Mac-implementatieoverzicht

Inleiding

Inhoud

Bij Apple zijn we ervan overtuigd dat mensen het beste werken als ze toegang hebben tot de beste tools en technologie. Daarom zijn al onze producten zo ontworpen dat werknemers er creatiever, productiever en op nieuwe manieren mee kunnen werken, op kantoor of onderweg. En zo willen de moderne werknemers het ook: met betere toegang tot informatie, de mogelijkheid om naadloos samen te werken en content te delen, en de vrijheid om overal verbonden te zijn en te kunnen werken.

Het configureren en implementeren van Mac in een moderne zakelijke omgeving is nog nooit zo eenvoudig geweest. Dankzij de speciale voorzieningen van Apple, gecombineerd met een MDM-oplossing van een andere fabrikant, vormt de grootschalige implementatie en ondersteuning van Mac geen enkel probleem. Als uw organisatie intern al iOS- en iPadOS-devices heeft geïmplementeerd, hoeft er waarschijnlijk niet veel meer aan de infrastructuur te worden gedaan om de implementatie van macOS mogelijk te maken.

Recente verbeteringen in beveiliging, beheer en implementatie van de Mac maken de transitie mogelijk van gebundelde (‘monolithische’) systeemkopieën en traditionele mapbinding naar een naadloos initialisatiemodel en een implementatieproces waarbij de gebruiker centraal staat en dat vrijwel uitsluitend gebruikmaakt van tools die in macOS zijn ingebouwd.

In dit document vindt u alles wat u nodig hebt voor een grootschalige implementatie van Mac, van inzicht in uw bestaande infrastructuur tot devicebeheer en gestroomlijnde initialisatie. De onderwerpen in dit document worden in meer detail beschreven in de online implementatiehandleiding voor Mac: support.apple.com/guide/deployment-reference-macos

Aan de slag

Belangrijke eerste stappen in het implementatieproces zijn het bepalen van een implementatiestrategie en een uitrolplan, en een evaluatie van de manier waarop macOS op dit moment door werknemers wordt gebruikt. Betrek de relevante teams in een vroeg stadium bij het proces en zorg dat de visie en doelen van uw programma voor iedereen helder zijn. Soms beginnen teams met een proefperiode om eventuele problemen aan het licht te brengen die specifiek zijn voor hun omgeving. Het is essentieel dat de huidige gebruikers bij zo'n proces worden betrokken, zodat u weet hoe devices worden gebruikt in het netwerk en of er zaken zijn waar uw team rekening mee moet houden.

Met de informatie die in deze fase wordt verzameld, kunt u kijken welke rollen en functies het meest zouden profiteren van het gebruik van Mac. Op basis daarvan kan de IT-afdeling inschatten of macOS standaard in de hele organisatie moet worden aangeboden, of alleen als optie voor specifieke functies en taken.

In deze fase wordt ook vaak een uitgebreide lijst opgesteld met interne apps en tools die compatibel moeten zijn voordat Mac breed kan worden uitgerold. Besteed vooral aandacht aan de belangrijkste apps voor productiviteit, samenwerking en communicatie die door de meeste mensen worden gebruikt. Kritieke interne voorzieningen zoals het intranet, adreslijsten en declaratiebeheer zijn ook belangrijk voor de productiviteit van veel medewerkers binnen de organisatie.

Zorg dat u voor andere interne tools workarounds of alternatieve oplossingen documenteert en communiceert, en dat u eigenaars van apps tegelijkertijd stimuleert om hun apps te moderniseren. Laat mensen duidelijk weten welke zakelijke apps ze allemaal kunnen gebruiken als ze voor een Mac kiezen, en laat de vraag vanuit de gebruikers leidend zijn voor de prioritering van het moderniseringsproces. Maak zo nodig samen met eigenaars van applicaties een plan over hoe ze hun apps kunnen aanpassen met behulp van de macOS SDK en Swift. En vergeet niet dat vele zakelijke partners bij de ontwikkeling kunnen assisteren.

Vaak zijn Mac-computers eigendom van het bedrijf. Soms ook staan bedrijven werknemers toe hun eigen Mac op het werk te gebruiken in het kader van een BYOD-programma ('bring your own device'). Welk eigendomsmodel men ook selecteert, als werknemers kunnen kiezen voor Apple producten, kan de hele organisatie daarvan profiteren in de vorm van meer productiviteit, creativiteit, betrokkenheid en tevredenheid. Ook zijn de kosten lager wanneer de restwaarde van de devices en de besparingen op de ondersteuning worden meegerekend. Daarnaast kunnen organisaties profiteren van diverse lease- en financieringsopties om de initiële kosten te verminderen. De kosten kunnen nog verder worden gedrukt door werknemers bij een upgrade de mogelijkheid te geven om bij te dragen via een salariskorting, of door werknemers de optie te geven het device te kopen aan het eind van de leaseperiode of de beoogde zakelijke levensduur.

Het bedrijfsbeleid en de processen voor implementatie, beheer en ondersteuning die in dit document worden beschreven, kunnen in uw situatie anders zijn. Dit is afhankelijk van de informatie die uw team tijdens een pilot verzamelt. Niet elke gebruiker heeft precies hetzelfde beleid of dezelfde instellingen en apps nodig. Binnen een bedrijf kunnen de vereisten voor de verschillende teams enorm van elkaar verschillen.

Implementatiestappen

De implementatie van macOS bestaat uit vier belangrijke stappen: de omgeving voorbereiden, MDM configureren, devices implementeren voor werknemers en dagelijkse beheertaken uitvoeren.

1. Voorbereiden

De eerste stap bij elke implementatie is nadenken over de bestaande omgeving. In deze fase gaat het om een beter inzicht in uw netwerk en cruciale infrastructuur, en u richt de systemen in die nodig zijn voor een succesvolle implementatie.

Uw infrastructuur evalueren

Hoewel Mac naadloos geïntegreerd kan worden in de meeste standaard IT-omgevingen van bedrijven, is het wel belangrijk om een goed beeld te krijgen van uw bestaande infrastructuur, zodat er maximaal kan worden geprofiteerd van de mogelijkheden van macOS. Als uw organisatie hier hulp bij nodig heeft, kunt u ondersteuning krijgen van Apple Professional Services en van technische teams van uw verkooppartner of reseller.

Wifi en netwerk

Stabiele, betrouwbare toegang tot een draadloos netwerk is essentieel voor het instellen en configureren van macOS-devices. Controleer of uw wifinetwerk correct is ontworpen. Denk daarbij aan de plaatsing en voeding van toegangspunten voor roaming- en capaciteitsbehoeften.

Als devices geen contact kunnen maken met Apple servers, de Apple Push Notification-service (APNs), iCloud of de iTunes Store, moet u misschien ook de instellingen van webproxy's of firewallpoorten aanpassen. Net als bij iPad en iPhone is er bij sommige onderdelen van het Mac-implementatieproces, vooral met nieuwere Mac-hardware, toegang tot deze diensten nodig, bijvoorbeeld om tijdens de installatie firmware te kunnen updaten.

Apple en Cisco hebben de communicatie van Mac-computers met een draadloos Cisco-netwerk geoptimaliseerd, met ondersteuning voor geavanceerde netwerkfeatures in macOS zoals Quality of Service (QoS). Als u Cisco-netwerkapparatuur hebt, kunt u met uw interne teams regelen dat Mac uw kritieke verkeer optimaliseert.

U moet ook de VPN-infrastructuur onder de loep nemen, zodat u weet dat gebruikers op afstand veilige toegang hebben tot bedrijfsinformatie. Gebruik eventueel de VPN on Demand-voorziening van macOS, zodat er alleen een VPN-verbinding wordt opgezet als dat echt noodzakelijk is. Als u van plan bent gebruik te maken van app-gebonden VPN, moet u zorgen dat de VPN-gateways deze mogelijkheden ondersteunen, en dat u voldoende licenties aanschaft voor het betreffende aantal gebruikers en verbindingen.

Controleer of uw netwerkinfrastructuur goed is ingesteld voor ondersteuning van Bonjour, het op standaarden gebaseerde netwerkprotocol van Apple waarbij geen configuratie nodig is. Dankzij Bonjour kunnen devices automatisch voorzieningen op een netwerk opsporen. Via Bonjour maakt macOS verbinding met AirPrint-printers en AirPlay-devices zoals Apple TV. Sommige apps en ingebouwde macOS-features gebruiken Bonjour ook om andere devices op te sporen om daarmee samen te werken en gegevens uit te wisselen.

Lees meer over het ontwerp van een wifinetwerk:
support.apple.com/guide/deployment-reference-macos

Lees meer over de configuratie van uw netwerk voor MDM:
https://support.apple.com/HT210060

Lees meer over Bonjour:
support.apple.com/guide/deployment-reference-macos

Identiteiten beheren
macOS kan voor het beheer van identiteiten en andere gebruikersgegevens een adreslijstvoorziening benaderen, zoals Active Directory, Open Directory of LDAP. Sommige MDM-leveranciers bieden tools om hun beheeroplossingen snel te integreren met Active Directory en LDAP-adreslijsten. Met andere tools, zoals de Kerberos Single Sign-on-extensie in macOS Catalina, is integratie met Active Directory-beleid en -functionaliteit mogelijk zonder dat er een traditionele bind en mobiele account nodig zijn. Verschillende soorten certificaten van zowel interne als externe certificeringsinstanties (CA's) kunnen ook door uw MDM-oplossing worden beheerd, zodat identiteiten automatisch worden vertrouwd.

Lees meer over de nieuwe Kerberos Single Sign-on-extensie:
support.apple.com/guide/deployment-reference-macos

Lees meer over integratie met Active Directory:
support.apple.com/guide/deployment-reference-macos

Basisvoorzieningen voor werknemers
Controleer of de Microsoft Exchange-voorziening up-to-date is en of de configuratie geschikt is voor ondersteuning van alle gebruikers in het netwerk. Mocht u geen Exchange gebruiken: macOS is ook compatibel met op standaarden gebaseerde servers zoals IMAP, POP, SMTP, CalDAV, CardDAV en LDAP. Test basisworkflows voor e-mail, contacten en agenda's, evenals de andere bedrijfssoftware voor productiviteit en samenwerking waarmee de meeste kritieke dagelijkse workflows voor gebruikers worden uitgevoerd.

Lees meer over het configureren van Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Lees meer over op standaarden gebaseerde voorzieningen:
support.apple.com/guide/deployment-reference-macos

Materiaalcaching
Met de cachingfeature van macOS wordt lokaal een kopie bewaard van materiaal dat vaak van Apple servers wordt opgevraagd. Hierdoor is er minder bandbreedte nodig om materiaal naar uw netwerk te downloaden. Door te cachen kunt u het downloaden en distribueren van software via de Mac App Store versnellen. Met deze voorziening kunnen ook software-updates worden gecachet, zodat die sneller worden gedownload naar de macOS-, iOS- of iPadOS-devices van de organisatie. En met oplossingen van Cisco en Akamai kan ook ander materiaal worden gecachet.

Lees meer over materiaalcaching:
support.apple.com/guide/deployment-reference-macos

Een beheeroplossing implementeren

Met MDM kunnen organisaties Mac veilig opnemen in de bedrijfsomgeving, instellingen draadloos configureren en bijwerken, apps implementeren, controleren of aan beleid wordt voldaan, gegevens opvragen bij devices en beheerde devices op afstand wissen of vergrendelen. De IT-afdeling kan profielen aanmaken voor het beheren van gebruikersaccounts, het configureren van de systeeminstellingen, het opleggen van beperkingen en het instellen van een wachtwoordbeleid, allemaal via dezelfde oplossing voor Mobile Device Management die ze nu al gebruiken voor iPhone en iPad.

Achter de schermen gebruiken alle Apple platforms een gemeenschappelijk beheerframework van Apple, dat klanten in staat stelt met diverse MDM-oplossingen van derden te werken. Er is een breed scala aan oplossingen voor devicebeheer van andere fabrikanten beschikbaar, zoals Jamf, VMware en MobileIron. Veel van de macOS-frameworks voor devicebeheer zijn hetzelfde als die van iOS en iPadOS. Tussen de MDM-oplossingen van andere fabrikanten zit echter wel enig verschil in beheerfunctionaliteit, ondersteuning van besturingssystemen, prijsstructuur en hostingmodel. Ook de serviceniveaus voor integratie, training en ondersteuning kunnen verschillen. Voordat u een oplossing kiest, moet u goed overwegen welke features het belangrijkste zijn voor uw organisatie.

Wanneer u een MDM-oplossing hebt gekozen, moet u de Apple Push Certificates Portal bezoeken en inloggen om een nieuw MDM-pushcertificaat te maken.

Lees meer over implementatie van MDM:
support.apple.com/guide/deployment-reference-macos

Ga naar de Apple Push Certificates Portal:
identity.apple.com/pushcert/

Aanmelden bij Apple Business Manager

Apple Business Manager is een webportal waarmee IT-beheerders iPhone, iPad, iPod touch, Apple TV en Mac vanuit één locatie kunnen implementeren. Apple Business Manager werkt naadloos samen met uw MDM-oplossing (Mobile Device Management). Met Apple Business Manager kunt u moeiteloos de implementatie van devices automatiseren, apps kopen en content distribueren, en beheerde Apple ID's voor werknemers aanmaken.

Het Device Enrollment Program (DEP) en het Volume Purchase Program (VPP) zijn nu volledig geïntegreerd in Apple Business Manager, zodat organisaties alles wat ze nodig hebben voor de implementatie van Apple devices centraal kunnen regelen. Deze programma's zijn vanaf 1 december 2019 niet meer beschikbaar.

Devices

Met Apple Business Manager kunnen organisaties de aanmelding van devices automatiseren. Hiermee beschikken ze over een snelle en gestroomlijnde manier om Apple devices in eigendom van het bedrijf te implementeren en bij MDM aan te melden zonder elk device fysiek voor te bereiden.

- Het configuratieproces voor gebruikers kan worden vereenvoudigd door de stappen in de configuratie-assistent te stroomlijnen, waarmee wordt gegarandeerd dat werknemers direct na activering de juiste configuraties ontvangen. IT-teams kunnen deze ervaring nu nog beter op maat snijden door werknemers te voorzien van toestemmingsinformatie, corporate branding of moderne authenticatie.

- Het beheer van devices in eigendom van het bedrijf kan op een hoger plan worden getild met het gebruik van supervisie. Hiermee krijgt u aanvullende beheervoorzieningen (zoals niet-verwijderbare MDM-voorzieningen) die niet beschikbaar zijn in andere implementatiemodellen.
- U kunt standaard-MDM-servers op een eenvoudigere manier beheren door een standaardserver in te stellen op basis van het devicetype. En het is nu ook mogelijk om iPhones, iPads en Apple TV's handmatig via Apple Configurator 2 aan te melden, ongeacht de manier waarop u ze hebt gekocht.

Content

Met Apple Business Manager wordt het voor organisaties gemakkelijk om content in bulk aan te schaffen. Of uw medewerkers nu met iPhone, iPad of Mac werken, u kunt ze prachtige, kant-en-klare content bieden via flexibele en veilige distributieopties.

- U kunt grote aantallen apps, boeken en apps op maat aanschaffen – ook intern ontwikkelde apps. U kunt heel eenvoudig app-licenties overzetten naar een andere locatie en licenties delen met andere gebruikers binnen één locatie. U kunt een gecompileerde lijst van de aankoopgeschiedenis bekijken, met daarin onder andere het aantal licenties dat via MDM in gebruik is.
- U distribueert apps en boeken rechtstreeks naar beheerde devices of geautoriseerde gebruikers en houdt eenvoudig bij welke content aan welke gebruiker of welk device is toegewezen. Met beheerde distributie hebt u het gehele distributieproces onder controle, terwijl de apps volledig uw eigendom blijven. Apps die niet meer nodig zijn op een device of voor een gebruiker, kunnen worden ingetrokken en opnieuw worden toegewezen binnen de organisatie.
- Betalen kan op verschillende manieren, bijvoorbeeld met creditcard of via een inkooporder. Organisaties kunnen bij Apple of een erkende Apple reseller volumekrediet kopen voor een bepaald bedrag in de lokale valuta. Dit wordt vervolgens elektronisch overgemaakt naar de accounthouder als Store-tegoed. Deze optie is niet overal beschikbaar.
- U kunt een app distribueren naar devices of gebruikers in elk land waar de app beschikbaar is, zodat de apps ook internationaal kunnen worden gedistribueerd. Ontwikkelaars kunnen hun apps in meerdere landen beschikbaar maken via het normale App Store-publicatieproces.

Opmerking: De mogelijkheid om boeken aan te schaffen via Apple Business Manager is in bepaalde landen niet beschikbaar. Ga naar support.apple.com/HT207305 voor informatie over de beschikbaarheid van features en aanschafmethoden.

Gebruikers

Apple Business Manager biedt organisaties de mogelijkheid werknemersaccounts te maken en beheren die geïntegreerd worden met de bestaande infrastructuur en toegang bieden tot apps en voorzieningen van Apple en tot Apple Business Manager.

- Voor werknemers kunt u beheerde Apple ID's maken zodat ze kunnen samenwerken met apps en voorzieningen van Apple en toegang krijgen tot werkgegevens in beheerde apps die gebruikmaken van iCloud Drive. Deze accounts zijn eigendom van en worden beheerd door de betreffende organisatie.
- Door Apple Business Manager aan Microsoft Azure Active Directory te koppelen kunt u gebundelde authenticatie toepassen. Beheerde Apple ID's

worden automatisch aangemaakt wanneer werknemers zich voor de eerste keer aanmelden bij een compatibel Apple device met hun bestaande inloggegevens.

- Met de nieuwe features voor gebruikersinschrijving in iOS 13, iPadOS en macOS Catalina kunnen beheerde Apple ID's naast een persoonlijke Apple ID worden gebruikt op devices die eigendom zijn van werknemers. Beheerde Apple ID's kunnen ook op elk device worden gebruikt als primaire (en enige) Apple ID. Beheerde Apple ID's hebben bovendien toegang tot iCloud op het web, na de eerste aanmelding op een Apple device.
- U kunt andere rollen aan IT-teams binnen de organisatie toewijzen voor een effectief beheer van devices, apps en accounts binnen Apple Business Manager. U gebruikt de beheerdersrol om waar nodig algemene voorwaarden te accepteren en gemakkelijk de verantwoordelijkheid over te dragen als iemand de organisatie verlaat.

Opmerking: iCloud Drive wordt momenteel niet ondersteund met gebruikersinschrijving. iCloud Drive kan met een beheerde Apple ID worden gebruikt wanneer dit de enige Apple ID op een device is.

Lees meer over Apple Business Manager: apple.com/nl/business/it

Aanmelden bij het Apple Developer Enterprise Program

Het Apple Developer Enterprise Program biedt een complete set tools voor het ontwikkelen, testen en distribueren van apps. U kunt apps distribueren via een MDM-oplossing of door ze te hosten op een webserver. Mac-apps en installatieprogramma's kunnen met uw Developer ID voor Gatekeeper worden ondertekend en geauthenticeerd, zodat macOS nog beter wordt beschermd tegen malware.

Lees meer over het Developer Enterprise Program: developer.apple.com/programs/enterprise

2. Configureren

Bij de configuratie geeft u beleidsregels op en zorgt u ervoor dat uw MDM-oplossing klaar is om Macs voor de werknemers te configureren.

Inzicht in beveiliging voor macOS

Beveiliging en privacy zijn fundamentele elementen in het ontwerp van alle hardware, software en voorzieningen van Apple. We beschermen de privacy van onze klanten met geavanceerde versleutelingstechnieken plus een strikt beleid waarin is vastgelegd hoe er met alle gegevens wordt omgegaan. De volgende elementen maken het platform voor Apple devices zo veilig:

- Methoden om devices te beveiligen tegen ongeoorloofd gebruik
- Beveiliging van de gegevens, ook wanneer het device kwijt is of gestolen wordt
- Netwerkprotocollen en versleuteling voor gegevensoverdracht
- Apps kunnen veilig worden gebruikt zonder de integriteit van het platform in gevaar te brengen

Alle Apple devices zijn ontwikkeld met meerdere beveiligingslagen, zodat ze veilig van netwerkdiensten gebruik kunnen maken en belangrijke gegevens worden beschermd. macOS, iOS en iPadOS bieden ook beveiliging via beleid met toegangscodes en wachtwoorden, dat via MDM kan worden geregeld en

afgedwongen. Een gebruiker of beheerder kan op afstand alle privégegevens wissen als een device in de verkeerde handen terechtkomt.

De IT-afdeling kan door middel van MDM een aantal beleidsregels inzetten om devices veilig te houden. Met MDM kunnen bijvoorbeeld FileVault en herstelcode-escrow worden afgedwongen, er kan een specifiek wachtwoordbeleid of een screensaververgrendeling worden gedefinieerd of de ingebouwde firewall kan worden ingeschakeld.

Lees meer over Apple platformbeveiliging: apple.com/security/

Interne beleidsregels opstellen

Als u bedrijfsbeleid wilt ontwikkelen, stelt u eerst algemene regels op die gelden voor de meeste Mac-gebruikers in uw bedrijf. In uw MDM-oplossing kunt u zaken per gebruiker aanpassen, zoals accounts of toegang tot bepaalde apps. Daarnaast kunt u specifieke beleidsregels voor organisaties of kleinere groepen gebruikers instellen, zoals de implementatie van afdelingsspecifieke software of instellingen.

Werk samen met uw interne teams uit hoe het bestaande bedrijfsbeleid moet worden aangepast aan het gebruik van Mac-computers. Sommige basisbeleidsregels blijven voor alle platforms hetzelfde, zoals eisen voor de complexiteit van een wachtwoord en de regelmatige wijziging ervan, screensavertime-outs en acceptabel gebruik.

Als in uw bedrijfsbeleid het gebruik van een specifieke technologie op een ander platform verplicht is, stel dan vast waar het precies om gaat en herformuleer het beleid zodanig dat het kan worden toegepast op ingebouwde technologieën van macOS. In plaats van verplicht te stellen dat van alle computers een complete schijf wordt versleuteld met behulp van een oplossing van een andere fabrikant, kunt u beter in beleid vastleggen dat bedrijfsgegevens moeten worden versleuteld als ze inactief zijn. Dit kan dan met FileVault worden geregeld. Als in het beleid is vastgelegd dat specifieke software tegen malware moet worden beschermd, kunt u uw teams voorlichten over ingebouwde voorzieningen zoals Gatekeeper en het beleid hieraan aanpassen.

Instellingen configureren in MDM

Om het beheer van bedrijfsbeleid mogelijk te maken en te zorgen dat medewerkers toegang hebben tot de nodige middelen, wordt elke Mac veilig aangemeld bij uw MDM-oplossing. De MDM-oplossing past beleid en instellingen dan toe door middel van configuratieprofielen. Configuratieprofielen zijn XML-bestanden die via MDM worden aangemaakt. Hiermee kunt u instellingen naar devices distribueren. Met configuratieprofielen wordt de configuratie van instellingen, accounts, beleidsregels, beperkingen en inloggegevens geautomatiseerd. Om de beveiliging van uw systemen te verbeteren, kunnen de profielen worden ondertekend en versleuteld.

Nadat een device bij MDM is aangemeld, kan de beheerder een MDM-beleidsinstelling, -informatieverzoek of -commando initiëren. Wanneer er een netwerkverbinding is, ontvangt het device dan een melding via de Apple Push Notification-service (APNs). Vervolgens wordt er via een veilige verbinding een directe communicatie met de MDM-oplossing tot stand gebracht om de actie van de beheerder te verwerken. Communicatie vindt alleen plaats tussen MDM en het device, en APNs stuurt geen vertrouwelijke of privégegevens door. Als een device uit het beheer wordt verwijderd, worden de instellingen en het

beleid die bij dat configuratieprofiel horen, ook verwijderd. Een bedrijf kan een device zo nodig ook op afstand wissen.

Veel organisaties voegen hun MDM-oplossing toe aan hun bestaande adreslijstvoorzieningen. De configuratie-assistent in macOS kan gebruikers bij de automatische aanmelding van het device vragen om met de gegevens van hun adreslijstservice in te loggen. Met macOS Catalina zijn er nieuwe opties voor een aangepast aanmeldingsproces, waarbij de configuratie-assistent identificatie kan tonen vanuit cloudproviders. Zodra het device aan een specifieke gebruiker is toegewezen, kan MDM configuraties en accounts specifiek voor personen of groepen aanpassen. Een individuele Microsoft Exchange-account van een gebruiker kan bijvoorbeeld tijdens de aanmelding automatisch worden ingericht. Ook is het mogelijk certificaatidentiteiten te gebruiken voor technologieën als 802.1x en VPN.

Deze systemen geven zoveel controle dat bedrijven het vaak geen probleem vinden om gebruikers beheerderstoegang tot hun Mac te geven, zodat ze zelf hun instellingen naar wens kunnen aanpassen, apps kunnen installeren en problemen kunnen oplossen. Allemaal terwijl ze via MDM onder controle van het bedrijfsbeleid blijven. Met dit model wordt het soort rechten en controlemechanismen gevolgd dat geldt voor gebruikers met een beheerde iPhone of iPad.

Lees meer over configuratieprofielen:
support.apple.com/guide/deployment-reference-macos

Voorbereiden op automatische aanmelding van devices

De gemakkelijkste methode om een device bij MDM aan te melden is met de functies voor automatische device-aanmelding van Apple Business Manager. Zo kan aanmelding plaatsvinden zonder dat de IT-afdeling eraan te pas hoeft te komen, en bepaalde schermen van de configuratie-assistent kunnen worden gestroomlijnd zodat gebruikers het proces sneller kunnen afronden.

Om automatische device-aanmelding te configureren, moet u eerst uw MDM-oplossing met een veilig token aan uw Apple Business Manager-account koppelen. Een MDM-oplossing wordt door middel van tweestapsverificatie veilig geautoriseerd. Uw MDM-leverancier kan u documentatie geven over de specifieke details voor de betreffende implementatie.

Als devices al in gebruik zijn bij medewerkers of in bezit zijn van individuele personen, kan er één configuratieprofiel door de gebruiker worden geopend en in Systeemvoorkeuren worden gecontroleerd om de aanmelding te voltooien. Deze procedure wordt wel ‘door gebruiker goedgekeurde MDM-aanmelding’ genoemd. Voor het beheer van bepaalde beveiligingsgevoelige instellingen (zoals het kernelextensiebeleid en beleidsbeheer voor privacyvoorkeuren) moet aanmelding ofwel plaatsvinden via device-aanmelding ofwel door middel van door gebruiker goedgekeurde MDM-aanmelding.

Lees meer over het laden van kernelextensies:
support.apple.com/guide/deployment-reference-macos

Lees meer over beleidsbeheer voor privacyvoorkeuren:
support.apple.com/guide/mdm

Voorbereiding op distributie van apps en boeken

Apple biedt diverse programma's waarmee uw organisatie de apps en content die voor macOS beschikbaar zijn optimaal kan benutten. Hiermee kunt u apps en boeken distribueren die via Apple Business Manager zijn aangeschaft, en ook uw eigen interne apps. Zo beschikken de werknemers over alles wat ze nodig hebben om productief te kunnen werken. Met MDM kunt u ook apps distribueren en pakketten installeren voor software die niet verkrijgbaar is in de Mac App Store.

Uw MDM-oplossing kan beheerde distributie gebruiken om apps en boeken te distribueren die via Apple Business Manager zijn aangeschaft in een land waar de app verkrijgbaar is. Om beheerde distributie in te schakelen, moet u uw MDM-oplossing eerst met een veilig token aan uw Apple Business Manager-account koppelen. Nadat de verbinding met uw MDM-oplossing tot stand is gebracht, kunt u apps en boeken toewijzen, zelfs als de App Store op het device is uitgeschakeld. U kunt apps ook direct aan devices toewijzen. Daarmee wordt de implementatie aanzienlijk gemakkelijker, omdat elke gebruiker van dat device dan toegang heeft tot elke app.

Lees meer over content aanschaffen via Apple Business Manager:
support.apple.com/guide/apple-business-manager

Lees meer over de distributie van apps en boeken:
support.apple.com/guide/apple-business-manager

Extra content voorbereiden

Met uw MDM-oplossing kunt u extra pakketten distribueren met content die niet afkomstig is uit de Mac App Store. Dit is een gebruikelijke aanpak voor veel zakelijke softwarepakketten, zoals eigen interne apps of apps als Chrome of Firefox. Verplichte software kan met deze methode worden gepusht en automatisch worden geïnstalleerd na het voltooien van de aanmelding. Lettertypen, scripts of andere items kunnen ook via pakketten worden geïnstalleerd en uitgevoerd. Zorg ervoor dat de pakketten correct zijn ondertekend met uw Developer ID van het Developer Enterprise Program.

Lees meer over de installatie van extra content:
support.apple.com/guide/deployment-reference-macos

3. Implementeren

Met macOS is het eenvoudig om devices bij werknemers te implementeren en eventueel te personaliseren, zodat ze aan de slag kunnen zonder dat de IT-afdeling eraan te pas hoeft te komen.

Configuratie-assistent gebruiken

Na het aanzetten kunnen werknemers de configuratie-assistent in macOS gebruiken om hun taal- en regiovoorkeuren in te stellen en een netwerkverbinding te maken. Zodra de gebruikers een internetverbinding hebben gemaakt, worden ze via een reeks vensters van de configuratie-assistent door de basisinstellingen voor hun nieuwe Mac geleid. Tijdens deze procedure kunnen devices die zijn aangemeld bij Apple Business Manager automatisch worden aangemeld bij MDM. Macs die zijn aangemeld, kunnen ook zodanig worden geconfigureerd dat bepaalde schermen worden overgeslagen. Denk hierbij aan de algemene voorwaarden, het inlogvenster voor Apple ID en locatievoorzieningen.

MDM kan dan na het eerste gebruik van de configuratie-assistent worden gebruikt om diverse instellingen te implementeren. Er kan bijvoorbeeld worden vastgelegd of gebruikers beheerdersbevoegdheden hebben voor hun computer. Net als met iPhone en iPad kunnen gebruikers controle hebben over hun device terwijl ze toch voldoen aan het bedrijfsbeleid en de instellingen die door MDM worden beheerd. Om te zorgen dat gebruikers na het voltooien van de configuratie-assistent meteen productief kunnen zijn, moeten alleen de belangrijkste apps en pakketten op de achtergrond worden gedownload en geïnstalleerd, zodat werknemers zo min mogelijk worden gehinderd en direct met hun werk kunnen beginnen. Voor grotere apps kan de gebruiker het downloaden en installeren op de achtergrond plannen in de selfservice-tool van uw MDM-oplossing.

Zakelijke accounts configureren

MDM kan mailaccounts en andere gebruikersaccounts automatisch configureren. Afhankelijk van de MDM-oplossing en de integratie met uw interne systemen kunnen de accountgegevens vooraf worden aangevuld met namen, e-mailadressen en certificaatidentiteiten voor identiteitscontrole en ondertekening.

Personalisatie door gebruiker toestaan

Als u gebruikers de mogelijkheid biedt het device te personaliseren, kan dat de productiviteit verhogen. Gebruikers bepalen dan namelijk zelf met welke apps en materialen ze hun taken het best kunnen uitvoeren om hun doelen te behalen. En met beheerde Apple ID's en gebruikersinschrijving in macOS Catalina beschikken organisaties nu over nieuwe opties om gebruikers toegang tot Apple diensten te geven met een Apple ID van de organisatie, eventueel naast een persoonlijke Apple ID.

Apple ID en beheerde Apple ID

Wanneer werknemers met een Apple ID inloggen bij Apple diensten zoals FaceTime, iMessage, de App Store en iCloud, hebben ze toegang tot allerlei materiaal waarmee ze hun werk kunnen stroomlijnen, hun productiviteit kunnen vergroten en gemakkelijker kunnen samenwerken. Net als andere Apple ID's worden beheerde Apple ID's gebruikt voor aanmelding bij een eigen device. Ook worden ze gebruikt voor toegang tot Apple diensten, zoals iCloud en samenwerking met iWork en Notities, en voor Apple Business Manager. Anders dan gewone Apple ID's zijn beheerde Apple ID's eigendom van de organisatie en worden ze door de organisatie beheerd, bijvoorbeeld voor wachtwoordherstel en beheer op basis van rollen. Voor sommige instellingen van beheerde Apple ID's gelden bepaalde beperkingen.

Voor devices die zijn aangemeld met gebruikersinschrijving is een beheerde Apple ID nodig. Gebruikersinschrijving ondersteunt een optionele persoonlijke Apple ID; andere aanmeldingsmethoden ondersteunen ofwel een persoonlijke Apple ID, ofwel een beheerde Apple ID. Alleen gebruikersinschrijving ondersteunt het gebruik van meerdere Apple ID's.

Om deze voorzieningen optimaal te benutten moeten gebruikers hun eigen Apple ID gebruiken of de beheerde Apple ID die voor hen is aangemaakt. Gebruikers die geen Apple ID hebben, kunnen er al een aanmaken voordat ze een device krijgen. En met de configuratie-assistent kunnen gebruikers bovendien een persoonlijke Apple ID aanmaken als dat nodig is. Voor het aanmaken van een Apple ID is geen creditcard nodig.

Lees meer over beheerde Apple ID's:
support.apple.com/guide/deployment-reference-macos

iCloud

Met iCloud kunnen gebruikers automatisch documenten en persoonlijke content synchroniseren, zoals contacten, agenda's, documenten en foto's, en die gegevens actueel houden op meerdere devices. Met Zoek mijn kunnen gebruikers een verloren of gestolen Mac, iPhone, iPad of iPod touch terugvinden. Specifieke onderdelen van iCloud, zoals iCloud-sleutelhanger en iCloud Drive, kunnen worden uitgeschakeld met beperkingen die handmatig of via MDM op het device zijn ingesteld. Zo hebben organisaties meer controle over welke gegevens op welke account zijn opgeslagen.

Lees meer over het beheer van iCloud:
support.apple.com/guide/deployment-reference-macos

4. Beheren

Zodra uw gebruikers aan de slag zijn, hebt u allerlei mogelijkheden tot uw beschikking voor het beheer van devices en content gedurende de gehele levenscyclus.

Devices beheren

Een beheerd device kan aan de hand van een aantal specifieke taken worden beheerd door MDM. Denk hierbij aan het opvragen van informatie van devices en het initiëren van taken om devices te beheren die niet in overeenstemming zijn met het beleid of die kwijt zijn geraakt of zijn gestolen.

Informatieverzoeken

Een MDM-oplossing kan allerlei informatie van een device opvragen om te controleren of gebruikers de juiste apps en instellingen gebruiken. De informatieverzoeken kunnen hardware betreffen, zoals het serienummer of het model van het device, of software, zoals de macOS-versie of een lijst met geïnstalleerde apps. Ook kan MDM informatie opvragen over belangrijke beveiligingsvoorzieningen zoals FileVault of de ingebouwde firewall.

Beheertaken

Voor een beheerd device kan MDM allerlei beheertaken uitvoeren, zoals het automatisch wijzigen van de configuratie-instellingen (zonder tussenkomst van de gebruiker), een macOS-update uitvoeren, wachtwoorden beheren en een device op afstand vergrendelen of wissen.

Lees meer over beheertaken:
support.apple.com/guide/deployment-reference-macos

Software-updates beheren

De IT-afdeling kan gebruikers de keuze geven naar het nieuwste besturingssysteem te upgraden wanneer dat beschikbaar is. De IT-afdeling kan een prereleaseversie van macOS testen en zo garanderen dat compatibiliteitsproblemen van apps snel worden vastgesteld en aan ontwikkelaars worden doorgegeven voordat de uiteindelijke versie uitkomt. Via het Apple Beta Software Program of AppleSeed for IT kan de IT-afdeling worden betrokken bij het testen van releases. U doet er goed aan om Mac-computers up-to-date te houden, zodat uw gebruikers en hun gegevens zo goed mogelijk beschermd blijven. Voer updates regelmatig uit, zodra u hebt vastgesteld dat uw workflow compatibel is met de nieuwe versie van macOS.

MDM kan macOS-updates automatisch pushen naar een Mac die is aangemeld. Macs die zijn aangemeld, kunnen ook zo worden geconfigureerd dat updates en meldingen over updates maximaal 90 dagen worden uitgesteld als kritieke systemen daar nog niet klaar voor zijn. Gebruikers kunnen updates dan pas handmatig uitvoeren als het beleid wordt verwijderd of als MDM een installatiecommando stuurt.

Apple is geen voorstander van het gebruik van gebundelde ('monolithische') systeemkopieën voor macOS-upgrades. Net als iPhone en iPad maken Mac-computers vaak gebruik van firmware-updates die specifiek voor één model zijn. En voor updates aan het Mac-besturingssysteem is het nodig dat deze firmware-updates direct door Apple worden geïnstalleerd. De betrouwbaarste strategie daarvoor is het gebruik van het installatieprogramma van macOS of MDM-commando's.

Extra software beheren

Organisaties moeten vaak extra apps buiten de oorspronkelijke set distribueren naar hun gebruikers. Dit kan voor kritieke apps en updates automatisch door MDM worden gedaan, of op aanvraag door werknemers in staat te stellen apps aan te vragen via een selfservice-portal van uw MDM-oplossing. Deze portals kunnen software installeren die is aangeschaft bij de App Store of via Apple Business Manager, maar ze kunnen ook overweg met apps, scripts en andere hulpmiddelen die niet uit de App Store afkomstig zijn.

De meeste software kan automatisch worden geïnstalleerd, maar soms moet de gebruiker bij de installatie bepaalde dingen doen. Voor de veiligheid kunnen apps waarvoor kernelextensies vereist zijn, nu alleen worden geladen met toestemming van de gebruiker. Dit heet 'laden van door de gebruiker goedgekeurde kernelextensies' en kan door MDM worden beheerd.

Beveiliging van devices onderhouden

Behalve de oorspronkelijke set beveiligingsbeleidsregels die al van kracht waren voordat de devices waren geïmplementeerd, dient uw team ook de naleving van het beleid op computers in de gaten te houden en daar via MDM zoveel mogelijk informatie over op te vragen. De beveiliging van de devices kan worden bewaakt, maar er kan ook informatie worden verzameld over de installatie van softwarepatches. De meeste organisaties zijn tevreden met de tools voor versleuteling en bescherming die al in elke Mac zijn ingebouwd. Sommige organisaties stellen echter het gebruik verplicht van extra diensten voor het synchroniseren en delen van bestanden, of van tools ter preventie van het lekken van bedrijfsgegevens, en voor gedetailleerde rapportage over vertrouwelijke gegevens.

Met de functie 'Zoek mijn Mac' van iCloud kan een Mac op afstand worden gewist en gedeactiveerd als hij kwijtgeraakt of gestolen is. Een IT-team kan ook met MDM op afstand gegevens wissen.

Devices opnieuw in gebruik nemen

Wanneer een werknemer weggaat bij de organisatie, kan met Internet Recovery en de lokale herstelpartitie een Mac gemakkelijk opnieuw in gebruik worden genomen voor een andere gebruiker. De inhoud van de Mac wordt dan gewist en de nieuwste versie van het besturingssysteem wordt geïnstalleerd. Als een Mac in Apple Business Manager aan een specifieke gebruiker is toegewezen, wordt de Mac automatisch opnieuw aangemeld bij MDM tijdens het uitvoeren van de configuratie-assistent, worden instellingen geconfigureerd voor de

nieuwe gebruiker, wordt bedrijfsbeleid toegepast en wordt alle relevante software geïmplementeerd. Mac-computers die niet zijn aangemeld, kunnen met hetzelfde proces worden gewist en opnieuw in gebruik worden genomen, waarna ze handmatig opnieuw kunnen worden aangemeld.

Ondersteuningsopties

Veel organisaties hebben ondervonden dat Mac-gebruikers maar weinig IT-ondersteuning nodig hebben. Om zelfredzaamheid aan te moedigen en de kwaliteit van de ondersteuning naar een hoger plan te tillen, ontwikkelen veel IT-afdelingen tools voor zelfondersteuning. Voorbeelden daarvan zijn het opzetten van een uitgebreide Mac-ondersteuningssite, selfservice-forums en een helpdesk op locatie. Met MDM kunnen gebruikers zelf ondersteuningstaken uitvoeren, zoals het installeren of updaten van software in een selfservice-portal.

Wat ondersteuning betreft, kunnen gebruikers beter niet helemaal aan zichzelf worden overgelaten. Het beste is een samenwerkende aanpak van problemen, waarbij gebruikers in staat worden gesteld eerst te kijken of ze een probleem zelf kunnen oplossen voordat ze de helpdesk bellen. Stimuleer betrokkenheid van werknemers bij het proces en laat ze problemen zelf onderzoeken voordat ze hulp inroepen.

Wanneer de verantwoordelijkheid voor ondersteuning wordt gedeeld, hebben werknemers minder uitvaltijd. Er zijn minder ondersteuningsmedewerkers nodig en er worden in totaal minder ondersteuningskosten gemaakt. Voor organisaties die meer nodig hebben biedt AppleCare diverse programma's en diensten die de interne ondersteuning voor werknemers en IT'ers kunnen aanvullen.

AppleCare for Enterprise

Bedrijven die optimaal gedekt willen zijn, kunnen met AppleCare for Enterprise de werklast van hun interne helpdesk verlichten. Medewerkers krijgen namelijk 24 uur per dag, zeven dagen per week technische ondersteuning via de telefoon, met een reactietijd van één uur voor problemen met de hoogste prioriteit. Het programma biedt integratiescenario's op het niveau van de IT-afdeling, inclusief MDM en Active Directory.

AppleCare OS Support

Via AppleCare OS Support beschikt uw IT-afdeling over professionele ondersteuning per telefoon en e-mail voor implementaties van iOS, iPadOS, macOS en macOS Server. U hebt 24 uur per dag en 7 dagen per week recht op ondersteuning, plus een eigen Technical Account Manager, afhankelijk van het gekozen ondersteuningsniveau. Via AppleCare OS Support heeft uw IT-personeel direct contact met technici voor vragen over integratie, migratie en geavanceerde serverproblemen, en kan het veel efficiënter te werk gaan bij implementatie en beheer van devices en het oplossen van problemen.

AppleCare Help Desk Support

Met AppleCare Help Desk Support kunt u met voorrang telefonisch contact opnemen met ervaren ondersteuningsmedewerkers van Apple. Bovendien krijgt u de beschikking over een verzameling tools voor het opsporen en oplossen van problemen met hardware van Apple. Hierdoor kunnen grote organisaties problemen sneller en efficiënter oplossen en blijven de opleidingskosten beperkt. Met het AppleCare Help Desk Support-plan kunt u een onbeperkt aantal aanvragen indienen voor het opsporen en verhelpen van problemen met hardware en software en het isoleren van problemen met iOS- en iPadOS-devices.

AppleCare en AppleCare+ voor Mac

Elke Mac-computer wordt geleverd met een beperkte garantie van één jaar en gratis telefonische ondersteuning gedurende 90 dagen na de aankoopdatum. U kunt deze dekking uitbreiden tot drie jaar vanaf de oorspronkelijke aankoopdatum met AppleCare+ of het AppleCare Protection Plan. Werknemers kunnen Apple Support bellen met vragen over hardware of software van Apple. Daarnaast biedt Apple handige serviceopties als een device gerepareerd moet worden. AppleCare+ voor Mac biedt bovendien aanvullende dekking voor bepaalde schadevoorvallen als gevolg van een ongeluk. Per incident worden servicekosten in rekening gebracht.

Lees meer over opties voor AppleCare-ondersteuning:
apple.com/nl/support/professional/

Samenvatting

Ongeacht of uw bedrijf Mac-computers implementeert onder een groep gebruikers of binnen de gehele organisatie, beschikt u over een groot aantal opties om devices eenvoudig te implementeren en te beheren. Als u de juiste strategieën kiest voor uw organisatie, kunnen uw werknemers productiever en op een heel andere manier werken.

Lees meer over implementatie, beheer en beveiliging van macOS:
support.apple.com/guide/deployment-reference-macos

Lees meer over MDM-instellingen voor IT:
support.apple.com/guide/mdm

Lees meer over Apple Business Manager:
support.apple.com/guide/apple-business-manager

Lees meer over beheerde Apple ID's voor bedrijven:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Lees meer over Apple at Work:
www.apple.com/nl/business/

Lees meer over features voor IT :
www.apple.com/nl/business/it/

Lees meer over Apple platformbeveiliging:
www.apple.com/security/

Bekijk beschikbare AppleCare-programma's:
www.apple.com/nl/support/professional/

Ontdek Apple cursussen en certificering:
training.apple.com

Neem contact op met Apple Professional Services:
consultingservices@apple.com