Mac Implementierung: Überblick

Einführung

Inhalt

Der Mac zusammen mit macOS ermöglicht es Mitarbeiter:innen, von überall aus ihr Bestes zu geben. Und IT-Abteilungen müssen weniger Zeit für die Verwaltung von Geräten aufwenden. So können sie sich auf die Unternehmensstrategie und andere Anforderungen konzentrieren statt nur technische Probleme zu lösen und Kosten zu senken.

Dieses Dokument unterstützt Sie bei der Implementierung von macOS Geräten in Ihrer Organisation und hilft Ihnen, einen grundlegenden Implementierungsplan zu entwickeln, der am besten zu Ihrer Umgebung passt.

Weitere Infos zu diesen Themen und den Neuerungen bei der Implementierung der neuesten macOS Updates finden Sie online im Handbuch zur Implementierung von Apple Plattformen.

Eigentumsmodelle

Die zwei häufigsten Eigentumsmodelle für macOS Geräte in Organisationen sind:

- Eigentum der Organisation
- Eigentum der Benutzer:innen

Jedes Modell hat seine Vorteile, daher ist es wichtig, dass Sie sich für das Modell entscheiden, das am besten zu Ihrer Organisation passt. Obwohl die meisten Organisationen ein bestimmtes Modell bevorzugen, kommen in Ihrer Umgebung möglicherweise mehrere Modelle zum Einsatz.

Nachdem Sie das passende Modell für Ihre Organisation identifiziert haben, kann Ihr Team die Implementierungs- und Verwaltungsfunktionen von Apple im Detail erkunden.

Geräte im Besitz der Organisation

Beim Modell mit Geräten im Besitz der Organisation erwirbt diese die Geräte bei Apple oder einem teilnehmenden autorisierten Apple Händler oder Mobilfunkanbieter. Wenn jede:r Benutzer:in ein Gerät erhält, nennt man das eine 1-to-1-Implementierung. Geräte können auch abwechselnd von mehreren Benutzer:innen verwendet werden, was häufig als Implementierung mit geteilter Nutzung bezeichnet wird. „Geteiltes iPad" ist ein Eigentumsmodell, bei dem mehrere Benutzer:innen ein iPad Gerät gemeinsam nutzen können, ohne Daten zu teilen. Dies ist ein Beispiel für eine Implementierung mit geteilter Nutzung. Organisationen können in ihren Umgebungen eine Kombination aus geteilten und 1-to-1-Implementierungsmodellen nutzen.

Bei einem Modell mit Geräten im Besitz der Organisation hat die IT-Abteilung mehr Kontrolle durch die Betreuung und automatische Geräteregistrierung, mit der Organisationen die Geräte direkt nach dem Auspacken konfigurieren und verwalten können.

Weitere Infos zu Einschränkungen für betreute Geräte: support.apple.com/guide/mdm

Die IT hat mehr Kontrolle, wenn sie Apple Geräte betreut.

- Accounts konfigurieren
- Globale Proxys konfigurieren
- Apps installieren, konfigurieren und entfernen
- Komplexen Code verlangen
- Alle Einschränkungen durchsetzen
- Verzeichnis von allen Apps aufrufen
- Das gesamte Gerät per Fernzugriff löschen
- Softwareupdates verwalten
- Systemapps entfernen
- Das Hintergrundbild ändern
- Auf eine einzelne App beschränken
- Aktivierungssperre umgehen
- WLAN einschalten
- Gerät in den Modus „Verloren" versetzen

Benutzereigene Geräte

Bei einem Modell mit Geräten im Besitz der Benutzer:innen erwerben diese die Geräte, richten sie ein und konfigurieren sie. Diese Implementierungen werden auch als BYOD-Implementierungen (Bring Your Own Device) bezeichnet. BYOD-Implementierungen sind bei macOS Geräten seltener, können aber dennoch in Ihrer Organisation eingesetzt werden. Um Services der Organisation zu nutzen – wie WLAN, Mail und Kalender – oder um Geräte für bestimmte Bildungs- oder Unternehmensanforderungen zu konfigurieren, registrieren Benutzer:innen ihre Geräte normalerweise in der MDM-Lösung (Mobile Device Management) der Organisation. Das wird Benutzerregistrierung genannt.

Die Benutzerregistrierung von persönlichen Geräten ermöglicht es, Ressourcen und Daten des Unternehmens auf sichere Weise zu verwalten und gleichzeitig die Privatsphäre und die persönlichen Daten und Apps der Benutzer:innen zu respektieren. Die IT-Abteilung kann bestimmte Funktionen, die in der Tabelle unten beschrieben werden, durchsetzen, darauf zugreifen und sie verwalten.

Um auf die Daten des Unternehmens auf ihren Geräten zuzugreifen, nutzen die Benutzer:innen ihre verwaltete Apple ID. Eine verwaltete Apple ID ist Teil des Registrierungsprofils und Benutzer:innen müssen erfolgreich authentifiziert werden, damit die Registrierung abgeschlossen werden kann. Die verwaltete Apple ID kann neben der persönlichen Apple ID verwendet werden, mit der sich Benutzer:innen bereits angemeldet haben, und beide bleiben völlig voneinander getrennt. Auf diese Weise werden die Daten auf dem Gerät voneinander getrennt. Für Organisationen mit iCloud Speicherplatz wird ein separates iCloud Drive für alle Daten erstellt, die unter der verwalteten Apple ID gespeichert werden.

Weitere Infos zur Benutzerregistrierung mit MDM:
support.apple.com/guide/mdm

MDM Funktionen sind für persönliche Geräte eingeschränkt.

- ✓ Accounts konfigurieren
- ✓ VPN pro App konfigurieren
- ✓ Apps installieren und konfigurieren
- ✓ Eingabe eines Codes verlangen
- ✓ Bestimmte Einschränkungen durchsetzen
- ✓ Verzeichnis von Arbeitsapps aufrufen
- ✓ Nur Arbeitsdaten löschen
- ✗ Auf persönliche Daten zugreifen
- ✗ Verzeichnis von persönlichen Apps aufrufen
- ✗ Persönliche Daten löschen
- ✗ Protokolle auf dem Gerät speichern
- ✗ Persönliche Apps übernehmen
- ✗ Komplexen Code verlangen
- ✗ Das gesamte Gerät per Fernzugriff löschen
- ✗ Auf den Gerätestandort zugreifen

Implementierungsschritte

Dieser Abschnitt enthält einen Überblick über die Schritte für die Implementierung von Geräten und Inhalten: Umgebung vorbereiten, Geräte einrichten, Geräte bereitstellen und Geräte verwalten. Die verwendeten Schritte hängen davon ab, ob die Geräte der Organisation oder den Benutzer:innen gehören.

Ausführliche Informationen zu diesen Schritten gibt es online im Apple Implementierungshandbuch.

1. Integration und Einrichtung

Nachdem Sie ermittelt haben, welches Modell für Ihre Organisation das richtige ist, befolgen Sie diese Schritte, um den Grundstein für die Implementierung zu legen.

MDM-Lösung. Die Verwaltungsarchitektur von Apple für macOS gibt Organisationen die Möglichkeit, Geräte sicher in der Unternehmensumgebung zu registrieren, Einstellungen drahtlos zu konfigurieren und zu aktualisieren, die Einhaltung von Richtlinien zu überwachen, Apps und Bücher zu bereitzustellen und verwaltete Geräte per Fernzugriff zu löschen oder zu sperren. Diese Verwaltungsfunktionen werden von MDM-Lösungen anderer Anbieter unterstützt. Es ist eine Reihe von MDM-Lösungen anderer Anbieter verfügbar, um verschiedene Serverplattformen zu unterstützen. Jede Lösung bietet andere Verwaltungskonsolen und Features zu unterschiedlichen Preisen.

Apple Business Manager. Ein webbasiertes Portal für IT-Administratoren zur Bereitstellung von iPhone, iPad, iPod touch, Apple TV und Mac Computern von einem zentralen Ort aus. Apple Business Manager arbeitet nahtlos mit Ihrer MDM-Lösung zusammen und macht es einfach, die Implementierung von Geräten zu automatisieren, Apps und Inhalte zu kaufen und verwaltete Apple IDs für Mitarbeiter:innen zu erstellen.

Verwaltete Apple IDs. Mit einer Apple ID können sich Benutzer:innen bei Apple Services wie FaceTime, iMessage, dem App Store und iCloud anmelden und auf eine Vielzahl von Inhalten und Services zugreifen, die die Produktivität steigern und die Zusammenarbeit unterstützen. Wie alle Apple IDs dienen verwaltete Apple IDs zur Anmeldung bei einem persönlichen Gerät und sind ein wesentlicher Bestandteil der Verwaltung von Apple Geräten. Verwaltete Apple IDs ermöglichen den Zugriff auf Apple Services – inklusive iCloud und die Zusammenarbeit mit iWork und Notizen – genauso wie eine persönliche Apple ID. Verwaltete Apple IDs gehören jedoch der Organisation und werden auch von dieser verwaltet, etwa zum Zurücksetzen von Passwörtern und zur funktionsbasierten Verwaltung. Verwaltete Apple IDs haben bestimmte eingeschränkte Einstellungen.

Weitere Infos zu verwalteten Apple IDs:
support.apple.com/guide/apple-business-manager

WLAN und Netzwerk. Apple Geräte haben eine sichere integrierte drahtlose Netzwerkkonnektivität. Vergewissern Sie sich, dass das WLAN Ihres Unternehmens mehrere Geräte mit gleichzeitigen Verbindungen von all Ihren Benutzer:innen unterstützen kann. Apple und Cisco haben die Kommunikation zwischen Mac Computern und einem drahtlosen Netzwerk von Cisco optimiert, u. a. werden innovative Netzwerk-Features in macOS 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. Sie sollten außerdem sicherstellen, dass die 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 Thema WLAN und Netzwerke:
support.apple.com/guide/deployment-reference-ios

Weitere Infos zum Konfigurieren des Netzwerks für MDM:
support.apple.com/HT210060

Weitere Infos zu Bonjour:
developer.apple.com/library

VPN. 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.

E-Mail, Inhalte und Kalender. Das iPhone, das iPad und der Mac funktionieren mit Microsoft Exchange, Office 365 und anderen beliebten E-Mail Diensten wie G Suite, um direkt über eine verschlüsselte SSL-Verbindung auf Push-Funktionen für E-Mails, Kalender, Kontakte und Aufgaben zuzugreifen. Überprüfen Sie bei der Verwendung von Microsoft Exchange, ob der ActiveSync Dienst auf dem aktuellen Stand und so konfiguriert ist, dass alle Benutzer:innen im Netzwerk unterstützt werden können. Wenn Sie die Cloud-basierte Version von Office 365 verwenden, stellen Sie sicher, dass Sie für die Anzahl der voraussichtlich verbundenen macOS Geräte über ausreichend Lizenzen verfügen.

Identitäten verwalten. 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 LDAP- und Active Directory Verzeichnissen zu integrieren. Zusätzliche Tools wie die Kerberos Single Sign-on Erweiterung in macOS Catalina erlauben eine Integration mit Active Directory Richtlinien und Funktionen, ohne dass eine herkömmliche Bindung und ein mobiler Account nötig sind. Und Ihre MDM-Lösung kann unterschiedliche Arten von Zertifikaten von internen und externen Zertifizierungsstellen verwalten, sodass Identitäten automatisch als vertrauenswürdig gelten.

Weitere Infos zum neuen Kerberos Single Sign-On:
support.apple.com/guide/deployment

Weitere Infos zur Verzeichnisintegration:
support.apple.com/guide/deployment

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:innen abdeckt.

Weitere Infos zur Konfiguration von Microsoft Exchange:
support.apple.com/guide/deployment

Weitere Infos zu auf Standards basierenden Diensten:
support.apple.com/guide/deployment

Inhaltscaching. 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 beschleunigen. Auch Softwareupdates können zum schnelleren Laden auf die Geräte Ihrer Organisation – egal ob macOS, iOS oder iPadOS – zwischengespeichert werden. Zusätzliche Inhalte können Sie auch mit Lösungen anderer Anbieter von Cisco und Akamai zwischenspeichern.

Weitere Infos zum Inhaltscaching:
support.apple.com/guide/deployment

2. Planung und Bereitstellung der Implementierung

Sobald Sie die Grundlagen geschaffen haben, können Sie Ihre Geräte konfigurieren und die Verteilung von Inhalten vorbereiten. Alle Eigentums- und Implementierungsmodelle funktionieren am besten, wenn sie mit einer MDM-Lösung und Apple Business Manager oder mit einer MDM-Lösung und Apple Configurator 2 verwendet werden.

Automatische Geräteregistrierung

Die automatische Geräteregistrierung ist eine schnelle und optimierte Möglichkeit, unternehmenseigene Apple Geräte zu implementieren und bei der MDM-Lösung zu registrieren, ohne dass sie dafür einzeln in die Hand genommen oder vorbereitet werden müssen. IT-Teams können den Einrichtungsprozess für Endbenutzer:innen vereinfachen, indem sie die Schritte im Systemassistenten optimieren und so sicherstellen, dass die Mitarbeiter:innen direkt nach der Aktivierung ihrer Geräte die richtigen Konfigurationen erhalten. Über die automatische Geräteregistrierung können nur Geräte implementiert werden, die direkt bei Apple oder bei teilnehmenden autorisierten Apple Händlern oder Mobilfunkanbietern gekauft wurden. Es kann jedoch einige Mac Computer geben, die außerhalb der üblichen Kanäle, die die automatische Geräteregistrierung unterstützen, erworben oder gespendet werden. Für diese Situationen hat Apple die neue App Apple Configurator für das iPhone eingeführt. Apple Configurator für iPhone macht es leicht, jeden unterstützten Mac mit macOS Monterey in Apple Business Manager zu Ihrer Organisation hinzuzufügen, damit IT-Teams all die großartigen Features für die Geräteverwaltung nutzen können, die die automatische Geräteregistrierung ermöglicht.

Weitere Infos zu Apple Configurator für iPhone:
support.apple.com/guide/apple-configurator/welcome/ios

Geräteregistrierung

Geräte können auch manuell über Apple Configurator 2 und die MDM-Lösung Ihres Unternehmens implementiert werden. Geräte im Besitz des Unternehmens oder der Benutzer:innen können über die Geräteregistrierung implementiert werden. Geräte, die manuell verwaltet werden, verhalten sich wie jedes andere zugewiesene Gerät, mit obligatorischer Betreuung und MDM-Registrierung. Diese Implementierungsmethode ist optimal für IT-Teams, die Geräte verwalten, die nicht direkt bei Apple oder über teilnehmende autorisierte Apple Händler oder Mobilfunkanbieter erworben wurden.

Weitere Infos zu Apple Configurator 2:
support.apple.com/de-de/apple-configurator

Benutzerregistrierung

Geräte im Besitz der Benutzer:innen können über die Benutzerregistrierung konfiguriert und implementiert werden. So kann die IT-Abteilung die Unternehmensdaten schützen, ohne die Geräte zu sperren. Weitere Infos zur Benutzerregistrierung gibt es im Abschnitt über Eigentumsmodelle.

Unabhängig davon, ob ein Gerät im Besitz des Unternehmens oder der Benutzer:innen ist, behalten IT-Teams bei der Bereitstellung von Geräten über den Systemassistenten die Kontrolle über die Einrichtung. Der Systemassistent wird über Ihre MDM-Lösung konfiguriert. So können Benutzer:innen direkt anfangen, mit ihren Geräten zu arbeiten.

Sobald ein Gerät registriert ist, können Administrator:innen eine MDM-Richtlinie, eine MDM-Option oder einen MDM-Befehl einleiten; welche Verwaltungsaktionen für ein Gerät verfügbar sind, hängt von der Betreuung und der Registrierungsmethode ab. Das macOS Gerät wird dann mithilfe des Apple Push-Benachrichtigungsdienstes (APNs) über die Aktion der Administrator:innen benachrichtigt, damit es über eine sichere Verbindung direkt mit seinem MDM-Server kommunizieren kann. Über eine Netzwerkverbindung können APNs Befehle an Geräte überall auf der Welt senden. APNS überträgt jedoch keine vertraulichen oder geschützten Informationen.

3. Konfigurationsverwaltung

Apple Geräte haben eine integrierte, sichere Verwaltungsarchitektur, die es der IT ermöglicht, Geräte mit vielen verschiedenen administrativen Funktionen zu verwalten. Diese Verwaltungsarchitektur kann in vier Bereiche unterteilt werden:

Konfigurationsprofile

Konfigurationsprofile bestehen aus Payloads, die bestimmte Einstellungen und Autorisierungsinformationen auf Apple Geräte laden. Sie automatisieren die Konfiguration von Einstellungen, Accounts, Einschränkungen und Anmeldedaten. Abhängig vom Anbieter der MDM-Lösung und deren Integration in die internen Systeme können Account-Payloads mit dem Namen und der E-Mail Adresse von Benutzer:innen sowie ggf. mit Zertifikatsidentitäten zur Authentifizierung und Signierung vorausgefüllt werden.

Einschränkungen

Durch Einschränkungen können Sie Sicherheitsrichtlinien durchsetzen und Benutzer:innen dabei unterstützen, sich zu konzentrieren, ohne die Geräte zu sperren. Zu den Einschränkungen gehören zum Beispiel Features wie „Alle Inhalte & Einstellungen löschen", die den Mac schnell auf die aktuelle Systemversion zurücksetzen und dabei alle Benutzerdaten kryptografisch entfernen.

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. Und Sie können Benutzer:innen für bis zu 90 Tage daran hindern, ein betreutes Gerät manuell drahtlos zu aktualisieren. Softwareupdates auf betreuten Geräten können außerdem mit Ihrer Lösung für mobile Geräteverwaltung (MDM) im Voraus geplant werden.

Abfragen

Ein MDM-Server kann eine Vielzahl von Geräteinformationen abfragen, darunter Hardwareinformationen wie Seriennummer, Geräte-UDID oder WLAN MAC-Adresse sowie Softwareinformationen wie die macOS Version und eine detaillierte Liste aller Apps, die auf dem Gerät installiert sind. Mithilfe dieser Informationen kann Ihre MDM-Lösung beispielsweise Bestandsinformationen aktualisieren, fundierte Verwaltungsentscheidungen treffen und Verwaltungsaufgaben automatisieren, beispielsweise um sicherzustellen, dass die Benutzer:innen stets die geeigneten Apps installiert haben. Und die MDM-Lösung kann den Zustand wichtiger Sicherheitsfeatures abfragen, wie beispielsweise FileVault oder die integrierte Firewall.

Verwaltete Softwareupdates

Das IT-Team kann Benutzer:innen 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:innen und ihre Daten zu schützen. Aktualisieren Sie häufig, sobald Sie feststellen, dass Ihr Arbeitsablauf mit einer neuen Version von macOS kompatibel ist.

Ihre MDM-Lösung kann macOS Updates automatisch per Push auf registrierte Mac Computer übertragen. Registrierte Mac Computer können auch so konfiguriert werden, dass sie Updates und entsprechende Benachrichtigungen bis zu 90 Tage zurückstellen, falls wichtige Systeme nicht bereit dafür sind. Die Benutzer:innen 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 Aktualisierung das macOS Installationsprogramm oder MDM-Befehle zu verwenden.

Verwaltete zusätzliche Software

Organisationen müssen Benutzer:innen oft zusätzliche Apps zur Verfügung stellen, die über die ursprüngliche Software hinausgehen. Kritische Apps und Updates können von Ihrer MDM-Lösung automatisch verteilt werden. Oder Sie erlauben Ihren Benutzer:innen, 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 Apple Business Manager 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, müssen Benutzer:innen bei Apps, die Kernelerweiterungen erfordern, jetzt eine Einwilligung geben, damit sie geladen werden. Dies nennt man „Laden von Kernelerweiterungen nach Benutzergenehmigung“ und es kann von der MDM-Lösung verwaltet werden.

4. Verteilung von Inhalten

Nach der Registrierung können Administrator:innen auch die verwaltete Verteilung nutzen. Dadurch können Sie mit MDM oder Apple Configurator 2 alle Apps und Bücher, die Sie im Apple Business Manager Store gekauft haben, in jedem Land verwalten, in dem diese Apps verfügbar sind. Zur Aktivierung der verwalteten Verteilung müssen Sie zuerst Ihre MDM-Lösung mithilfe eines sicheren Tokens mit Ihrem Apple Business Manager Account verknüpfen. Sobald Sie mit Ihrem MDM-Server verbunden sind, können Sie Apple Business Manager Apps und Bücher zuweisen, selbst wenn der App Store auf dem betreffenden Gerät deaktiviert ist.

Es gibt zwei Arten von Inhalten, die an Benutzer:innen verteilt werden können: verwaltete Apps und verwaltete Bücher und Dokumente. Verwaltete Apps können per Fernzugriff über einen MDM-Server bereitgestellt und entfernt werden. Bei Aufhebung der MDM-Registrierung des Geräts durch die Benutzer:innen werden sie ebenfalls entfernt. Das Entfernen der App löscht auch alle mit der App verbundenen Daten. Verwaltete Bücher und Dokumente können automatisch auf die Geräte der Benutzer:innen gepusht werden. Sie können nur mit anderen verwalteten Apps geteilt oder über verwaltete Accounts per E-Mail verschickt werden. Verwaltete Dokumente können automatisch entfernt werden, aber verwaltete Bücher können nicht widerrufen oder neu zugewiesen werden, selbst wenn sie über den Apple Business Manager zugewiesen wurden.

Es gibt zwei Möglichkeiten, wie Inhalte an Benutzer:innen verteilt werden können:

Apps Geräten zuweisen. Mit Ihrer MDM-Lösung oder Apple Configurator 2 können Sie Apps direkt den Geräten zuweisen. Diese Methode spart mehrere Schritte bei der ersten Bereitstellung und macht sie deutlich einfacher und schneller. Gleichzeitig haben Sie aber die volle Kontrolle über verwaltete Geräte und Inhalte. Nachdem eine App einem Gerät zugewiesen wurde, wird die App per MDM auf das Gerät gepusht, ohne dass eine Einladung erforderlich ist. Alle Benutzer:innen dieses Geräts können auf die App zugreifen.

Apps und Bücher Benutzer:innen zuweisen. Alternativ können Sie Ihre MDM-Lösung nutzen, um Benutzer:innen per E-Mail oder Push-Benachrichtigung zum Download von Apps und Büchern einzuladen. Zum Annehmen der Einladung melden sich die Benutzer:innen mit einer persönlichen Apple ID auf ihren Geräten an. Die Apple ID wird bei Apple Business Manager unter vollständiger Wahrung des Datenschutzes registriert und ist für Administrator:innen nicht sichtbar. Sobald Benutzer:innen der Einladung zustimmen, werden sie mit Ihrem MDM-Server verbunden, damit sie zugewiesene Apps und Bücher empfangen können. Apps sind automatisch auf allen Geräten der Benutzer:innen zum Laden verfügbar, ohne zusätzlichen Aufwand oder zusätzliche Kosten.

Wenn Benutzer:innen oder Geräte die zugewiesenen Apps nicht mehr benötigen, können Sie die Zuweisung widerrufen und die Apps anderen Benutzer:innen oder Geräten zuweisen. Ihre Organisation bleibt so Eigentümer der gekauften Apps und behält die volle Kontrolle darüber. Bücher bleiben jedoch im Eigentum der Empfänger:innen, nachdem sie verteilt worden sind, und können nicht widerrufen oder neu zugewiesen werden.

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 Chrome oder Firefox. 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.

Gerätesicherheit

Apple Geräte sind von Grund auf sicher. Sobald die Geräte eingerichtet sind, können die Unternehmensdaten durch integrierte Sicherheitsfunktionen und zusätzliche Kontrollen, die über MDM ermöglicht werden, verwaltet und geschützt werden. Diese Aufgaben können von Ihrer IT übernommen werden. Gemeinsame, App-übergreifende Frameworks ermöglichen die Konfiguration und laufende Verwaltung von Einstellungen.

Weitere Infos zur Apple Plattformsicherheit:
support.apple.com/guide/security/welcome/web

Unternehmensdaten schützen. IT-Mitarbeiter:innen können Sicherheitsrichtlinien über MDM durchsetzen und überwachen. Wenn zum Beispiel ein Code über MDM auf macOS Geräten notwendig ist, wird der Datenschutz automatisch aktiviert und die Dateiverschlüsselung für das Gerät gewährleistet. Und mit MDM können WLAN und VPN konfiguriert und Zertifikate für eine zusätzliche Sicherheit bereitgestellt werden.

MDM-Lösungen ermöglichen eine fein abgestimmte Geräteverwaltung ohne Container. So bleiben Unternehmensdaten sicher. Und durch integrierte Sicherheitsfunktionen kann die IT Daten verschlüsseln, Geräte vor Malware schützen und Sicherheitseinstellungen durchsetzen, ohne Tools von anderen Anbietern zu benötigen.

Sperren, orten und löschen. Wenn ein Gerät verloren geht, müssen Unternehmensdaten nicht auch verloren gehen. Bei iOS, iPadOS und macOS Geräten kann die IT alle vertraulichen Daten per Fernzugriff sperren und löschen, um die Daten des Unternehmens zu schützen. Bei betreuten macOS Geräten kann die IT „Wo ist?" aktivieren, um den Standort eines Geräts zu sehen. Die IT hat außerdem die Tools, um Unternehmensapps zu verwalten, die sofort von einem Gerät entfernt werden können, ohne persönliche Daten zu löschen.

Apps. Durch ein gemeinsames Framework und ein kontrolliertes Ökosystem sind Apps auf Apple Plattformen von Anfang an sicher. Unsere Programme für Entwickler:innen verifizieren die Identität von Entwickler:innen, und Apps werden vom System geprüft, bevor sie in den App Store kommen. Apple stellt Entwickler:innen Frameworks für Funktionen zur Verfügung, wie Anmelden, App-Erweiterungen, Berechtigungen und Sandboxing, um ein noch höheres Maß an Sicherheit zu gewährleisten.

Modus „Verloren". Mit Ihrer MDM-Lösung können Sie ein betreutes Gerät per Fernzugriff in den Modus „Verloren" versetzen. Dadurch wird das Gerät gesperrt und es besteht die Möglichkeit, eine Nachricht mit einer Telefonnummer auf dem Sperrbildschirm anzuzeigen. Im Modus „Verloren" können betreute Geräte, die verloren gingen oder gestohlen wurden, geortet werden, da die MDM-Lösung per Fernzugriff den Standort abfragt, an dem sie zuletzt online waren. Für den Modus „Verloren" muss „Wo ist?" nicht aktiviert sein.

Aktivierungssperre. Bei Geräten mit macOS Catalina oder neuer können Sie eine MDM-Lösung verwenden, um die Aktivierungssperre einzuschalten, wenn „Wo ist?" auf einem betreuten Gerät von einem Benutzer aktiviert wird. Auf diese Weise kann Ihre Organisation von der Diebstahlschutzfunktion der Aktivierungssperre profitieren. Sie können das Feature aber dennoch umgehen, wenn zum Beispiel Benutzer:innen nicht in der Lage sind, sich mit ihrer Apple ID zu authentifizieren.

Supportoptionen

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

Eine bewährte Vorgehensweise ist, Benutzer:innen nicht völlig auf sich allein gestellt zu lassen und stattdessen einen gemeinsamen Ansatz für das Lösen von Problemen zu wählen. Ermutigen Sie Benutzer:innen dazu, sich an dem Prozess zu beteiligen, indem Sie ihnen ermöglichen, Probleme selbst zu untersuchen und zu beheben, bevor sie den Helpdesk anrufen.

Die gemeinsame Verantwortung für den Support reduziert Ausfallzeiten der Mitarbeiter:innen und senkt den Gesamtaufwand für Supportkosten und Personal. Für Organisationen, die mehr Support benötigen, bietet AppleCare zahlreiche Programme und Dienste, die interne Supportstrukturen für Mitarbeiter:innen 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:innen 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, iPadOS, macOS und macOS Server Implementierungen. Sie erhalten je nach gekaufter Supportstufe bis zu Rund-um-die-Uhr-Support und eine:n zugewiesene:n technische:n Accountmanager:in. Durch den direkten Kontakt zu Techniker:innen 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 Supportmitarbeiter:innen. Er umfasst auch eine Reihe von Werkzeugen für die Diagnose und Behebung bei Problemen mit Apple Hardware. So können große Organisationen 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 und iPadOS 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+ für Mac oder dem AppleCare Protection Plan auf drei Jahre ab Kaufdatum verlängern. Mitarbeiter:innen können den Apple Support bei Fragen zur Apple Hardware oder Software anrufen. Apple bietet zudem praktische Service-Optionen an, wenn Geräte repariert werden müssen. Außerdem sind im Leistungsumfang von AppleCare+ für Mac ausgewählte Reparaturen von Unfallschäden inbegriffen, für die jeweils eine Servicegebühr anfällt.

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

Zusammenfassung und Ressourcen

Wenn Ihr Unternehmen Mac Computer für eine Gruppe von Benutzer:innen oder innerhalb der gesamten Organisation implementieren möchte, haben Sie viele Optionen für die einfache Implementierung und Verwaltung der Geräte. Die Wahl der richtigen Strategien kann es den Mitarbeiter:innen Ihrer Organisation 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:
support.apple.com/guide/deployment/welcome/web

Apple Configurator – Benutzerhandbuch:
support.apple.com/guide/apple-configurator/welcome/ios

Weitere Infos zu Apple Business Manager:
support.apple.com/de-de/guide/apple-business-manager

Weitere Infos zu verwalteten Apple IDs für Unternehmen:
apple.com/de/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Weitere Infos zu Apple at Work:
apple.com/de/business

Weitere Infos zu Features für die IT:
apple.com/de/business/it

Weitere Infos zur Apple Plattformsicherheit:
apple.com/security

Weitere Infos zu verfügbaren AppleCare Programmen:
apple.com/de/support/professional

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

Kontakt zu Apple Professional Services:
consultingservices@apple.com

Betasoftware testen, auf Testpläne zugreifen und Feedback geben:
appleseed.apple.com/sp/welcome