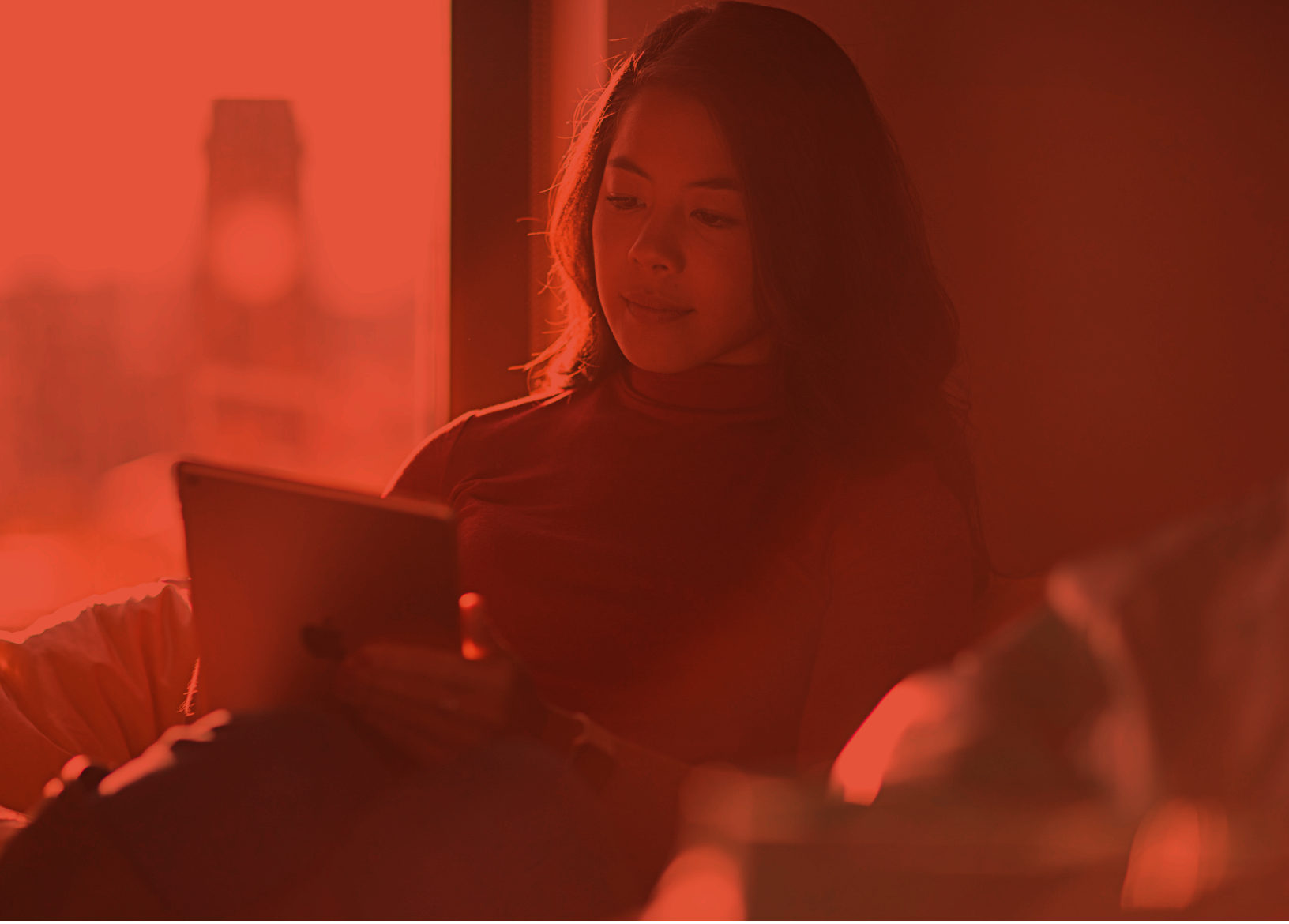
BYOD funktioniert nur, wenn die Mitarbeiter*innen wissen, dass ihr Unternehmen keinen Zugriff auf persönliche Daten hat und die Benutzerfreundlichkeit gewahrt bleibt. Jamf und Apple tun beides.

Benutzerregistrierung mit Jamf Pro:

- Bietet Transparenz darüber, wie die IT-Abteilung persönliche Geräte vor und während der Registrierung verwaltet
- Ermöglicht Mitarbeiter*innen die nahtlose Nutzung nativer Apple Apps für private und berufliche Zwecke
- Ermöglicht es Mitarbeiter*innen, überprüfte Apps selbst mit **Self Service**
- herunterzuladen.Erlaubt es Benutzer*innen, eine persönliche Apple ID für ihre persönlichen Daten und eine verwaltete Apple ID für Unternehmensdaten zu verwalten
- Verringert das Potenzial für Phishing-Versuche durch die kontoabhängige Benutzeranmeldung - Benutzer*innen authentifizieren sich über die Einstellungs-App mit einer verwalteten Apple ID auf dem Gerät

Jamf Trust: Wie mobile BYOD-Sicherheit funktioniert

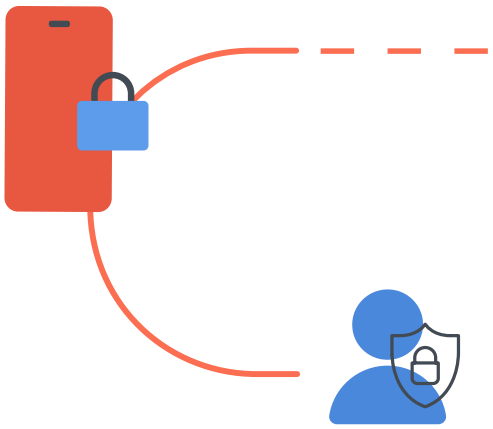
Damit alle sicher und produktiv arbeiten können, müssen wir die Dinge einfach halten. Administrator*innen stellen **Jamf Trust** auf den Geräten der Mitarbeiter*innen bereit: eine einzige App, die die Zugriffs- und Sicherheitsfunktionen von Jamf Connect und Jamf Protect auf mobilen Geräten bereitstellt. Jamf Trust arbeitet nur mit dem Arbeitskonto des Geräts, das persönliche Konto bleibt privat.



Jamf kennt Apple.

Betriebssystemspezifische Lösungen für BYOD sind für die organisatorische Sicherheit, den Zugriff und die Gerätekonfiguration unerlässlich. Die Benutzerfreundlichkeit, die Sicherheit und die Datenschutzfunktionen von Apple bieten eine ideale Umgebung für Unternehmen und Mitarbeiter*innen gleichermaßen, um BYO-Geräte zu registrieren. Und niemand hat mehr Erfahrung mit Apple als Jamf.

Wenden Sie sich**an Ihren Jamf Vertreter/Ihre Jamf Vertreterin oder an Ihren bevorzugten Partner**, um mehr darüber zu erfahren, wie Jamf die organisatorische Sicherheit und den persönlichen Datenschutz verbessern kann.



Testversion anfordern