jamf

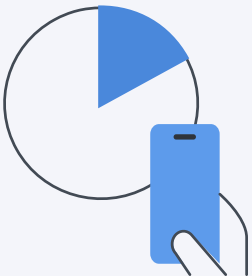
Jamf mobile BYOD: **sicher, privat, einfach.**

Der jüngste Bericht von Jamf **Security360** ergab, dass im Jahr 2022 **21 % der Mitarbeiter*innen**Geräte **verwenden**, die falsch konfiguriert sind, was ein **Risiko** für sie darstellt

Wenn Geräte auf Arbeitsressourcen zugreife, müssen sie für den Erfolg vorbereitet sein.

Mitarbeiter*innen nutzen mobil ohne Rücksicht

17 % der Mitarbeiter*innen **nutzen ihre persönlichen Geräte** für die Arbeit - ohne die IT-Abteilung zu informieren.



QUELLE: ZIPPIA

BYODmuss nutzbar, sicher und privat sein.

Wenn Sie den Arbeitsbereich der Geräte konfigurieren und sichern und die nahtlose Nutzung von Arbeits- und Privatappsermöglichen, werden die Mitarbeiter*innen diese auch eher nutzen. Es ist wichtig klarzustellen, dass für diese Geräte das gleiche Maß an Privatsphäre gelten muss wie für Geräte, die nicht an einem BYOD-Programm teilnehmen. Mit Jamf können Administrator*innen:

- Konfigurieren der Nur-Arbeitseinstellungen
- Sichere Verbindungen zu Geschäftsapps
- Aufbauend auf der starken Sicherheitsposition von Apple
- Trennung von Arbeits- und Privatvolumen zur Wahrung der Privatsphäre des Endbenutzers/der Endbenutzerin

Lernen Sie von Apple, was MDM leisten kann und was nicht.

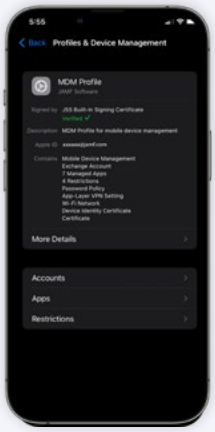
Wie Jamf BYOD ermöglicht

Unsere Lösungen arbeiten zusammen, um Apps, Daten und Geschäftsverbindungen zu verwalten und zu sichern 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 Privatvolumen mit Apples User Enrollment. Dadurch wird verhindert, dass Organisationen persönliche Daten einsehen oder kontrollieren können.

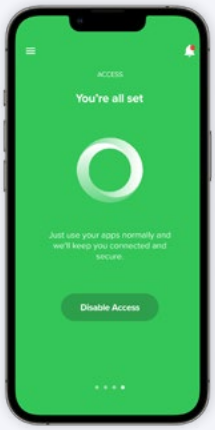
- Konfigurieren Sie den Zugang zu Unternehmensdiensten, einschließlich WiFi, E-Mail und Kontakte
- Verteilen und Verwalten der gesamten Bibliothek von iOS oder iPadOS Apps für die Arbeit
- Einsatz von Richtlinien zum Schutz vor Datenverlust, die den Datenfluss von verwalteten zu nicht verwalteten Apps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



Sicherer Zugriff und Konnektivität

Jamf Connect stellt sicher, dass nur autorisierte Benutzer auf verwalteten Geräten auf Arbeitsappps und Daten zugreifen können. Jamf Trust ist die Endbenutzer-App für 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 Unternehmensdaten. 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
- Schützen Sie Netzwerke und Geräte mit Malware-Schutz
- Erkennen und Abfangen von Man-in-the-Middle-Angriffen (MitM)
- Sicherheitsprüfungen wie die Überwachung auf veraltete oder anfällige Betriebssystemversionen durchführen

jamf

www.jamf.com/de

Aktualisiert 2/2022.

Finden Sie all diese Möglichkeiten an einem Ort mit dem Jamf Business Plan. **Testversion anfordern.**

Oder wenden Sie sich an Ihren Jamf Vertreter/Ihre Jamf Vertreterin oder bevorzugten Reseller.