Hantera enheter och företagsdata i iOS

Innehåll

Översikt

Företag överallt skapar möjligheter för sina anställda med iPhone och iPad.

Nyckeln till en framgångsrik mobilstrategi är att skapa balans mellan IT-avdelningens styrning och användarnas möjligheter. Genom att anpassa iOS-enheterna med egna appar och eget innehåll tar användarna delvis över ägarskapet och ansvaret, vilket medför ökat engagemang och högre produktivitet. Det här är möjligt tack vare Apples hanteringsramverk. Det erbjuder smarta sätt att hantera företagets data och appar i bakgrunden, samtidigt som jobbdata och personliga data hålls åtskilda på ett smidigt sätt. Det blir dessutom tydligt för användarna hur deras enheter hanteras och att deras integritet skyddas.

Det här dokumentet innehåller råd om hur nödvändig IT-styrning kan upprätthållas samtidigt som användarna förses med bästa möjliga verktyg för sina uppgifter. Informationen kompletterar referensdokumentet om driftsättning av iOS, som är en heltäckande teknisk referens på webben för driftsättning och hantering av iOS-enheter i företaget.

Referensdokumentet om driftsättning av iOS finns på help.apple.com/deployment/ios.

Grundläggande om hantering

Med iOS kan du effektivisera iPhone- och iPad-driftsättningen med hjälp av olika inbyggda tekniker som förenklar kontoinställning, konfigurering av policyer, appdistribution och trådlöst upprättande av enhetsbegränsningar.

Vår syn på hantering

Apples hanteringsramverk utgör grunden för hanteringen av mobila enheter. Ramverket är inbyggt i iOS för att en organisation enkelt ska kunna hantera sådant som de måste hantera, utan att ingripa för mycket och utan att ta bort funktioner eller försämra funktionaliteten. Apples hanteringsramverk ger detaljkontroll över företagets alla enheter, appar och data via MDM-lösningar från tredje part. Viktigast av allt är att du får den kontroll du behöver, utan att behöva försämra användarupplevelsen eller inkräkta på medarbetarnas integritet.

Andra metoder för enhetshantering på marknaden kan ha andra benämningar för MDM-funktionalitet, till exempel EMM (Enterprise Mobility Management) eller MAM (Mobile Application Management). Men alla de här lösningarna har ett gemensamt syfte: trådlös hantering av organisationens enheter och företagsdata. Och eftersom Apples hanteringsramverk är inbyggt i iOS behöver du ingen separat agentapp från MDM-leverantören.

Skilja på företagsdata och privat information

Oavsett om företaget stöder användarägda eller företagsägda enheter, är det möjligt att på samma gång uppfylla it-chefens mål och upprätthålla användarnas produktivitet. Arbetsrelaterad och personlig information hanteras var för sig, utan att användarupplevelsen påverkas. På så sätt kan den senaste produktivitetsappen och dina företagsappar finnas sida vid sida på användarens enhet – och medarbetarna kan arbeta med större frihet. iOS åstadkommer detta utan inblandning av tredjepartslösningar, exempelvis behållare, som kan vara frustrerande för användarna och försämra användarupplevelsen.

Olika hanteringsmodeller och hur de fungerar

Många gånger har behållare använts för att lösa problem på andra plattformar – problem som inte förekommer i iOS. Vissa behållare använder sig av dubbla identiteter, vilket skapar två separata miljöer som körs på samma enhet. Andra fokuserar på att kapsla in hela appen i en behållare, via kodbaserad integrering eller så kallade app wrapping-lösningar. Alla de här metoderna innebär försämringar av användarnas produktivitet, antingen för att de kräver in- och utloggning mellan flera arbetsutrymmen eller för att de delvis bygger på företagsägd kod, vilket ofta orsakar problem med appkompatibiliteten i samband med uppdateringar av operativsystemet.

Organisationer som har gått ifrån behållare märker att de systemspecifika hanteringskontrollerna i iOS möjliggör en optimal personlig upplevelse för användare samt ökar deras produktivitet. I stället för att göra det svårt för användare att använda sina enheter för såväl arbete som privat bruk kan du använda policykontroller som smidigt hanterar dataflödet i bakgrunden.

Hantera företagsdata

Med iOS behöver du inte låsa företagets enheter. Viktiga tekniker styr flödet av företagsdata mellan appar och förhindrar dataläckage till användarens personliga appar eller molntjänster.

Hanterat innehåll

Hanterat innehåll omfattar installation, konfigurering, hantering och borttagning av appar från App Store samt interna appar, böcker och domäner

- **Hanterade appar.** Appar som installeras via MDM kallas ”hanterade appar”. Det kan vara kostnadsfria appar eller betalappar från App Store eller interna företagsappar, som alla kan installeras trådlöst via MDM. Hanterade appar innehåller ofta känslig information och har bättre kontrollmöjligheter än appar som användaren har laddat ner. MDM-servern kan på begäran ta bort hanterade appar och data som associeras med dessa eller specificera om apparna ska tas bort när MDM-profilen tas bort. MDM-servern kan dessutom förhindra att data i hanterade appar säkerhetskopieras till iTunes eller iCloud.
- **Hanterade konton.** MDM kan automatiskt ställa in användarnas e-post och andra konton så att de kommer igång snabbt. Beroende på leverantör av MDM-lösning och integrering med interna system kan kontons payload även förkonfigureras med användarens namn, e-postadress och eventuella certifikatidentiteter för autentisering och signering. MDM kan konfigurera följande typer av konton: IMAP/POP, CalDAV, kalenderprenumerationer, CardDAV, Exchange ActiveSync och LDAP.
- **Hanterade böcker.** Med hjälp av MDM kan du nu skicka böcker, ePub-böcker och PDF-dokument automatiskt till enheter. På så sätt har användarna alltid det material de behöver. Hanterade böcker kan endast delas med andra hanterade appar och mejlas från hanterade konton. När materialet inte längre behövs kan det fjärraderas.

- **Hanterade domäner.** Nedladdningar från Safari betraktas som hanterade dokument om de härrör från en hanterad domän. Specifika webbadresser och underdomäner kan hanteras. Om en användare till exempel laddar ner en pdf-fil från en hanterad domän, kräver domänen att pdf-filen är kompatibel med alla hanterade dokumentinställningar. Sökvägar till domänen är hanterade som standard.

Hanterad distribution

Med hanterad distribution kan du administrera appar och böcker som köpts via programmet för volyminköp (VPP) med hjälp av företagets MDM-lösning eller Apple Configurator 2. För att aktivera hanterad distribution måste du först koppla MDM-lösningen till ditt VPP-konto med hjälp av en säker token. När MDM-servern anslutits till VPP kan du tilldela appar till enheter direkt, utan att användaren behöver ett Apple-ID. Användarna meddelas då det finns appar som väntar på att installeras på deras enheter. Om en enhet är övervakad distribueras appar till den utan att användaren meddelas.

Om organisationen behöver behålla fullständig kontroll över appar med en MDM-lösning ska apparna tilldelas en enhet direkt.

Hanterad appkonfiguration

Med hanterad appkonfiguration konfigurerar MDM-lösningen appar under eller efter driftsättningen med hjälp av det systemspecifika iOS-hanteringsramverket. Det här ramverket hjälper utvecklare att välja vilka konfigurationsinställningar som ska gälla då deras app installeras som en hanterad app. Medarbetarna kan direkt börja använda appar som konfigurerats på detta sätt, utan någon anpassad inställning. IT-ansvariga kan vara säkra på att företagsdata i appar hanteras på ett säkert sätt, utan att det krävs några företagsägda SDK:er eller app wrapping.

Apputvecklare har tillgång till funktioner som kan aktiveras när hanterad appkonfiguration används, till exempel att konfigurera appar, förhindra säkerhetskopiering av appar, avaktivera skärmavbilder och fjärradera appar.

AppConfig Community utvecklar verktyg och bästa praxis för systemspecifika funktioner hos mobila operativsystem. Ledande leverantörer av MDM-lösningar från forumet har etablerat ett standardschema som alla apputvecklare kan använda som stöd för hanterad appkonfiguration. Genom att möjliggöra ett mer konsekvent, öppnare och enklare sätt att konfigurera och skydda mobilappar bidrar forumet till att fler företag omfamnar mobilitet.

Mer information om AppConfig Community finns på www.appconfig.org.

Hanterat dataflöde

MDM-lösningar har specifika funktioner för noggrann hantering av företagsdata, så att dessa hindras från att läcka ut till användarens personliga appar och molntjänster.

- **Hanterad öppning.** Hanterad öppning tillämpar en uppsättning begränsningar som förhindrar att bilagor och dokument från hanterade källor öppnas på ohanterade platser och vice versa.

  Du kan exempelvis förhindra att en konfidentiell e-postbilaga i organisationens hanterade e-postkonto öppnas i någon av användarens personliga appar. Arbetsdokumentet kan endast öppnas av appar som är installerade och hanterade av MDM. Användarens ohanterade personliga appar visas inte i listan över appar som kan användas för att öppna bilagan. Utöver hanterade appar, konton, böcker och domäner finns det ett flertal tillägg som respekterar de begränsningar som gäller för hanterad öppning.

För att skydda företagets data kan detta arbetsdokument endast öppnas av appar som är installerade och hanterade av MDM.

- **Hanterade tillägg.** Apptilläggen ger tredjepartsutvecklare möjlighet att tillhandahålla funktioner till andra appar eller centrala iOS-funktioner, som Notiscenter, vilket möjliggör nya arbetsflöden mellan appar. Hanterad öppning förhindrar att ohanterade tilläggsfunktioner interagerar med hanterade appar. Här är några exempel på olika typer av apptillägg:
  - Med **dokumentapptillägg** kan produktivitetsappar öppna dokument från olika molntjänster utan att behöva skapa kopior på enheten.
  - Med **åtgärdstillägg** kan användare redigera eller visa innehåll i en annan app. Man kan till exempel använda en åtgärd för att översätta text från ett annat språk direkt i Safari.
  - Med **anpassade tangentbordstillägg** kan andra tangentbord användas utöver de som finns inbyggda i iOS. Hanterad öppning kan förhindra att ej godkända tangentbord visas i företagets appar.
  - **Idag-tillägg,** även kallade widgetar, används för att ge användarna lättöverskådlig information i Idag-vyn i Notiscenter. Det är ett bra sätt för användarna att snabbt få aktuell information från en app och ett enkelt sätt att öppna fullversionen av appen för den som vill veta mer.
  - **Delningstillägg** ger användaren ett bekvämt sätt att dela innehåll med andra enheter, som sociala nätverk eller uppladdningstjänster. I appar som har en delningsknapp kan användaren till exempel välja ett delningstillägg som representerar ett socialt nätverk och använda det för att publicera en kommentar eller annat innehåll.

Flexibla hanteringsalternativ

Apples hanteringsramverk är flexibelt och låter dig balansera hanteringen av såväl användarägda som företagsägda enheter i företaget. När du använder en tredjepartslösning för MDM med iOS får du tillgång till ett brett spektrum av alternativ för enhetshantering och kan välja att skapa allt från en väldigt öppen till en detaljstyrd miljö.

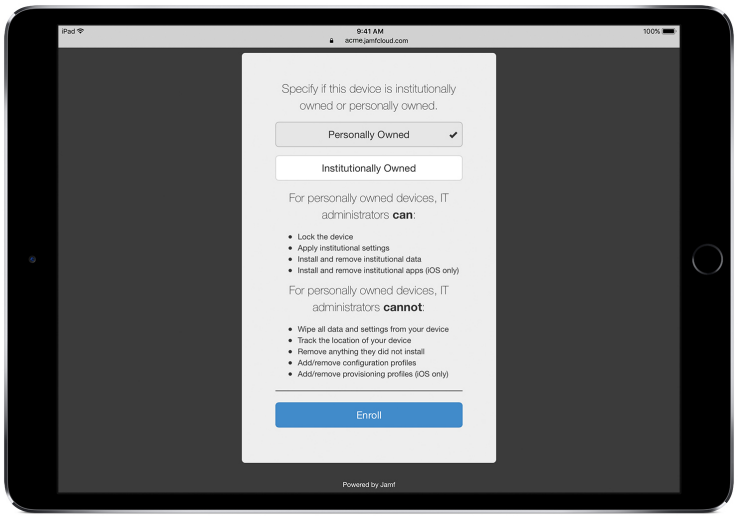
Ägarskapsmodeller

Den eller de ägarskapsmodeller för enheter som tillämpas på ditt företag kommer att diktera hur du hanterar enheter och appar. De två ägarskapsmodellerna för iOS-enheter som ofta används på företag är användarägda respektive företagsägda enheter.

Användarägda enheter

Med en användarägd modell finns möjligheter i iOS att låta användarna göra anpassade inställningar, visa hur deras enheter är konfigurerade samt garantera att företaget inte har åtkomst till användarnas personliga information.

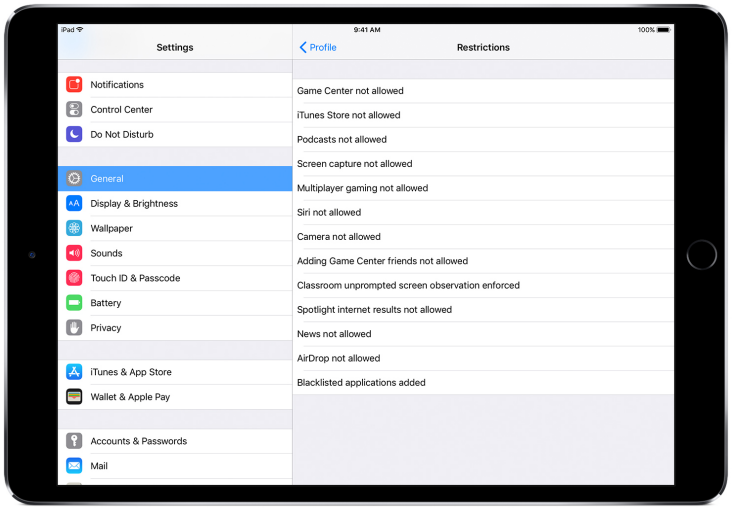
- **Frivillig registrering och avregistrering.** När enheter köps in och ställs in av användarna, ett förfarande som kallas BYOD, kan företaget fortfarande ge användarna åtkomst till företagstjänster som wifi, e-post och kalender. Användarna måste då själva välja att registrera sina enheter i företagets MDM-lösning. När användarna för första gången registrerar sig i MDM på en iOS-enhet får de information om vad MDM-servern kan komma åt på deras enhet och vilka funktioner den konfigurerar. På så sätt blir det tydligt för användaren vad som hanteras, vilket är viktigt för förtroendet mellan företag och användare. Det är viktigt att låta användarna veta att om de inte känner sig bekväma med denna hanteringsmodell kan de välja att avregistrera sig genom att ta bort hanteringsprofilen från enheten. Om de gör det raderas också alla företagskonton och företagsappar som installerats via MDM från enheten.



MDM-lösningar från tredje part har ofta användarvänliga gränssnitt för anställda, så att de ska känna sig bekväma med att registrera sig.*

*Skärmbild med tillstånd av Jamf.

- **Ökad transparens.** När användarna har registrerat sig i MDM kan de enkelt se i Inställningar vilka appar, böcker och konton som hanteras och vilka begränsningar som är aktiva. Alla företagets inställningar, konton och innehåll som installeras via MDM flaggas som ”hanterade” i iOS.



Användargränssnittet för konfigurationsprofiler i Inställningar visar användarna exakt vad som har konfigurerats på deras enheter.

- **Användarnas integritet.** En MDM-server gör det möjligt att interagera med iOS-enheter, men det betyder inte att du kan se alla inställningar och all kontoinformation. Du kan hantera företagets konton, inställningar och information som tillhandahålls via MDM, men du kommer inte åt användarnas personliga konton. Faktum är att samma funktioner som håller data säkra i företagshanterade appar också skyddar användarnas privata innehåll från att hamna i företagets dataflöde.

  Följande exempel visar vad en tredjeparts MDM-server kan se (och inte) på en personlig iOS-enhet:

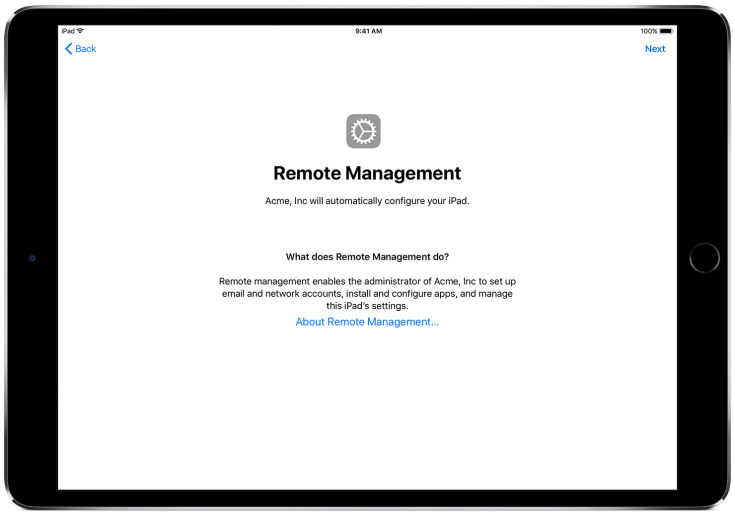
MDM ser:	**MDM ser inte privata data, som:**
Enhetsnamn	E-post, kalendrar och kontakter (jobb/privat)
Telefonnummer	Sms eller iMessage-meddelanden
Serienummer	Webbläsarhistorik i Safari
Modellnamn och -nummer	FaceTime- eller telefonsamtalsloggar
Tillgänglig kapacitet och utrymme	Privata påminnelser och anteckningar
iOS-versionsnummer	Hur ofta appar används
Installerade appar	Enhetens platsinformation

- **Anpassa enheter.** Företag har upptäckt att om de låter användarna anpassa sina enheter med egna Apple-ID:n ökar medarbetarnas känsla av ägarskap och ansvar. Dessutom ökar deras produktivitet när de själva får avgöra vilka appar och vilket innehåll de behöver för att utföra arbetet.

Organisationsägda enheter

Med en företagsägd driftsättningsmodell kan du förse varje användare med en enhet, även kallat driftsättning av anpassningsbara enheter. Du kan också välja att rotera enheterna bland användarna, vilket kallas driftsättning av delade enheter. iOS har funktioner som automatiserad registrering, låsbara MDM-inställningar, enhetsövervakning och alltid-på-VPN, vilka garanterar att enheterna konfigureras enligt organisationens specifika krav. Det ger ökad kontroll samtidigt som företagsdata skyddas.

- **Automatiserad registrering.** Programmet för enhetsregistrering (DEP) gör det möjligt att automatisera MDM-registreringen under den inledande inställningen av de iPhone-, iPad- och Mac-enheter som organisationen äger. Du kan se till att registreringen blir obligatorisk och permanent. Du kan också sätta enheterna i övervakat läge under registreringen samt låta användarna hoppa över vissa grundläggande inställningssteg.



Med DEP konfigurerar din MDM-lösning automatiskt dina iOS-enheter via inställningsassistenten.

- **Övervakade enheter.** Övervakning erbjuder ytterligare hanteringsmöjligheter för organisationsägda iOS-enheter, däribland möjlighet att aktivera ett webbfilter via en global proxy, så att användarens surfvanor håller sig inom organisationens riktlinjer, användarna hindras från att återställa sina enheter till fabriksinställningarna och mycket mer. Som standard är alla iOS-enheter oövervakade. Du kan antingen aktivera övervakningsläget via DEP eller aktivera övervakning manuellt med hjälp av Apple Configurator 2.

Även om du inte tänker använda några övervakade funktioner i dagsläget kan du överväga att övervaka enheterna när du ställer in dem, så att du kan välja att dra nytta av övervakade funktioner längre fram. Annars kan du tvingas radera redan driftsatta enheter. Övervakning handlar inte om att låsa en enhet. Snarare gör det företagsägda enheter bättre genom utökade hanteringsmöjligheter. På lång sikt kommer övervakning medföra fler alternativ för ditt företag.

En fullständig förteckning över övervakade inställningar finns i referensdokumentet om driftsättning av iOS.

Begränsningar

iOS stöder följande kategorier av begränsningar, som du kan konfigurera trådlöst så att de uppfyller företagets krav utan att användarna påverkas:

- AirPrint
- Appinstallation
- Appanvändning
- Appen Klassrum
- Enhet
- iCloud
- Begränsningar i Profilhanteraren för användare/användargrupper

- Safari
- Säkerhets- och integritetsinställningar
- Siri

I följande kategorier finns även alternativ som kan konfigureras via en MDM-lösning:

- Inställningar för automatiserad MDM-registrering
- Skärmar i Inställningsassistent

Ytterligare hanteringsmöjligheter

Anrop till enheter

Förutom att konfigurera enheter kan en MDM-server anropa enheter och begära in olika typer av information, som uppgifter om enheter, nätverk, appar samt information om regelefterlevnad och säkerhet. Informationen bidrar till att säkerställa att enheterna alltid följer gällande policyer. MDM-servern bestämmer hur ofta information ska samlas in.

Här följer några exempel på sådan information som kan begäras in från en iOS-enhet:

- Enhetsinformation (namn)
- Modell, iOS-version, serienummer
- Nätverksinformation
- Roamingstatus, MAC-adresser
- Installerade appar
- Appnamn, version, storlek
- Data om regelefterlevnad och säkerhet
- Installerade inställningar, policyer, certifikat
- Krypteringsstatus

Hanteringsåtgärder

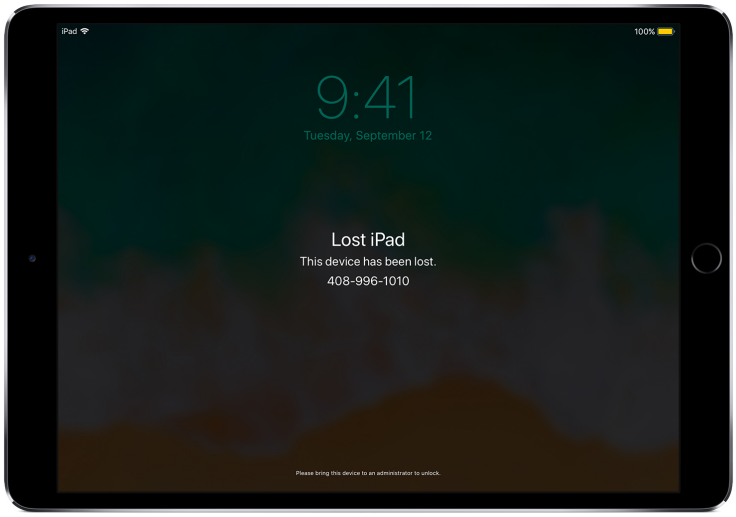
På hanterade enheter kan en MDM-server utföra en mängd olika administratörsåtgärder. Det handlar till exempel om att konfigurera inställningar automatiskt utan att användaren behöver göra något, utföra en iOS-uppdatering på en enhet låst med lösenkod, fjärrlåsa eller fjärradera en enhet eller radera lösenkoder så att användare kan återställa bortglömda lösenord. En MDM-server kan även begära att en iOS-enhet ska spegla innehållet till en specifik målenhet via AirPlay eller avsluta en pågående AirPlay-session.

Förlorat läge

Med iOS 9.3 eller senare kan MDM-lösningen fjärraktivera Förlorat läge på en övervakad enhet. Åtgärden låser enheten och kan även visa ett meddelande med ett telefonnummer på låsskärmen.

Med Förlorat läge kan du lokalisera en övervakad enhet som har tappats bort eller stulits, eftersom MDM anropar enheter trådlöst och efterfrågar deras position senast de var online. Förlorat läge kräver inte att Hitta min iPhone är aktiverat.

Om MDM avaktiverar Förlorat läge på distans, låses enheten upp och dess position registreras. För att upprätthålla transparensen underrättas användaren om att Förlorat läge har stängts av.



När MDM-lösningen sätter en borttappad enhet i förlorat läge låser MDM enheten, gör så att meddelanden kan visas på skärmen och fastställer var enheten finns.

Aktiveringslås

Med iOS 7.1 eller senare används MDM för att slå på aktiveringslåset då en användare aktiverar Hitta min iPhone på en övervakad enhet. Då kan din organisation dra nytta av aktiveringslåsets stöldförebyggande funktion, samtidigt som ni kan kringgå funktionen om till exempel en användare lämnar organisationen utan att först ta bort aktiveringslåset med hjälp av sitt Apple-ID.

MDM-lösningen kan ta fram en lösenkod och tillåta användaren att slå på aktiveringslåset på enheten enligt följande:

- Om Hitta min iPhone är aktiverat när MDM-lösningen tillåter aktiveringslåset, slås aktiveringslåset på direkt.
- Om Hitta min iPhone är avaktiverat när MDM-lösningen tillåter aktiveringslåset, slås aktiveringslåset på nästa gång användaren aktiverar Hitta min iPhone.

Sammanfattning

Med iOS hanteringsramverk får du det bästa av två världar: it-avdelningen kan konfigurera, hantera och skydda enheterna och kontrollera företagsdata som passerar genom dem, samtidigt som medarbetarna får använda de enheter de gillar på ett sätt som passar dem – och åstadkomma fantastiska saker.