Yleiskatsaus Macin käyttöönottoon

Johdanto

Sisältö

Me Applella uskomme, että työntekijät yltävät parhaisiin suorituksiin, kun heillä on käytössään parhaat työkalut ja teknologia. Kaikki tuotteemme on suunniteltu tarjoamaan työntekijöille lisää mahdollisuuksia luovuuteen, tuottavuuteen ja uusiin työskentelytapoihin – niin toimistossa kuin liikkeellä oltaessakin. Tämä vastaa sitä, miten työntekijät haluavat työskennellä nykyajan maailmassa. Tieto on paremmin saatavilla, yhteistyö ja jakaminen sujuvat vaivattomasti ja yhteydenpito ja työskentely luonnistuvat paikasta riippumatta.

Mac-tietokoneiden määrittäminen ja käyttöönotto sujuvat nykypäivän yritysympäristössä helpommin kuin koskaan. Organisaatiosi voi ottaa Macin käyttöön ja tarjota sille tuen helposti laajassa mittakaavassa hyödyntämällä Applen keskeisiä palveluja ja muun valmistajan mobiililaitteiden hallintaratkaisua (mobile device management, MDM). Jos organisaatiossasi on jo otettu iOS- ja iPadOS-laitteet sisäisesti käyttöön, macOS:n käyttöönoton edellyttämästä infrastruktuuriin liittyvästä työstä on todennäköisesti suurin osa jo tehty.

Macin tietoturvan, hallinnan ja käyttöönoton uusimpien parannusten ansiosta organisaatio voi siirtyä monoliittisesta levykuvien tekemisestä ja perinteisestä hakemistosidonnaisuudesta vaivattomaan provisiointimalliin ja käyttöönottoprosessiin, jossa keskitytään kuhunkin yksittäiseen käyttäjään ja tukeudutaan lähes yksinomaan macOS:n sisäänrakennettuihin työkaluihin.

Tämä dokumentti opastaa kaikessa Macin laajamittaiseen käyttöönottoon tarvittavassa aina nykyisen infrastruktuurin ymmärtämisestä laitehallintaan ja sujuvaan provisiointiin saakka. Dokumentissa käsiteltyjä aiheita on kuvattu tarkemmin verkossa Macin käyttöönotto-oppaassa: support.apple.com/guide/deployment-reference-macos

Alkuun pääseminen

Tärkeitä alkuvaiheita käyttöönottoprosessissa ovat käyttöönottostrategian ja -suunnitelman laatiminen sekä työntekijöiden nykyisen macOS-käytön arviointi. Varmista, että kaikki tarvittavat tiimit ovat mukana varhaisessa vaiheessa ja toimivat ohjelmasi vision ja tavoitteiden mukaan. Jotkin tiimit aloittavat pienellä soveltuvuusselvityksellä havaitakseen mahdolliset omalle ympäristölleen ominaiset haasteet. Nykyisten käyttäjien mukaan ottaminen osana laajempaa pilottia on erittäin tärkeää, jotta saadaan näkemystä laitteiden käytöstä koko organisaatiossa ja mahdollisista ongelmista, joista tiimisi on hyvä tietää.

Tässä vaiheessa kerätty tieto voi auttaa määrittämään, missä työntekijöiden rooleissa ja tehtävissä Macista hyödyttäisiin eniten. IT-osasto voi sitten arvioida, tulisiko macOS tarjota standardiratkaisuna koko organisaatiolle vai valinnaisena tiettyjä työtehtäviä varten.

Tässä vaiheessa nousee usein esille myös joukko sisäisiä appeja ja työkaluja, joiden on oltava yhteensopivia ennen kuin Mac voidaan ottaa laajalti käyttöön. Keskity ensisijaisesti keskeisiin tuottavuuteen, yhteistyöhön ja viestintään liittyviin appeihin, jotka koskevat useimpia käyttäjiä. Keskeiset sisäiset palvelut, kuten yrityksen intranet, hakemisto ja kulujenhallintaohjelmisto, ovat niin ikään tuottavuuden kannalta tärkeitä suurelle osalle organisaatiota.

Dokumentoi muiden sisäisten työkalujen vaihtoehdot tai muut ratkaisutavat ja tiedota niistä. Kannusta samalla appien omistajia uudistamaan appejaan tarvittaessa. Kerro avoimesti käyttäjille kaikista erilaisista yritysapeista, joita he voivat käyttää valitessaan Macin, ja anna käyttäjien tarpeiden ohjata uudistushankkeiden priorisointia. Luo tarvittaessa appien omistajien kanssa suunnitelma siitä, miten he voivat päivittää appinsa hyödyntäen sekä macOS SDK -pakettia että Swiftiä ja eri yrityskumppaneita, jotka voivat auttaa kehitystyössä.

Mac-tietokoneet otetaan tavallisesti käyttöön yrityksen omistamina laitteina. Joissakin yrityksissä voidaan sallia työntekijöille Macin työkäyttö omien laitteiden käyttöön perustuvilla BYOD-ohjelmilla (bring-your-own-device). Omistamismallista riippumatta valinnanvapauden tarjoaminen työntekijöille Applen tuotteiden suhteen voi hyödyttää koko organisaatiota: työntekijöiden tuottavuus, luovuus, sitoutuneisuus ja työtyytyväisyys kasvavat. Lisäksi kulut laskevat, kun huomioidaan jäännösarvot ja tuki. Organisaatiot voivat myös pienentää aloituskustannuksia erilaisten leasing- ja rahoitusvaihtoehtojen avulla. Lisäksi organisaatiot voivat kompensoida kuluja siten, että ne tarjoavat työntekijöille mahdollisuuden osallistua laitepäivityksen kustannuksiin palkasta tehtävin vähennyksin tai ne voivat myös antaa työntekijöiden ostaa laitteet leasing-kauden tai laitteen elinkaaren lopussa.

Yrityksen käytännöt ja tässä dokumentissa kuvatut käyttöönotto-, hallinta- ja tukiprosessit voivat olla erilaisia riippuen tiimisi pilottiprojektin aikana keräämistä tiedoista. Kaikki käyttäjät eivät tarvitse tarkalleen samoja käytäntöjä, asetuksia ja appeja, koska eri ryhmien tai tiimien vaatimukset vaihtelevat usein huomattavasti yrityksen sisällä.

Käyttöönoton vaiheet

macOS:n käyttöönotossa on neljä päävaihetta: ympäristön valmistelu, MDM:n määritys, laitteiden käyttöönotto työntekijöiden parissa ja jatkuvat hallintatehtävät.

1. Valmistelu

Käyttöönoton ensimmäinen vaihe on olemassa olevan ympäristön tarkastelu. Tässä vaiheessa muodostetaan parempi näkemys yrityksen verkosta ja keskeisestä infrastruktuurista ja huolehditaan onnistuneeseen käyttöönottoon tarvittavista järjestelmistä.

Infrastruktuurin arvioiminen

Vaikka Mac integroituu saumattomasti suurimpaan osaan yritysten tavallisista IT-ympäristöistä, on silti tärkeää arvioida olemassa oleva infrastruktuuri ja varmistaa, että organisaatiosi saa kaikki macOS:n tarjoamat hyödyt. Jos organisaatiosi tarvitsee tässä apua, voit pyytää sitä Applen ammattilaispalveluista sekä yhteistyökumppanin tai jälleenmyyjän teknisiltä tiimeiltä.

Wi-Fi ja verkko
Jatkuva ja luotettava pääsy langattomaan verkkoon on ensisijaisen tärkeää macOS-laitteiden käyttöönotossa ja määrityksessä. Varmista, että yrityksesi Wi-Fi-verkko on hyvin suunniteltu. Mieti tarkkaan etenkin yhteyspisteiden sijoitusta ja virransaantia, jotta voit vastata roaming- ja kapasiteettitarpeisiin.

Voit myös joutua säätämään verkkovälipalvelimien tai palomuurin porttien määrityksiä, jos laitteet eivät saa yhteyttä Applen palvelimiin, Applen push-ilmoituspalveluun (APNS), iCloudiin tai iTunes Storeen. Varsinkin uudemmilla Mac-laitteilla Macin käyttöönottoprosessin tietyt osat vaativat iPadin ja iPhonen tavoin pääsyn näihin palveluihin sellaisia toimintoja kuten asennuksen aikana tehtävää laiteohjelmiston päivittämistä varten.

Apple ja Cisco ovat optimoineet Mac-tietokoneiden viestinnän Ciscon langattoman verkon kanssa tukien macOS:n edistyksellisiä verkko-ominaisuuksia, kuten Quality of Serviceä (QoS). Jos käytössäsi on Cisco-verkkolaitteisto, varmista yhteistyössä sisäisten tiimiesi kanssa, että Mac voi optimoida tärkeän liikenteen.

Yritysten on lisäksi arvioitava VPN-infrastruktuuri ja varmistettava, että käyttäjät voivat käyttää yrityksen resursseja turvallisesti etänä. Harkitse macOS:n VPN on Demand -ominaisuuden käyttämistä, jolloin VPN-yhteys käynnistetään vain tarvittaessa. Jos aiot käyttää appikohtaista VPN:ää, tarkista, että VPN-yhdyskäytävät tukevat sen ominaisuuksia ja että hankit tarpeeksi lisenssejä kattamaan kaikki käyttäjät ja yhteydet.

Varmista, että verkon infrastruktuuri on määritetty toimimaan Applen luoman standardipohjaisen ja helposti asennettavan Bonjour-verkkoprotokollan kanssa. Bonjourin avulla laitteet löytävät palvelut verkosta automaattisesti. macOS käyttää Bonjouria muodostaakseen yhteyden AirPrint-yhteensopiviin tulostimiin ja AirPlay-yhteensopiviin laitteisiin, kuten Apple TV:hen. Jotkin apit ja macOS:n vakio-ominaisuudet käyttävät Bonjouria myös toisten laitteiden etsimiseen yhteistyötä ja jakamista varten.

Lisätietoja Wi-Fi-verkon suunnittelusta:
support.apple.com/guide/deployment-reference-macos

Lisätietoja verkon määrittämisestä MDM:ää varten:
support.apple.com/HT210060

Lisätietoa Bonjourista:
support.apple.com/guide/deployment-reference-macos

Identiteettien hallinta
macOS voi käyttää identiteettien ja muiden käyttäjätietojen hallintaan hakemistopalvelimia, kuten Open Directory, Active Directory ja LDAP. Jotkut MDM-ratkaisujen myyjät tarjoavat työkaluja, joilla heidän hallintaratkaisunsa voidaan integroida suoraan Active Directory- ja LDAP-hakemistojen kanssa. Lisätyökalut, kuten macOS Catalinan Kerberos-kertakirjautuminen-laajennus, mahdollistavat integroinnin Active Directory -käytäntöjen ja -toimintojen kanssa edellyttämättä perinteistä sidonnaisuutta ja mobiilitiliä. Sekä sisäisten että ulkoisten varmentajien (certificate authority, CA) eri tyyppisiä varmenteita voidaan hallita myös yrityksesi MDM-ratkaisulla siten, että identiteetteihin luotetaan automaattisesti.

Lisätietoja uudesta Kerberos-kertakirjautuminen-laajennuksesta:
support.apple.com/guide/deployment-reference-macos

Lisätietoja hakemistointegraatiosta:
support.apple.com/guide/deployment-reference-macos

Keskeiset työntekijäpalvelut
Varmista, että Microsoft Exchange -palvelusi on ajan tasalla ja määritetty tukemaan verkon kaikkia käyttäjiä. Jos et käytä Exchangea, macOS toimii myös standardipohjaisilla palvelimilla, kuten IMAP, POP, SMTP, CalDAV, CardDAV ja LDAP. Testaa perustyönkulkuja sähköpostilla, yhteystiedoilla ja kalentereilla sekä muilla yrityksen tuottavuus- ja yhteistyöohjelmistoilla, jotka kattavat suurimman osan käyttäjien tärkeistä päivittäisistä työnkuluista.

Lisätietoja Microsoft Exchangen määrityksestä:
support.apple.com/guide/deployment-reference-macos

Lisätietoja standardipohjaisista palveluista:
support.apple.com/guide/deployment-reference-macos

Sisältövälimuisti
macOS:ään sisäänrakennettu välimuistipalvelu säilyttää paikallisen kopion Applen palvelimilta usein pyydetystä sisällöstä. Tämä auttaa vähentämään sisällön lataamiseen tarvittavaa verkon kaistanleveyttä. Välimuistia käyttämällä voit nopeuttaa ohjelmistojen lataamista ja toimittamista Mac App Storen kautta. Ohjelmistopäivityksetkin voidaan tallentaa välimuistiin, mikä nopeuttaa niiden lataamista organisaation macOS-, iOS- ja iPadOS-laitteisiin. Myös muuta sisältöä voidaan tallentaa välimuistiin muiden valmistajien, kuten Ciscon ja Akamain, ratkaisuilla.

Lisätietoja sisältövälimuistista:
support.apple.com/guide/deployment-reference-macos

Hallintaratkaisun valinta

MDM:n avulla organisaatiot voivat ottaa Macin käyttöön turvallisesti yritysympäristössä, määrittää ja päivittää asetuksia langattomasti, ottaa käyttöön appeja, valvoa käytäntöjen noudattamista, tehdä kyselyjä laitteille sekä tyhjentää tai lukita hallittuja laitteita etänä. IT-tiimi voi helposti luoda profiileja käyttäjätilien hallintaan, määrittää järjestelmäasetuksia, ottaa käyttöön rajoituksia ja asettaa salasanakäytäntöjä – kaikki samasta mobiililaitteiden hallintaratkaisusta, joka on jo käytössä iPhonessa ja iPadissa.

Kaikki Applen alustat käyttävät taustalla yhteistä Applen hallintasovelluskehystä, jonka ansiosta asiakkaat voivat käyttää erilaisia muiden valmistajien MDM-ratkaisuja. Laaja valikoima laitteiden hallintaratkaisuja on tarjolla muilta valmistajilta kuten Jamf, VMware ja MobileIron. Vaikka macOS käyttää useita samoja laitehallinnan sovelluskehyksiä kuin iOS ja iPadOS, muiden valmistajien MDM-ratkaisut eroavat toisistaan hieman ylläpitotoimintojen, käyttöjärjestelmän tuen, hintarakenteiden ja palvelumallin suhteen. Ne voivat myös tarjota eritasoisia integraatio-, koulutus- ja tukipalveluita. Arvioi ennen ratkaisun valintaa, mitkä ominaisuudet ovat organisaatiollesi tarpeellisimpia.

Kun käytettävä MDM-ratkaisu on valittu, sinun on vierailtava Apple Push Certificates Portal -portaalissa, kirjauduttava sisään ja luotava uusi MDM-push-varmenne.

Lisätietoja MDM:n käyttöönotosta:
support.apple.com/guide/deployment-reference-macos

Vieraile Apple Push Certificates Portal -sivustolla:
identity.apple.com/pushcert/

Rekisteröidy Apple Business Manageriin

Apple Business Manager on verkkopohjainen portaali IT-ylläpitäjille iPhonen, iPadin, iPod touchin, Apple TV:n ja Macin käyttöönottoon yhdestä paikasta. Apple Business Manager toimii saumattomasti yhdessä mobiililaitteen hallintaratkaisun (MDM) kanssa ja sen avulla voidaan helposti automatisoida laitteiden käyttöönoton hallinta, hankkia appeja ja jakaa sisältöä sekä luoda hallittuja Apple ID:itä työntekijöille.

Laiterekisteröintiohjelma (DEP) ja määrälisenssiohjelma (VPP) on nyt täysin integroitu Apple Business Manageriin, joten organisaatiot voivat nyt keskittää kaikki organisaation Apple-laitteiden käyttöönottoon tarvittavat asiat yhteen paikkaan. Nämä ohjelmat eivät ole enää saatavilla 1. joulukuuta 2019 alkaen.

Laitteet

Apple Business Managerin mahdollistama automaattinen laiterekisteröinti tarjoaa organisaatioille nopean ja sujuvan tavan ottaa käyttöön ja rekisteröidä MDM:ään yrityksen omistamia Apple-laitteita ilman, että jokainen laite täytyy käsitellä tai valmistella fyysisesti.

- Helpota käyttöönottoa käyttäjille selkeyttämällä vaiheet käyttöönottoapurissa varmistaen, että työntekijät saavat oikeat määritykset heti aktivoinnin jälkeen. IT-tiimit voivat nyt muokata kokemusta entisestään tarjoamalla työntekijöille suostumustekstiä, yritysbrändäystä ja nykyaikaista todentamista.

- Yrityksen omistamia laitteita voidaan hallita paremmin käyttämällä valvontaa, joka tarjoaa lisää laitehallintavaihtoehtoja, joita ei ole saatavilla muille käyttöönottomalleille, pysyvä MDM mukaan lukien.
- Hallitse MDM-oletuspalvelimia entistä helpommin asettamalla laitetyyppikohtainen oletuspalvelin. Nyt voit myös rekisteröidä iPhonen, iPadin ja Apple TV:n käsin Apple Configurator 2:lla laitteiden hankintatavasta riippumatta.

Sisältö

Apple Business Manager tarjoaa organisaatioille mahdollisuuden hankkia helposti suuria määriä sisältöä. Käyttivätpä työntekijät iPhonea, iPadia tai Macia, voit tarjota upeaa ja käyttövalmista sisältöä joustavien ja turvallisten jakeluvaihtoehtojen avulla.

- Osta suuria määrejä appeja, kirjoja ja räätälöityjä appeja, mukaan lukien organisaation sisällä kehitetyt apit. Voit helposti siirtää appilisenssejä sijaintien välillä ja jakaa lisenssejä samassa sijainnissa olevien ostajien kesken. Näet myös kootun luettelon ostohistoriasta, mukaan lukien MDM:n kautta käytössä olevien lisenssien määrän.
- Jaa appeja ja kirjoja suoraan hallittuihin laitteisiin tai valtuutetuille käyttäjille ja seuraa kätevästi sitä, mitä sisältöä on jaettu kullekin käyttäjälle tai laitteelle. Hallitulla jakelulla voit hallita koko jakeluprosessia säilyttäen samalla appien omistuksen. Niiden appien käyttöoikeus, joita tietty laite tai käyttäjä ei enää tarvitse, voidaan poistaa, ja ne voidaan määrittää uudelleen organisaation sisällä.
- Käytä eri maksutapoja, kuten luottokortteja ja hankintatilauksia. Organisaatiot voivat ostaa määrälisenssiluottoa (alueilla, joissa se on saatavilla) Applelta tai Applen valtuutetulta jälleenmyyjältä tietyllä summalla, joka toimitetaan tilin haltijalle sähköisesti luottona.
- Jaa appi laitteisiin tai käyttäjille kaikissa maissa, joissa se on saatavilla. Näin voit jaella niitä kansainvälisellä tasolla. Kehittäjät voivat tuoda appinsa saataville useissa maissa tavallisen App Store -julkaisuprosessin kautta.

Huomaa: Kirjaostokset Apple Business Managerissa eivät ole saatavilla kaikissa maissa tai kaikilla alueilla. Lisätietoja ominaisuuksien ja ostotapojen saatavuudesta on osoitteessa support.apple.com/HT207305.

Ihmiset

Apple Business Managerin avulla organisaatiot voivat luoda ja hallita työntekijöiden tilejä, jotka integroituvat olemassa olevaan infrastruktuuriin, ja tarjota pääsyn Applen appeihin ja palveluihin sekä Apple Business Manageriin.

- Luo hallittuja Apple ID:itä, joiden avulla työntekijät voivat tehdä yhteistyötä Applen appien ja palveluiden parissa ja päästä käsiksi iCloud Drivea käyttävissä hallituissa apeissa oleviin työtietoihin. Nämä tilit ovat kunkin organisaation omistamia ja hallinnoimia.
- Hyödynnä yhdistettyä todennusta yhdistämällä Apple Business Manager Microsoft Azure Active Directoryn kanssa. Hallitut Apple ID:t luodaan automaattisesti, kun kukin työntekijä kirjautuu ensimmäistä kertaa yhteensopivaan Apple-laitteeseen olemassa olevilla tunnuksillaan.
- Käytä hallittuja Apple ID:itä työntekijän omistamalla laitteella yhdessä henkilökohtaisen Apple ID:n kanssa iOS 13:n, iPadOS:n ja macOS Catalinan

uusilla käyttäjän rekisteröintiominaisuuksilla. Vaihtoehtoisesti voidaan käyttää hallittuja Apple ID:itä ensisijaisena (ja ainoana) Apple ID:nä missä tahansa laitteessa. Hallitut Apple ID:t voivat myös käyttää iCloudia verkossa sen jälkeen, kun Apple-laitteeseen on kirjauduttu ensimmäistä kertaa.

- Määritä muita rooleja organisaatiosi IT-tiimeille, jotta voit tehokkaasti hallita laitteita, appeja ja tilejä Apple Business Managerissa. Käytä ylläpitäjän roolia ehtojen hyväksymiseen tarpeen vaatiessa ja vastuiden helppoon siirtämiseen, kun joku lähtee organisaatiosta.

Huomaa: iCloud Drivea ei tällä hetkellä tueta käyttäjän rekisteröinnissä. iCloud Drivea voidaan käyttää hallitulla Apple ID:llä, jos se on laitteen ainoa Apple ID.

Lisätietoja Apple Business Managerista: apple.com/fi/business/it

Rekisteröityminen Applen Developer Enterprise Program -ohjelmaan

Applen Developer Enterprise Program -ohjelma tarjoaa kattavat työkalut appien kehittämiseen, testaamiseen ja käyttäjille jakamiseen. Appeja voidaan jakaa verkkopalvelimen tai MDM-ratkaisun kautta. Kehittäjän tunnuksellasi Mac-apit ja -asentajat voidaan todistaa oikeiksi Gatekeeperille, joka auttaa suojaamaan macOS:ää haittaohjelmilta.

Lisätietoja Developer Enterprise Program -ohjelmasta: developer.apple.com/programs/enterprise

2. Määritys

Käyttöönoton määritysvaiheen aikana luodaan yrityksen käytännöt ja valmistellaan MDM-ratkaisu työntekijöiden Macien määrittämistä varten.

macOS:n tietoturvan ymmärtäminen

Tietoturva ja yksityisyys ovat olennainen osa Applen laitteiston, ohjelmiston ja palveluiden suunnittelua. Suojaamme asiakkaidemme yksityisyyttä vahvalla salauksella ja tiukoilla käytännöillä, jotka määrittävät tietojen käsittelytavat. Suojatun alustan tarjoaminen Apple-laitteille pitää sisällään seuraavat asiat:

- menetelmät, jotka estävät laitteiden luvattoman käytön
- levossa olevan datan suojaus myös silloin, kun laite katoaa tai varastetaan
- verkkoprotokollat ja datan salaus liikkeessä
- appien suojatun toiminnan mahdollistaminen ilman, että alustan luotettavuudesta tingitään

Kaikkiin Apple-laitteisiin on rakennettu useita suojaustasoja, jotta ne voivat käyttää verkkopalveluja turvallisesti ja suojata tärkeitä tietoja. macOS, iOS ja iPadOS tarjoavat suojausta myös pääsykoodi- ja salasanakäytännöillä, jotka voidaan toimittaa ja pakottaa käyttöön MDM:n avulla. Käyttäjä tai ylläpitäjä voi poistaa kaikki henkilökohtaiset tiedot käyttämällä etäkomentoa, jos laite joutuu vääriin käsiin.

IT-osasto voi MDM:n avulla ottaa käyttöön useita eri käytäntöjä laitteiden suojaamiseksi. Näitä ovat esimerkiksi FileVault ja palautusavaimen luottamusketju MDM:n kanssa, tietyn salasanakäytännön tai näytönsäästäjän lukituksen pakottaminen ja sisäänrakennetun palomuurin käyttäminen.

Lisätietoja Apple Platform Securitysta: apple.com/security/

Yrityksen käytäntöjen luominen

Aloita yrityksen käytäntöjen kehittäminen vakiinnuttamalla yleisiä käytäntöjä, jotka koskevat suurinta osaa yrityksesi Mac-käyttäjistä. MDM-ratkaisusi avulla voit määrittää käyttäjäkohtaisia asetuksia, esimerkiksi tilejä tai pääsyn tiettyihin appeihin. Voit myös asettaa tiettyjä käytäntöjä organisaatioille tai muille pienemmille käyttäjäryhmille. Yksi esimerkki tästä on osastokohtaisten ohjelmistojen tai asetusten käyttöönotto.

Päivitä olemassa olevat yrityksen käytännöt yhteistyössä sisäisten tiimien kanssa niin, että ne sisältävät Mac-tietokoneiden käytön. Jotkin keskeiset käytännöt pysyvät samoina kaikilla alustoilla, kuten esimerkiksi salasanojen monimutkaisuuteen ja vaihtoon liittyvät vaatimukset, näytönsäästäjien ajastus ja hyväksyttävä käyttö.

Mikäli yrityksesi käytäntö vaatii tiettyä toisella alustalla käytettävää teknologiaa, selvitä taustalla vaikuttava ongelma ja mukauta käytäntö kattamaan macOS:n sisäänrakennetut teknologiat. Sen sijaan, että vaadittaisiin kaikkia tietokoneita käyttämään tiettyä muun valmistajan ratkaisua koko levyn salaamiseen, harkitse sellaista käytäntöä, joka edellyttää levossa olevien yritystietojen salaamista, ja tämän käytännön toteuttamista FileVaultilla. Jos käytäntö edellyttää tiettyä ohjelmistoa haittaohjelmilta suojautumiseen, perehdytä tiimit sisäänrakennettuihin ominaisuuksiin (kuten Gatekeeper) ja päivitä sitten käytäntöä niin, että se hyväksyy myös kyseisten ominaisuuksien käytön.

Asetusten määrittäminen MDM:ssä

Jotta yrityksen käytäntöjä voidaan hallita ja työntekijöiden pääsy tarvittaviin resursseihin varmistaa, jokainen Mac rekisteröidään turvallisesti MDM-ratkaisuusi. MDM-ratkaisut soveltavat sitten käytäntöjä ja asetuksia asetusprofiilien avulla. Asetusprofiilit ovat MDM-ratkaisun luomia XML-tiedostoja, jotka mahdollistavat asetusten jakamisen laitteisiin. Nämä profiilit automatisoivat asetusten, tilien, käytäntöjen, rajoitusten ja tunnistetietojen määritykset. Ne voidaan allekirjoittaa ja salata, jolloin järjestelmät ovat vieläkin turvallisempia.

Kun laite on rekisteröity MDM:ään, ylläpitäjä voi suorittaa MDM-käytännön, -kyselyn tai -komennon. Tämän jälkeen laite saa verkkoyhteydessä ollessaan Applen push-ilmoituspalvelun (APNS) kautta ilmoituksen, joka ohjaa sitä kommunikoimaan suoraan MDM-ratkaisun kanssa suojatun yhteyden kautta, jotta ylläpitäjän toimenpide voidaan käsitellä. APNS ei välitä luottamuksellista tai omisteista tietoa, koska kommunikaatio on pelkästään MDM-ratkaisun ja laitteen välistä. Jos laite poistetaan hallinnasta, kyseisen asetusprofiilin hallinnoimat asetukset ja käytännöt poistetaan. Yritys voi myös tarvittaessa tyhjentää laitteen etänä.

Monet organisaatiot liittävät MDM-ratkaisun olemassa oleviin hakemistopalveluihinsa. macOS:n käyttöönottoapuri voi kehottaa käyttäjiä kirjautumaan sisään hakemistopalvelun tunnistetiedoillaan automaattisen laiterekisteröinnin yhteydessä. macOS Catalinan uusien rekisteröinnin muokkausvaihtoehtojen ansiosta käyttöönottoapuri voi näyttää todennuksen pilvipohjaisilta tunnistetietojen tarjoajilta. Kun laite on määritetty tietylle käyttäjälle, MDM voi muokata määrityksiä ja tilejä käyttäjä- tai ryhmäkohtaisesti.

Esimerkiksi käyttäjän Microsoft Exchange -tili voidaan ottaa käyttöön automaattisesti rekisteröitymisen aikana. On myös mahdollista käyttää varmenteita esimerkiksi 802.1x- ja VPN-teknologioille.

Näiden järjestelmien tarjoamat hallintamahdollisuudet huomioiden yrityksissä annetaan usein mielellään käyttäjille ylläpito-oikeudet omaan Maciinsa. Näin he voivat vapaasti muokata asetuksia, asentaa appeja ja ratkaista ongelmia. Samalla he pysyvät kuitenkin yrityksen käytäntöjen hallinnassa MDM:n kautta. Tässä mallissa noudatetaan samantyyppisiä käyttöoikeuksia ja rajoituksia kuin mitä käyttäjillä on hallinnan piirissä olevassa iPhonessa tai iPadissa.

Lisätietoja asetusprofiileista:
support.apple.com/guide/deployment-reference-macos

Automaattisen laiterekisteröinnin valmistelu

Helpoin tapa rekisteröidä laite MDM:ään on tehdä se käyttöönottoapurin suorittamisen aikana Apple Business Managerin automaattisten laiterekisteröintiominaisuuksien kautta. Tämä mahdollistaa rekisteröinnin ilman IT-osaston toimenpiteitä, ja prosessia voidaan nopeuttaa käyttäjien kannalta selkeyttämällä käyttöönottoapurin tiettyjä valikoita.

Jotta voit tehdä automaattisen laiterekisteröinnin määritykset, sinun tulee ensin linkittää MDM-ratkaisusi Apple Business Manager -tiliisi suojaustunnusta käyttäen. Kaksivaiheinen vahvistusprosessi valtuuttaa MDM-ratkaisun turvallisesti. Saat sen käyttöönottoon liittyvät tarkemmat dokumentit MDM-palveluntarjoajaltasi.

Jos laitteet ovat jo työntekijöiden käytössä tai heidän omistamiaan, käyttäjä voi avata yksittäisen asetusprofiilin, joka voidaan varmentaa Järjestelmäasetuksissa rekisteröinnin loppuun saattamiseksi. Tätä kutsutaan käyttäjän hyväksymäksi MDM-rekisteröinniksi. Rekisteröinnin tulee tapahtua joko laiterekisteröinnin kautta tai käyttäjän hyväksymän MDM-rekisteröinnin kautta, jotta tiettyjä tietoturvan kannalta kriittisiä asetuksia (kuten kernelin laajennuskäytäntöä ja Yksityisyysasetukset-käytännön ohjausta) voidaan hallita.

Lisätietoja kernelin laajennusten latauksesta:
support.apple.com/guide/deployment-reference-macos

Lisätietoja Yksityisyysasetukset-käytännön ohjauksesta:
support.apple.com/guide/mdm

Appien ja kirjojen jakamiseen valmistautuminen

Apple tarjoaa kattavia ohjelmakokonaisuuksia, jotka auttavat organisaatiotasi hyödyntämään macOS:lle saatavia upeita appeja ja sisältöä. Ne mahdollistavat Apple Business Managerin kautta hankittujen appien ja kirjojen tai yrityksen omien sisäisten appien jakamisen työntekijöille, jotta heillä on kaikki tarvitsemansa tuottavaan työskentelyyn. MDM voi myös jakaa appeja ja asentaa ohjelmistopaketteja, joita ei ole saatavilla Mac App Storessa.

MDM-ratkaisusi voi käyttää hallittua jakelua Apple Business Managerin kautta hankittujen appien ja kirjojen hallintaan maissa, joissa appi on saatavilla. Jos haluat käyttää hallittua jakelua, sinun on ensin linkitettävä MDM-ratkaisusi Apple Business Manager -tiliisi suojaustunnuksen avulla. Kun olet muodostanut

yhteyden MDM-ratkaisuun, voit jakaa käyttäjille appeja ja kirjoja, vaikka App Store ei olisi laitteella käytössä. Voit jakaa appeja myös suoraan laitteisiin, mikä helpottaa käyttöönottoa huomattavasti, koska kenellä tahansa laitetta käyttävällä on tällöin pääsy kaikkiin appeihin.

Lisätietoja sisällön ostamisesta Apple Business Managerissa:
support.apple.com/guide/apple-business-manager

Lisätietoja appien ja kirjojen jakamisesta:
support.apple.com/guide/apple-business-manager

Muun sisällön valmistelu

Voit jakaa MDM-ratkaisusi avulla muita paketteja, joiden sisältö ei ole peräisin Mac App Storesta. Tämä on yleinen lähestymistapa monien yritysohjelmistopakettien osalta, esimerkkeinä räätälöidyt sisäiset apit tai Chromen ja Firefoxin kaltaiset apit. Tarvittavat ohjelmistot voidaan jakaa tällä menetelmällä ja asentaa automaattisesti rekisteröinnin suorittamisen jälkeen. Fontit, skriptit tai muut vastaavat voidaan myös asentaa ja suorittaa paketteina. Varmista, että nämä paketit on allekirjoitettu asianmukaisesti omalla Developer Enterprise Program -ohjelman kehittäjän tunnuksellasi.

Lisätietoja muun sisällön asentamisesta:
support.apple.com/guide/deployment-reference-macos

3. Käyttöönotto

macOS:n ansiosta laitteet voidaan antaa helposti työntekijöiden käyttöön, niitä voidaan personoida tarpeen mukaan ja niiden käyttö voidaan aloittaa ilman IT-osaston toimenpiteitä.

Käyttöönottoapurin käyttäminen

Työntekijät voivat hyödyntää käyttöönottoapuria macOS:ssä käynnistyksen aikana ja tehdä kieli- ja alueasetuksia sekä muodostaa yhteyden verkkoon. Kun laite yhdistää internetiin, käyttöönottoapurin valikot opastavat käyttäjiä uuden Macin käyttöönoton perusvaiheissa. Apple Business Manageriin rekisteröidyt laitteet voidaan rekisteröidä automaattisesti MDM:ään tämän prosessin aikana. Laiterekisteröidyt Macit voidaan myös määrittää ohittamaan tiettyjä valikkoja, kuten esimerkiksi ehtojen lukeminen, Apple ID -kirjautuminen ja Sijaintipalvelut.

Käyttöönottoapurin jälkeen voidaan MDM:n avulla määrittää monenlaisia alkuasetuksia. Näihin sisältyy muun muassa sen määrittäminen, saako käyttäjä täydet ylläpito-oikeudet tietokoneeseensa. Aivan kuten iPhonen ja iPadinkin kohdalla, tämä mahdollistaa käyttäjille omien laitteidensa hallinnan, mutta samalla he noudattavat MDM:llä hallittuja yrityksen käytäntöjä ja asetuksia. Jotta käyttäjät voisivat olla välittömästi tuottavia käyttöönottoapurin suorittamisen jälkeen, vain kaikkein tärkeimpien appien ja pakettien tulisi alkaa latautua ja asentua taustalla. Näin käyttäjä voi alkaa työskennellä häiriöttömästi. Käyttäjä voi aikatauluttaa suuremmat apit latautumaan ja asentumaan taustalla tai myöhempänä ajankohtana MDM-ratkaisun itsepalvelutyökalussa.

Yritystilien määrittäminen

MDM:llä voidaan ottaa sähköposti ja muita käyttäjätilejä automaattisesti käyttöön. Riippuen käyttämästäsi MDM-ratkaisusta ja sen integraatiosta sisäisten järjestelmien kanssa tilien tietosisältöihin voidaan sisällyttää valmiiksi myös käyttäjän nimi, sähköpostiosoite sekä varmenteet todentamista ja allekirjoittamista varten.

Käyttäjäkohtaisen personoinnin salliminen

Tuottavuus voi lisääntyä, jos käyttäjät voivat personoida laitteitaan. Silloin he voivat itse päättää, mitkä apit ja sisällöt parhaiten auttavat heitä suorittamaan tehtävänsä ja saavuttamaan tavoitteensa. Hallittujen Apple ID:iden ja macOS Catalinan käyttäjän rekisteröinnin myötä organisaatioilla on uusia tapoja tarjota käyttäjille pääsy Applen palveluihin organisaation omistamalla Apple ID:llä tai henkilökohtaisella Apple ID:llä.

Apple ID ja hallittu Apple ID

Kun työntekijät kirjautuvat Apple ID:llä Applen palveluihin kuten FaceTimeen, iMessageen, App Storeen ja iCloudiin, he pääsevät monenlaiseen sisältöön, joka sujuvoittaa tehtäviä yrityksessä, parantaa tuottavuutta ja tukee yhteistyötä. Hallittuja Apple ID:itä käytetään tavallisen Apple ID:n tavoin sisäänkirjautumiseen henkilökohtaisessa laitteessa. Niilläkin pääsee Applen palveluihin – mukaan lukien iCloud ja iWorkin ja Muistiinpanojen yhteistyöominaisuudet – ja Apple Business Manageriin. Toisin kuin tavalliset Apple ID:t, hallitut Apple ID:t ovat organisaation omistamia ja organisaatio hallitsee niitä muun muassa salasanan nollaamisen ja rooliin perustuvan ylläpidon osalta. Hallituilla Apple ID:illä on tiettyjä rajoitettuja asetuksia.

Käyttäjän rekisteröinnin kautta rekisteröidyt laitteet vaativat hallitun Apple ID:n. Käyttäjän rekisteröinti tukee valinnaista henkilökohtaista Apple ID:tä. Muut rekisteröintivaihtoehdot puolestaan tukevat joko henkilökohtaista Apple ID:tä tai hallittua Apple ID:tä. Vain käyttäjän rekisteröinti tukee useaa Apple ID:tä.

Saadakseen parhaan hyödyn näistä palveluista käyttäjien kannattaa käyttää omia Apple ID:itä tai heille luotuja hallittuja Apple ID:itä. Käyttäjät, joilla ei ole Apple ID:tä, voivat luoda sellaisen jo ennen kuin saavat laitteen. Käyttöönottoapurilla käyttäjä voi myös luoda henkilökohtaisen Apple ID:n, jos hänellä ei sellaista ole. Käyttäjät eivät tarvitse luottokorttia Apple ID:n luomiseen.

Lisätietoja hallituista Apple ID:istä:
support.apple.com/guide/deployment-reference-macos

iCloud

iCloudilla käyttäjät voivat automaattisesti synkronoida dokumentteja ja henkilökohtaista sisältöä, kuten yhteystietoja, kalentereita, dokumentteja ja valokuvia, ja pitää ne ajan tasalla useiden laitteiden kesken. Missä on…? -ominaisuudella käyttäjät voivat paikantaa kadonneen tai varastetun Macin, iPhonen, iPadin tai iPod touchin. Tietyt iCloudin osat (kuten iCloud-avainnippu ja iCloud Drive) voidaan poistaa käytöstä asettamalla rajoituksia joko käsin laitteella tai MDM:n kautta. Näin organisaatiot voivat paremmin hallita sitä, mitä tietoja tallennetaan millekin tilille.

Lisätietoja iCloudin hallitsemisesta:
support.apple.com/guide/deployment-reference-macos

4. Hallinta

Kun käyttäjät ovat päässeet alkuun, saatavilla on laaja valikoima ylläpitotoimintoja laitteiden ja sisällön hallintaan ja ylläpitoon pidemmällä aikavälillä.

Laitteiden hallinta

MDM-ratkaisut voivat suorittaa tiettyjä ylläpitotoimintoja hallitulle laitteelle. Näihin toimintoihin lukeutuvat tietojen kyseleminen laitteilta sekä käytäntöjä noudattamattomiin, kadonneisiin tai varastettuihin laitteisiin kohdistetut hallintatoimet.

Kyselyt

MDM-ratkaisu voi kysellä laitteilta monenlaisia tietoja ja auttaa varmistamaan, että käyttäjillä on laitteissa oikeat apit ja asetukset. Kyselyt voivat koskea laitteistoa, kuten esimerkiksi sarjanumeroa tai laitteen mallia, tai ohjelmistoa, kuten macOS-versiota tai luetteloa asennetuista apeista. Lisäksi MDM voi kysellä keskeisten suojausominaisuuksien kuten FileVaultin tai sisäänrakennetun palomuurin tilaa.

Hallintatoimet

MDM-ratkaisu voi suorittaa hallitussa laitteessa useita erilaisia ylläpitotoimia, kuten määritysasetusten automaattinen muuttaminen ilman käyttäjän toimenpiteitä, macOS-version päivittäminen, laitteen lukitseminen tai tyhjentäminen etänä tai salasanojen hallinta.

Lisätietoja hallintatehtävistä:
support.apple.com/guide/deployment-reference-macos

Ohjelmistopäivitysten hallinta

IT-osasto voi antaa käyttäjien päivittää uusimpaan käyttöjärjestelmään sen tullessa saataville. Testaamalla macOS:n ennakkoversion IT-osasto voi varmistaa, että appien yhteensopivuusongelmat huomataan ajoissa. Näin kehittäjät voivat korjata ne jo ennen lopullista julkistusta. IT-osasto voi osallistua kunkin version testaamiseen Apple Beta Software Program- tai AppleSeed for IT -ohjelman kautta. Valitse kokonaisvaltainen lähestymistapa Mac-tietokoneiden pitämiseen ajan tasalla käyttäjien ja heidän tietojensa suojaamiseksi. Päivitä useasti ja heti, kun olet todennut yrityksesi työnkulut yhteensopiviksi uuden macOS-version kanssa.

MDM voi lähettää macOS-päivitykset automaattisesti laiterekisteröityyn Maciin. Laiterekisteröity Mac voidaan myös määrittää siirtämään päivityksiä ja päivitysilmoituksia enintään 90 päivän verran, jos tärkeät järjestelmät eivät ole valmiina. Käyttäjät eivät voi käynnistää päivityksiä manuaalisesti ennen kuin käytäntö poistetaan tai MDM lähettää asennuskomennon.

Apple ei suosittele tai tue monoliittista järjestelmän kuvantamista macOS-päivityksiä varten. iPhonen ja iPadin tavoin Mac-tietokoneet tarvitsevat usein niiden malleille sopivat laiteohjelmistopäivitykset. Vastaavasti Mac-käyttöjärjestelmän päivitykset määräävät, että nämä laiteohjelmistopäivitykset asennetaan suoraan Applelta. Kaikkein varminta on käyttää päivittämiseen macOS-asentajaa tai MDM-komentoja.

Lisäohjelmistojen hallinta

Organisaatioiden on usein jaettava alkuvaiheen appien jälkeen käyttäjilleen lisäappeja. Tämä voidaan hoitaa automaattisesti MDM:llä tärkeiden appien ja päivitysten osalta tai tarpeen mukaan niin, että työntekijät voivat pyytää appeja MDM-ratkaisun tarjoaman itsepalveluportaalin kautta. Näiden portaalien avulla voidaan asentaa App Storesta Apple Business Managerin kautta hankittuja ohjelmistoja, muualta kuin App Storesta hankittuja appeja, skriptejä sekä muita työkaluja.

Useimmat ohjelmistot voidaan asentaa automaattisesti, mutta tietyt asennukset voivat vaatia käyttäjän toimenpiteitä. Tietoturvan parantamiseksi kernelin laajennuksia vaativat apit edellyttävät nyt käyttäjän suostumusta latautuakseen. Tämä tunnetaan käyttäjän hyväksymänä kernelin laajennuksen latauksena ja sitä voidaan hallita MDM:llä.

Laitteen tietoturvan ylläpito

Laadittuaan ensin ennen laitteiden käyttöönottoa alkuvaiheen tietoturvakäytännöt tiimisi kannattaa jatkossa valvoa koneita käytäntöjen noudattamisen osalta ja hakea mahdollisimman paljon raportteja MDM-ratkaisun kautta. Tähän voi sisältyä kunkin laitteen tietoturvan tilan valvonta tai tietojen kerääminen ohjelmistopatchien asennuksesta. Vaikka useimmissa organisaatioissa käytetään mielellään natiiveja työkaluja Macien salaamiseen ja suojaukseen, joissakin organisaatioissa voidaan vaatia käyttämään muita tiedostojen synkronointi- ja jakopalveluita tai tietojen katoamisen estäviä työkaluja, joilla estetään yritystietojen vuotaminen ja tuotetaan luottamuksellista tietoa koskevia perusteellisia raportteja.

iCloudin Etsi Macini -ominaisuus voi käynnistää etätyhjennyksen, joka poistaa kaikki tiedot ja deaktivoi Macin, jos se on kadonnut tai varastettu. IT-tiimit voivat suorittaa etätyhjennyksen myös MDM:llä.

Laitteiden antaminen uusille käyttäjille

Kun työntekijä lähtee organisaatiosta, Mac voidaan antaa helposti toiselle käyttäjälle internet-palautuksen ja paikallisen palautusosion avulla. Näin voidaan tyhjentää Macin sisältö ja asentaa käyttöjärjestelmän uusin versio. Mac, joka on liitetty tiettyyn MDM:ään Apple Business Managerissa, rekisteröityy MDM:ään uudelleen automaattisesti käyttöönottoapurin aikana, määrittää uuden käyttäjän asetukset, soveltaa yrityksen käytäntöjä ja ottaa käyttöön kaikki tarvittavat ohjelmistot. Rekisteröimättömät Mac-tietokoneet voidaan tyhjentää samalla prosessilla ja sitten rekisteröidä uudelleen manuaalisesti.

Tukivaihtoehdot

Monissa Macia käyttävissä organisaatioissa tarvitaan vain vähän IT-osaston tukea. Useimmat IT-osastot kehittävät itsenäisen tuen työkaluja, jotka kannustavat omatoimisuuteen tukiasioissa ja parantavat tuen laatua. Esimerkkejä ovat kattavan Mac-tukisivun luominen sekä itsenäisen tuen foorumien ja paikallisen teknisen tuen tarjoaminen. MDM-ratkaisut voivat myös tarjota käyttäjille mahdollisuuden suorittaa tukitehtäviä, kuten asentaa tai päivittää ohjelmistoja itsepalveluportaalista.

Paras käytäntö on, ettei yritysten tulisi pakottaa käyttäjiä olemaan täysin itsenäisen tuen varassa. Sen sijaan kannattaa lähestyä ongelmanratkaisua yhteistyön näkökulmasta ja keskittyä siihen, että käyttäjillä on mahdollisuus ratkaista ongelmia itse ennen yhteyden ottamista tukipalveluihin. Kannusta käyttäjiä panostamaan prosessissa yhteistyöhön ja tutkimaan ongelmia itse ennen avun pyytämistä.

Jaetun tukivastuun ansiosta käyttäjien käyttökatkot ovat lyhyempiä ja tukikustannukset sekä henkilöstöresurssien tarve vähenevät. Vaativammille organisaatioille AppleCare tarjoaa monenlaisia ohjelmia ja palveluja, jotka täydentävät työntekijöiden ja IT-osaston käytössä olevia sisäisiä tukirakenteita.

AppleCare for Enterprise

Kattavaa turvaa hakevien yritysten kohdalla AppleCare for Enterprise voi auttaa vähentämään sisäisten tukipalveluiden kuormitusta tarjoamalla teknistä tukea työntekijöille puhelimitse ympäri vuorokauden tunnin vasteajoilla kiireellisimmän vakavuusluokan ongelmissa. Ohjelma kattaa IT-osastotason integrointiskenaariot, MDM ja Active Directory mukaan lukien.

AppleCare OS Support

AppleCare OS Support tarjoaa IT-osastollesi suuryritystason puhelin- ja sähköpostitukea iOS:n, iPadOS:n, macOS:n ja macOS Serverin käyttöönotoissa. Ostetun tuen tasosta riippuen se tarjoaa jopa ympärivuorokautista tukea sekä oman Technical Account Managerin. AppleCare OS Support tarjoaa suoran yhteyden teknisiin asiantuntijoihin kysymyksissä, jotka koskevat integrointia, siirtymistä ja monimutkaisia palvelintoimintoja. Näin se voi lisätä IT-henkilöstösi tehokkuutta laitteiden käyttöönotossa ja hallinnassa sekä ongelmien ratkaisussa.

AppleCare Help Desk Support

AppleCare Help Desk Support tarjoaa nopean puhelinyhteyden Applen kokeneeseen tekniseen tukihenkilöstöön. Palvelu sisältää myös työkalupaketin, jolla voidaan diagnosoida ja ratkaista Apple-laitteistoihin liittyviä ongelmia. Näin suuret organisaatiot voivat hyödyntää resursseja tehokkaammin, parantaa vasteaikaa ja vähentää koulutuskuluja. AppleCare Help Desk Support kattaa rajoittamattoman määrän tukitapahtumia, jotka koskevat laitteiston ja ohjelmiston diagnosointia ja vianetsintää iOS- ja iPadOS-laitteista.

AppleCare ja AppleCare+ Macille

Jokaisella Macilla on vuoden rajoitettu takuu ja 90 päivän ilmainen tekninen puhelintuki ostopäivästä lukien. Huoltoturva voidaan laajentaa kolmeen vuoteen alkuperäisestä ostopäivästä alkaen hankkimalla AppleCare+ tai AppleCare Protection Plan. Työntekijät voivat soittaa Applen tukeen, kun heillä on Applen laitteistoihin tai ohjelmistoihin liittyviä kysymyksiä. Applella on myös kätevät huoltovaihtoehdot laitteiden korjaamista varten. AppleCare+ Macille tarjoaa lisäksi tiettyjen käsittelystä aiheutuneiden vahinkotapausten turvan. Näistä tapauksista peritään palvelumaksu.

Lisätietoja AppleCare-tukivaihtoehdoista:
apple.com/fi/support/professional/

Yhteenveto

Riippumatta siitä, ottaako yrityksesi Mac-tietokoneita käyttöön vain joidenkin käyttäjien vai koko organisaation osalta, laitteiden käyttöönottoon ja hallintaan on useita helppoja vaihtoehtoja. Valitsemalla organisaatiollesi sopivat strategiat voit auttaa työntekijöitäsi toimimaan tuottavammin ja hoitamaan työnsä aivan uusin tavoin.

Lisätietoja macOS:n käyttöönotosta, hallinnasta ja tietoturvaominaisuuksista:
support.apple.com/guide/deployment-reference-macos

Lisätietoja mobiililaitteiden hallinnan asetuksista IT:lle:
support.apple.com/guide/mdm

Lisätietoja Apple Business Managerista:
support.apple.com/guide/apple-business-manager

Lisätietoja hallituista Apple ID:istä yrityksille:
apple.com/business/docs/site/
Overview_of_Managed_Apple_IDs_for_Business.pdf

Lisätietoja Apple at Work -ohjelmasta:
www.apple.com/fi/business/

Lisätietoja IT-ominaisuuksista:
www.apple.com/fi/business/it/

Lisätietoja Apple Platform Securitysta:
www.apple.com/security/

Selaa saatavilla olevia AppleCare-ohjelmia:
www.apple.com/fi/support/professional/

Tutustu Applen koulutukseen ja sertifiointeihin:
training.apple.com

Ota yhteyttä Applen ammattilaispalveluihin:
consultingservices@apple.com