jamf

Ein praktischer Leitfaden für die moderne Apple Geräteverwaltung mit einem DDM

Schnellere Updates, bessere Gerätetransparenz und weniger manueller Aufwand für wachsende Apple Flotten

Wachsende Apple-Infrastrukturen stoßen bei herkömmlichen Verwaltungsprozessen oft an ihre Grenzen und bremsen den Betrieb aus. Schlanke IT-Teams, die bereits einer hohen Arbeitsbelastung ausgesetzt sind, registrieren langsamere Updates, eine verzögerte Sichtbarkeit des Gerätestatus und einen höheren Aufwand für manuelle Korrekturen. Ein DDM kann helfen.

Inwiefern können die IT-Mitarbeiter durch ein DDM Zeit sparen und die Ergebnisse verbessern?

Einfachere Arbeitsabläufe

Die Einführung von Tools und Prozessen, die ein DDM verwenden, kann die Verwaltung von Geräten vereinfachen, da weniger Skripte, Check-Ins und manuelle Arbeitsabläufe erforderlich sind.

Bessere flottenweite Sichtbarkeit der Geräte

Da die Geräte mithilfe dieses Protokolls ihren Status proaktiv melden können, erhalten IT-Teams einen klaren Überblick in Echtzeit über jedes Gerät und jede App.

Schnellere Updates

Wenn Geräte Änderungen an ihrer Konfiguration proaktiv melden, erhöht dies die Effizienz durch schnellere und zuverlässigere Patches und Betriebssystem-Updates, was wiederum den Bedarf an Fehlerbehebungen reduziert.

Ein besseres Erlebnis für die Endbenutzer

Wenn Geräte auf Änderungen ihres eigenen Gerätezustands reagieren können, können mehr Sicherheitsupdates und Konfigurationsänderungen im Hintergrund ausgeführt werden, ohne die tägliche Arbeit zu unterbrechen.

Was ist ein DDM und warum sollten Sie es verwenden?

Ein DDM ist ein Protokoll für macOS, iOS, iPadOS watchOS, visionOS und tvOS, das es Apple-Geräten ermöglicht, Konfigurationsänderungen proaktiv zu melden, selbstständig Konfigurationen durchzusetzen und auf Zustandsänderungen zu reagieren. In Jamf werden die Funktionen der deklarativen Geräteverwaltung durch Dinge wie Entwürfe bereitgestellt.

Der Wechsel von serverbasierten Befehlen des herkömmlichen MDM hin zu DDM-Protokollen führt zu:

- Weniger Abhängigkeit von wiederholten Serverbefehlen, die das System verlangsamen
- Proaktivere Meldung von Änderungen des Gerätestatus
- Stärkere Durchsetzung der Konformität auf dem Gerät selbst, wodurch die Behebung nahezu sofort erfolgt
- Geringerer Bedarf an manueller Nachbereitung

Vereinfachte Verwaltung verbessert die Sicherheit

DDM vereinfacht die Verwaltungsabläufe und verbessert Ihren Sicherheitsstatus durch:

- **Minimierung von Konfigurationsabweichungen**
- **Schnellere Updates**
- **Standardisierung und Stärkung der Baselines**
- **Automatisierte Reaktion auf dem Gerät**

Dadurch werden manuelle Eingriffe bei allgemeinen Arbeitsabläufen reduziert und eine einheitliche Konformität in großem Umfang gewährleistet. Ein DDM ermöglicht außerdem proaktive Cybersicherheit anstelle von reaktiven Maßnahmen, um mit einer weitaus komplexeren Angriffslandschaft Schritt zu halten, die mit zunehmender Unternehmensgröße entstehen. Wenn Geräte verdächtige Vorgänge sofort in einer Sandbox isolieren, bleibt die Sicherheit im Netzwerk gewahrt.

Wie ein DDM Ihr Unternehmen jetzt schon beeinflussen kann

Bei einem DDM geht es nicht nur um reibungslose Skalierung oder Zeitersparnis für die IT. Ein DDM ermöglicht zudem völlig neue Ansätze in Ihrer gesamten Organisation und Ihren Workflows.

Eine einheitliche Konfiguration über alle Geräte hinweg erhöht die Zuverlässigkeit und Konsistenz in Ihrem Unternehmen.

Konsistenz ist wichtig. Bei einheitlichen unternehmensweiten Richtlinien und Konfigurationen erhält ein Unternehmen folgende Vorteile:

- Weniger Support-Tickets und weniger manuelle Korrekturen oder Nacharbeiten
- Ein höheres Sicherheitsniveau und Schutz vor Fehlkonfigurationen, die zu unbefugtem Zugriff führen könnten
- Vorhersehbares Verhalten bei allen Geräten, was die Fehlersuche erleichtert

DDM findet Fehler

Wenn Verwaltungs- und Sicherheitstools zusammenarbeiten, werden Unstimmigkeiten schneller erkannt und das Problem kann schneller gelöst werden - oft ohne dass die Mitarbeiter eingreifen müssen. Außerdem werden durch die Automatisierung der Einrichtung und der Durchsetzung der Konformität menschliche Fehler reduziert.

Ein DDM verwaltet Standardkonfigurationen

Mit einem DDM bleiben Updates und Baselines erhalten, denn sollten Abweichungen auftreten, ist Ihr System so eingerichtet, dass es sich bei allen Problemen – außer bei ungewöhnlich komplexen Fällen – selbst korrigiert.

Das Ergebnis: Die Mitarbeiter erleben weniger technische Probleme oder Verlangsamungen und bemerken nicht einmal, wenn neue Sicherheitsprotokolle im Hintergrund arbeiten.

Und die IT-Abteilung hat mehr Zeit, um sich auf größere technische Probleme zu konzentrieren, die die tägliche Arbeit im gesamten Unternehmen weiter verbessern können.

Warum das autonome Melden des Gerätestatus fast alles verändert

Proaktive Meldung über den Zustand der Geräte

Dank DDM bedeutet die autonome Meldung des Gerätestatus, dass Geräte den Management-Server automatisch benachrichtigen, wenn sich Schlüsselwerte (z. B. die Betriebssystemversion) geändert haben. So entsteht ein reaktionsfähiges Betriebssysteminventar, das proaktiv zeitnahe Updates gewährleistet.

Bessere Sichtbarkeit der Flotte

Wenn sich die Geräte selbstständig beim Management-Server melden, erhält die IT-Abteilung einen kontinuierlichen Überblick über ihre gesamte Flotte.

Dadurch erhalten Sie folgende Informationen:

- Standort des Geräts
- Zustand der Konfiguration
- Betriebssystemversion und installierte Apps

Die IT-Abteilung kann auch sehen, welche Geräte auf Angriffe oder verdächtige Verhaltensweisen reagiert haben - und wie die Reaktionen darauf ausgesehen haben.

Selbst wenn die IT-Abteilung dank der Automatisierungen des DDM nicht eingreifen muss, bekommt sie ein Gefühl dafür, wo die Sicherheit verbessert werden muss - oder wer im Unternehmen eine Auffrischung in Sachen Phishing braucht.

Wenn die IT-Teams Änderungen in Bezug auf den Gerätestatus in Echtzeit erkennen können, gibt es weniger Überraschungen. Wenn ein Gerät plötzlich aus der Konformität fällt, z. B. durch das Entfernen eines Passworts oder das Löschen einer wichtigen App, weiß die IT-Abteilung sofort Bescheid.

Sofortige Erkenntnis und proaktive Fehlerbehebung können den entscheidenden Unterschied machen. Ohne dies entdecken Teams einen ausgeklügelten Malware-Angriff möglicherweise erst Stunden später beim nächsten geplanten Server-Check-in.

Planbarere Update-Zyklen

Die Durchsetzung von Updates war lange Zeit ein großes Problem für IT-Abteilungen.

Vor dem DDM

Als die IT-Abteilung noch Updates für Betriebssysteme, Apps, Richtlinien oder Konfigurationen ohne DDM durchführen musste, konnten zahlreiche Dinge schief gehen:

- Mitarbeiter haben wichtige Updates immer wieder aufgeschoben, um ihre Arbeit nicht zu unterbrechen
- MDM-Befehle, die kritische Updates erzwingen, bevor es zu spät ist, konnten stundenlange Arbeit vernichten
- Ohne detaillierte und klare Kenntnisse über den Gerätestatus verteilte die IT Updates ins Blaue hinein, was gelegentlich zu unvorhersehbaren Problemen führte.

Verwendung eines DDM

Anders sieht es in Ökosystemen aus, die das DDM-Protokoll verwenden.

Auf der Grundlage von Richtlinien, die von der IT-Abteilung festgelegt wurden, meldet ein Gerät kontinuierlich seinen Status, sodass die IT-Abteilung einen genauen Überblick über die Vorgänge in Echtzeit erhält. Ob ein Update aussteht, heruntergeladen oder installiert wird oder ob ein Problem aufgetreten ist – die Teams können den Fortschritt sehen, ohne den Geräten hinterherlaufen oder sich auf die Informationen der Benutzer verlassen zu müssen.

- Ein DDM hält die Benutzer auf dem Laufenden. Die Geräte benachrichtigen die Benutzer über anstehende Updates und helfen ihnen, den richtigen Zeitpunkt für die Installation auszuwählen.
- Wenn die Endbenutzer nichts unternehmen, erzwingt das Gerät die Aktualisierung von selbst.
- Die Uhrzeit und das Datum der Aktualisierung basieren auf der lokalen Zeit des Kunden, so dass das Update außerhalb der Arbeitszeit erfolgt. Geräte mit einem DDM-Protokoll können sogar ausgeschaltete Geräte aktualisieren: Das Update wird ausgeführt, sobald der Benutzer das nächste Mal das Gerät einschaltet.
- Die IT schickt Updates nicht länger „ins Blaue hinein“: Viele Updates können ohne jegliches Eingreifen der IT-Abteilung durchgeführt werden, bei voller Transparenz des Gerätezustands und unter Verwendung vorprogrammierter Reaktionen auf gängige Konformitätsprobleme.

Dies gewährleistet, dass die Geräte sicher und auf dem neuesten Stand bleiben, ohne dass die IT-Abteilung eingreifen muss und ohne die Arbeit der Endbenutzer zu unterbrechen oder zu stören.

Proaktive Planung statt reaktiver Fehlersuche und Problemlösung

DDM reduziert den Bedarf an reaktiver Fehlerbehebung, indem die Kontrolle vom Management-Server direkt auf das Gerät verlagert wird.

Wenn etwas schief läuft, melden die Geräte dem Server aussagekräftige Statusänderungen, die sich an den vorherigen Richtlinien und Anweisungen der IT-Abteilung orientieren.

Dies kann ein fehlgeschlagenes Update aufgrund eines schwachen Akkus oder fehlenden Speichers sein oder eine Sicherheitsänderung wie Status der FileVault-Verschlüsselung.

Dank dieser Transparenz kann die IT-Abteilung auch dann schnell eingreifen, wenn direkte Unterstützung benötigt wird - oft bevor es für den Benutzer zu Einschränkungen kommt.

Wie wirkt sich eine vorausschauende Planung auf Unternehmen aus?

Das Ergebnis ist ein planbares, kontrolliertes Update-Erlebnis. Die IT-Abteilung verbringt weniger Zeit mit der Verfolgung des Fortschritts oder der Fehlerbehebung bei einzelnen Geräten und konzentriert sich mehr auf die Ergebnisse.

Und dann ist da noch der Faktor „es funktioniert einfach".

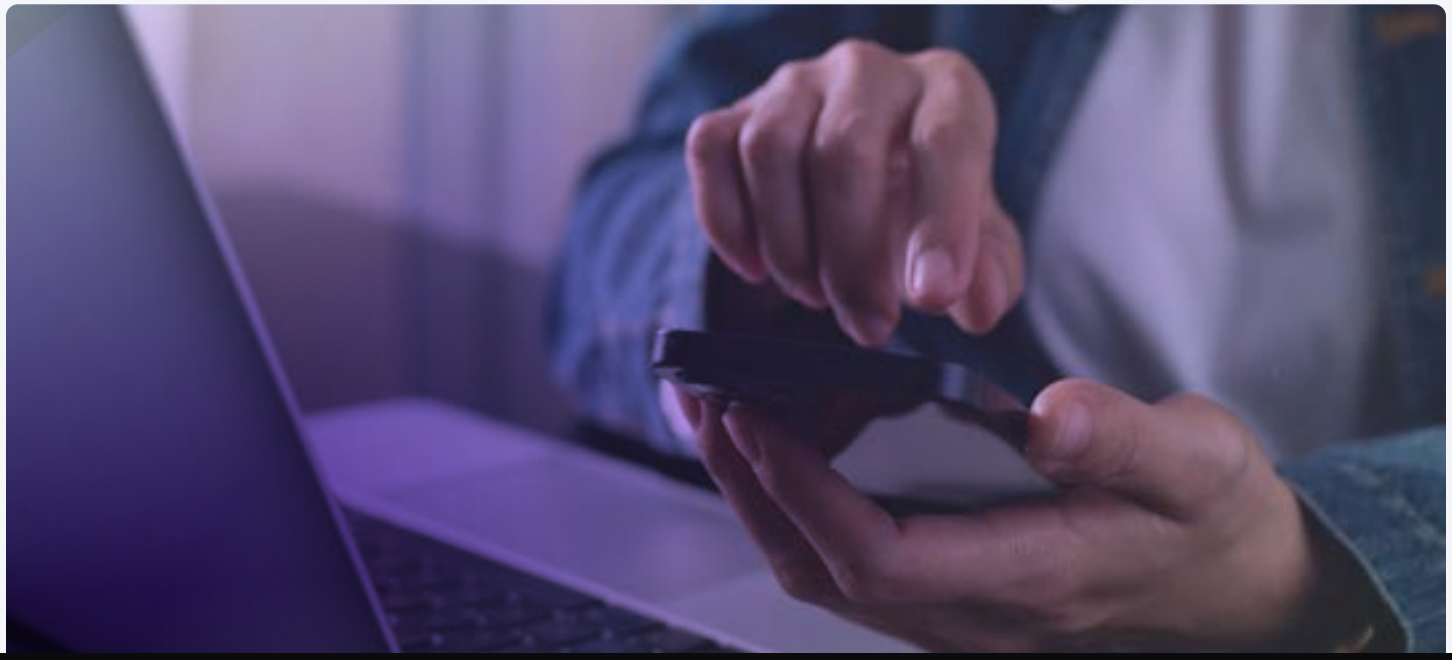
Wenn Geräte konsistent konfiguriert, kontinuierlich aktualisiert und durch integrierte Intelligenz gesteuert werden, gibt es einfach weniger Probleme. Automatisierte Reaktionen sorgen dafür, dass die Geräte den Richtlinien entsprechen, was die Reibungsverluste für die Benutzer verringert und den Support-Bedarf an Support minimiert.

Skalieren, Automatisieren und Optimieren von Arbeitsabläufen mit einem DDM

Ein DDM ist ein modernes Verwaltungsprotokoll, das wachsenden IT-Teams hilft, Geräte effizienter zu verwalten, Reibungsverluste im Betrieb zu reduzieren und die Skalierung effektiver zu unterstützen.

Außerdem kann ein DDM die Erfahrung der Endbenutzer verbessern, indem Updates im Hintergrund durchgeführt werden und die Konformität automatisiert wird. Das führt zu einer höheren Produktivität und zufriedeneren Mitarbeitern.

Mit einem DDM sparen Sie Zeit, können skalieren, ohne den Aufwand zu erhöhen, und sorgen für mehr Cybersicherheit.



jamf

www.jamf.com/de/

Wir erläutern Ihnen, warum ein DDM die Verwaltung vereinfacht und die Sicherheit erhöht.
Fordern Sie eine kostenlose Testversion an.