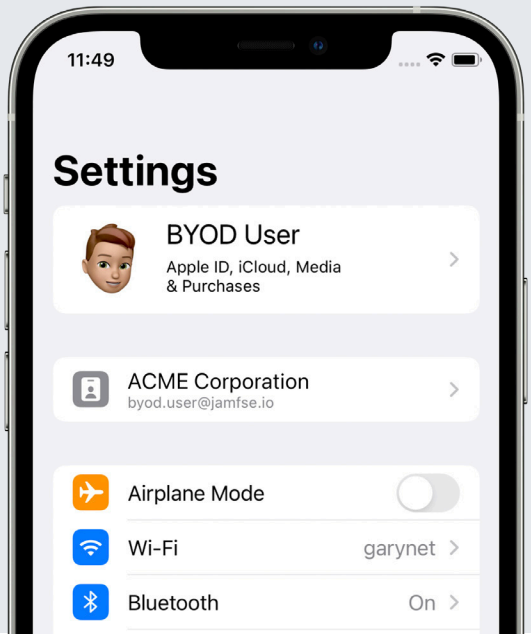
jamf

Jamf BYOD:
verlicht beveiligings- en privacyzorgen



Het gebruik maken van het potentieel van een succesvol BYOD programma komt neer op het vergroten van de gebruikersadoptie door een oplossing te vinden die twee zekerheden biedt: beveiliging van **de organisatie en privacy van gebruikers**. Een platform zoals Jamf biedt deze twee aspecten die organisatorische ondersteuning mogelijk maken voor werknemers terwijl de angst van de gebruiker om de IT-afdeling onbelemmerde toegang tot persoonlijke gegevens te bieden in de kiem wordt gesmoord.

De **Jamf BYOD-opties voor iOS en iPadOS 15 of later, Account-Driven User Enrollment of Profile-Driven User Enrollment**, maakt het voor organisaties eenvoudig om succesvol persoonlijke devices te implementeren voor werk terwijl de privacy van gebruikers behouden blijft. Met Jamf kunnen IT-Admins bedrijfsmiddelen en -gegevens beveiligen en de kosten voor het aankopen van devices verminderen en het gebruik van devices op flexibele wijze mogelijk maken voor zowel werk als persoonlijke taken, zonder de gegevens of de privacy van de gebruiker in gevaar te brengen, terwijl de Apple-gebruikers de ervaring krijgen die ze verwachten.

Belangrijke elementen voor een succesvol BYOD programma

- De zorgen voor IT-beveiliging verlichten
- De kosten en complexiteit van het programma verminderen
- Zorg dragen voor de privacy van de gebruiker
- Het bieden van een bekende gebruikerservaring

= Grotere gebruikers-adoptie

Succes is wanneer iedereen wint

Als organisaties een BYOD-programma hebben dat beveiliging en privacy bovenaan de lijst zet, profiteren zowel IT als werknemers.

Werknemersvoordelen

- Beveiligde toegang tot bedrijfsmiddelen
- Persoonlijke apps, gegevens en gebruik blijven privé en beschermd
- De bekende Apple ervaring voor zowel persoonlijk gebruik als voor werk
- Transparantie over de manier waarop IT hun persoonlijke device beheert

Organisatorische voordelen

- Werknemers blijven productief met toegang tot bedrijfsmiddelen waar ze ook zijn
- Precies genoeg beheer van het device om te zorgen voor veilige bedrijfsmiddelen en gegevens
- Minder kosten door minder devices te kopen

IT-beheerders hebben nog steeds de nodige beheermiddelen:

- Het device vergrendelen
- Bedrijfsconfiguraties toepassen
- Het installeren en verwijderen van zakelijke apps en boeken
- Beveiligingsinfo van het device verzamelen
- Beperkingen toevoegen en verwijderen om bedrijfsgegevens te beschermen

IT-beheerders kunnen niet:

- Persoonlijke gegevens bekijken of wissen
- Persoonlijke apps beperken of verwijderen
- De locatie volgen
- Persoonlijke informatie van gebruikers verzamelen

Het is belangrijk dat zowel IT en eindgebruiker de voordelen van een BYOD-programma duidelijk begrijpen voor hun eigen standpunten; persoonlijke privacy is belangrijk voor eindgebruikers en beveiliging is prioriteit voor IT-managers. Grote organisaties kiezen een pakket dat specifiek is ontwikkeld voor BYOD. Het inschrijven van BYO-devices bij Jamf is de gemakkelijkste manier om gebruikers en IT tegemoet te komen en het succes van BYOD voor organisaties van ieder formaat te bereiken.

Ontdek hoe eenvoudig een BYOD-workflow kan zijn voor Jamf gebruikers in Jamf en Apple BYOD Programs Done Better of vraag een proefversie aan en begin vandaag.

jamf

www.jamf.com

Als je nieuwsgierig bent naar hoe Jamf je BYOD devices kan verbeteren, ga naar **jamf.com.**