



# Verbinden, verwalten und schützen Sie Apple Geräte, Apps und Unternehmensressourcen.

Jamf Apple Enterprise Management ermöglicht es Ihrer Organisation, Apple Geräte erfolgreich einzusetzen.



Unternehmen müssen in der Lage sein, bei jedem Apple Gerät nahtlos Technologien zu integrieren, die Geschäftsinitiativen vorantreiben. Dazu bieten sie den Benutzern einen sicheren Zugriff auf die benötigten Ressourcen und ermöglichen der IT, die in der heutigen modernen Arbeitsumgebung erforderlichen Funktionen bereitzustellen. Sie bieten Informationssicherheit mit der Gewissheit, dass Geräte und Daten jederzeit geschützt sind. Gleichzeitig bieten sie jedem Mitarbeiter ein außergewöhnliches Erlebnis.

Jamf ist die einzige Apple Enterprise Management-Lösung, die den gesamten Lebenszyklus von Apple im Unternehmen automatisiert, einschließlich Gerätebereitstellung, -verwaltung und -sicherheit, ohne die Endbenutzererfahrung zu beeinträchtigen, oder zu erfordern, dass die IT-Abteilung das Gerät berührt. Von dem Moment an, an dem ein Apple Gerät ausgepackt wird bis zum Tag, an dem es durch ein neues ersetzt wird, optimiert Jamf das gesamte Apple Erlebnis für IT-Personal und Endbenutzer.

**Laut Hobson & Company verbringen Unternehmen, die Jamf einsetzen, 80 % weniger Zeit mit der Bereitstellung von Geräten, 90 % weniger Zeit mit der Verwaltung von Anwendungen und Inventar und reduzieren die Wahrscheinlichkeit einer Sicherheitsverletzung um zwei Basispunkte.<sup>1</sup>**

1. <https://www.jamf.com/de/ressourcen/whitepaper/steigerung-des-roi-argumente-fur-eine-bewahrte-verwaltungslosung-fur-apple-gerate/>

# Eine konsistente, native Apple Erfahrung, die Mitarbeitern mehr Autonomie bietet.



## Zero-Touch Deployment

Stellen Sie allen Mitarbeitern überall Geräte bereit. Durch die Integration in Apple Bereitstellungsprogramme automatisieren Sie Registrierung und Konfiguration und bieten eine skalierbare, berührungslose Erfahrung mit jedem verpackten Neugerät, das für jeden individuell angepasst wird.



## Identitätsbasierter Zugriff

Stellen Sie Geräte mit geschäftskritischen Anwendungen bereit, die auf den Cloud-Identitätsdaten der Mitarbeiter basieren, wobei für jede Anmeldung eine Multifaktor-Authentifizierung nötig ist.



## Individuell angepasste Ressourcen on-demand

Bieten Sie Ihren Benutzern einen Self Service App Store mit Ihrem eigenen Branding. Geben Sie ihnen die Möglichkeit, Apps zu installieren, Software zu aktualisieren und ihr eigenes Gerät zu warten, ohne ein Helpdesk-Ticket einzureichen.



## Bestandsverwaltung

Erfassen Sie automatisch Benutzer-, Hardware-, Software- und Sicherheitsgerätedaten oder passen Sie Bestandskonfigurationen an. Nutzen Sie automatisierte Bestandsdaten und dynamische Smart Groups, um Aktionen wie Betriebssystemaktualisierungen auszulösen.



## Erweiterte Sichtbarkeit

Mit Dashboards, Echtzeit-Warnungen und Berichten über integrierte Sicherheits-Frameworks von Apple wie XProtect, Gatekeeper und MRT wissen Sie, wenn verdächtige Aktivitäten auftreten.



## Geräteverwaltung

Durch Fernverwaltung und die Nutzung von Konfigurationsprofilen, Richtlinien, intelligenter Zielgruppenorientierung und Skripten können Sie fortgeschrittene Workflows nutzen, um die Verwaltung von Mac, iPad, iPhone und Apple TV zu automatisieren. Und mit einer robusten API und 300 Integrationen von Ressourcen anderer Anbieter verbessert Jamf den Wert Ihres vorhandenen Technologie-Stacks.



## Optimierte App-Verwaltung

Erwerben Sie Apps in großen Mengen und wählen Sie Ihre Bereitstellungsmethode, um sie automatisch für die Benutzer verfügbar zu machen (keine Apple ID erforderlich). Erstellen Sie benutzerdefinierte App- und Softwarepakete und halten Sie Software von Drittanbietern automatisch auf dem neuesten Stand.



## Vorbeugung und Beseitigung von Gefahren

Erhalten Sie Echtzeit-Warnungen auf dem Gerät, um Aktivitäten zu analysieren und dann zu entscheiden, ob Sie Bedrohungen proaktiv blockieren, isolieren oder beseitigen möchten. Verhindern Sie bekannte macOS Malware, einschließlich der Bedrohungen und Angriffe, die nur in der Apple Architektur zu finden sind.



## Sicherheitsmanagement

Sichern Sie Geräte, indem Sie native Apple Sicherheitsfunktionen nutzen, z. B. Verschlüsselung unter macOS und iOS sowie Passcodes unter iOS erzwingen, Richtlinien ausführen, um FileVault für macOS zu aktivieren, schädliche Software eindämmen und Apple Geräte patchen.

Schöpfen Sie noch heute das ganze Potenzial von Apple und Jamf aus, um die Produktivität zu steigern und Support- und Betriebskosten zu senken. [Test starten](#)



[www.jamf.com](http://www.jamf.com)

© 2002-22021021 Jamf, LLC. Alle Rechte vorbehalten.

Um mehr darüber zu erfahren, wie sich Jamf auf Ihre Implementierungen von macOS, iPadOS, iOS und tvOS auswirken kann, besuchen Sie bitte [jamf.com/de](http://jamf.com/de)