



Moderne Verwaltung

Die Zukunft von MDM

Die besten IT-Manager*innen kennen ihre Technik in- und auswendig. Sie wissen, dass die effektivste Technologie erst nach sorgfältiger Abwägung ausgewählt wird, was die Mitarbeiter*innen eines Unternehmens und seine individuellen Geschäftsziele unterstützt. Außerdem wissen sie, dass sie zwar den heutigen Arbeitsplatz unterstützen, aber auch bereit sein müssen, sich an die veränderten Anforderungen der Zukunft anzupassen. Das bedeutet, dass wir hybrides Arbeiten durch moderne Geräteverwaltungs-Praktiken, die den Mitarbeiter*innen ein sicheres und nahtloses Geräteerlebnis von überall aus ermöglichen, begrüßen und fördern müssen.

In einer Apple Umgebung rennt der Einfallsreichtum voraus, wobei Apple selbst die Führung übernimmt. Sie setzen ihre Innovationen fort, um den Anforderungen des Unternehmens gerecht zu werden. Mit dem Tempo Schritt zu halten, bedeutet, die Herausforderung zu meistern, eine mobile Belegschaft zu unterstützen und die Anforderungen der Benutzer*innen mit der Geschwindigkeit von Apple zu erfüllen.

Studien zeigen, dass flexible Unternehmen niedrigere Betriebskosten haben, die besten Talente anziehen und halten und einen Anstieg der Mitarbeiterproduktivität verzeichnen, wenn sie zu hybriden oder dezentralen Verfahren übergehen.

MDM-Anbieter*innen wie Jamf, die an der Schnittstelle zwischen Apple und dem Unternehmen angesiedelt sind, bemühen sich, die Innovationen von Apple zu nutzen und sie auf Unternehmensebene zu verbreiten und zu maximieren. Daher muss sichergestellt werden, dass die Strategien die künftigen Bedürfnisse widerspiegeln.

„Die besten
Erfahrungen von
heute sind die
Erwartungen von
morgen“

- Fletcher Previn,
CIO bei Cisco

Quelle: [Mac im Unternehmen:
Die Zukunft der Arbeit
mit der Wahlfreiheit der
Mitarbeiter*innen gestalten](#)



Was ist moderne Verwaltung?

Moderne Verwaltung kombiniert die Verwaltung und Sicherheit von Geräten, Benutzer*innen, Betriebssystemen und Apps in der Cloud. Moderne Verwaltung geht weit über das traditionelle Mobile Device Management (Mobilgeräteverwaltung, MDM) hinaus und kann als die nächste Evolutionsstufe der Endpoint-Verwaltung und -sicherheit angesehen werden. Dieser Ansatz bietet eine ganzheitliche Perspektive durch die Integration dieser Elemente, was zu einer verbesserten Sicherheit, Verwaltung und Situationskenntnis für IT-Abteilungen führt und ein reaktionsschnelleres Handeln ermöglicht.

Kurz gesagt: Die Einführung moderner Verwaltungspraktiken mit Apple bedeutet, dass die Mitarbeiter*innen eine sichere und nahtlose Geräteerfahrung haben, egal wo sie arbeiten. Das bedeutet, dass die IT-Abteilung über die nötigen Werkzeuge und Systeme verfügt, um die Anforderungen der modernen Arbeitswelt zu erfüllen.

Diese nächste Entwicklung sollte Unternehmen dazu veranlassen, über ihre Apple Umgebung nachzudenken und sich die Frage zu stellen:

- Haben wir eine Strategie, die eine moderne Art der Verwaltung und Sicherung von Geräten widerspiegelt?
- Welche Vorteile bringt die Einführung einer modernen Verwaltung?
- Was verlieren wir, wenn wir nicht mithalten?

Eine Geschichte des traditionellen Apple Management

IT-Administrator*innen haben sich jahrelang an die traditionelle Verwaltung gehalten, die bis vor kurzem für die Mitarbeiter*innen sinnvoll war. Die herkömmliche Verwaltung basiert auf einem gerätezentrierten Modell, bei dem unternehmenseigene Geräte den Mitarbeiter*innen zugewiesen werden und nur diese autorisierten Geräte für wichtige Apps und Dienste auf das firmeneigene Netzwerk zugreifen können. In der dynamischen Arbeitswelt von heute wird dieser Ansatz den Bedürfnissen der Mitarbeiter*innen jedoch nicht gerecht.

Um die Entwicklung von Apple bei der Bewältigung dieser Herausforderungen besser zu verstehen, sollten wir einen Blick auf die Geschichte der Verwaltung von Apple Geräten werfen.

Vor dem Mobile Device Management (Mobilgeräteverwaltung, MDM): die Binärdatei

Bevor Apple 2010 sein MDM-Protokoll veröffentlichte, war das einzige Apple Gerät, das Unternehmen verwalteten, macOS. Zum Zeitpunkt der Registrierung würden diese verwalteten Macs einige lokale Binärdateien erhalten, diese lokalen Binärdateien hätten Root-Rechte und wären in der Lage, Daten über den Mac abzurufen und nach einem festgelegten Zeitplan an einen Verwaltungsserver zu senden. Sie können dem lokalen Client auch anweisen, programmatische Maßnahmen zu ergreifen, indem sie Pakete herunterladen und lokale Skripte ausführen. **Dies wurde als forced pull-Geräteverwaltung bezeichnet.**

Es lässt sich nicht leugnen, dass die Verwaltung von macOS Geräten in dieser Zeit einen enormen Aufwand an IT-Ressourcen erforderte.



Frühes MDM: Fokus auf Geräte

Dann kam das iPhone auf den Plan und veränderte den MDM-Stil. Ein Agent/eine Agentin mit Root-Zugriff, der regelmäßig einen Verwaltungsserver kontaktiert, war verschwunden. MDM erforderte Push-Benachrichtigungen.

Herkömmliches MDM beruht darauf, dass ein Gerät eine dauerhafte Verbindung zu Apple und einem Verwaltungsserver unterhält und Apple bittet, ein verwaltetes Gerät „nach Hause zu telefonieren“, um eine Einstellung zu erhalten, einen Befehl oder eine Abfrage zu empfangen oder eine App zu installieren.

Hier ist ein Beispiel dafür, wie das aussehen könnte:

1. Der Befehl könnte lauten :
„Aktualisieren Sie Ihr Betriebssystem“
2. Die nächste Frage könnte dann lauten :
„Was ist Ihr aktuelles Betriebssystem?“
3. Ein Administrator/eine Administratorin könnte dann noch einmal nachfragen, um sicherzustellen, dass der Befehl korrekt ausgeführt wurde:
„Wie sieht es jetzt aus?“

...kein Update? Ich schätze, Sie werden morgen wieder nachsehen.

Beim herkömmlichen MDM erhalten Administrator*innen Bestätigungen, wenn Befehle empfangen oder ausgeführt wurden, und sie können eine Vielzahl von Informationen vom Gerät anfordern und erhalten. **Aber die Verwaltung muss fragen, und zwar wiederholt.** Manchmal bedeutet das, dass man eine Menge doppelter Informationen zurückbekommt. Bei Befehlen, die komplex sind oder bedingte Workflows enthalten, erhöht sich der Informationsfluss hin und her. Wenn Sie Ihren Verwaltungsserver auffordern, diese Informationen zu analysieren und möglicherweise Berechnungen anhand der Änderungen durchzuführen, kann dies zu entsprechenden Befehlen und Abfragen führen.

Da immer mehr persönliche Geräte am Arbeitsplatz auftauchen, verfügen BYOD-Workflows mit User Enrollment über eine bewusst begrenzte Teilmenge der MDM-Funktionalität und Sichtbarkeit. Verwaltete Apple IDs erschließen neue Arbeitsabläufe. Die Komplexität der Geräteverwaltung hat erheblich zugenommen. **Es ist nicht mehr so einfach wie früher: Volle Verwaltung oder gar nichts.**

Glücklicherweise hat das Protokoll in den letzten 20 Jahren einige neue Tricks mit mehr Befehlen und granulareren Einstellungen erhalten. All dies hat zu Apples deklarativem Geräteverwaltung (DDM) Protokoll geführt.

Nutzung der Innovation: Deklarative Geräteverwaltung

Das **deklarative Geräteverwaltung** wurde als die Zukunft der Geräteverwaltung bezeichnet. Es ist auch eine wichtige Verbesserung, um die Sicherheitsabläufe zu optimieren. Deklarationen können sehr viel detailliertere, im Voraus festgelegte Anweisungen senden, die dem Gerät mitteilen, wie es sich unter bestimmten Bedingungen verhalten soll. Diese Anweisungen werden mit Statusberichten kombiniert, um den Verwaltungsserver zu alarmieren, wenn sich bestimmte Werte auf dem Gerät ändern.

Mit anderen Worten: Ein Gerät ergreift proaktiv Maßnahmen, wenn es gegen die Vorschriften verstößt, und kann aktualisierte Informationen direkt an den Server senden. Es muss nicht darauf warten, dass der Server es um einen Bericht bittet, das Problem meldet und dann darauf wartet, dass der Server ihm sagt, was zu tun ist. **Dadurch sind die Geräteinformationen genauer und die Richtlinien zur Geräte-Compliance können schneller umgesetzt werden.** Dadurch wird auch der Netzwerkverkehr erheblich reduziert, was zu einer deutlichen Steigerung der Leistung und Geschwindigkeit führt.

Die deklarative Geräteverwaltung markiert einen Trend in der Entwicklung zu einer modernen Verwaltung. Durch die Verbesserungen in der deklarativen Verwaltung wird MDM Administrator*innen die Möglichkeit geben, kompliziertere und innovativere Strategien zu entwickeln. Dadurch wird die Gerätesicherheit standardmäßig erhöht, während gleichzeitig sichergestellt wird, dass die Mitarbeiter*innen umgehend benachrichtigt werden, wenn sich wichtige Bedingungen ändern.

MDM sein wird:

1.

Sicherer (durch die Möglichkeit, dass Deklarationen die Compliance von vornherein festlegen, und durch die Begrenzung der programmatischen Interaktionen mit Low-Level-Binärprogrammen)

2.

Nativer (durch Ermöglichung von Endbenutzerinteraktionen auf der Grundlage von Deklarationen)

3.

Mehr Nutzen durch die Erweiterung der bereits soliden Grundlage von MDM mit DDM

Vorteile einer modernen Verwaltungsstrategie

Da hybrides Arbeiten für unsere Mitarbeiter*innen immer mehr zur Norm wird - und auch von ihnen erwartet wird -, hat sich die Art und Weise, wie wir ihnen Zugang zu den Werkzeugen bieten, die sie benötigen, um erfolgreich innovativ zu sein, etwas zu schaffen und zusammenzuarbeiten, weiterentwickelt. **Die Nutzer*innen wünschen sich ein dynamisches Erlebnis, bei dem die Bereitstellung der benötigten Daten und Werkzeuge im Mittelpunkt steht, und zwar von nahezu jedem Ort aus und unter Nutzung des gesamten Apple Ökosystems.**

Betriebssystem-, Appsoftware- und Sicherheitsupdates liefern regelmäßig neue Funktionen und Schutzmaßnahmen, um die Benutzerfreundlichkeit zu verbessern und Geräte vor Angriffen zu schützen. Die heutigen schnelleren Entwicklungszyklen und Feedback-Schleifen machen es einfacher, Aktualisierungen schnell an die Benutzer*innen weiterzugeben. Dies kann





dazu führen, dass ein Gerät mehrmals pro Woche aktualisiert wird, was die Benutzerfreundlichkeit beeinträchtigen kann. Die Nutzer*innen wollen die Vorteile von Aktualisierungen, Funktionen sowie Leistungs- und Sicherheitsverbesserungen nutzen. Aber sie wollen nicht, dass ein Gerät ihnen sagt, dass sie aufhören und neu starten sollen, wenn sie gerade mitten in einem kritischen Projekt oder in ihrer produktivsten Arbeitszeit sind.

Dies bedeutet eine Migration von der traditionellen, lokalen Struktur zu einem modernen, Cloudbasierten System, das jeden Apple Gerätetyp überall effektiv verwaltet und sichert.

Die Verlagerung in die Cloud ermöglicht es Unternehmen, sich schneller zu bewegen, und bietet im Vergleich zu lokalen Ressourcen flexible Ressourcen, wie und wann die Benutzer*innen sie benötigen. Moderne Tools automatisieren routinemäßige IT-Funktionen, wodurch die Belastung durch zeitraubende IT-Aufgaben verringert wird und die Administrator*innen mehr Zeit für andere spezifische Aufgaben haben. Self-Service-Tools helfen Endnutzer*innen und der IT-Abteilung, da die IT-Abteilung weniger Tickets ausstellen oder Passwörter zurücksetzen muss und die Mitarbeiter*innen sofortigen Zugriff auf Apps und Informationen erhalten.

Cloudimplementierungen bieten auch eine Reihe von Sicherheitsvorteilen gegenüber lokalen Implementierungen. Dazu gehören insbesondere Sicherheitsmerkmale und -dienste der Cloud wie:

- Verifizierte Registrierung, um die Integrität jedes in Ihrem Unternehmen verwalteten Geräts zu gewährleisten, indem integrierte Registrierungsmethoden wie die automatische und die Benutzerregistrierung genutzt werden
- Identitäts- und Zugriffsmanagement, um zu kontrollieren, wer auf der Grundlage der Cloudidentität einer Person Zugriff auf welche Ressourcen hat, und so den unbefugten Zugriff auf sensible Daten und Apps zu verhindern
- Verwaltung von Zugriffsrechten, um Nutzer*innen nur so viel Zugang zu sensiblen Datenteilen zu geben, wie sie benötigen
- Granulare Zugriffsrichtlinien für Apps und Daten, um sicherzustellen, dass nur autorisierte Benutzer*innen auf sanktionierten (verwalteten) Geräten auf Arbeitsapps und Daten zugreifen können
- Sicherer Netzwerkverkehr, um sicherzustellen, dass der gesamte Arbeitsverkehr sicher verschlüsselt wird, um unbefugten Zugriff zu verhindern
- Bedingter Zugriff mit Echtzeit-Sicherheitsdaten von verwalteten Geräten, die kontinuierlich Risikosignale auswerten und den Zugriff auf Arbeitsressourcen auf der Grundlage von anpassbaren Risikoschwellenwerten automatisch einschränken

Eine zunehmend verteilte Belegschaft, die ein breites Spektrum an Geräten nutzt, stellt viele Herausforderungen dar. Wenn Sie moderne Verwaltungspraktiken anwenden, sind Sie der Herausforderung mehr als gewachsen und können sowohl für die Benutzer*innen als auch für die IT-Teams eine einheitliche Erfahrung gewährleisten.

Der beste Weg zur Einführung einer modernen Verwaltung für Apple ist Jamf

Jamf gibt es im Bereich Apple MDM schon seit mehr als zwanzig Jahren. Unsere enge Zusammenarbeit mit Apple bedeutet, dass wir eine neue Version vom ersten Tag an unterstützen, wenn sie auf den Markt kommt.

Aber in der Welt der Technik können sich mehr als zwanzig Jahre wie ein ganzes Leben anfühlen. Das mag manche Leute dazu verleiten, zu denken, dass wir ein wenig in unseren Gewohnheiten verhaftet sind. **Aber Apple entwickelt sich weiter und Jamf gleich mit.** Beide Unternehmen haben sich auf den Weg zu einer hochmodernen Verwaltung gemacht, das zu einer vollständigen Umgestaltung der Geräteverwaltung und -sicherheit geführt hat.

Jamf hat sich bei der Umstellung auf cloudbasierte Lösungen als führend erwiesen. Dieser Wandel wurde durch die Erkenntnis vorangetrieben, dass mit der wachsenden Anzahl von Geräten in einer Umgebung auch ein entsprechender Bedarf an skalierbaren, global zugänglichen Diensten für deren effektive Verwaltung besteht. Daher bietet Jamf die Möglichkeit, Ihren Jamf Pro MDM-Server mit [Jamf Cloud](#) zu hosten.

Neben dem Hosting Ihres Servers in der Cloud bietet [Jamf Pro](#) eine Reihe von cloudbasierten Funktionen wie [App-Installer](#), [Jamf Cloud Vertriebservice](#) und [verwaltete Software-Aktualisierungen über deklarative Geräteverwaltung](#).

Die Verwaltung von Software-Aktualisierungen ist eine Kernfunktion der Geräteverwaltung, und wir wissen, dass dies etwas ist, was unsere Community braucht. Dank der engen Zusammenarbeit mit Apple war Jamf in der Lage, mit verwalteten Software-Aktualisierungen über DDM sofort loszulegen. Admins in Jamf Cloud können jetzt Software-Aktualisierungen planen und erzwingen, die bis zu einem bestimmten Datum und einer bestimmten Uhrzeit abgeschlossen sein müssen. Dank DDM werden diese Updates automatisch auf alle entsprechenden Macs und mobilen Geräte übertragen. Die Unterstützung dieses Workflows verbessert nicht nur die Softwareaktualisierung für Administrator*innen und verringert die Abhängigkeit von Drittanbieter-Tools, sondern trägt auch dazu bei, dass die Geräte mit den neuesten Betriebssystem-Aktualisierungen und Sicherheitskorrekturen konform bleiben.

Um sicherzustellen, dass nur autorisierte Benutzer*innen auf Unternehmensressourcen zugreifen, integriert sich [Jamf Connect](#) mit Cloud Identitätsanbietern für eine moderne, sichere Mac Authentifizierung mit Just-in-Time-Bereitstellung von lokalen Mac Konten und Kennwortsynchronisierung. Ein Benutzer/Eine Benutzerin kann sein Gerät auspacken, einschalten und auf alle Unternehmensapps und -ressourcen zugreifen, nachdem er sich mit einem einzigen Satz von Cloud Identitätsdaten angemeldet hat - jederzeit und von überall.





**Revolutionieren Sie mit einer modernen Verwaltungsstrategie:
Entfesseln Sie die Möglichkeiten Ihres Apple Ökosystems**

Eine Cloud Umgebung in Verbindung mit deklarativen Geräteverwaltung bedeutet eine schnellere, reibungslosere und sicherere Art und Weise, Ihre Geräte zu verwalten und zu schützen. Es bietet die Benutzerfreundlichkeit, die der moderne Arbeitsplatz benötigt, und befreit gleichzeitig von den IT-Belastungen der traditionellen Verwaltung.

Wenn Sie bereit sind, sich Apple und Jamf auf dem Weg zu einer **modernen Verwaltung anzuschließen** und alle Vorteile der Cloud und von DDM nutzen möchten, können wir Ihnen helfen!