Einführungshandbuch

Mac Implementierung

Überblick

Inhalt

Überblick
Erste Schritte
Implementierungsschritte
Supportoptionen
Zusammenfassung

Bei Apple sind wir davon überzeugt, dass Mitarbeiter ihr Bestes geben können, wenn ihnen die besten Tools und Technologien zur Verfügung stehen. Wir haben alle unsere Produkte so entwickelt, dass sie Mitarbeiter dabei unterstützen, kreativer und produktiver zu sein und auf eine ganz neue Art und Weise zu arbeiten – egal ob im Büro oder unterwegs. Das entspricht auch dem, was Mitarbeiter im digitalen Zeitalter erwarten: Einen besseren Zugriff auf Informationen, nahtloses Zusammenarbeiten und Teilen sowie die Freiheit, vernetzt zu bleiben und von überall aus zu arbeiten.

Noch nie war es so einfach, Mac Computer in einer modernen Unternehmensumgebung einzurichten und zu implementieren. Mit zentralen Diensten von Apple – kombiniert mit einer Lösung für die mobile Geräteverwaltung (Mobile Device Management, MDM) eines anderen Anbieters – kann Ihr Unternehmen ganz einfach macOS Geräte nach Bedarf implementieren und unterstützen. Wenn Ihr Unternehmen bereits iOS Geräte implementiert hat, ist der größte Teil der für die macOS Implementierung erforderlichen Infrastrukturarbeiten wahrscheinlich schon abgeschlossen.

Aktuelle Verbesserungen bei der Sicherheit, Verwaltung und Implementierung von macOS erlauben Unternehmen den Wechsel von monolithischem Imaging und herkömmlicher Verzeichnisbindung zu einem nahtlosen Bereitstellungsmodell und einem Implementierungsprozess, der die einzelnen Benutzer in den Mittelpunkt stellt und fast ausschließlich in macOS integrierte Tools verwendet.

Dieses Dokument unterstützt Sie bei allen erforderlichen Schritten, um macOS nach Bedarf zu implementieren – angefangen bei der Evaluierung Ihrer bestehenden Infrastruktur über die Geräteverwaltung bis hin zu einer optimierten Bereitstellung. Ausführlichere Infos zu den in diesem Dokument behandelten Themen finden Sie online in der Referenz zur macOS Implementierung:
help.apple.com/deployment/macos

Erste Schritte

Wichtige erste Schritte im Implementierungsprozess sind die Entwicklung einer Implementierungsstrategie und eines Einführungsplans sowie die Evaluierung der Nutzung bestehender macOS Geräte durch die Mitarbeiter. Sorgen Sie dafür, dass die zuständigen Teams frühzeitig eingebunden werden und die Vision und Ziele Ihres Programms mittragen. Manche Teams starten mit einem kleinen Pilotprojekt oder Machbarkeitsnachweis, um festzustellen, ob in ihrer Umgebung besondere Herausforderungen zu bewältigen sind. Dies ist auch ein wichtiger Zeitpunkt, um sich mit den Benutzern auszutauschen, die bereits mit Mac arbeiten. So erfahren Sie mehr über die Nutzung von Geräten im Netzwerk und können Ihr Team gegebenenfalls über Probleme informieren.

Die in dieser Phase gesammelten Informationen können Ihnen helfen herauszufinden, welche Mitarbeiterrollen und -funktionen am meisten vom Mac profitieren würden. Das IT-Team kann anschließend beurteilen, ob Sie macOS standardmäßig im gesamten Unternehmen oder als Option für bestimmte Jobfunktionen anbieten sollten.

Häufig wird in dieser Phase eine umfassende Liste interner Apps und Tools zusammengestellt, die kompatibel sein müssen, bevor Mac Computer im großen Rahmen eingeführt werden können. Konzentrieren Sie sich in erster Linie auf die zentralen Produktivitäts-, Kollaborations- und Kommunikationsapps, mit denen die meisten Benutzer arbeiten. Kritische interne Dienste wie das unternehmenseigene Intranet, Verzeichnis und Ausgabenmanagement-Programm sind ebenfalls wichtig für die Produktivität großer Teile des Unternehmens.

Dokumentieren und kommunizieren Sie Workarounds oder Alternativen für andere interne Tools und ermutigen Sie die Anwendungseigner, je nach Bedarf auf modernere Apps umzusteigen. Kommunizieren Sie gegenüber den Benutzern offen, welche verschiedenen Unternehmensapps sie verwenden können, wenn sie sich für Mac entscheiden, und lassen Sie die Priorisierung der Modernisierungsmaßnahmen von der tatsächlichen Nachfrage steuern. Erstellen Sie gegebenenfalls gemeinsam mit den Anwendungseignern einen Plan für die Aktualisierung ihrer Apps mit dem macOS SDK und Swift sowie den zahlreichen Unternehmenspartnern, die Sie bei der Entwicklung unterstützen können.

Mac Computer werden üblicherweise als unternehmenseigene Geräte ausgegeben. Manche Unternehmen erlauben ihren Mitarbeitern aber auch, im Rahmen von Bring-Your-Own-Device(BYOD)-Programmen, ihren privaten Mac zu nutzen. Wenn Mitarbeiter die Wahl haben, mit Apple Produkten zu arbeiten, kann das dem gesamten Unternehmen Vorteile bringen: Mehr Produktivität, Kreativität, Einsatz und Zufriedenheit der Mitarbeiter mit ihrem Job sowie geringere Kosten in Bezug auf Restwerte und Support. Unternehmen können darüber hinaus von unterschiedlichen Leasing- und Finanzierungsoptionen profitieren, um ihre Investitionskosten zu reduzieren. Unternehmen können beispielsweise Kosten ausgleichen, indem sie Mitarbeitern erlauben, ein Upgrade durch Gehaltsabzüge mitzutragen oder das Gerät zum Ende der Leasingzeit bzw. des Lebenszyklus abzukaufen.

Ihre Unternehmensrichtlinien sowie die in diesem Dokument beschriebenen Implementierungs- Verwaltungs- und Supportprozesse können entsprechend den von Ihrem Team in einem Pilotprojekt gesammelten Informationen abweichen. Nicht alle Benutzer brauchen genau die gleichen Richtlinien, Einstellungen und Apps – häufig unterscheiden sich beispielsweise die Anforderungen zwischen den unterschiedlichen Gruppen oder Teams im Unternehmen enorm.

Implementierungsschritte

Bei der macOS Implementierung gibt es vier grundlegende Schritte: Umgebung vorbereiten, MDM-Lösung einrichten, Geräte für die Mitarbeiter bereitstellen und anschließend laufende Verwaltungsaufgaben abschließen.

1. Vorbereiten

Der erste Schritt für jede Implementierung ist die Betrachtung der vorhandenen Umgebung. In dieser Phase ist es wichtig, Ihr Netzwerk und Ihre zentrale Infrastruktur besser zu verstehen sowie die für die erfolgreiche Implementierung erforderlichen Systeme einzurichten.

Infrastruktur evaluieren

Zwar integriert sich Mac nahtlos in die meisten Standardumgebungen der Unternehmens-IT, aber dennoch ist es wichtig, Ihre bestehende Infrastruktur zu evaluieren. Nur so können Sie sicherstellen, dass Ihr Unternehmen alle Vorteile von macOS auch nutzen kann. Wenn Ihr Unternehmen in diesem Bereich Unterstützung braucht, können Sie sich an Apple Professional Services sowie die technischen Teams Ihres Vertriebspartners oder Händlers wenden.

WLAN und Netzwerk
Für die Einrichtung und Konfiguration von macOS Geräten ist eine stabile WLAN-Verbindung unverzichtbar. Stellen Sie sicher, dass das WLAN Ihres Unternehmens richtig aufgesetzt ist. Prüfen Sie unter anderem den Standort und die Stromversorgung der Zugangspunkte, um Roaming- und Kapazitätsanforderungen zu erfüllen.

Wenn Ihre Geräte nicht auf Apple Server, den Apple Push-Benachrichtigungsdienst (APNs), iCloud oder den iTunes Store zugreifen können, müssen Sie möglicherweise auch die Konfiguration von Webproxies oder Firewallports anpassen. Genau wie bei iOS müssen bestimmte Komponenten im macOS Implementierungsprozess – vor allem bei der neueren Mac Hardware – konstant auf diese Dienste zugreifen.

Apple und Cisco haben die Kommunikation zwischen Mac Computern und einem drahtlosen Netzwerk von Cisco optimiert, u. a. werden innovative Netzwerk-Features in macOS High Sierra wie Quality of Service (QoS) unterstützt. Falls Sie Netzwerkgeräte von Cisco nutzen, arbeiten Sie mit Ihren internen Teams zusammen, um sicherzustellen, dass Mac kritischen Datenverkehr optimieren kann.

Für einen sicheren Fernzugriff auf Unternehmensressourcen muss außerdem die VPN-Infrastruktur evaluiert werden. Das macOS Feature „VPN On Demand" ermöglicht es, eine VPN-Verbindung nur dann zu starten, wenn sie benötigt wird. Wenn Sie VPN pro App verwenden möchten, prüfen Sie, dass Ihre VPN-Gateways diese Funktionen unterstützen und dass Sie genügend Lizenzen erworben haben, um die entsprechende Anzahl an Benutzern und Verbindungen abzudecken.

Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur ordnungsgemäß mit Bonjour zusammenarbeitet. Bonjour ist das auf Standards basierende Netzwerkprotokoll von Apple, das ohne Konfiguration auskommt. Es ermöglicht Geräten, automatisch Dienste in einem Netzwerk zu finden. macOS verwendet Bonjour, um sich mit AirPrint kompatiblen Druckern sowie AirPlay kompatiblen Geräten wie Apple TV zu verbinden. Manche Apps und integrierten macOS Features verwenden Bonjour auch, um andere Geräte für elektronisches Teamwork und Netzwerkfreigaben zu erkennen.

Weitere Infos zum Netzwerkdesign:
help.apple.com/deployment/macos

Weitere Infos zur Konfiguration Ihres Netzwerks für MDM:
help.apple.com/deployment/macos

Weitere Infos zu Bonjour:
help.apple.com/deployment/macos

Verwaltung von Identitäten
macOS kann zur Verwaltung von Identitäten und anderen Benutzerdaten auf Verzeichnisdienste wie Active Directory, Open Directory und LDAP zugreifen. Manche MDM-Anbieter stellen Tools bereit, um ihre Lösungen standardmäßig mit Active-Directory- und LDAP-Verzeichnissen zu integrieren. Zusätzliche Tools wie Enterprise Connect von Apple Professional Services oder NoMAD von Orchard & Grove erlauben eine Integration mit Active Directory Richtlinien und Funktionen, ohne dass eine herkömmliche Bindung nötig ist. Ihre MDM-Lösung kann außerdem unterschiedliche Arten von Zertifikaten von internen und externen Zertifizierungsstellen verwalten, sodass Identitäten automatisch als vertrauenswürdig gelten.

Weitere Infos zur Integration in Verzeichnisdienste:
help.apple.com/deployment/macos

Weitere Infos zur Verwaltung von Zertifikaten:
help.apple.com/deployment/macos

Zentrale Mitarbeiterdienste
Sorgen Sie dafür, dass Ihr Microsoft Exchange Dienst auf dem neuesten Stand und so konfiguriert ist, dass er alle Benutzer im Netzwerk unterstützt. Wird Exchange nicht verwendet, kann macOS auch mit standardbasierten Servern per IMAP, POP, SMTP, CalDAV, CardDAV und LDAP verwendet werden. Prüfen Sie grundlegende Workflows für E-Mail, Kontakte und Kalender sowie für andere in Unternehmen eingesetzte Produktivitäts- und Kollaborationssoftware, die den höchsten Anteil der wichtigen, täglichen Arbeitsabläufe der Benutzer abdeckt.

Weitere Infos zur Konfiguration von Microsoft Exchange:
help.apple.com/deployment/macos

Weitere Infos zu standardbasierten Diensten:
help.apple.com/deployment/macos

Caching

Der in macOS integrierte Cachingdienst speichert eine lokale Kopie häufig angeforderter Inhalte von Apple Servern, um so die Bandbreite zu minimieren, die zum Laden von Inhalten in Ihrem Netzwerk erforderlich ist. Mit Caching können Sie das Laden und Bereitstellen von Software aus dem Mac App Store, iTunes Store und iBooks Store beschleunigen.

Auch Softwareupdates können zum schnelleren Laden auf Ihre Unternehmensgeräte – egal, ob macOS oder iOS – im Cache zwischengespeichert werden.

Weitere Infos zum Caching: help.apple.com/deployment/macos

Eine Verwaltungslösung festlegen

Mit MDM können Unternehmen Mac Computer sicher in ihrer Unternehmensumgebung registrieren, drahtlos Einstellungen konfigurieren und aktualisieren, Apps bereitstellen, die Richtlinieneinhaltung überwachen, Geräte abfragen und verwaltete Geräte per Fernzugriff löschen oder sperren. Die IT kann ganz einfach Profile erstellen, um Benutzeraccounts zu verwalten, Systemeinstellungen zu konfigurieren, Einschränkungen durchzusetzen und Passwortrichtlinien festzulegen – und all dies ist über dieselbe Lösung für die mobile Geräteverwaltung möglich, die bereits für iPhone und iPad verwendet wird.

Sowohl macOS als auch iOS basieren auf einer gemeinsamen Verwaltungsarchitektur von Apple, die es Kunden erlaubt, unterschiedliche MDM-Lösungen anderer Anbieter zu verwenden. Anbieter wie Jamf, VMware und MobileIron stellen vielfältige Lösungen zur Geräteverwaltung bereit. Während sich macOS und iOS zum großen Teil dieselben Frameworks für die Geräteverwaltung teilen, gibt es bei diesen Lösungen kleine Unterschiede bei den Admin-Funktionen, unterstützten Betriebssystemen, Preisstrukturen und Hostingmodellen. Auch das Serviceangebot für Integration, Schulung und Support kann sich unterscheiden. Überlegen Sie sich, welche Verwaltungsfeatures für Ihr Unternehmen am wichtigsten sind, bevor Sie eine Lösung auswählen.

Wenn Sie sich für eine MDM-Lösung entschieden und mit der Konfiguration begonnen haben, müssen Sie sich beim Apple Push Certificates Portal anmelden, um ein neues Push-Zertifikat für MDM zu erstellen.

Weitere Infos zur Implementierung von MDM: help.apple.com/deployment/macos

Apple Push Certificates Portal: identity.apple.com/pushcert/

Bei Apple Diensten registrieren

Apple bietet eine Reihe von Diensten, mit denen Sie Ihre Implementierung auf einfache Weise optimieren können. Wenn Sie Apple Dienste zum ersten Mal nutzen, erhält der bei der Registrierung erstellte Account die höchsten Administratorrechte für diese Dienste und hat die komplette administrative Kontrolle über die einzelnen Dienste für Ihr Unternehmen. Sie können denselben Account zur Registrierung bei weiteren Apple Diensten verwenden.

Programm zur Geräteregistrierung

Mit dem Programm zur Geräteregistrierung (Device Enrolment Program, DEP) von Apple können Sie unternehmenseigene Mac Systeme, die Sie direkt bei Apple oder autorisierten Apple Händlern gekauft haben, schnell und effizient implementieren. Sie können die Ersteinrichtung von Mac Computern vereinfachen, indem Sie die MDM-Registrierung automatisieren, ohne dass Sie die Macs manuell konfigurieren oder vorbereiten müssen, bevor die Benutzer sie erhalten. Darüber hinaus können Sie den Konfigurationsprozess für Benutzer weiter vereinfachen, indem Sie bestimmte Schritte aus dem Systemassistenten entfernen.

Weitere Infos zum Programm zur Geräteregistrierung:
www.apple.com/de/business/dep/

Programm für Volumenlizenzen

Mit dem Programm für Volumenlizenzen (Volume Purchase Program, VPP) von Apple können Unternehmen macOS Apps und Bücher in großen Stückzahlen kaufen und an Mitarbeiter verteilen. Sie können mit einer Firmenkreditkarte oder mit dem VPP Guthaben zahlen, das Sie über eine Bestellung (PO) auf Rechnung erworben haben. Das VPP kann in MDM-Lösungen integriert und verwendet werden, um Apps und Bücher an Geräte und Benutzer in jedem Land zu verteilen, in dem die Apps und Bücher verfügbar sind. Mit der verwalteten Verteilung können Sie einzelne Lizenzen zurückziehen und je nach Bedarf anderen Mitarbeitern zuweisen.

Weitere Infos zum Programm für Volumenlizenzen:
www.apple.com/de/business/vpp/

Developer Enterprise Program

Das Developer Enterprise Program von Apple bietet alle nötigen Tools zum Entwickeln, Testen und Verteilen von macOS oder iOS Apps an die Benutzer. Sie können Apps verteilen, indem Sie diese auf einem Webserver hosten oder eine MDM-Lösung verwenden. Mac Apps und Installationsprogramme können mit Ihrer Entwickler-ID signiert werden, um die Kompatibilität mit dem in macOS zum Schutz vor Malware integrierten Gatekeeper sicherzustellen.

Weitere Infos zum Developer Enterprise Program:
developer.apple.com/programs/enterprise

2. Einrichten

Bei der Einrichtung müssen Sie Unternehmensrichtlinien festlegen und Ihre Lösung für die mobile Geräteverwaltung vorbereiten, damit Sie die Mac Computer für Ihre Mitarbeiter konfigurieren können.

macOS Sicherheit verstehen

Sicherheit und Datenschutz haben oberste Priorität beim Design all unserer Hardware, Software und Services. Wir schützen die Privatsphäre unserer Kunden durch starke Verschlüsselung und strikte Richtlinien, die den Umgang mit allen Daten betreffen. Eine sichere IT-Plattform für Apple Geräte umfasst:

- Methoden, um die unbefugte Nutzung von Geräten zu verhindern
- Schutz gespeicherter Daten, auch bei Verlust oder Diebstahl eines Geräts
- Netzwerkprotokolle und Verschlüsselung der Daten bei der Übertragung
- Sichere App-Ausführung, ohne die Plattformintegrität zu gefährden

macOS und iOS verfügen über mehrere Sicherheitsebenen, sodass Apple Geräte sicher auf Netzwerkdienste zugreifen und wichtige Daten schützen können. macOS und iOS bieten darüber hinaus Sicherheit durch Code- und Passwortrichtlinien, die sich mit MDM bereitstellen und durchsetzen lassen. Und falls ein Apple Gerät in die falschen Hände gerät, kann der Benutzer oder Administrator mit einem Fernlöschbefehl alle privaten Daten löschen. Mit MDM kann das IT-Team eine Reihe von Richtlinien zum Schutz der Mac Systeme implementieren. Beispiele hierfür sind die Durchsetzung von FileVault und der Verwahrung des Wiederherstellungsschlüssels mit MDM, das Erzwingen einer bestimmten Passwortrichtlinie oder der Bildschirmschoner-Sperre und die Aktivierung der integrierten Firewall.

Weitere Infos über die in macOS integrierte Sicherheit:
www.apple.com/de/macos/security/

Ausführliche Infos zu den macOS Sicherheitsfeatures:
help.apple.com/deployment/macos

Unternehmensrichtlinien festlegen

Beginnen Sie damit, eine Unternehmensrichtlinie zu entwickeln, indem Sie allgemeine Richtlinien für die Mehrheit der Mac Benutzer in Ihrem Unternehmen festlegen. Ihre MDM-Lösung erlaubt es Ihnen, benutzerspezifische Anpassungen wie Accounts oder den Zugriff auf bestimmte Apps zu definieren. Sie können auch konkrete Richtlinien für Unternehmen oder andere kleinere Untergruppen von Benutzern festlegen, z. B. für die Bereitstellung abteilungsspezifischer Software oder Einstellungen.

Aktualisieren Sie gemeinsam mit Ihren internen Teams bestehende Unternehmensrichtlinien, um die Nutzung von Mac Computern miteinzubeziehen. Einige zentrale Richtlinien bleiben über alle Plattformen hinweg unverändert, z. B. Anforderungen zur Komplexität und zum turnusmäßigen Wechsel von Passwörtern, Zeitlimits für Bildschirmschoner und zulässige Nutzung.

Wenn Ihre Unternehmensrichtlinie eine bestimmte Technologie vorsieht, die auf einer anderen Plattform läuft, machen Sie sich ein Bild von den Zusammenhängen und passen Sie die Richtlinie an, um integrierte Technologien auf macOS miteinzubeziehen. Statt zu verlangen, dass alle Computer eine bestimmte Lösung eines anderen Anbieters zur Verschlüsselung der kompletten Festplatte nutzen, könnten Sie in einer Richtlinie festlegen, dass Unternehmensdaten in ruhendem Zustand verschlüsselt werden müssen, und setzen Sie dies mit FileVault um. Schreibt die Richtlinie einen bestimmten Softwaretitel zum Schutz vor Malware vor, informieren Sie die Teams über integrierte Features wie Gatekeeper und passen Sie dann die Richtlinie entsprechend an.

Einstellungen in MDM konfigurieren

Um die Verwaltung von Unternehmensrichtlinien zu ermöglichen und den Zugriff der Mitarbeiter auf die erforderlichen Ressourcen sicherzustellen, wird jeder Mac sicher bei Ihrer MDM-Lösung registriert. Die MDM-Lösung wendet anschließend Richtlinien und Einstellungen mithilfe von Konfigurationsprofilen an. Konfigurationsprofile sind von Ihrer MDM-Lösung erstellte XML-Dateien, die die Verteilung von Einstellungen an macOS und iOS Geräte erlauben. Diese Profile automatisieren die Konfiguration von Einstellungen, Accounts, Richtlinien, Einschränkungen und Anmeldedaten. Sie können signiert und verschlüsselt werden, um die Sicherheit Ihrer Systeme zu erhöhen.

Sobald ein Gerät bei MDM registriert ist, kann der Administrator eine MDM-Richtlinie, eine MDM-Abfrage oder einen MDM-Befehl anstoßen. Mit einer Netzwerkverbindung erhält das Gerät anschließend eine Benachrichtigung über den Apple Push-Benachrichtigungsdienst (APNs) mit der Anweisung, direkt mit der MDM-Lösung über eine sichere Verbindung zu kommunizieren, um die Aktion des Administrators zu verarbeiten. Da die Verbindung nur zwischen der MDM-Lösung und dem Gerät besteht, übermittelt der APNs keine vertraulichen oder unternehmensinternen Informationen. Wird ein Gerät aus der Verwaltung herausgenommen, werden auch die Einstellungen und Richtlinien entfernt, die von diesem Konfigurationsprofil gesteuert werden. Bei Bedarf können Unternehmen ein Gerät auch fernlöschen.

Viele Unternehmen binden Ihre MDM-Lösung an ihre bestehenden Verzeichnisdienste an. Der Systemassistent in macOS kann Benutzer auffordern, sich bei der Erstregistrierung mit den Anmeldedaten für ihren Verzeichnisdienst anzumelden. Sobald das Gerät einem bestimmten Benutzer zugewiesen ist, kann die MDM-Lösung Konfigurationen und Accounts für eine bestimmte Person oder Gruppe individuell anpassen. Beispielsweise kann der persönliche Microsoft Exchange Account eines Benutzers bei der Registrierung automatisch bereitgestellt werden. Außerdem ist es möglich, Zertifikatidentitäten für Technologien wie 802.1x, VPN etc. zu verwenden.

Da diese Systeme eine effiziente Kontrolle erlauben, haben Unternehmen häufig kein Problem damit, Benutzern den vollen administrativen Zugriff für ihren Mac einzuräumen, sodass sie ihre Einstellungen umfassend personalisieren, Apps installieren und Probleme selbst beheben können, während sie sich über MDM immer noch innerhalb der Kontrolle der Unternehmensrichtlinien befinden. Dieses Modell berücksichtigt die Art der Berechtigungen und Kontrollen, die Benutzer über ihr iOS Gerät haben, wenn sie unter Verwaltung stehen.

Weitere Infos zu Konfigurationsprofilen: help.apple.com/deployment/macos

Für die Geräteregistrierung vorbereiten

Die einfachste Art, Geräte bei der MDM-Lösung zu registrieren, bietet der Systemassistent im Rahmen des Programms zur Geräteregistrierung. Dies erlaubt eine Registrierung ohne Eingriff des IT-Teams und ermöglicht eine Optimierung bestimmter Bildschirme des Systemassistenten, um den Prozess für die Benutzer schneller zu machen.

Um das Programm zur Geräteregistrierung zu konfigurieren, verknüpfen Sie Ihre MDM-Lösung über einen sicheren Token mit Ihrem DEP Account. Ein zweistufiger Bestätigungsprozess gewährleistet die sichere Autorisierung der MDM-Lösung. Ihr MDM-Anbieter kann Ihnen Dokumentation zu den Einzelheiten der speziellen Implementierung bereitstellen.

Bei Geräten, die bereits von den Mitarbeitern genutzt werden oder sich in ihrem privaten Besitz befinden, kann der Benutzer ein einziges Konfigurationsprofil öffnen und in den Systemeinstellungen verifizieren, um die Registrierung abzuschließen. Diese Vorgehensweise ist als MDM-Registrierung mit Benutzereinwilligung bekannt. Die Registrierung muss entweder im Rahmen des Programms zur Geräteregistrierung oder der MDM-Registrierung mit Benutzereinwilligung erfolgen, damit bestimmte sicherheitsrelevante Einstellungen (wie die Richtlinie für Kernelerweiterungen) in macOS High Sierra verwaltet werden können.

Weitere Infos zu Kernelerweiterungen und MDM-Registrierung mit Benutzereinwilligung: support.apple.com/HT208019

Verteilung von Apps und Büchern vorbereiten

Apple bietet umfangreiche Programme, mit denen Ihr Unternehmen von den großartigen für macOS erhältlichen Apps und Inhalten profitieren kann. Dadurch können Sie über das VPP gekaufte Apps und Bücher oder eigene interne Apps an die Mitarbeiter verteilen, damit diese sofort produktiv arbeiten können. Die MDM-Lösung kann auch Apps und Installationspakete für Software verteilen, die nicht im Mac App Store verfügbar ist.

Ihre MDM-Lösung kann die verwaltete Verteilung nutzen, um im VPP Store gekaufte Apps und Bücher in jedem Land zu verteilen, in dem die App verfügbar ist. Zur Aktivierung der verwalteten Verteilung müssen Sie zuerst Ihre MDM-Lösung mithilfe eines sicheren Tokens mit Ihrem VPP Account verknüpfen. Sobald Sie mit Ihrer MDM-Lösung verbunden sind, können Sie VPP Apps und Bücher Benutzern zuweisen, selbst wenn der App Store auf dem betreffenden Gerät deaktiviert ist. Sie können Apps auch direkt Geräten zuweisen. Das macht die Implementierung erheblich einfacher, da alle Benutzer auf diesem Gerät auf jede App zugreifen können.

Weitere Infos zum Kauf von Inhalten über das VPP:
help.apple.com/deployment/macos

Weitere Infos zur Verteilung von Apps und Büchern:
help.apple.com/deployment/macos

Zusätzliche Inhalte vorbereiten

Ihre MDM-Lösung kann Sie bei der Verteilung zusätzlicher Pakete mit Inhalten unterstützen, die nicht aus dem Mac App Store stammen. Dies ist ein gängiger Ansatz für Unternehmenssoftware, z. B. interne, eigene Apps oder Anwendungen wie Microsoft Office. Mit dieser Methode kann die erforderliche Software per Push bereitgestellt und nach der Registrierung automatisch installiert werden. Auch Schriften, Skripte etc. können über Pakete installiert und ausgeführt werden. Stellen Sie sicher, dass diese Pakete ordnungsgemäß mit Ihrer Entwickler-ID aus dem Developer Enterprise Programm signiert sind.

Weitere Infos zur Installation zusätzlicher Inhalte:
help.apple.com/deployment/macos

3. Bereitstellen

Mit macOS ist es ganz einfach, Geräte für Mitarbeiter bereitzustellen, sie bei Bedarf zu personalisieren und ohne Unterstützung des IT-Teams in Betrieb zu nehmen.

Den Systemassistenten nutzen

Mitarbeiter können mit dem Systemassistenten in macOS beim Start ihre Einstellungen für Sprache und Region festlegen und sich mit einem Netzwerk verbinden. Beim Verbindungsaufbau mit dem Internet bekommen die Benutzer mehrere Fenster des Systemassistenten angezeigt, die sie durch die wichtigsten Schritte zum Einrichten eines neuen Mac führen. Beim DEP registrierte Geräte können bei diesem Prozess automatisch bei der MDM-Lösung registriert werden. Mac Systeme, die beim DEP registriert sind, können zudem so konfiguriert werden, dass sie bestimmte Bildschirme, wie beispielsweise zur Lizenzvereinbarung, Apple ID Anmeldung oder den Ortungsdiensten, überspringen.

Nach Abschluss des Systemassistenten können mit der MDM-Lösung bei der Erstkonfiguration dann verschiedenste Einstellungen implementiert werden, u. a. lässt sich definieren, ob ein Benutzer sämtliche administrativen Berechtigungen über seinen Computer erhält. Genau wie bei iOS Geräten erhalten Benutzer so die Kontrolle über ihr Gerät, während gleichzeitig die von der MDM-Lösung verwalteten Unternehmensrichtlinien und -einstellungen eingehalten werden. Damit Benutzer sofort nach Abschluss des Systemassistenten produktiv arbeiten können, sollten nur die wichtigsten Apps und Pakete im Hintergrund geladen und installiert werden, sodass der Mitarbeiter ungestört mit seiner Arbeit loslegen kann. Benutzer können im Self-Service-Tool Ihrer MDM-Lösung den Zeitpunkt bestimmen, wann größere Anwendungen im Hintergrund geladen und installiert werden sollen.

Weitere Infos zur Konfiguration des Systemassistenten über das DEP:
help.apple.com/deployment/macos/

Unternehmensaccounts konfigurieren

Mit MDM lassen sich E-Mail- und andere Accounts automatisch einrichten. Je nach eingesetzter MDM-Lösung und ihrer Integration mit Ihren internen Systemen können Account-Payloads auch mit dem Namen und der E-Mail-Adresse des Benutzers sowie Zertifikatsidentitäten zur Authentifizierung und Signierung vorausgefüllt werden.

Benutzerpersonalisierung erlauben

Wenn Benutzer die Möglichkeit haben, ihre Geräte zu personalisieren, können sie produktiver arbeiten. Dann können sie nämlich selbst entscheiden, mit welchen Apps und Inhalten sie ihre Aufgaben und Ziele am besten erreichen können.

Apple ID
Die Apple ID ist eine Identität, mit der sich Benutzer bei verschiedenen Apple Diensten wie FaceTime, iMessage, iTunes Store, App Store, iBooks Store und iCloud anmelden können. Mit diesen Diensten erhalten Benutzer Zugriff auf eine Vielzahl von Inhalten zur Optimierung geschäftlicher Aufgaben, Steigerung der Produktivität und Unterstützung der Zusammenarbeit.

Um diese Dienste optimal nutzen zu können, sollten die Benutzer ihre eigene Apple ID verwenden. Benutzer, die noch keine Apple ID haben, können eine erstellen, noch bevor sie ein Gerät erhalten. Der Systemassistent ermöglicht dem Benutzer ebenfalls, eine persönliche Apple ID zu erstellen, falls er noch keine hat. Die Benutzer brauchen keine Kreditkarte, um eine Apple ID zu erstellen.

Weitere Infos zu Apple IDs: help.apple.com/deployment/macos

iCloud
Mit iCloud können Benutzer automatisch Dokumente und persönliche Inhalte wie Kontakte, Kalender, Dokumente und Fotos synchronisieren und sie zwischen verschiedenen Geräten aktuell halten. „Mein iPhone suchen" unterstützt Benutzer dabei, verlorene oder gestohlene Mac Computer bzw. iPhone, iPad oder iPod touch Geräte zu orten. Einige Dienste von iCloud – wie der iCloud Schlüsselbund und iCloud Drive – lassen sich anhand von Einschränkungen, die entweder manuell auf dem Gerät eingegeben oder über die MDM-Lösung festgelegt werden, deaktivieren. Die Benutzer können so iCloud für ihre persönlichen Daten verwenden, ohne dass dort Unternehmensinformationen gespeichert werden.

Weitere Infos zur Verwaltung von iCloud: help.apple.com/deployment/macos

4. Verwalten

Sobald Ihre Benutzer einsatzbereit sind, steht ein breites Spektrum an administrativen Funktionen zur Verfügung, mit denen Sie Ihre Geräte und Inhalte fortlaufend verwalten und warten können.

Geräte verwalten

Die MDM-Lösung kann verwaltete Geräte mithilfe einer Reihe spezifischer Aufgaben verwalten. Zu diesen Aufgaben zählen das Abfragen von Geräteinformationen sowie das Anstoßen von Verwaltungsaufgaben, mit denen Sie Geräte verwalten können, die gegen eine Richtlinie verstoßen, verloren gehen oder gestohlen werden.

Abfragen

Eine MDM-Lösung kann Geräte nach verschiedenen Informationen abfragen, um sicherzustellen, dass Benutzer die geeigneten Apps und Einstellungen verwenden. Diese Abfragen können sich auf die Hardware beziehen, z. B. die Seriennummer oder das Gerätemodell, oder auf die Software, z. B. die macOS Version oder eine Liste installierter Apps. Darüber hinaus kann die MDM-Lösung den Zustand wichtiger Sicherheitsfeatures abfragen, wie beispielsweise FileVault oder die integrierte Firewall.

Verwaltungsaufgaben

Wenn ein Gerät verwaltet wird, kann ein MDM-Server eine Vielzahl von Verwaltungsaufgaben ausführen, darunter das automatische Ändern von Konfigurationseinstellungen ohne Benutzereingriff, die Durchführung eines macOS Updates, das Sperren oder Löschen eines Geräts per Fernzugriff oder das Verwalten von Passwörtern.

Die vollständige Liste der Verwaltungsaufgaben finden Sie hier:
help.apple.com/deployment/macos

Softwareupdates verwalten

Das IT-Team kann Benutzern die Möglichkeit geben, ein Upgrade auf das neueste Betriebssystem gleich bei Verfügbarkeit durchzuführen. Durch Testen einer Vorabversion von macOS kann das IT-Team Probleme bei der Programmkompatibilität frühzeitig erkennen und gemeinsam mit den Entwicklern vor Veröffentlichung der endgültigen Version beseitigen. Über das Apple Beta Software-Programm oder AppleSeed for IT kann das IT-Team die einzelnen Releases vorab testen. Ein umfassender Ansatz unterstützt Sie dabei, Ihre Mac Computer aktuell zu halten, um Ihre Benutzer und ihre Daten zu schützen. Aktualisieren Sie schnell und führen Sie Upgrades durch, sobald Sie feststellen, dass Ihr Arbeitsablauf mit einer wichtigen neuen Version von macOS kompatibel ist.

Ihre MDM-Lösung kann macOS Updates automatisch per Push auf beim DEP registrierte Mac Computer übertragen. Beim DEP registrierte Mac Computer können auch so konfiguriert werden, dass sie Updates und entsprechende Benachrichtigungen bis zu 90 Tage zurückstellen, falls kritische Systeme nicht bereit dafür sind. Die Benutzer können Updates erst dann manuell starten, wenn die Richtlinie entfernt wurde oder die MDM-Lösung einen Installationsbefehl versendet.

Apple empfiehlt oder unterstützt kein monolithisches System-Imaging für macOS Upgrades. Wie beim iPhone oder iPad benötigen Mac Computer häufig Firmware-Updates für ihr spezifisches Modell. Dementsprechend ist es bei Aktualisierungen des Mac Betriebssystems erforderlich, dass diese Firmware-Updates direkt von Apple installiert werden. Am zuverlässigsten ist es daher, für die Implementierung das macOS Installationsprogramm zu verwenden. Laden Sie das macOS High Sierra Installationsprogramm und installieren Sie es am gleichen Ort wie die Internetwiederherstellung, ein startfähiges externes Installationsprogramm oder NetInstall (Teil des System-Image-Dienstprogramms).

Zusätzliche Software verwalten

Neben den anfänglich bereitgestellten Apps müssen Unternehmen häufig zusätzliche Apps an ihre Benutzer ausgeben. Kritische Apps und Updates können von Ihrer MDM-Lösung automatisch verteilt werden. Oder Sie erlauben Ihren Benutzern, bei Bedarf Apps über ein von Ihrer MDM-Lösung bereitgestelltes Self-Service-Portal anzufordern. Mit diesen Portalen lässt sich nicht nur Software installieren, die im App Store über das VPP gekauft wurde, sondern auch Apps, die nicht aus dem App Store stammen, sowie Skripte und andere Dienstprogramme.

Zwar kann die meiste Software automatisch installiert werden, doch bei bestimmten Installationen ist möglicherweise ein Benutzereingriff erforderlich. Um die Sicherheit zu verbessern, muss der Benutzer bei Apps, die Kernelerweiterungen erfordern, neu seine Einwilligung geben, damit sie geladen werden. Dies nennt man „Laden von Kernelerweiterungen nach Benutzergenehmigung" und kann von der MDM-Lösung verwaltet werden.

Weitere Infos zum Laden von Kernelerweiterungen nach Benutzergenehmigung: help.apple.com/deployment/macos

Gerätesicherheit gewährleisten

Nachdem Sie die ersten Sicherheitsrichtlinien vor der Geräteimplementierung erstellt haben, möchte Ihr Team nun wahrscheinlich überwachen, dass diese Richtlinien auf den Geräten eingehalten werden, und so viel Reporting wie möglich aus Ihrer MDM-Lösung herausholen. Dies könnte die Überwachung des Sicherheitsstatus der einzelnen Geräte beinhalten oder das Einholen von Informationen zur Installation von Softwarepatches. Obwohl es für die meisten Unternehmen kein Problem ist, native Tools zur Verschlüsselung und zum Schutz der einzelnen Mac Computer zu verwenden, bestehen einige Unternehmen auf den Einsatz von zusätzlichen Diensten zum Synchronisieren und Teilen von Dateien oder Tools zum Schutz vor Datenverlust, um Datenlecks im Unternehmen zu verhindern und ein detailliertes Reporting zu sensiblen Daten bereitzustellen.

Das iCloud Feature „Meinen Mac suchen" erlaubt es, per Fernzugriff sämtliche Daten zu löschen und einen Mac Computer zu deaktivieren, falls er verloren geht oder gestohlen wird. Das IT-Team kann Daten auch mit Ihrer MDM-Lösung fernlöschen.

Geräte erneut bereitstellen

Ein Mac Computer lässt sich mit der Internetwiederherstellung und der lokalen Wiederherstellungspartition ganz einfach erneut für einen anderen Benutzer bereitstellen, wenn ein Mitarbeiter das Unternehmen verlässt. Dadurch können Sie die Inhalte auf dem Mac Computer löschen und die neueste Version des Betriebssystems installieren. Ein beim DEP registrierter Mac Computer registriert sich während der Ausführung des Systemassistenten automatisch erneut bei der MDM-Lösung, konfiguriert die Einstellungen für den neuen Benutzer, wendet Unternehmensrichtlinien an und stellt die erforderliche Software bereit.

Nicht beim DEP registrierte Mac Computer können mit demselben Prozess gelöscht und erneut bereitgestellt und anschließend manuell registriert werden.

Weitere Infos zur Internetwiederherstellung: help.apple.com/deployment/macos

Supportoptionen

Viele Unternehmen stellen fest, dass Mac Benutzer nur minimalen IT-Support benötigen. Damit sich Mitarbeiter selbst helfen können und um die Supportqualität zu verbessern, entwickeln die meisten IT-Teams Self-Support-Tools. Beispiele hierfür umfassen die Entwicklung einer zuverlässigen Mac Support-Webseite, das Angebot von Selbsthilfeforen und die Bereitstellung von technischer Vor-Ort-Hilfe. Mit MDM-Lösungen können Benutzer auch Supportaufgaben wie die Installation oder Aktualisierung von Software in einem Self-Service-Portal durchführen.

Unternehmen sollten die Benutzer allerdings nicht zwingen, ihre Probleme ohne jegliche Unterstützung zu lösen. Stattdessen empfehlen wir, einen kollaborativen Ansatz bei der Problemlösung zu verfolgen und die Benutzer zu ermutigen, Problemen erst einmal selbst auf den Grund zu gehen, bevor sie den Helpdesk anrufen. Motivieren Sie die Benutzer, sich an der Problemlösung zu beteiligen und sich erst einmal selbst zu bemühen, bevor sie um Unterstützung bitten.

Durch eine geteilte Verantwortung für den Support lassen sich Ausfallzeiten für die Mitarbeiter sowie der Gesamtaufwand in Form von Supportkosten und Personaleinsatz reduzieren. Für Unternehmen, die mehr Support benötigen, bietet AppleCare zahlreiche Programme und Dienste, die interne Supportstrukturen für Mitarbeiter und IT-Teams ergänzen.

AppleCare for Enterprise

Falls Ihr Unternehmen umfassenden Schutz wünscht, kann AppleCare for Enterprise Sie bei der Entlastung Ihres internen Helpdesks unterstützen. Dies geschieht durch die Bereitstellung von technischem Support für Mitarbeiter per Telefon, rund um die Uhr mit Antwortzeiten von einer Stunde für Probleme mit höchster Priorität. Das Programm unterstützt IT-Abteilungen zudem bei Integrationsszenarien, einschließlich MDM und Active Directory.

AppleCare OS Support

AppleCare OS Support bietet Ihrer IT-Abteilung unternehmensspezifischen Support per Telefon und E-Mail für iOS, macOS und macOS Server Implementierungen. Sie erhalten je nach gekaufter Supportstufe bis zu Rund-um-die-Uhr-Support und einen zugewiesenen technischen Accountmanager. Durch den direkten Kontakt zum Techniker bei Fragen zu Integration, Migration und komplexen Problemen beim Serverbetrieb kann AppleCare OS Support die Effizienz Ihres IT-Teams bei der Implementierung und Verwaltung von Geräten und bei der Problembehebung steigern.

AppleCare Help Desk Support

Mit dem AppleCare Help Desk Support erhalten Sie vorrangigen telefonischen Support von erfahrenen Apple Supportmitarbeitern. Er umfasst auch eine Reihe von Werkzeugen für die Diagnose und Behebung bei Problemen mit Apple Hardware. So können große Unternehmen ihre Ressourcen effizienter verwalten, die Reaktionszeiten verbessern und Schulungskosten reduzieren. Der AppleCare Help Desk Support bietet unbegrenzten Support für Hardware- und Softwarediagnosen sowie Problembehebung und Problemeingrenzung für iOS Geräte.

AppleCare und AppleCare+ für Mac

Für jeden Mac Computer gilt eine einjährige eingeschränkte Herstellergarantie. Zusätzlich kann innerhalb von 90 Tagen ab Kaufdatum technischer Telefonsupport in Anspruch genommen werden. Der Anspruch auf Service lässt sich mit AppleCare+ oder dem AppleCare Protection Plan auf drei Jahre ab Kaufdatum verlängern. Mitarbeiter können den Apple Support bei Fragen zur Apple Hardware oder Software anrufen. Apple bietet zudem praktische Service-Optionen an, wenn Geräte repariert werden müssen. Bei AppleCare+ für Mac sind darüber hinaus ausgewählte Reparaturen von Unfallschäden inbegriffen,
für die jeweils eine Servicegebühr anfällt.

Weitere Infos zu den AppleCare Supportoptionen:
www.apple.com/de/support/professional/

Zusammenfassung

Wenn Ihr Unternehmen Mac Computer für eine Gruppe von Benutzern oder im gesamten Unternehmen implementieren möchte, haben Sie viele Optionen für die einfache Implementierung und Verwaltung der Geräte. Die Wahl der richtigen Strategien kann es den Mitarbeitern Ihres Unternehmens ermöglichen, produktiver zu arbeiten und ihre Arbeit auf völlig neue Art und Weise zu erledigen.

Weitere Infos zur Implementierung, Verwaltung und zu Sicherheitsfeatures von macOS: help.apple.com/deployment/macos/

Weitere Infos zu Apple in Unternehmen:
www.apple.com/de/business/

Mehr zu den verfügbaren AppleCare Programmen:
www.apple.com/de/support/professional/

Mehr zu Apple Training und Zertifizierung:
training.apple.com

Kontakt zu Apple Professional Services:
consultingservices@apple.com