ÜBERBLICK ÜBER MAC, IPAD, IPHONE UND APPLE TV GERÄTE

EINFÜHRUNG IN DIE

Sicherheit von Apple Geräten

Ein gut geplanter Cyberangriff oder das versehentliche Herunterladen von Schadsoftware können schlagartig die gesamte Geschäftstätigkeit einer Organisation zum Erliegen bringen. Angesichts des zunehmend raffinierteren Vorgehens von Hackern machen sich immer mehr Organisationen Sorgen um ihr Endergebnis sowie ihre Kunden-, Mitarbeiter- bzw. Schülerdaten und müssen sichergehen Sicherheit zu gewährleisten.

Tatsächlich sind Sicherheitsfragen ebenso wie andere IT-Fragen auch für Apple Geräte relevant.

Apple hat in der Vergangenheit enorm in die Sicherheitsmerkmale der Geräte investiert und sich schnell als führende Marke in puncto Gerätesicherheit und Datenschutz etabliert. Dennoch ist kein Betriebssystem gegen alle Sicherheitsbedrohungen immun.

Administratoren müssen deshalb nicht nur umgehend auf Sicherheitsprobleme reagieren, sondern versuchen, sie proaktiv zu verhindern.

Dieser Leitfaden richtet sich an Administratoren und IT-Verantwortliche, die sich ernsthaft mit der Sicherheit von Apple Geräten in ihrer Organisation beschäftigen. Er bietet darüber hinaus grundlegende Informationen für Einsteiger und dient Experten für die Verwaltung von Apple Geräten als Auffrischung ihrer bereits vorhandenen Kenntnisse.

Einführung in die Sicherheit von Apple Geräten

Die grundlegenden Bestandteile

Um die Hardware und die Daten Ihrer Organisation optimal zu schützen, müssen verschiedene Maßnahmen ergriffen werden und nahtlos ineinandergreifen. Diese Maßnahmen bilden sechs grundlegende Bestandteile:

Native Sicherheit von Apple Geräten

In macOS, iOS und tvOS integrierte Sicherheitsfeatures

Page 4

Schutz auf Geräteebene

Schutz der physischen Geräte und ihre Benutzer

Page 6

Verschlüsselung von Daten

Grundlagen der Verschlüsselung ruhender und übertragener Daten

Page 8

Überwachung der Richtlinienkonformität

Überwachung von Geräten zur Ermittlung notwendiger Aktualisierungen

Page 11

Anwendungssicherheit und Patching

Aktualität der Software

Page 12

Sichere Bereitstellung

Bereitstellung der Geräte unter Einhaltung strengster Sicherheitsmaßnahmen

Page 14

Teil 1: Native Sicherheit von Apple Geräten

Schöpfen Sie das Potenzial der integrierten Sicherheitsfeatures bei der Geräteverwaltung umfassend aus

macOS (Betriebssystem auf Mac Computern), iOS (Betriebssystem auf iPad und iPhone Geräten) und tvOS (Betriebssystem auf Apple TV Geräten) verfügen über umfangreiche integrierte Sicherheitsfeatures, die zahlreiche Vorteile bieten:

- Betriebssysteme von Apple basieren auf Unix, einer gut erforschten und entwickelten Plattform mit ausgezeichneter Stabilität
- Leistungsstarkes Sicherheits-Framework der Betriebssysteme
- Gerätesicherheit durch Sperren und Orten von Geräten
- Möglichkeit zur Implementierung und Konfiguration von Sicherheitskontrollmechanismen mithilfe einer Lösung für das Mobile Device Management (MDM)

Mit einer MDM Lösung können diese integrierten Sicherheitsfeatures konfiguriert und auf einer großen Anzahl von Geräten gleichzeitig bereitgestellt (und durchgesetzt) werden. Auf diese Weise können Sie nicht nur für die Sicherheit einzelner Mac Computer, sondern von mehreren tausend Geräten sorgen. Darüber hinaus stehen Ihnen mit einer MDM Lösung wesentlich umfangreichere Sicherheitsfeatures zur Verfügung, wie z. B. das Sperren von Geräten, die verloren wurden oder die Organisation verlassen haben, und das Löschen der darauf gespeicherten Daten.

Sicherheitsfeatures im Detail

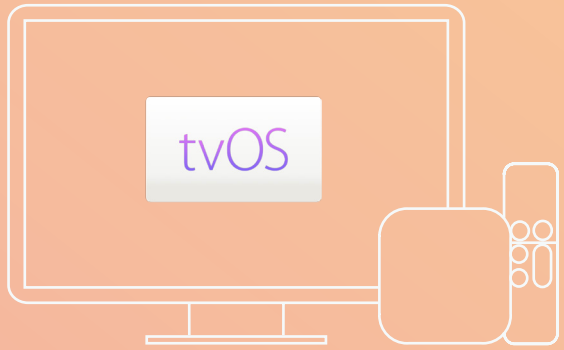
Native Sicherheitsfeatures in macOS, iOS und tvOS

macOS Features

- Software-Updates
- Systemintegritätsschutz
- Gatekeeper
- App Store
- FileVault Verschlüsselung
- XProtect
- App-Sandboxing
- Datenschutzeinstellungen

iOS Features

- Software Updates
- Secure System
- App Store
- Touch ID
- Hardware Encryption
- App Sandboxing
- Privacy
- Supervision
- Remote device finder for lost devices



tvOS Features

- Software-Updates direkt von Apple
- Geprüfte und sichere Apps im App Store
- Betreuung (mittels MDM)
- App-Einschränkungen
- Einstellungen und Passwörter für AirPlay
- Standardeinstellungen für Banner/Bildschirme

Teil 2: Schutz auf Geräteebene

Orten und schützen Sie Geräte ebenso wie ihre Benutzer

Das Sicherheits-Framework einer Organisation und die Daten der Endbenutzer können am einfachsten umgangen werden, indem man sich Zugang zu einem einzelnen Gerät verschafft. Ganz gleich, ob es sich bei den Benutzern Ihrer Organisation um Schüler, Lehrkräfte, Pflegepersonal, externe Arbeitnehmer, Verkäufer oder häufig reisende Mitarbeiter handelt – ihre Geräte könnten sich zu jedem Zeitpunkt an unzähligen Orten befinden.

Verlorene oder gestohlene Geräte

Ein verlorenes oder gestohlenes iPad, iPhone oder Mac Gerät bedeutet nicht nur einen finanziellen Verlust: Es stellt auch ein enormes Sicherheitsrisiko dar. Der dadurch entstehende Schaden ist kaum absehbar: Mit einem verlorenen Laptop erhält ein Dieb nicht nur Zugang zu den privaten Daten des Benutzers, sondern möglicherweise auch zur Datenbank der gesamten Organisation. Ein ehemaliger Mitarbeiter, der noch immer seinen Arbeitslaptop besitzt, kann vertrauliche Informationen öffentlich machen oder an die Konkurrenz weitergeben. Auch die Einschleusung von Schadsoftware von einer externen Quelle ist denkbar.

Geräte gehen verloren oder werden gestohlen. Unfälle und kurze Momente der Unachtsamkeit können jederzeit vorkommen. Deshalb geht es beim Treffen der nötigen Vorkehrungen nicht um die Frage ob, sondern lediglich wann jemand sein Gerät aus den Augen verliert.

Darüber hinaus erfordern viele Geräte – insbesondere solche, die an Schüler und Patienten ausgegeben oder die von mehreren Benutzern gemeinsam genutzt werden – zusätzliche Schutzmechanismen gegen missbräuchliche Verwendung, versehentliche Offenlegung persönlicher Daten oder Wiedergabe anstößiger Inhalte.

So legen Sie Sicherheitsmechanismen und Einschränkungen manuell fest:

Mac

- Geben Sie auf jedem Gerät die Verwendung von Passwörtern vor.
- Aktivieren Sie in den Systemeinstellungen unter „iCloud“ die Option „Meinen Mac suchen“.
- Sorgen Sie dafür, dass sich alle Benutzer mit einem Passwort, das sie sich merken, bei iCloud anmelden.
- Verfolgen Sie alle Mac Computer anhand der Seriennummern.
- Melden Sie ein verlorenes oder gestohlenes Gerät auf elektronischem Weg an Apple.
- Aktivieren Sie auf jedem Gerät die Kindersicherung, um den Zugriff auf bestimmte Websites zu blockieren (Betrifft nur den Safari Browser).

iPad and iPhone

- Geben Sie auf jedem Gerät die Verwendung von Passwörtern vor.
- Aktivieren Sie in den Systemeinstellungen unter „iCloud“ die Option „Mein iPhone suchen“.
- Sorgen Sie dafür, dass sich alle Benutzer mit einem Passwort, das sie sich merken, bei iCloud anmelden.
- Melden Sie ein verlorenes oder gestohlenes Gerät auf elektronischem Weg an Apple.
- Aktivieren Sie die Kindersicherung, indem Sie auf jedem Gerät mehrere Konten anlegen.

Apple TV

- Geben Sie auf jedem Apple TV Gerät die Verwendung von Passwörtern vor.
- Schränken Sie die Nutzungsmöglichkeiten ein:
  - Navigieren Sie im Hauptmenü zu „Einstellungen“ > „Allgemein“ > „Einschränkungen“.
  - Aktivieren Sie die Einschränkungen.
  - Geben Sie bei Aufforderung einen vierstelligen Code ein.
  - Geben Sie den vierstelligen Code zum Bestätigen erneut ein und wählen Sie „OK“.
  - Merken Sie sich den Code.
  - Wiederholen Sie den Vorgang für alle anderen Apple TV Geräte.

Schutz auf Geräteebene

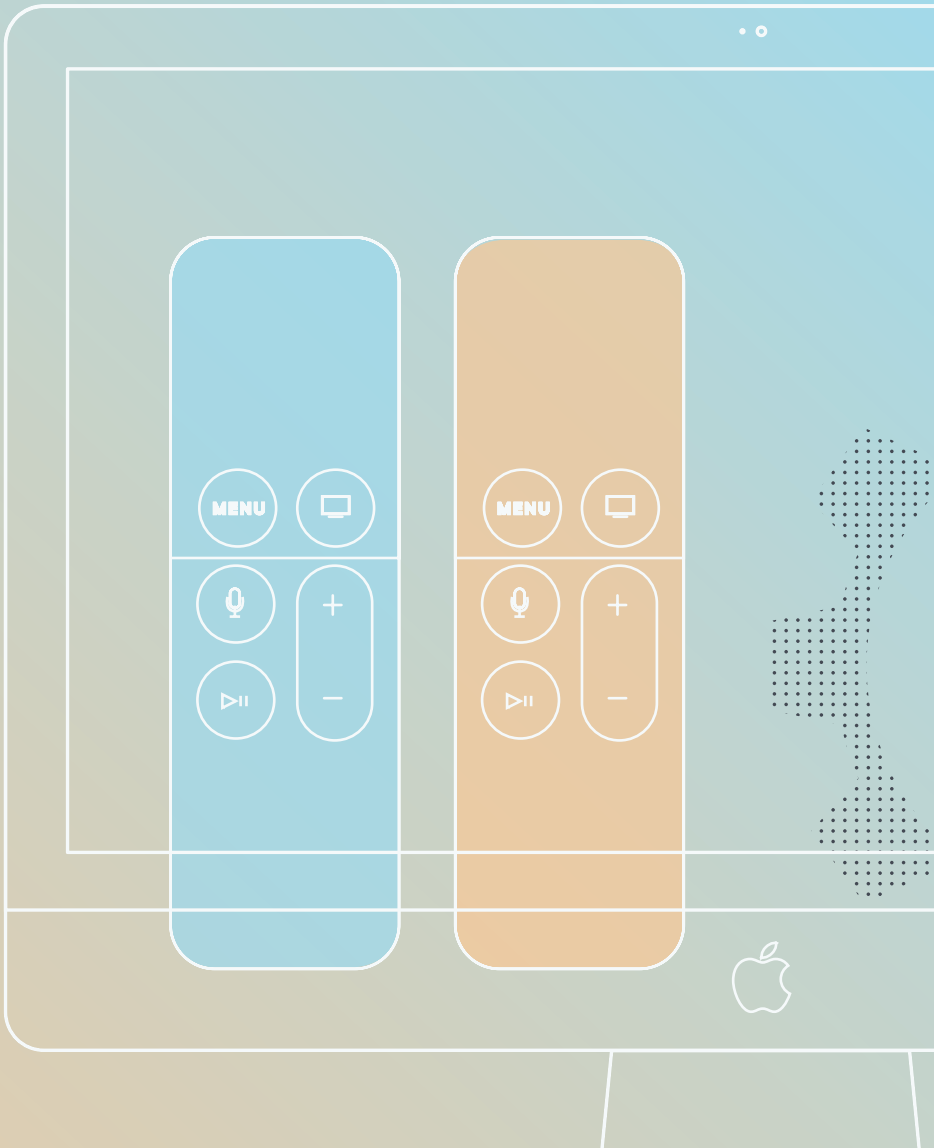
Schränken Sie die Verwendung von AirPlay auf Apple TV Geräten ein:

- Navigieren Sie im Hauptmenü zu „Einstellungen“ > „AirPlay“
- Aktivieren bzw. deaktivieren Sie AirPlay.
- Wählen Sie die gewünschte Option aus:
  - Allen
  - Allen im selben Netzwerk
- Wiederholen Sie den Vorgang für alle anderen Apple TV Geräte.

So legen Sie Sicherheitsmechanismen und Einschränkungen für mehrere Geräte gleichzeitig mit einer MDM Lösung (z. B. Jamf) fest:

Mac, iPad, iPhone und Apple TV Geräte:

- Konfigurieren Sie alle Einschränkungen und Sicherheitsfeatures bei der erstmaligen Verwendung oder Geräteeinrichtung mithilfe von Konfigurationsprofilen oder Richtlinien.
- Sperren Sie ein verlorenes oder missbräuchlich verwendetes Gerät aus der Ferne.
- Löschen Sie die Daten auf einem verlorenen oder missbräuchlich verwendeten Gerät aus der Ferne.
- Ermöglichen Sie die gemeinsame Verwendung von Geräten durch mehrere Benutzer, wobei jeder Benutzer eigene Anmeldedaten erhält und die Geräteeinstellung individuell anpassen kann oder alle Benutzerdaten nach jedem Gebrauch gelöscht werden, z. B. bei Geräten für Patienten.



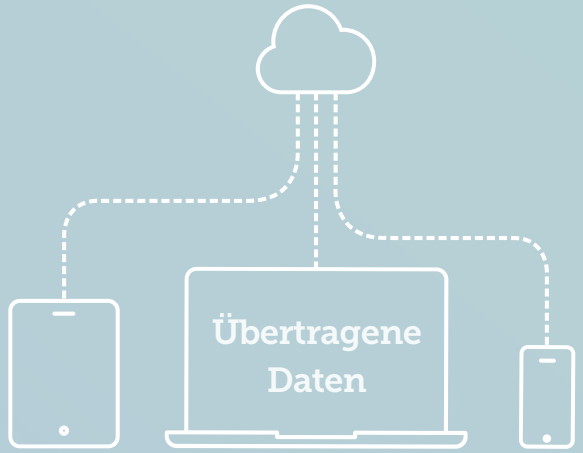
Teil 3: Verschlüsselung von Daten

Machen Sie sich mit den Grundlagen der Sicherheit ruhender und übertragener Daten vertraut

Ganz gleich, ob es darum geht, Schülerdaten an einer Schule, Patientenakten im Krankenhaus oder geistiges Eigentum in einem Unternehmen zu schützen, die Verschlüsselung von Daten ist für Organisationen keine Option mehr, sondern eine Pflicht. Für Unternehmen hat es sich bewährt, grundsätzlich alle Daten auf jedem Gerät zu verschlüsseln.

In diesem Zusammenhang wird zwischen zwei Arten von Daten unterschieden:

Verschlüsselung auf Festplatten- oder Geräteebene.



Informationen die drahtlos von einem Ort zum anderen übermittelt werden.

Verschlüsselung von Daten

Ruhende Daten:

Verschlüsselung auf Festplatten- oder Geräteebene.

- macOS verfügt bereits über eine integrierte Festplattenverschlüsselung: FileVault. Sie benötigen daher keine zusätzliche Software, um Daten auf der Festplatte eines Mac Computers zu verschlüsseln.
- FileVault ist nach FIPS 140-2 zertifiziert. Das bedeutet, dass das Verschlüsselungssystem von Apple die strengsten Verschlüsselungsvorgaben der US-Regierung erfüllt.
- FileVault kann manuell, also direkt von den Benutzern auf ihren jeweiligen Geräten, oder aus der Ferne von der IT-Abteilung (mithilfe von Jamf) auf Hunderten oder sogar Tausenden von Geräten gleichzeitig aktiviert werden.
- Bei Verwendung von Jamf werden die Verschlüsselungsschlüssel zentral gespeichert, sodass sie ggf. auch dann auf die Daten zugreifen können, wenn der Verantwortliche die Organisation verlässt oder das Passwort vergisst.

So aktivieren Sie FileVault manuell:

1. Navigieren Sie in den Systemeinstellungen zu „Sicherheit“ > „FileVault“.
2. Aktivieren Sie die Option mithilfe der Umschaltfläche.
3. Wiederholen Sie den Vorgang für alle anderen Geräte.

Um FileVault auf einer großen Anzahl von Geräten innerhalb einer Organisation zu aktivieren, sollten Sie die Verwendung einer MDM Lösung in Erwägung ziehen. Mit dieser können Sie die Verschlüsselung in einem automatisierten Workflow bereitstellen und durchsetzen.

Stellen Sie zum Beispiel ein Konfigurationsprofil oder eine Richtlinie bereit, mit der FileVault auf den ausgewählten Geräten aktiviert wird. Die Verschlüsselungsschlüssel können dann von der IT-Abteilung abgerufen werden, sollte ein Gerät irgendwann entschlüsselt werden müssen.

1. Erstellen Sie in Jamf ein Konfigurationsprofil einfach durch Auswahl der gewünschten Optionen.
2. Stellen Sie es auf beliebig vielen Geräten bereit.
3. Es gibt keinen Schritt 3.

In Jamf können Sie darüber hinaus festlegen, dass Wiederherstellungsschlüssel automatisch an Ihre IT-Abteilung gesendet werden – selbst wenn FileVault vom Benutzer manuell aktiviert wird. Die IT-Abteilung kann den Schlüssel dann in der Verwaltungslösung hinterlegen.

Und was ist mit iPads oder iPhones?

Auf iOS Geräten ist die Verschlüsselung sogar noch einfacher. iOS Geräte werden automatisch verschlüsselt, sobald ein Code festgelegt wird. Auch dieser Vorgang kann sowohl manuell auf einzelnen Geräten als auch automatisiert mithilfe von Jamf auf mehreren Geräten gleichzeitig durchgeführt werden. Sie können zudem Kriterien für die Code-Erstellung, z. B. eine bestimmte Länge oder Komplexität, vorgeben.

Verschlüsselung von Daten

Übertragene Daten:

Zum Schutz von Daten während der Übertragung von einem Gerät auf ein anderes kann ein Virtual Private Network, kurz VPN, eingerichtet werden.

Mitarbeiter, die viel reisen oder außerhalb des Büros tätig sind, sollten sich stets über ein VPN mit dem Netzwerk Ihrer Organisation verbinden. Diese Vorgehensweise hat sich bewährt, da dabei eine sichere Verbindung zu Ihrem vertrauenswürdigen Unternehmensnetzwerk aufgebaut wird. Somit ist eine End-to-End-Verschlüsselung der übertragenen Daten sichergestellt.

Anforderungen

- Eine sichere Netzwerkverbindung
- Ein VPN-Server

Sowohl macOS als auch iOS Geräte verfügen über integrierte VPN-Clients, die Verbindungen zu einer Reihe renommierter VPN-Dienstanbieter unterstützen.

Vorgehensweise

So stellen Sie manuell eine Verbindung zu einem VPN her:

Nachdem Sie einen VPN-Anbieter eingerichtet haben:

1. Navigieren Sie zu „Einstellungen“ > „Netzwerk“.
2. Geben Sie auf dem Gerät die Adresse des VPN-Servers ein.
3. Wählen Sie sie in Ihren Netzwerkoptionen aus.
4. Wiederholen Sie den Vorgang für alle anderen Geräte.

So stellen Sie auf mehreren Geräte gleichzeitig eine Verbindung zu einem VPN her:

Nachdem Sie einen VPN-Anbieter eingerichtet haben:

1. Erstellen Sie in einer MDM-Lösung (z. B. Jamf) ein Konfigurationsprofil für iOS und/oder Mac Geräte.
2. Stellen Sie die Konfigurationsprofile auf beliebig vielen Geräten bereit.
3. Sie haben es sicher schon erraten: Es gibt keinen Schritt 3.

Wie kann ich sicher sein, dass die Verschlüsselung lückenlos ist?

Eine hervorragende Möglichkeit, für Sicherheit und eine durchgehende Verschlüsselung zu sorgen, ist eine in der Cloud gehostete MDM Lösung. Mit einer bewährten Lösung wie Jamf Cloud können Sie sicher sein, dass Ihr Server und Ihre Daten geschützt sind und dass Updates und Sicherheitspatches umgehend verfügbar sind.

Teil 4: Überwachung der Richtlinienkonformität

Stellen Sie auf allen Geräten Protokolle und Kontrollmechanismen bereit

Ein Sicherheitssystem ist nur so wirksam wie seine schwächste Komponente. Für optimalen Schutz müssen Administratoren deshalb die Geräte ihrer Organisation durchgehend überwachen, um sicherzustellen, dass jedes Gerät auf dem neusten Stand gehalten wird, die neusten Patches erhält und mit den richtigen Einstellungen für die Verschlüsselung konfiguriert ist.

So überwachen Sie die Richtlinienkonformität manuell:

Um den Schutz und die Sicherheit aller Geräte in Ihrer Organisation zu gewährleisten, müssen Sie jedes Gerät fortwährend überprüfen.

1. Nehmen Sie jedes einzelne Gerät zur Hand.
2. Überprüfen Sie auf jedem Gerät, dass:
   - die neusten Software-Updates installiert sind,
   - die Verschlüsselung aktiviert ist,
   - keine Schadsoftware und kein Virus eingeschleust wurde.
3. Und weil immer nur das neuste Update den besten Schutz bietet, müssen Sie diesen Vorgang immer wieder aufs Neue durchführen.
4. Und ständig wiederholen.
5. Dies erfordert fortwährende Achtsamkeit, großes Engagement und Kooperation seitens der Endbenutzer.

So überwachen Sie die Richtlinienkonformität mithilfe von Jamf:

Um den Schutz und die Sicherheit aller Geräte in Ihrer Organisation zu gewährleisten, nutzen Sie einfach die Funktionen für den Gerätebestand in Jamf:

1. Zeigen Sie Informationen zu allen Geräten gleichzeitig und in Echtzeit an.
2. Stellen Sie auf jedem nicht ordnungsgemäß geschützten Gerät Updates und Sicherheitseinstellungen bereit.
3. Richtig: Es gibt keinen Schritt 3.

Wenn Administratoren den Status jedes Geräts anzeigen können, wissen sie genau, auf welchem Gerät Updates bereitgestellt und Sicherheitsfeatures konfiguriert werden müssen. Darüber hinaus können sie dynamische Gruppen nach Abteilung, Berechtigungen, Geräten oder sonstigen für ihre jeweilige Organisation geeigneten Kategorien erstellen, um Updates auf lediglich bestimmten oder allen Geräten bereitzustellen.

Teil 5: Anwendungssicherheit und Patching

Halten Sie die Software auf allen Geräten auf dem neusten Stand und gewährleisten Sie die Anwendungssicherheit

Anwendungssicherheit:
Sie müssen unbedingt sicherstellen, dass Ihre Anwendungen weder Schadsoftware noch schädlichen Code enthalten. Wenn Ihre Anwendungsquellen nicht vertrauenswürdig sind, steht die Sicherheit auf dem Spiel.

Apple hat die folgenden Features entwickelt, um das Herunterladen und Verwenden von Apps so sicher wie möglich zu machen:

- Durch das **Sandboxing-Modell** wird jede App in einem eigenen Bereich ausgeführt und die Kommunikation mit anderen Apps verhindert. Damit Apps gemeinsam genutzte Daten in anderen Apps lesen und schreiben können, ist die explizite Genehmigung durch den Benutzer oder den Administrator notwendig.
- Im **App Store** verfügbare Apps wurden alle hinsichtlich ihrer Sicherheit überprüft. Der App Store ist deshalb die einzige Möglichkeit, Apps auf ein iOS Gerät zu laden. Dies trägt wesentlich zur Gerätesicherheit bei. Auch auf Mac Geräten kann festgelegt werden, dass Apps nur aus dem App Store bezogen werden können. So können Administratoren die Sicherheit der Geräte umfassend kontrollieren.
- Das **Gatekeeper Feature** für macOS kann entweder vom Benutzer auf dem eigenen Gerät aktiviert oder von Administratoren mithilfe einer MDM Lösung wie Jamf auf allen Geräten gleichzeitig konfiguriert werden. Mit Gatekeeper stehen für das Herunterladen von Apps drei Optionen zur Verfügung
  - Mac App Store
  - Mac App Store und bestimmte Entwickler
  - Überall

Als bewährte Vorgehensweise sollten Sie die Option „Mac App Store und bestimmte Entwickler“ auswählen, insbesondere wenn Sie eigene Anwendungen erstellen oder App-Pakete neu erstellen. Signieren Sie diese Apps selbst, damit sie von Gatekeeper als vertrauenswürdig eingestuft werden.

Auf Mac Computern kann als Anwendungsquelle zwar auch „Überall“ ausgewählt werden, allerdings sollten Sie bedenken, dass die Sicherheit der Daten während der Übertragung nur dann gewährleistet ist, wenn Sie die Herkunft der App kennen und die App von einem vertrauenswürdigen Entwickler signiert wurde.

So konfigurieren Sie die Optionen für Gatekeeper manuell:

1. Navigieren Sie zu: „Einstellungen“ > „Sicherheit“ > „Allgemein“.
2. Wählen Sie eine der drei verfügbaren Optionen aus.
3. Wiederholen Sie diesen Vorgang für jedes Gerät in Ihrer Organisation.

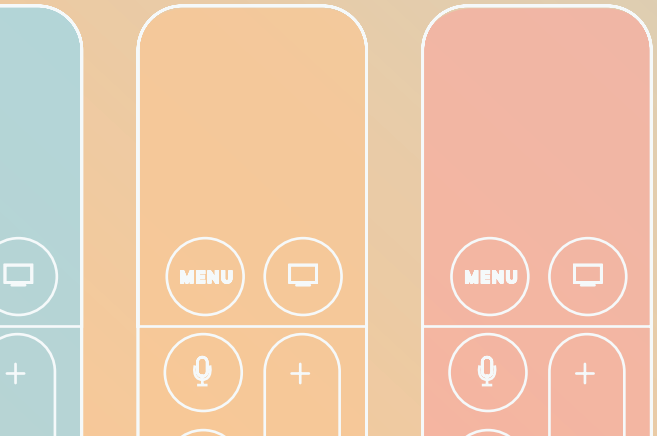
So konfigurieren Sie die Optionen für Gatekeeper mithilfe von Jamf:

Folgen Sie dem üblichen Muster. Konfigurieren Sie ein Konfigurationsprofil und stellen Sie es auf allen Geräten gleichzeitig bereit. Fertig.

Anwendungssicherheit und Patching

Patching:
Jede Software enthält Fehler, denn Software wird von Menschen entwickelt, die Fehler machen. Das lässt sich nicht verhindern.

Deshalb ist es für Organisationen wichtig eine Strategie zu entwickeln, mit der Fehlerkorrekturen schnellstmöglich implementiert werden – insbesondere, wenn es sich um Fehler im Zusammenhang mit Sicherheitslücken handelt.



Optionen für die manuelle Verwaltung von Patches:

- Weisen Sie Ihre Benutzer an, Updates selbst durchzuführen, sobald sie eine Mitteilung zur Verfügbarkeit eines Updates erhalten.
- Sammeln Sie alle Geräte ein, wenn für eine App ein neuer Softwarepatch veröffentlicht wird, und laden Sie ihn manuell auf jedes Gerät herunter.
- Erfassen Sie im Zuge Ihrer manuellen Überprüfung der Richtlinienkonformität alle Geräte, auf denen noch Softwarepatches installiert werden müssen.

All diese Möglichkeiten sind anfällig für Fehler. Ganz gleich, wie engagiert ein Endbenutzer in dieser Hinsicht auch sein mag, mangelndes technisches Wissen oder ein voller Terminplan können dazu führen, dass der Endbenutzer überhaupt nicht bemerkt, dass ein Update ansteht. Das Einsammeln aller Geräte, wenn für eine App ein neuer Softwarepatch veröffentlicht wird, ist enorm zeitaufwändig. Zusätzlich führt die manuelle Erfassung aller zu patchenden Geräte im Rahmen einer manuellen Überprüfung der Richtlinienkonformität dazu dass Ihre Organisation so lange anfällig für Angriffe oder Schadsoftware ist, bis die Konformität für die betroffenen Geräte widerhergestellt wurde.

Optionen für die Verwaltung von Patches mithilfe von Patches:

- Jamf erhält alle Mitteilungen über automatische Updates und Softwarepatches zusammen mit den nötigen Tools, um diese Patches auf allen Geräten Ihrer Organisation bereitzustellen. Dadurch werden Sie in puncto Softwarepatches nie wieder kalt erwischt.
- Sie können Ihren Benutzern darüber hinaus die Durchführung von Updates mithilfe des Self Service App-Katalogs in Jamf vereinfachen. Dann werden Ihre Benutzer aufgefordert, ein neu verfügbares Update zu installieren, ehe sie die betreffende App weiterverwenden können.
- Alternativ können Sie die Durchführung von Updates durch die Benutzer verhindern und stattdessen Softwarepatches mithilfe von Richtlinien auf Geräten in einer dynamischen Gruppe oder auf allen Geräten bereitstellen.

Teil 6: Sichere Bereitstellung

Sorgen Sie mit Jamf und der Apple Geräteregistrierung für eine sichere Bereitstellung von Geräten und Software

Der erste Schritt für eine sichere Bereitstellung für alle Ihre Geräte ist die Registrierung mithilfe des kostenlosen Programms zur Geräteregistrierung von Apple.

Im Rahmen der Geräteregistrierung registrieren Sie alle Geräte Ihrer Organisation bei Apple und legen fest, dass alle diese Geräte mit der MDM Lösung Ihrer Organisation verwaltet werden sollen. Sobald ein Gerät diesem Programm zum ersten Mal hinzugefügt wird, wird es automatisch in der MDM Lösung Ihrer Organisation registriert. Sie können dann nicht nur die Sicherheitsmechanismen und Updates auf diesem Gerät wesentlich schneller und umfassender konfigurieren, sondern auch alle von Ihnen erstellen Konfigurationsprofile darauf bereitstellen. Dadurch sparen Sie nicht nur Zeit, sondern sorgen auch für einen optimalen Schutz und können sicher sein, alle Geräte zu erfassen.

jamf

Ihre Vorteile mit Jamf:

Vollautomatische Geräteregistrierung

Skalierbare Bereitstellung

Sichere Konfigurationen

Für Mac, iPad, iPhone und Apple TV Geräte

Mit der Sicherheit von Geräten und Daten ist nicht zu spaßen.

Organisationen können einem potenziellen Cyberangriff oder Diebstahl einen Riegel vorschieben, indem sie sich für Apple Geräte und damit für ein Höchstmaß an Sicherheit entscheiden. Mit Jamf können Sie sich die integrierten Sicherheitsfeatures wesentlich einfacher, schneller und umfassender zunutze machen als mit manuellen Sicherheitsverfahren.

jamf

Tappen Sie nicht länger im Dunkeln und beugen Sie böse Überraschungen wirksam vor. Ergreifen Sie Maßnahmen, um die Geräte und Daten Ihrer Organisation ebenso wie die Privatsphäre Ihrer Benutzer zu schützen.

Sorgen Sie für den bestmöglichen Schutz Ihrer Organisation und laden Sie eine kostenlose Testversion von Jamf herunter oder kontaktieren Sie einen Kundenbetreuer bei Jamf, um mehr zu erfahren.

Produkt testen **Kontakt**

Gerne können Sie sich auch an einen autorisierten Händler für Apple Geräte Ihrer Wahl wenden, um Jamf zu testen.