BYOD voor mobiele apparaten met Jamf en Apple

Werkapparaten kunnen *elk* apparaat zijn.

En ze zijn niet beperkt tot door het bedrijf uitgegeven exemplaren.

Het werkapparaat van een werknemer is niet alleen een laptop die door het bedrijf wordt verstrekt; het is elk apparaat dat toegang heeft tot werkresources, inclusief smartphones of tablets die eigendom zijn van de werknemer. Dat is Bring Your Own Device (BYOD), of je nu een formeel BYOD-programma hebt of niet.

Uit **een recent onderzoek van ZIPPIA** bleek zelfs dat **17% van de werknemers** hun persoonlijke apparaten gebruikt voor het werk, zonder dit aan IT te melden.

Gebruikers nemen nu al hun eigen apparaten mee naar het werk; daar heb je geen keuze in.

Dit is een ernstig veiligheidsrisico. IT kan apparaten waar ze niets vanaf weten niet beschermen. Uit het recente **Security 360-rapport** van Jamf blijkt bijvoorbeeld dat '21% van de werknemers verkeerd geconfigureerde apparaten gebruikt, waardoor ze worden blootgesteld aan risico's.'

Je hebt wel de keuze om een formeel en volledig BYOD-programma aan te bieden dat gegevens en netwerken veilig houdt. Een oplossing die gebruikers tevreden houdt en productief laat werken, terwijl tegelijkertijd hun privacy en je gegevens worden beschermd.

Wat heeft een persoonlijk werkapparaat nodig?

BYOD moet bruikbaar, veilig en privé zijn.

Betere beveiliging moet ook gepaard gaan met een uitstekende gebruikerservaring. Je wilt dat je personeel maximaal productief is en apparaten op de veiligste manier gebruikt. Je moet het ze dus gemakkelijk maken.

Organisaties moeten het werkgedeelte van apparaten configureren en beveiligen en tegelijkertijd naadloos gebruik tussen werk- en persoonlijke apps mogelijk maken. En het is belangrijk om duidelijk te maken dat deze apparaten hetzelfde niveau van persoonlijke privacy hebben als apparaten die niet zijn ingeschreven.

Historische BYOD-opties

Organisaties en werknemers maken zich zorgen over de adoptie en implementatie van historische BYOD-oplossingen. Dergelijke uitdagingen, zoals de privacy van werknemers, de ervaring van werknemers en de beveiliging van de organisatie, kunnen een belemmering vormen voor de inzet van BYOD.

Hoe zit het met Mobile Application Management (MAM)?

Alleen met MAM:

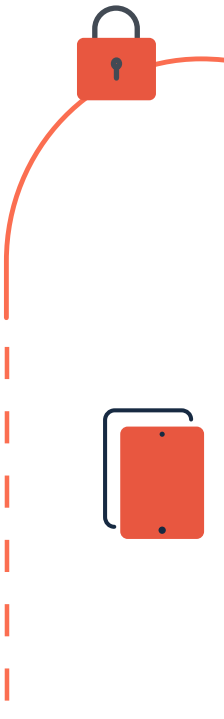
- IT kan geen wifi of e-mail configureren en kan niet automatisch apps installeren, zelfs niet als die in grote volumes zijn gekocht
- Gebruikers moeten zelf apps downloaden en kunnen kiezen uit een beperkt aantal
- Bedrijven hebben hogere ontwikkelingskosten: apps moeten specifiek voor MAM worden ontwikkeld

Volledig apparaatbeheer:

- Door het hele apparaat te beheren, legt een volledig kader voor apparaatbeheer privacyschendingen op en is het veel te invasief. Geen enkele werknemer wil dit soort BYOD-inschrijving.

Geen oplossing of niet beheerde apparaten:

- Wanneer werknemers persoonlijke apparaten gebruiken om toegang te krijgen tot bedrijfsmiddelen zonder dat ze zich bewust zijn van de beveiliging van de organisatie of van IT of InfoSec



Een succesvol BYOD-programma maakt gebruik van Jamf en Apple.

De Apple functies die bedrijfsgegevens beveiligen, beschermen ook de persoonlijke content van een gebruiker tegen inzage of interactie door het bedrijf. Het zijn twee apparaten in één.

Hoe ondersteunt Jamf BYOD?

Door gebruik te maken van Apple's eigen workflows voor **gebruikersinschrijving** en een beheerd Apple ID (MAID) worden aparte werk- en privéaccounts ingesteld, waardoor de privacy van werknemers wordt beschermd. Jamf helpt organisaties vervolgens bij het beveiligen en configureren van de werkaccount van het apparaat. IT kan ervoor zorgen dat apparaten voldoen aan de bedrijfsnormen en toegang en appmachtigingen verlenen op basis van individuele of afdelingsbehoeften.

Jamf bouwt voort op de sterke beveiligingsmaatregelen en ongeëvenaarde privacybescherming van Apple:

- de privacy van werknemers strikt beschermen
- zakelijke toegang bieden zonder onderbreking van de gebruikerservaring
- beschermen tegen bedreigingen voor apps en bedrijfsgegevens
- veilige verbindingen met zakelijke apps

Apple neemt persoonlijke privacy serieus.

Met de gebruikersinschrijving en ingebouwde privacybescherming van Apple kunnen Apple beheerders alleen het werkaccount van een apparaat configureren; het is onmogelijk voor hen om toegang te krijgen tot het persoonlijke account, om welke reden dan ook.

Er zijn duidelijke grenzen aan wat organisaties kunnen doen met een MDM (Mobile Device Management).

Met een MDM

Corporate IT kan:

- accounts configureren
- toegang krijgen tot de beheerde apps
- alleen beheerde gegevens verwijderen
- apps installeren en configureren
- een wachtwoordcode vereisen die zes tekens lang is
- bepaalde beperkingen afdwingen
- VPN per app configureren

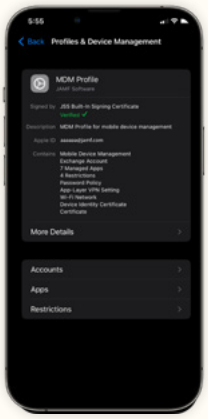
Corporate IT kan dit niet:

- persoonlijke informatie, gebruiksgegevens of logbestanden bekijken
- toegang tot persoonlijke apps
- persoonlijke gegevens verwijderen
- beheer van een persoonlijke app overnemen
- een complexe wachtwoordcode of wachtwoord vereisen
- toegang tot de locatie van het apparaat
- toegang tot unieke apparaat-id's
- het hele apparaat op afstand wissen
- activeringsslot beheren
- toegang krijgen tot de roamingstatus
- Verloren-modus inschakelen

BRON: APPLE. 'GEBRUIKERSINSCHRIJVING EN MDM.'

Hoe Jamf BYOD mogelijk maakt

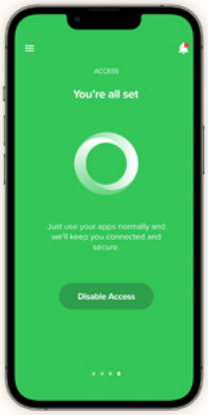
Onze oplossingen werken samen om apps, gegevens en bedrijfsverbindingen te beheren en te beveiligen, waardoor **Trusted Access** mogelijk wordt. Ze verzekeren gebruikers ook dat hun privacy intact blijft.



Apparaatinschrijving die de privacy beschermt

Jamf Pro scheidt werk- en persoonlijke accounts met de gebruikersinschrijving van Apple. Dit voorkomt dat organisaties persoonlijke gegevens kunnen inzien of controleren.

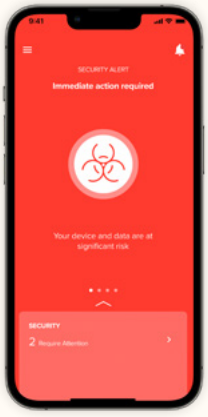
- Toegang configureren tot bedrijfsdiensten zoals wifi, e-mail en contactpersonen
- De volledige bibliotheek met iOS- of iPadOS-apps distribueren en beheren
- Beleid voor voorkoming van gegevensverlies implementeren om te voorkomen dat gegevens van beheerde naar onbeheerde apps stromen
- De native Apple ervaring bieden die iOS-gebruikers willen, van aanmelding tot dagelijks gebruik



Veilige toegang en connectiviteit

Jamf Connect zorgt ervoor dat alleen bevoegde gebruikers op beheerde apparaten toegang hebben tot werk-apps- en gegevens. Jamf Trust is de eindgebruiker-app voor Jamf Connect.

- Bied veilige, versleutelde verbindingen naar bedrijfstoepassingen met Zero Trust Network Access (ZTNA)
- Beheer netwerkverkeer op appniveau en behoud privacy door ZTNA te configureren via VPN per app



Bescherming van mobiele eindpunten

Jamf Protect verbetert de sterke beveiliging van Apple om organisatorische gegevens te beschermen. Jamf Trust is de eindgebruiker-app voor Jamf Protect.

- Beheer apprisico's met workflows die apps doorlichten om kwetsbare of lekkende apps te verwijderen
- Man-in-the-Middle (MitM)-aanvallen detecteren en onderscheppen
- Beveiligingscontroles uitvoeren, zoals controleren op verouderde of kwetsbare versies van het besturingssysteem (OS)

De werknemerservaring

Als medewerkers toegang krijgen tot werkresources, zorg dan voor de ervaring die Apple gebruikers verwachten.

BYOD werkt alleen als werknemers weten dat hun organisatie geen toegang heeft tot persoonlijke informatie en hun gebruikerservaring behoudt. Jamf en Apple doen beide.

Gebruikersinschrijving met Jamf Pro:

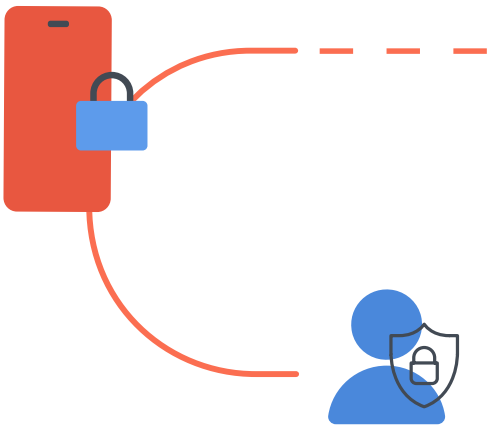
- Biedt transparantie over hoe IT persoonlijke apparaten beheert voor en tijdens de inschrijving
- Stelt werknemers in staat om native Apple apps naadloos te gebruiken voor zowel privé- als werkdoeleinden
- Stelt werknemers in staat om zelf gescreende apps te downloaden met **Self Service**
- Stelt gebruikers in staat om een persoonlijke Apple ID te gebruiken voor hun persoonlijke gegevens en een beheerde Apple ID voor bedrijfsgegevens
- Verlaagt de kans op phishing-pogingen met account-gestuurde gebruikersinschrijving: gebruikers verifiëren zich op het apparaat vanuit de Instellingen-app met behulp van een beheerde Apple ID

Jamf Trust: Hoe mobiele BYOD-beveiliging werkt

Om iedereen veilig en productief te houden, moet je het eenvoudig houden. Beheerders implementeren **Jamf Trust** op apparaten van werknemers: een enkele app die de toegangs- en beveiligingsmogelijkheden van zowel Jamf Connect als Jamf Protect levert aan mobiele apparaten. Jamf Trust werkt alleen op de werkaccount van het apparaat en laat de persoonlijke account privé.

Jamf kent Apple

Specifieke oplossingen voor besturingssystemen voor BYOD zijn van vitaal belang voor organisatorische beveiliging, toegang en apparaatconfiguratie. De gebruiksvriendelijkheid, beveiliging en privacykenmerken van Apple bieden een ideale omgeving voor organisaties en werknemers om BYO-apparaten in te schrijven. En niemand heeft meer Apple expertise dan Jamf.



Neem contact op **met je Jamf vertegenwoordiger of met de reseller van je keuze** voor meer informatie over hoe Jamf de veiligheid van je organisatie en je persoonlijke privacy kan verbeteren.

Proefversie aanvragen