A Mac központi bevezetésének áttekintése

Bevezetés

Tartalom

Az Apple-nél hiszünk abban, hogy az alkalmazottak akkor végezhetik a legjobban a munkájukat, ha a legjobb eszközökkel és technológiával dolgozhatnak. Az összes termékünket úgy tervezzük, hogy új módokon ösztönözze az alkalmazottak kreativitását, teljesítményét és munkavégzését, az irodában és azon kívül is. Ez egybecseng a mai munkavállalók elvárásaival, amelynek kulcselemei az információhoz való egyszerűbb hozzáférés, a zökkenőmentes együttműködés és megosztás, illetve az internetnek köszönhetően bárhonnan végezhető munka által biztosított szabadság.

A Mac gépek beállítása és üzembe helyezése napjaink üzleti környezetében minden eddiginél egyszerűbb. Az Apple fő szolgáltatásai és egy harmadik féltől származó mobileszköz-felügyeleti megoldás (MDM) segítségével cége nagy mennyiségben is egyszerűen kivitelezheti a Mac üzembe helyezését és támogatását. Amennyiben cégénél már használnak központilag kihelyezett iOS- és iPadOS-készülékeket, a macOS bevezetéséhez szükséges infrastruktúra nagy része valószínűleg már rendelkezésre áll.

A Mac legújabb biztonsági, felügyeleti, illetve üzembe helyezésre vonatkozó fejlesztései lehetővé teszik a cégek számára, hogy a monolitikus lemezképkészítés és a hagyományos címtárkötés helyett olyan leegyszerűsített telepítési modellre és üzembehelyezési folyamatra térjenek át, amely az egyes felhasználók köré épül, és szinte kizárólag a macOS beépített eszközeire támaszkodik.

Ebben a dokumentumban a Mac megfelelő léptékű telepítéséhez szükséges összes útmutatás megtalálható, a már meglévő infrastruktúra ismertetésétől az eszközfelügyeleten át a leegyszerűsített telepítésig. A dokumentumban szereplő témák részletesebb kifejtése a Mac online üzembehelyezési útmutatójában érhető el:
support.apple.com/guide/deployment-reference-macos

Első lépések

A bevezetési folyamat fontos első lépése a bevezetési stratégia és a bevezetési terv összeállítása, illetve annak felmérése, hogy hány alkalmazott használ már most is macOS-t. Fontos gondoskodni arról, hogy az érintett csapatok már a kezdetekkor megismerjék és elfogadják a program elképzeléseit és célkitűzéseit. Egyes csapatok kezdetnek akár kisebb megvalósíthatósági próbákat is tehetnek, hogy beazonosíthassák a saját munkakörnyezetükre jellemző kihívásokat. Egy szélesebb körű tesztüzem keretében mindenképpen érdemes egyeztetni a meglévő felhasználókkal annak átlátásához, hogy milyen módokon használják a cég eszközeit, és hogy a csapatnak milyen lehetséges problémákra kell odafigyelnie.

Az ebben a szakaszban gyűjtött információk segíthetnek meghatározni, hogy mely munkakörök és részlegek profitálhatnak a leginkább a Mac használatából. Ezek alapján az informatikai részleg fel tudja mérni, hogy a macOS-t az egész cégben, vagy csak egyes munkaterületeken érdemes-e bevezetni.

Emellett általában ilyenkor áll össze egy átfogó lista azokról a belső alkalmazásokról és eszközökről, amelyeket még a Mac általános bevezetése előtt kompatibilissé kell tenni. A hangsúlyt elsősorban azokra a teljesítményt, együttműködést és kommunikációt szolgáló, alapvető alkalmazásokra kell helyezni, amelyeket a legtöbb felhasználó használ. Az elengedhetetlen házon belüli szolgáltatások – például a vállalati belső hálózat, a címtár vagy a költséggazdálkodási szoftver – szintén kiemelten fontosak a cég teljesítménye szempontjából.

Az egyéb belső eszközökre vonatkozó esetleges kerülő megoldások és alternatívák dokumentálása és egyeztetése mellett az egyes alkalmazástulajdonosokat is ösztönözni kell a szükséges modernizációra. Folytasson nyílt és őszinte párbeszédet a felhasználókkal arról, milyen üzleti alkalmazások állnak majd a rendelkezésükre, ha a Mac mellett döntenek, és figyeljen oda rá, hogy a megújítási törekvések hajtóereje elsősorban a felhasználói igény legyen. Szükség esetén érdemes lehet összeállítani egy tervet az alkalmazástulajdonosokkal az alkalmazásaik frissítésével kapcsolatban, hogy a macOS SDK, a Swift, valamint a fejlesztésben segítő vállalati partnerek által nyújtott előnyöket is ki lehessen aknázni.

A Mac gépek általában a cég tulajdonában vannak. Egyes vállalatok olykor egy saját eszközök használatát támogató (BYOD-) program keretében megengedik alkalmazottaiknak a saját tulajdonú Macek használatát. Az Apple-termékeket választó alkalmazottak döntésének figyelembe vétele a birtoklási modelltől függetlenül az egész cég számára előnyös lehet, mivel növelheti a munkaerő hatékonyságát, kreativitását, elkötelezettségét és szakmai elégedettségét, alacsonyabb támogatási költségeket eredményez, és növeli az eszközök maradványértékét. A cégeknek emellett számos finanszírozási és lízinglehetőség is a rendelkezésére áll a kezdeti költségek csökkentéséhez. A cégek azzal is ellensúlyozhatják a költségeket, ha a fejlesztések során a bérelszámolásnál kompenzálják az alkalmazottakat, vagy megengedik nekik, hogy a lízing lejárta vagy az eszköz leselejtezése után megvásárolják a gépet.

Az egyes vállalatok szabályzatai, illetve üzembehelyezési, felügyeleti és támogatási folyamatai eltérhetnek az ebben a dokumentumban foglaltaktól annak függvényében, hogy a próbaüzem során milyen adatokat tud összegyűjteni a csapat. Nem minden felhasználónál lehet pontosan ugyanazokat a szabályzatokat, beállításokat és alkalmazásokat használni, mivel a különböző csoportok vagy csapatok igényei egy cégen belül gyökeresen eltérőek lehetnek.

A központi bevezetés lépései

A macOS központi bevezetésének négy fő lépése van: a környezet előkészítése, egy MDM-megoldás beállítása, az alkalmazottak eszközeinek üzembe helyezése, majd a folyamatos felügyeleti feladatok ellátása.

1. Előkészítés

A központi bevezetés első lépése mindig a meglévő környezet felmérése. Ez a szakasz magában foglalja a hálózat és a fő infrastruktúra áttekintését, valamint a sikeres bevezetéshez szükséges rendszerek beállítását.

Az infrastruktúra kiértékelése

Bár a Mac gördülékenyen integrálható a legtöbb hagyományos vállalati informatikai környezetbe, fontos a meglévő infrastruktúra felmérése, így meggyőződhet arról, hogy vállalata a macOS összes előnyét ki tudja használni. Ha a cégnek ezen a téren segítségre van szüksége, az Apple szakmai szolgáltatásokat nyújtó csapata, valamint az értékesítési partner vagy a viszonteladó műszaki csapata nyújthat támogatást.

Wi-Fi és hálózatkezelés
A folyamatos és megbízható hozzáférés egy vezeték nélküli hálózathoz elengedhetetlen a macOS-eszközök telepítéséhez és konfigurálásához. Győződjön meg arról, hogy a vállalat Wi-Fi-hálózata megfelelően van kialakítva, beleértve a hozzáférési pontok elhelyezését és jelerősségét. Így gondoskodhat a szükséges mobilitásról és kapacitásról.

Webproxyjainak vagy tűzfalportjainak konfigurálására is szükség lehet, ha az eszközök nem férnek hozzá az Apple szervereihez, az Apple push-értesítési szolgáltatáshoz, az iCloudhoz vagy az iTunes Store-hoz. Az iPhone-hoz és iPadhez hasonlóan a Mac központi bevezetése során is – különösen az újabb Mac-hardvereknél – hozzáférést kell biztosítani ezekhez a szolgáltatásokhoz, például annak érdekében, hogy a telepítés során frissíteni lehessen a firmware-t.

Az Apple és a Cisco optimalizálta a Mac gépek és a Cisco vezeték nélküli hálózatai közötti kommunikációt, így olyan fejlett hálózati szolgáltatások is elérhetővé váltak a macOS rendszerben, mint például a szolgáltatásminőség (QoS). Cisco hálózati eszköz használata esetén javasolt együttműködni a cég belsős csapataival annak érdekében, hogy a Mac optimalizálni tudja a kritikus jelentőségű forgalmat.

A vállalatoknak emellett a VPN-infrastruktúrát is fel kell mérniük, ha gondoskodni szeretnének róla, hogy az alkalmazottak távolról is biztonságosan férhessenek hozzá a vállalati erőforrásokhoz. Fontolja meg a macOS Igény szerinti VPN szolgáltatásának használatát, hogy csak akkor létesüljön VPN-kapcsolat, amikor ténylegesen szükség van rá. Ha alkalmazásonkénti VPN használatát tervezi, ellenőrizze, hogy a VPN-átjárói támogatják-e ezeket a képességeket, illetve hogy elég licencet vásárolt-e a megfelelő számú felhasználó és kapcsolat kiszolgálásához.

Ellenőrizze, hogy a hálózati infrastruktúra megfelelően működik-e a Bonjourral, az Apple szabványalapú, konfigurálást nem igénylő hálózati protokolljával. A Bonjour lehetővé teszi, hogy az eszközök automatikusan észleljék a szolgáltatásokat a hálózaton. A macOS a Bonjour segítségével csatlakozik az AirPrint-kompatibilis nyomtatókhoz és az olyan AirPlay-kompatibilis eszközökhöz, mint például az Apple TV. Egyes alkalmazások és beépített macOS-funkciók a Bonjourral észlelik az együttműködéshez vagy megosztáshoz elérhető többi eszközt is.

További információ a Wi-Fi-hálózat megtervezéséről:
support.apple.com/guide/deployment-reference-macos

További információ a hálózat MDM-mel kompatibilis beállításáról:
support.apple.com/HT210060

További információ a Bonjourról:
support.apple.com/guide/deployment-reference-macos

Identitások kezelése
A macOS képes elérni az olyan identitás- és felhasználóiadat-kezelő címtárszolgáltatásokat, mint például az Active Directory, az Open Directory és az LDAP. Az MDM-megoldások egyes gyártói használatra kész eszközöket kínálnak a saját felügyeleti megoldásaik és az Active Directory, illetve az LDAP-címtárak közötti integrációhoz. Olyan eszközök is rendelkezésre állnak, mint a macOS Catalina Kerberos egyszeri bejelentkezési bővítménye, amely hagyományos kötések és mobil fiókok nélkül is lehetővé teszi az integrációt az Active Directory szabályzataival és funkcióival. A cég MDM-megoldása a belsős és külsős hitelesítésszolgáltatók (CA) különféle típusú tanúsítványait is tudja kezelni, így az identitások automatikusan megbízhatók lesznek.

További információ az új Kerberos egyszeri bejelentkezési bővítményről:
support.apple.com/guide/deployment-reference-macos

További információ a címtár-integrációról:
support.apple.com/guide/deployment-reference-macos

Fő alkalmazotti szolgáltatások
Ellenőrizze, hogy a Microsoft Exchange naprakész-e, és úgy van-e konfigurálva, hogy támogassa a hálózaton lévő összes felhasználó hozzáférését. Ha nem az Exchange-et használja, a macOS az olyan szabványokon alapuló szerverekkel is együttműködik, mint például az IMAP, a POP, az SMTP, a CalDAV, a CardDAV és az LDAP. Tesztelheti az e-mailezéshez, a névjegyzékhez és a naptárakhoz tartozó alapvető munkafolyamatokat, illetve az egyéb, vállalati teljesítménnyel és együttműködéssel kapcsolatos szoftvereket is, amelyek a felhasználók napi munkafolyamatainak túlnyomó részét teszik ki.

További információ a Microsoft Exchange beállításáról:
support.apple.com/guide/deployment-reference-macos

További információ a szabványalapú szolgáltatásokról:
support.apple.com/guide/deployment-reference-macos

Tartalmak gyorsítótárazása
A macOS beépített gyorsítótár-szolgáltatása tárolja az Apple-szerverekről gyakran lekért tartalmak helyi másolatát, ezáltal minimálisra csökkenti a letöltéshez szükséges sávszélességet a hálózaton. A gyorsítótár felgyorsítja a Mac App Store áruházból származó szoftverek letöltését és közzétételét. Szoftverfrissítéseket is képes tárolni a céges macOS-, iOS- vagy iPadOS-eszközökre történő gyorsabb letöltés érdekében. A Cisco és az Akamai külső féltől származó megoldásaival további tartalmak is gyorsítótárazhatók.

További információ a tartalom-gyorsítótárazásról:
support.apple.com/guide/deployment-reference-macos

Felügyeleti megoldás létrehozása

Az MDM lehetővé teszi a cégek számára, hogy biztonságosan regisztráljanak Mac gépeket a vállalati környezetben, vezeték nélküli módon konfigurálják és frissítsék a beállításokat, alkalmazásokat telepítsenek, felügyeljék a szabályzatoknak való megfelelőséget, információkat kérdezzenek le eszközökről, vagy akár távolról töröljenek vagy zároljanak felügyelt eszközöket. Az informatikai részleg egyszerűen hozhat létre profilokat a felhasználói fiókok kezeléséhez, a rendszerbeállítások konfigurálásához, a korlátozások kikényszerítéséhez és a jelszószabályzatok beállításához – és mindezt ugyanazzal a mobileszköz-felügyeleti megoldással tehetik meg, amelyet az iPhone-hoz és az iPadhez is használnak.

A háttérben az összes Apple-platform az Apple felügyeleti keretrendszerét használja, aminek köszönhetően az ügyfelek számos külső MDM-megoldás közül választhatnak. Számos eszközfelügyeleti megoldás érhető el, többek között olyan külső szolgáltatóktól, mint a Jamf, a VMware vagy a MobileIron. Bár a macOS sok esetben ugyanazt az eszközfelügyeleti keretrendszert használja, mint az iOS és az iPadOS, a külső MDM-megoldások némiképp eltérnek a rendszergazdai funkciók, az operációs rendszerek támogatása, az árképzési struktúra és az üzemeltetési modell terén. Az is előfordulhat, hogy eltérő szintű integrációs, képzési és támogatási szolgáltatásokat kínálnak. A végleges megoldás kiválasztása előtt érdemes felmérni, hogy az adott cég igényeihez mely funkciók illeszkednek a leginkább.

A használni kívánt MDM kiválasztása után keresse fel az Apple Push Certificates Portalt, jelentkezzen be, majd hozzon létre egy új, MDM típusú leküldéses tanúsítványt.

További információ az MDM központi bevezetésével kapcsolatban:
support.apple.com/guide/deployment-reference-macos

Látogasson el az Apple Push Certificates Portal oldalára:
identity.apple.com/pushcert/

Regisztráció az Apple Business Managerben

Az Apple Business Manager egy webes portál, amelyen a rendszergazdák egy helyről végezhetik el az iPhone, iPad, iPod touch, Apple TV és Mac eszközök üzembe helyezését. Az Apple Business Manager problémamentesen működik együtt a cég mobileszköz-felügyeleti (MDM-) megoldásával, és megkönnyíti az eszközök automatikus üzembe helyezését, az alkalmazásvásárlást és a tartalmak kiosztását, valamint az alkalmazottak felügyelt Apple ID azonosítóinak létrehozását.

A Készülékregisztrációs program (DEP) és a Mennyiségi vásárlási program (VPP) mostanra már az Apple Business Manager szerves részét képezi, így a szervezeteknek egyetlen helyen áll rendelkezésre minden, amire csak szükségük lehet az Apple-eszközök üzembe helyezéséhez. 2019. december 1-től ezek a programok nem lesznek elérhetők.

Eszközök

Az Apple Business Manager lehetővé teszi az automatizált eszközregisztrációt. Gyors és gördülékeny módot biztosít a vállalati tulajdonban lévő Apple-eszközök üzembe helyezésére és MDM-ben való regisztrációjára, anélkül, hogy a készülékeket kézbe kéne venni vagy elő kéne készíteni.

- Leegyszerűsíti a felhasználók által végrehajtandó beállítási folyamatot azzal, hogy egyes lépéseket gördülékenyebbé tesz a Beállítási asszisztensben,

így amikor az alkalmazottak aktiválják a készülékeket, azonnal a megfelelő beállítások lépnek érvénybe. Az informatikai részleg most még inkább testre szabhatja ezt a lehetőséget azáltal, hogy hozzájárulási szöveget, vállalati arculatot vagy modern hitelesítési eljárást biztosít az alkalmazottak számára.

- A felügyelet lehetővé teszi a vállalati tulajdonban lévő eszközök szigorúbb kézben tartását, ami olyan szintű eszközkezelést tesz lehetővé (például a nem eltávolítható MDM-et), ami más üzembe helyezési modelleknél nem érhető el.
- Az eszköztípus alapján beállított alapértelmezett szerverekkel könnyedén beállíthatók alapértelmezett MDM-szerverek. Emellett a beszerzési forrástól függetlenül manuálisan is regisztrálhat iPhone-okat, iPadeket és Apple TV-ket az Apple Configurator 2 használatával.

Tartalmak

Az Apple Business Managerrel a cégek egyszerűen vásárolhatnak tartalmakat nagy tételben. Alkalmazottaik iPhone-jához, iPadjéhez vagy Mac gépéhez nagyszerű, használatra kész tartalmakat biztosíthatnak, amelyeket rugalmasan és biztonságos módon tehetnek közzé.

- Az alkalmazásokat, könyveket és egyéni alkalmazásokat nagy tételben is beszerezheti, a belső fejlesztésű alkalmazásokkal egyetemben. Az alkalmazáslicencek egyszerűen átadhatók a helyszínek között, a licenceken pedig osztozhatnak az egy helyszínen tartózkodó beszerzők. A vásárlási előzmények egységes listája is megtekinthető azzal együtt, hogy éppen mennyi licencet használ az MDM-en keresztül.
- Közvetlenül a felügyelt eszközökre vagy a jogosult felhasználóknak oszthatja ki az alkalmazásokat és a könyveket, és egyszerűen nyomon követheti, hogy a tartalmak mely felhasználókhoz vagy készülékekhez lettek hozzárendelve. A felügyelt terjesztéssel az irányítása alatt tarthatja a terjesztési folyamatot, és az alkalmazások teljes tulajdonjoga is Önnél marad. Az egyes eszközökön vagy felhasználók számára szükségtelenné vált alkalmazások visszavonhatók, és a cégen belül hozzárendelhetők más készülékekhez vagy felhasználókhoz.
- Fizetni többféle módon is lehet, például hitelkártyával vagy beszerzési rendeléssel. A szervezetek VPP-egyenleget vásárolhatnak (ahol az elérhető) az Apple-től vagy egy hivatalos Apple-viszonteladótól a helyi pénznemben megadott összegért, amely elektronikus úton érkezik meg a fióktulajdonoshoz áruházi egyenleg formájában.
- Az alkalmazások minden olyan ország eszközei vagy felhasználói számára elérhetővé tehetők, ahol az adott alkalmazás beszerezhető, így a nemzetközi terjesztés is lehetővé válik. A fejlesztők több országban is elérhetővé tehetik alkalmazásaikat az App Store hagyományos terjesztési módszerével.

Megjegyzés: Az Apple Business Manageren keresztüli könyvvásárlás egyes országokban vagy régiókban nem érhető el. Az egyes funkciók és vásárlási módok elérhetőségéről a következő helyen tájékozódhat: support.apple.com/HT207305.

Személyek

Az Apple Business Manager lehetővé teszi, hogy a szervezetek a meglévő infrastruktúrát integráló alkalmazotti fiókokat hozzanak létre és kezeljenek, amelyek hozzáférést biztosítanak az Apple-alkalmazásokhoz és -szolgáltatásokhoz, valamint az Apple Business Managerhez.

- Létrehozhat felügyelt Apple ID-kat az alkalmazottaknak, hogy közösen dolgozhassanak az Apple-alkalmazásokban és -szolgáltatásokban, és

hozzáférhessenek az iCloud Drive-ot használó felügyelt alkalmazásokban található vállalati adatokhoz. Ezeket a fiókok a cég vagy szervezet kezelésében és tulajdonában vannak.

- Kihasználhatja az összevont hitelesítés előnyeit az Apple Business Manager és a Microsoft Azure Active Directory összekapcsolásával. A felügyelt Apple ID-k automatikusan létrejönnek, amikor az alkalmazottak először bejelentkeznek már meglévő hitelesítő adataikkal egy kompatibilis Apple-eszközön.
- A felügyelt Apple ID-k a személyes Apple ID-k mellett is beállíthatók az alkalmazottak saját tulajdonában lévő eszközökön, köszönhetően az iOS 13, az iPadOS és a macOS Catalina új felhasználói regisztrációs szolgáltatásainak. A felügyelt Apple ID-k ugyanakkor az eszköz elsődleges (és egyetlen) Apple ID azonosítójaként is használhatók. A felügyelt Apple ID-kkal az iCloudhoz is hozzá lehet férni az interneten, miután bejelentkeztek velük egy Apple-eszközre.
- Kijelölhet különböző szerepköröket a vállalati informatikai csapatoknak, hogy hatékonyan tudják kezelni az eszközöket, alkalmazásokat és fiókokat az Apple Business Managerben. A rendszergazdai szerepkör lehetővé teszi a használati feltételek elfogadását, ha arra szükség van, és megkönnyíti a feladatok átruházását, ha egy alkalmazott elhagyja a vállalatot.

Megjegyzés: az iCloud Drive használata Felhasználói regisztrációval egyelőre nem támogatott. Az iCloud Drive csak akkor használható felügyelt Apple ID-val, ha egy eszközön ez az egyetlen Apple ID azonosító.

További információ az Apple Business Managerről: apple.com/hu/business/it

Regisztráció az Apple Developer Enterprise Programba

Az Apple Developer Enterprise Program (az Apple vállalati fejlesztői programja) teljes körű eszközkészletet kínál az alkalmazások fejlesztéséhez, teszteléséhez és felhasználók közötti terjesztéséhez. Az alkalmazások terjesztése kétféleképpen lehetséges: webszerverről vagy MDM-megoldással. A Mac-alkalmazásokat és a telepítőket az Ön fejlesztői azonosítójával lehet aláírni és hitelesíteni a Gatekeeper számára (amely segít megvédeni a macOS-t a kártevőktől).

További információ a Developer Enterprise Programról:
developer.apple.com/programs/enterprise

2. Beállítás

A központi bevezetés beállításához meg kell határoznia a vállalati szabályzatokat, valamint fel kell készítenie a mobileszköz-felügyeleti megoldást a Mac gépek alkalmazotti használatra történő konfigurálásához.

A macOS biztonsági jellemzőinek ismertetése

Az adatok biztonságos és bizalmas kezelése az Apple minden hardvertermékének, szoftverének és szolgáltatásának alapvető eleme. Ügyfeleink adatainak biztonságáról a rendkívül hatékony titkosítás mellett az adatkezelésre vonatkozó szigorú szabályzatokkal gondoskodunk. Ahhoz, hogy az Apple-eszközök számítógépes platformja biztonságos legyen, a következőkről kell gondoskodni:

- Olyan módszerekről, amelyek megelőzik az eszközök jogosulatlan használatát.
- A tárolt adatok védelméről, még abban az esetben is, ha az eszköz elveszett vagy ellopták.
- Az átvitelhez használt hálózati protokollokról és adattitkosításról.

- Az alkalmazások biztonságos futtatásáról a platform integritásának megőrzése mellett.

Az Apple-eszközök többrétegű biztonsági megoldást használnak, így biztonságosan tudnak hozzáférni a hálózati szolgáltatásokhoz, és képesek megvédeni a fontos adatokat. A macOS, az iOS és az iPadOS emellett az MDM-mel végrehajtható és kikényszeríthető jelszószabályzatokkal is gondoskodik a biztonságról. A felhasználó vagy a rendszergazda egy paranccsal távolról is törölheti az összes személyes adatot, amennyiben az eszköz rossz kezekbe kerül.

Az informatikai részleg számos szabályzatot telepíthet az MDM-mel az eszközök biztonsága érdekében. Ilyen például a FileVault és a helyreállítási kulcs letétjének kényszerítése az MDM-mel, egy speciális jelszószabályzat vagy a zárolható képernyőkímélő használatának megkövetelése, illetve a beépített tűzfal engedélyezése.

További információ az Apple-platformok biztonságáról: apple.com/security/

Vállalati szabályzatok meghatározása

Kezdje a vállalati szabályzat kifejlesztését olyan általános szabályzatok bevezetésével, amelyek a cég Mac-felhasználóinak túlnyomó többségét érintik. Az MDM-megoldással az egyes felhasználókra szabott elemeket határozhat meg, például fiókokat vagy bizonyos alkalmazások hozzáférését. Emellett külön szabályzatokat is megadhat cégek vagy egyéb kisebb felhasználói alcsoportok számára, így például részlegspecifikus szoftvereket vagy beállításokat is közzétehet.

A belsős csapatokkal együttműködve frissítse a már meglévő céges szabályzatokat a Mac gépek használatát előkészítő lépések keretében. Néhány alapvető szabályzat minden platform esetében ugyanaz marad, így például a jelszavak összetettsége és a jelszócserére vonatkozó követelmények, a képernyőkímélő időtúllépése vagy a rendeltetésszerű használat szabályai.

Ha a vállalat szabályzata egy másik platform adott technológiájának használatát írja elő, a probléma alapos megismerése után úgy kell átalakítani a szabályzatot, hogy a macOS beépített technológiáival is alkalmazható legyen. Ahelyett, hogy az összes számítógép felhatalmazást kapna egy speciális külsős megoldás alkalmazására egy teljes lemez titkosításához, érdemes megfontolni egy olyan szabályzat létrehozását, amely meghatározza, hogy a helyben tárolt céges adatokat titkosítani kell a FileVault használatával. Ha az intézmény egy adott szoftver használatát írja elő kártékony szoftverek elleni védelemhez, ismertessék a dolgozókkal az olyan beépített funkciókat, amilyen például a Gatekeeper, és módosítsák a szabályzatot úgy, hogy megengedje ezeknek a funkcióknak a használatát.

Beállítások konfigurálása az MDM-ben

A vállalati szabályzatok felügyeletének engedélyezéséhez és annak biztosítása érdekében, hogy az alkalmazottak hozzáférhessenek a szükséges erőforrásokhoz, minden Mac gép biztonságosan regisztrálva lesz az MDM-megoldásban. Az MDM-megoldás ettől kezdve konfigurációs profilokkal alkalmazza a szabályzatokat és beállításokat. A konfigurációs profilok az MDM-megoldás által létrehozott XML-fájlok, amelyek lehetővé teszik a beállítások eszközökre történő terjesztését. Ezek a profilok automatizálják a beállítások, fiókok, szabályzatok, korlátozások és hitelesítő adatok konfigurálását. A rendszerek biztonságának növelése érdekében a profilokat aláírással és titkosítással lehet ellátni.

A készülékek MDM-es regisztrálása után a rendszergazdák MDM-szabályzatokat alkalmazhatnak, vagy lekérdezéseket és parancsokat indíthatnak. A hálózati

kapcsolat létrejöttével az eszköz ezután értesítést kap az Apple push-értesítési szolgáltatáson (APNS) keresztül, így egy biztonságos kapcsolaton keresztül közvetlenül kommunikálhat az MDM-megoldással a rendszergazda által kiadott művelet végrehajtásához. Mivel a kommunikáció kizárólag az MDM-megoldás és az eszköz között zajlik, az APN-értesítések nem tartalmaznak bizalmas vagy jogvédett információkat. Ha egy eszköz felügyelete megszűnik, az adott konfigurációs profil által vezérelt beállítások és szabályzatok eltávolítására is sor kerül. Szükség esetén a vállalat távolról is törölheti egy eszköz tartalmát.

Számos cég a meglévő címtárszolgáltatásához kapcsolja az MDM-megoldást. A macOS esetében a Beállítási asszisztens felkérheti a felhasználókat, hogy az automatizált eszközregisztráció során jelentkezzenek be a saját címtárszolgáltatásuk hitelesítő adataival. A macOS Catalinán a regisztráció új testreszabási lehetőségei engedélyezik a Beállítási asszisztens számára, hogy megjelenítse a felhőalapú identitásszolgáltatók általi hitelesítést. Miután az eszközt sikerült hozzárendelni egy adott felhasználóhoz, az MDM egy személy vagy csoport igényeihez szabhatja a beállításokat és fiókokat. Egy felhasználó saját Microsoft Exchange-fiókja például automatikusan engedélyezhető a regisztráció során. Tanúsítványidentitásokat is lehet használni olyan technológiákhoz, amilyen például a 802.1x vagy a VPN.

Az ilyen rendszerek által biztosított irányítás mellett a cégek gyakran rendszergazdai hozzáférést adnak a Mac gépekhez a felhasználóknak, akik így teljesen személyre szabhatják a beállításokat, alkalmazásokat telepíthetnek, illetve hibaelhárítást is végezhetnek, miközben az MDM-en keresztül végig a céges szabályzat irányítása alatt állnak. Ez a modell olyan jogosultságokat és irányítási szintet biztosít, amilyennel a felhasználók a felügyelet alatt álló iPhone-jukon vagy iPadjükön rendelkeznek.

További információ a konfigurációs profilokról:
support.apple.com/guide/deployment-reference-macos

Az automatizált eszközregisztráció előkészítése

Az eszközök MDM-es regisztrációját az Apple Business Manager automatizált eszközregisztrációs funkcióival lehet a legegyszerűbben elvégezni a Beállítási asszisztens használatakor. Így a regisztrációhoz nincs szükség az informatikai részleg közreműködésére, a Beállítási asszisztens egyes képernyőinek leegyszerűsítésével pedig megkönnyíthető a folyamat a felhasználók számára.

Az automatizált eszközregisztráció konfigurálásához egy biztonságos tokennel össze kell kapcsolnia az MDM-megoldást és az Apple Business Manager-fiókot. Egy kétlépcsős ellenőrzési folyamat végzi az MDM-megoldások biztonságos engedélyezését. MDM-beszállítójától igényelheti az adott MDM-re vonatkozó részletes dokumentációt.

Ha az eszközöket már használják az alkalmazottak, vagy nem a cég, hanem adott személyek tulajdonában vannak, a regisztrációhoz a felhasználó egyszerűen megnyithat egy konfigurációs profilt, és jóváhagyhatja a Rendszerbeállításokban. Ezt hívjuk felhasználó által jóváhagyott MDM-regisztrációnak. A regisztrációt a készülék regisztrációjával vagy a felhasználó által jóváhagyott MDM-regisztrációval kell lebonyolítani egyes biztonságilag kényes beállítások, például a kernelbővítmény-irányelv szabályozásának vagy az adatvédelmi beállításokra vonatkozó irányelv vezérlésének (TCC) kezeléséhez.

További információ a kernelbővítmények betöltéséről:
support.apple.com/guide/deployment-reference-macos

További információ az adatvédelmi beállítások irányelvének vezérléséről:
support.apple.com/guide/mdm

Felkészülés az alkalmazások és könyvek kiosztására

Az Apple széles körű programkínálattal rendelkezik, amelyekkel a cég kihasználhatja a macOS-hez elérhető kiváló alkalmazások és tartalmak előnyeit. Ezekkel a képességekkel kioszthatja az alkalmazottak között az Apple Business Managerben vásárolt és a vállalaton belüli saját alkalmazásokat és könyveket, így minden rendelkezésre áll a hatékony munkavégzéshez. Az MDM-mel olyan alkalmazások és szoftvertelepítő csomagok is kioszthatók, amelyek a Mac App Store-ban nem érhetők el.

MDM-megoldásán keresztül a felügyelt terjesztés használatával bármely olyan országban kioszthatja az Apple Business Managerben vásárolt alkalmazásokat és könyveket, amelyben az érintett alkalmazások elérhetők. A felügyelt terjesztés engedélyezéséhez először egy biztonságos tokennel össze kell kapcsolnia az MDM-megoldást és az Apple Business Manager-fiókot. Miután csatlakozott az MDM-megoldásához, az alkalmazások és könyvek felhasználókhoz való hozzárendelése akkor is lehetséges, ha az App Store elérése le van tiltva az adott eszközön. Emellett közvetlenül is hozzárendelhet alkalmazásokat eszközökhöz, ami jelentősen megkönnyíti a kiosztást, hiszen így az adott eszközök összes felhasználója hozzáférhet az alkalmazásokhoz.

További információ az Apple Business Manageren keresztüli vásárlásról:
support.apple.com/guide/apple-business-manager

További információ az alkalmazások és könyvek kiosztásáról:
support.apple.com/guide/apple-business-manager

További tartalmak előkészítése

Az MDM-megoldással olyan csomagokat is közzétehet, amelyeknek a tartalma nem a Mac App Store áruházból származik. Számos vállalati szoftvercsomagnál, például belső egyedi alkalmazásoknál vagy a Chrome-hoz és a Firefoxhoz hasonló alkalmazásoknál ez a követendő eljárás. A szükséges szoftverek ezzel a módszerrel úgy oszthatók ki, hogy a regisztráció után automatikusan települnek. A betűtípusok, parancsfájlok és egyéb elemek szintén telepíthetők csomagokon keresztül. Ügyeljen arra, hogy a csomagok el legyenek látva a vállalati fejlesztői programban használt fejlesztői azonosítójával.

További információ a további tartalmak telepítéséről:
support.apple.com/guide/deployment-reference-macos

3. Üzembe helyezés

A macOS-en az eszközök egyszerűen hozzárendelhetők a felhasználókhoz, és az informatikai osztály bármilyen beavatkozása nélkül, igény szerint testre szabhatók és üzembe helyezhetők.

A Beállítási asszisztens használata

Az első üzembe helyezéskor az alkalmazottak a macOS Beállítási asszisztens segédprogramjával megadhatják a nyelvi és területi beállításokat, és csatlakozhatnak egy hálózathoz. Az internethez való csatlakozás után a Beállítási asszisztens ablakainak sorozata nyílik meg, amelyek végigvezetik a felhasználókat az új Mac beállításának alapvető lépésein. A folyamat során az Apple Business Managerbe regisztrált gépek automatikusan regisztrálnak az MDM-be is. A regisztrált Maceken beállíthatja, hogy bizonyos képernyők,

például a Használati feltételek, az Apple ID-bejelentkezés, a Helymeghatározási szolgáltatások stb. ne jelenjenek meg.

Az MDM-mel a Beállítási asszisztens használata után sokféle beállítást lehet megadni a kezdeti konfigurálás során, például azt, hogy egy adott felhasználónak legyenek-e teljes rendszergazdai jogosultságai a számítógépén. Az iPhone-hoz és iPadhez hasonlóan a felhasználó kezében van az eszköze feletti irányítás, de csak az MDM által kezelt vállalati szabályzatok és beállítások keretein belül. Annak érdekében, hogy a felhasználók a Beállítási asszisztens lépéseinek elvégzése után azonnal munkához láthassanak, csak a legfontosabb alkalmazások és csomagok letöltése és telepítése kezdődik meg a háttérben. Így a rendszer nem akadályozza a felhasználót a munka megkezdésében. A nagyobb alkalmazások ütemezhetők a háttérben való letöltéshez és telepítéshez. A letöltést és telepítést a felhasználó is elindíthatja később, az MDM-megoldás önkiszolgáló eszközével.

Vállalati fiókok konfigurálása

Az MDM automatikusan üzembe helyezhet levelezési és egyéb felhasználói fiókokat. A használt MDM-megoldástól és a belső rendszerekkel való integrációtól függően a fiókcsomag előzetesen is feltölthető a felhasználónevekkel, e-mail-címekkel, illetve a hitelesítéshez és aláíráshoz tartozó tanúsítványidentitásokkal.

Felhasználói személyre szabás engedélyezése

Növelheti a hatékonyságot, ha engedélyezi a felhasználóknak az eszközök személyre szabását, mivel így a felhasználók maguk választhatják ki a feladataik és céljaik teljesítéséhez leginkább megfelelő alkalmazásokat és tartalmakat. A felügyelt Apple ID-kkal és a macOS Catalina felhasználói regisztrációs funkciójával a cégek mostantól új módokon biztosíthatnak hozzáférést a felhasználók számára az Apple-szolgáltatásokhoz egy céges tulajdonban levő Apple ID-ről, amelyet akár úgy is használhatnak, hogy mellette egy személyes Apple ID-jük is van.

Apple ID és felügyelt Apple ID

Ha az alkalmazottak Apple ID-val jelentkeznek be az Apple olyan szolgáltatásaiba, mint a FaceTime, az iMessage, az App Store vagy az iCloud, tartalmak széles köréhez férhetnek hozzá, amelyek leegyszerűsítik az üzleti feladatok elvégzését, növelik a hatékonyságot, és megkönnyítik az együttműködést. A többi Apple ID azonosítóhoz hasonlóan a felügyelt Apple ID-kkal is személyes eszközökre lehet bejelentkezni. Emellett az Apple-szolgáltatások (például az iCloud, vagy az iWork és a Jegyzetek együttműködési funkciói) és az Apple Business Manager elérésére is használhatók. Az Apple ID azonosítóktól eltérően a felügyelt Apple ID-kat a cég birtokolja és kezeli, beleértve a jelszó-visszaállításokat és a szerepköralapú felügyeletet. A felügyelt Apple ID-k egyes beállításai korlátozva vannak.

A felhasználói regisztrációval regisztrált eszközöknek rendelkezniük kell felügyelt Apple ID-val. A felhasználói regisztráció egy opcionális személyes Apple ID használatát is támogatja, míg a többi regisztrációs lehetőség vagy egy személyes, vagy egy felügyelt Apple ID használatát teszi lehetővé. Csak a felhasználói regisztráció támogatja több Apple ID használatát.

Annak érdekében, hogy ki tudják használni a szolgáltatások előnyeit, az alkalmazottaknak a saját Apple ID-jukat vagy a számukra létrehozott felügyelt Apple ID-t kell használniuk. Az Apple ID-val nem rendelkező felhasználók létrehozhatják saját azonosítójukat, mielőtt megkapnák az általuk használt eszközt. A felhasználók a Beállítási asszisztensben is létrehozhatják személyes Apple ID-jukat. A felhasználóknak nincs szüksége hitelkártyára az Apple ID létrehozásához.

További információ a felügyelt Apple ID azonosítókról:
support.apple.com/guide/deployment-reference-macos

iCloud
Az iClouddal a felhasználók több eszköz között automatikusan szinkronizálhatják és naprakészen tarthatják a dokumentumokat és személyes tartalmakat, például a névjegyzékeket, naptárakat, dokumentumokat és fényképeket. A felhasználók a Lokátor alkalmazással megkereshetik elveszett vagy ellopott Mac gépüket, illetve iPhone, iPad vagy iPod touch készülékeiket. Igény szerint letilthatja az iCloud egyes részeit, például az iCloud-kulcskarikát vagy az iCloud Drive-ot. Ez akár az eszközön manuálisan, akár az MDM-megoldáson keresztül is elvégezhető. A cégek így hatékonyabban felügyelhetik, hogy milyen adatokat tárolnak az egyes fiókokban.

További információ az iCloud kezeléséről:
support.apple.com/guide/deployment-reference-macos

4. Felügyelet

Ha a felhasználók készülékei használatra készen állnak, számos különféle adminisztratív képesség érhető el az eszközök és tartalmak folyamatos felügyeletéhez és karbantartásához.

Eszközök adminisztrálása

Az MDM-megoldások különféle műveleteken keresztül kezelhetik a felügyelt eszközöket. Ilyen például az információk lekérdezése, valamint olyan feladatok futtatása, amelyekkel felügyelni lehet a szabályzatoknak nem megfelelő, elvesztett vagy ellopott eszközöket.

Lekérdezések
Egy MDM-megoldás olyan információkat kérdezhet le az eszközökről, amelyek elősegítik, hogy a felhasználók a megfelelő alkalmazásokat és beállításokat használják. A lekérdezések vonatkozhatnak hardverre, például a sorozatszámokra vagy az eszközök típusazonosítójára, de szoftverre is, például a macOS verziójára vagy a telepített alkalmazások listájára. Az MDM a legfontosabb biztonsági szolgáltatások állapotát is lekérdezheti, például a FileVaultét vagy a beépített tűzfalét.

Felügyeleti feladatok
A felügyelt eszközökön az MDM-megoldás adminisztratív feladatok széles körét tudja végrehajtani, beleértve a konfigurációs beállítások automatikus, felhasználói közreműködés nélküli módosítását, a macOS frissítését, az eszközök távoli zárolását vagy törlését, illetve a jelszavak kezelését.

További információ a felügyeleti feladatokról:
support.apple.com/guide/deployment-reference-macos

Szoftverfrissítések kezelése

Az informatikai részleg felajánlhatja a felhasználóknak a legújabb operációs rendszerre való frissítés lehetőségét. A macOS kiadás előtti verziójának tesztelésével az informatikai részleg idejében azonosíthatja az alkalmazáskompatibilitási problémákat, és még a végső kiadás előtt, a fejlesztőkkel közösen megkezdheti ezek megoldását. Az informatikai részleg részt vehet az egyes kiadások tesztelésében az Apple-szoftverek bétaverziós programján vagy az AppleSeed IT programon keresztül. Mindig tartsa naprakészen a Mac gépeket, hogy a felhasználók és az adataik biztonságban

legyenek. Frissítsen gyakran, és váltson a macOS újabb verziójára, amint megállapíthatóvá vált, hogy a munkafolyamatok kompatibilisek az újabb verzióval.

Az MDM automatikusan is frissítheti a macOS-t a regisztrált Mac gépeken. A regisztrált Mac gépeket úgy is be lehet állítani, hogy akár 90 nappal elhalasszák a frissítéseket és a rájuk vonatkozó értesítéseket, ha a fontos rendszerek még nem állnak készen. A felhasználók manuálisan nem indíthatják el a frissítéseket, amíg ez a szabályzat érvényben van, vagy amíg az MDM nem küld telepítési parancsot.

Az Apple nem ajánlja vagy támogatja a macOS-frissítések monolitikus rendszerlemezképének készítését. Ahogy az iPhone-ok és az iPadek, a Mac gépek is az adott típusra jellemző firmware-ek frissítéseit igénylik. A többi eszközhöz hasonlóan a Mac operációs rendszere is megköveteli, hogy a firmware-ek frissítéseit közvetlenül az Apple-től telepítsék. A legmegbízhatóbb stratégia a macOS telepítőjének vagy az MDM-parancsoknak a használata.

További szoftverek kezelése

A cégeknek az alapértelmezett alkalmazásokon túl gyakran további alkalmazásokat is biztosítaniuk kell a felhasználóknak. A kulcsfontosságú alkalmazásokat és frissítéseket az MDM automatikusan is közzéteheti, de igény szerint is elérhetővé tehetők – a felhasználók ebben az esetben egy önkiszolgáló portálon keresztül igényelhetik az alkalmazásokat, amelyet az MDM-megoldás biztosít. Ezek a portálok az App Store áruházból az Apple Business Manageren keresztül vásárolt alkalmazások, nem az App Store-ból származó alkalmazások, parancsfájlok és egyéb segédprogramok telepítésére is használhatók.

A legtöbb szoftver automatikusan telepíthető, de előfordulhat, hogy egyes telepítésekhez felhasználói beavatkozásra van szükség. A biztonság érdekében a kernelbővítményt igénylő alkalmazások betöltéséhez mostantól felhasználói beleegyezés szükséges. Ezt felhasználó által jóváhagyott kernelbővítmény-betöltésnek hívjuk, ami az MDM-en keresztül is felügyelhető.

Az eszközbiztonság fenntartása

Az eszközök üzembe helyezésekor felállított kezdeti biztonsági szabályzatokon túl csapatának a megfelelőség biztosítása érdekében figyelnie kell a gépeket, és meg kell oldania, hogy a lehető legtöbb jelentés érkezzen be az MDM-megoldáson keresztül. Ebbe beletartozhat az egyes eszközök biztonsági állapotának figyelése, vagy a szoftverjavítások telepítésére vonatkozó adatgyűjtés. Ugyan a legtöbb vállalat natív eszközöket használ a Mac gépek titkosítására és védelmére, egyes cégek megkövetelhetnek kiegészítő fájlszinkronizálási, megosztási vagy veszteségmegelőzési eszközöket a vállalati adatok kiszivárgása elleni védelem és a bizalmas adatokhoz kapcsolódó részletesebb jelentések készítésének érdekében.

Az iCloud Mac keresése funkciójával távoli törlés indítható el, ami eltávolítja az összes adatot, és inaktiválja az elveszett vagy ellopott Mac gépeket. Az informatikai csapatok is elindíthatnak távoli törlést az MDM-en keresztül.

Eszközök újbóli kiosztása

A Mac gépek az internetes helyreállítással vagy a helyi helyreállítási partícióval egyszerűen újra üzembe helyezhetők, ha egy alkalmazott távozik a vállalattól. Ekkor a Mac gépek adatai törlődnek, és telepíteni lehet rajtuk az operációs rendszer legújabb verzióját. Az Apple Business Managerben egy adott MDM-hez rendelt

Mac gépek a Beállítási asszisztens használata közben automatikusan újra regisztrálnak az MDM-be, konfigurálják a beállításokat az új felhasználó számára, alkalmazzák a céges szabályzatokat, és központilag telepítenek minden szükséges szoftvert. A nem regisztrált Mac gépek is törölhetők és ismételten kioszthatók ugyanezzel az eljárással, de manuálisan kell újra regisztrálni őket.

Támogatási lehetőségek

Sok cégnél az a tapasztalat, hogy a Mac-felhasználóknak minimális informatikai támogatásra van szükségük. Az önkiszolgáló támogatás ösztönzésére és a támogatás minőségének növelésére a legtöbb informatikai csapat önkiszolgáló támogatási eszközöket fejleszt ki. Ilyen lehet például egy átfogó, a Mac gépekre kihegyezett támogatási weboldal kialakítása, amely önsegítő fórumokat és helyszíni műszaki segítséget kínál. Az MDM-megoldások lehetővé tehetik a felhasználóknak, hogy támogatási feladatokat hajtsanak végre, például egy önkiszolgáló portálról telepíthessék vagy frissíthessék a szoftvereket.

A legokosabb az, ha a vállalatok nem kényszerítik a felhasználókat arra, hogy mindenre kiterjedően maguk lássák el a támogatási feladatokat. Ehelyett együttműködő módon közelítse meg a problémamegoldás kérdését, és tegye lehetővé a felhasználók számára a hibaelhárítást, mielőtt a támogatási csapathoz kellene fordulniuk. Ösztönözze a felhasználókat arra, hogy ők is részeseivé váljanak a folyamatnak, és maguk is foglalkozzanak a felmerülő problémákkal, mielőtt segítséget kérnének.

Megosztott támogatási felelősség mellett az alkalmazottaknak kevesebbet kell munkavégzés nélkül várakozniuk, és alacsonyabban tartható a támogatási csapat költsége és létszáma. Az ennél összetettebb igényekkel rendelkező cégek számára az AppleCare többféle programot és szolgáltatást biztosít, amelyek kiegészíthetik az alkalmazottak és az informatikai részlegek rendelkezésére álló belső támogatási rendszereket.

AppleCare for Enterprise

A teljes garanciát igénylő vállalatok számára az AppleCare for Enterprise segíthet csökkenteni a belső ügyfélszolgálat terhelését az alkalmazottak számára elérhető napi 24 órás telefonos műszaki támogatással, amely egyórás válaszidőt garantál, amikor kritikus problémákkal keresik meg. A program informatikairészleg-szintű integrációs forgatókönyveket biztosít, beleértve az MDM és az Active Directory kezelését.

AppleCare operációsrendszer-támogatás

Az AppleCare operációsrendszer-támogatás vállalati szintű telefonos és e-mailes támogatást biztosít az informatikai részleg számára az iOS-, iPadOS-, macOS- és macOS Server-környezetekhez. A megvásárolt támogatási szinttől függően akár a nap 24 órájában elérhető a támogatás, és egy kijelölt műszaki ügyfélkapcsolati munkatárs is rendelkezésre állhat. A szakemberek közvetlenül megkereshetők az integrációval és migrálással kapcsolatos kérdésekkel, valamint a speciális szerverüzemeltetési problémákkal kapcsolatban, így az AppleCare operációsrendszer-támogatás növelheti az informatikai csapat hatékonyságát az eszközök üzembe helyezése és felügyelete, valamint a problémák megoldása során.

AppleCare Help Desk ügyféltámogatási szerződés

Az AppleCare Help Desk ügyféltámogatási szerződés elsőbbségi telefonos kapcsolatfelvételi lehetőséget biztosít az Apple vezető műszaki támogatási szakembereivel. A szolgáltatás egy eszközcsomagot is biztosít az Apple-hardvereszközök diagnosztizálásához és hibaelhárításához, amellyel a nagyobb cégek hatékonyabban felügyelhetik erőforrásaikat, javíthatják válaszidejüket és csökkenthetik a képzési költségeket. Az AppleCare Help Desk ügyféltámogatási szerződés keretében korlátlan számú támogatási kérést lehet leadni hardverek és szoftverek diagnosztizálásához, valamint az iOS- és iPadOS-készülékek hibaelhárításához és a problémák körülhatárolásához.

AppleCare és AppleCare+ a Mac gépekhez

Minden Mac géphez egyéves korlátozott jótállás és a vásárlás dátumától számított 90 napos telefonos műszaki támogatás jár. Az AppleCare+ vagy az AppleCare Protection Plan csomaggal a szervizgarancia meghosszabbítható a vásárlás napjától számított három évre. Az alkalmazottak az Apple-hardverekkel vagy -szoftverekkel kapcsolatos kérdéseikkel az Apple támogatási csapatához fordulhatnak. Az Apple kényelmes szervizelési lehetőségeket is biztosít, ha javításra szorulnak az eszközök. Emellett a Mac gépekre érvényes AppleCare+ csomag egyes véletlen károsodások megjavítását is fedezi (további szervizdíjak fejében).

További információ az AppleCare-támogatási lehetőségekről: apple.com/support/professional/

Összegzés

Függetlenül attól, hogy a vállalat egy felhasználói csoport vagy a cég minden tagja számára helyez üzembe Mac gépeket, számos lehetőség áll a rendelkezésére az eszközök leegyszerűsített üzembe helyezéséhez és felügyeletéhez. A cégnek leginkább megfelelő stratégiák kiválasztásával növelhető az alkalmazottak hatékonysága, és új munkamódszerek vezethetők be.

Információk a macOS üzembe helyezéséről, felügyeletéről és biztonsági funkcióiról:
support.apple.com/guide/deployment-reference-macos

Információk a mobileszköz-felügyelet beállításairól az informatikai részleg számára:
support.apple.com/guide/mdm

Információk az Apple Business Managerről:
support.apple.com/guide/apple-business-manager

További információ a felügyelt Apple ID-k üzleti célú használatáról:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Információk a Munkában az Apple programról:
www.apple.com/hu/business/

Információk az informatikai funkciókról:
www.apple.com/hu/business/it/

Információk az Apple-platformok biztonságáról:
www.apple.com/security/

Az elérhető AppleCare-programok áttekintése:
www.apple.com/support/professional/

Az Apple képzési és tanúsítási programjainak megismerése:
training.apple.com

Kapcsolatfelvétel az Apple szakmai szolgáltatásait nyújtó csapattal:
consultingservices@apple.com