Arbeiten im Homeoffice:

mehr Autonomie für Mitarbeiter

jamf

Die Arbeitswelt hat sich verändert. Es ist Zeit, sich anzupassen.

Die Tage eines ‘9-to-5’ Arbeitstages im Büro neigen sich dem Ende zu, da die Arbeit nicht mehr durch Ort und Zeit definiert und begrenzt ist. Inzwischen erlauben und befürworten 66% aller Unternehmen das Arbeiten von Zuhause und 16% aller Mitarbeiter arbeiten Vollzeit aus dem Home Office[1].
Was dies ermöglicht, ist die sich ständig entwickelnde Rolle der digitalen Technologie und wie diese es schafft Geschäftsprozesse und die Mitarbeitererfahrung zu verbessern. Dabei ist es wichtig, dass die entwickelnde Verantwortung der IT sich mit entwickelt.

Immer mehr Unternehmen lockern ihre Richtlinien für die Fernarbeit und die Arbeit von zu Hause aus - sei es aus Gründen der Gesundheit, der Mitarbeiterbindung oder der Mitarbeiterproduktivität.

In unserem E-Book erläutern wir, wie Sie Ihre Mitarbeiter und das gesamte Unternehmen mit den folgenden Maßnahmen dabei optimal unterstützen können:

- **Erfolgreiches Onboarding externer und interner Mitarbeiter**
- **Abgesicherte Anbindung der Mitarbeiter an Ressourcen, unabhängig vom Standort**
- **Unterstützung für dauerhaft und zeitweilig extern arbeitende Mitarbeiter**

Besseres Onboarding für alle

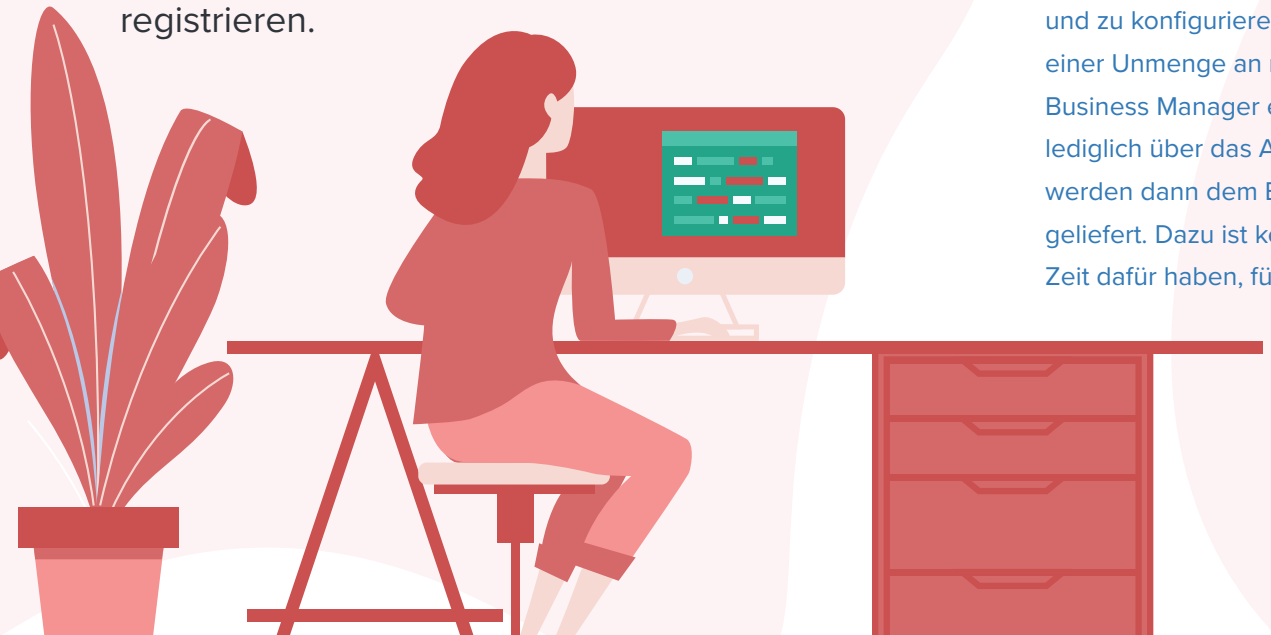
Die Geschwindigkeit, mit der Unternehmen ihre Mitarbeiter für eine produktive Arbeitsweise befähigen müssen, hängt direkt mit der Mitarbeiterbindungsquote und mit der Produktivität neu eingestellter Mitarbeiter zusammen. Wenn Unternehmen neue Mitarbeiter gut aufnehmen und integrieren, können Sie die Mitarbeiterbindungsquote um 82% und die Produktivität der Mitarbeiter um über 70%[2] steigern.

Deshalb ist es wichtig, dass Unternehmen die richtige Technologie anbieten und die richtigen Tools einsetzen, um einen vorgelegten Onboarding-Prozess für Mitarbeiter sowohl im Büro als auch im Homeoffice zu ermöglichen. Bei der Entscheidung, wie diese Ziele am besten erreicht werden können, sind jedoch nicht alle Technologien und Tools gleich gut geeignet.

Apple Hardware wird in Unternehmen in aller Welt immer häufiger eingesetzt. Die Benutzerfreundlichkeit und die wachsende Nachfrage seitens der Mitarbeiter bewegen viele Unternehmen dazu, die Nutzung von Mac, iPad und iPhone Geräten anzubieten und zu unterstützen. Dieser Trend bietet den Mitarbeitern, der IT-Abteilung und dem gesamten Unternehmen enorme Vorteile.

Effizientes Onboarding durch die IT-Abteilung

Die IT-Abteilung hat nur einmal die Chance, einen guten ersten Eindruck zu hinterlassen. Die IT kann mithilfe vom Apple Business Manager unternehmensweit eine Strategie der vollautomatischen Bereitstellung verfolgen. Wenn ein neues Gerät ausgepackt und eingeschaltet wird, weist Apple Business Manager den Mac, das iPad bzw. das iPhone an, sich automatisch bei der MDM-Lösung (Mobile Device Management) des Unternehmens zu registrieren.



Jamf Pro – der Premium-Standard für die Apple Verwaltung im Unternehmen – ist von Grund auf für die Unterstützung von Apple Business Manager konzipiert und eröffnet neue Dimensionen. Dank leistungsstarker Technologien wie etwa intelligente Gruppen, mit denen Umgebungen auf intelligente Weise vollautomatisch verwaltet werden können, ist Jamf Pro die optimale Plattform zur Unterstützung eines wachsenden Bestands von Mitarbeitern im Homeoffice. Für Kleinunternehmen bietet Jamf Jamf Now, eine MDM-Lösung für weniger Geräte und mit einfachen Verwaltungsmöglichkeiten.

Apple Business Manager – ein kostenloser Service von Apple – trägt in Verbindung mit einer Verwaltungslösung wie Jamf Pro oder Jamf Now auch zur Optimierung der Apple ID-Prozesse bei. Nutzen Sie verwaltete Apple IDs und kontrollieren Sie Einrichtung und Verwaltung der Apple ID in vollem Umfang. Mitarbeiter profitieren von einer Apple ID-Strategie, die auf die berufliche Nutzung ausgelegt ist, damit Klarheit darüber besteht, dass die private Apple ID nicht für die Arbeit genutzt wird. Administratoren erhalten weniger Supportanfragen, da die Endanwender ihre Passwörter ohne Support durch die IT-Abteilung eigenständig verwalten und zurücksetzen können.

Bei diesem Workflow entfällt die Notwendigkeit, alle Geräte einzeln auspacken und zur Hand nehmen zu müssen, um sie für die einzelnen Mitarbeiter zu personalisieren und zu konfigurieren. Vorbei sind die Zeiten, in denen die IT-Abteilung aufgrund einer Unmenge an neuer Hardware heillos überlastet war. Mit Jamf Pro und Apple Business Manager erfolgt die Bereitstellung neuer Geräte ganz einfach: Sie müssen lediglich über das Apple Business Manager Portal bestellt werden. Die Geräte werden dann dem Endanwender direkt in das Büro bzw. an die Privatadresse geliefert. Dazu ist keine weitere Beteiligung der IT-Mitarbeiter nötig, die somit mehr Zeit dafür haben, für Mitarbeiter auf andere Weise Support zu leisten.

Besseres Onboarding für alle

Um eine vollautomatische Bereitstellung neuer Geräte einzuführen, müssen sich Unternehmen lediglich

Vorbereitung

1. Registrieren Sie sich bei Apple Business Manager.
2. Verknüpfen Sie Ihren Apple Business Manager Account mit dem MDM-Server.
3. Konfigurieren Sie Ihre Einstellungen und passen Sie die Registrierung an Ihre Anforderungen an.

Kauf

1. Bestellen Sie Apple Hardware bei Apple oder bei einem autorisierten Apple Händler.
2. Weisen Sie Geräte für die Registrierung zu.

Einsatz

1. Senden Sie die original verpackten Apple Geräte direkt an die Mitarbeiter.
2. Der Mitarbeiter packt das Gerät aus und schaltet es ein.
3. Das Apple Gerät wird automatisch

Einfaches Onboarding der Mitarbeiter

Der erste Tag ist für neue Mitarbeiter immer schwierig. Erleichtern Sie ihnen den Einstieg und die Integration, indem Sie gleich am ersten Tag mithilfe von Zero-Touch Deployment die Tools bereitstellen, die die Mitarbeiter brauchen (und sich auch wünschen).

Es erfordert wirklich nur ein paar Klicks, damit Mitarbeiter im Eigenheim sofort produktiv arbeiten können. Mitarbeiter werden automatisch mit den Ressourcen für die Arbeit vernetzt, also mit E-Mail, VPN und Produktivitäts-Apps, und zwar auf genau dieselbe Weise wie die Mitarbeiter im Büro. Ihre Geräteverwaltungslösung sollte außerdem eine flexible Konfiguration der Registrierung ermöglichen, so dass Sie auf einfache Weise Videos, Dokumentation und andere Informationen bereitstellen können, wenn sich neue Mitarbeiter durch die Registrierungsdialoge auf den Geräten klicken.

Wenn Mitarbeiter im Homeoffice einmal online sind, finden sie dank Self Service – einem kostenlosen App-Portal, auf das alle Nutzer im Unternehmen zugreifen können – problemlos ihre bevorzugten Apps und andere wichtige Ressourcen und können diese rasch nutzen.

> Die IT-Mitarbeiter brauchen die Geräte nicht in die Hand nehmen, und die Mitarbeiter müssen auch nicht ins Büro kommen, um ihre Hardware zu erhalten.

Anbindung der Mitarbeiter

Um die Geräteimplementierung und das laufende Lifecycle-Management für externe und interne Mitarbeiter noch weiter zu differenzieren und abzustimmen, setzen Unternehmen mehr und mehr auf moderne Authentifizierungs- und Sicherheitsmaßnahmen.

Mit einer Authentifizierungs- und Identity Management-Lösung wie Jamf Connect können Unternehmen eine Strategie nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“ umsetzen. Dies ist ganz entscheidend bei Mitarbeitern, die möglicherweise über ungesicherte Netzwerke auf vertrauliche Informationen und Ressourcen zugreifen.

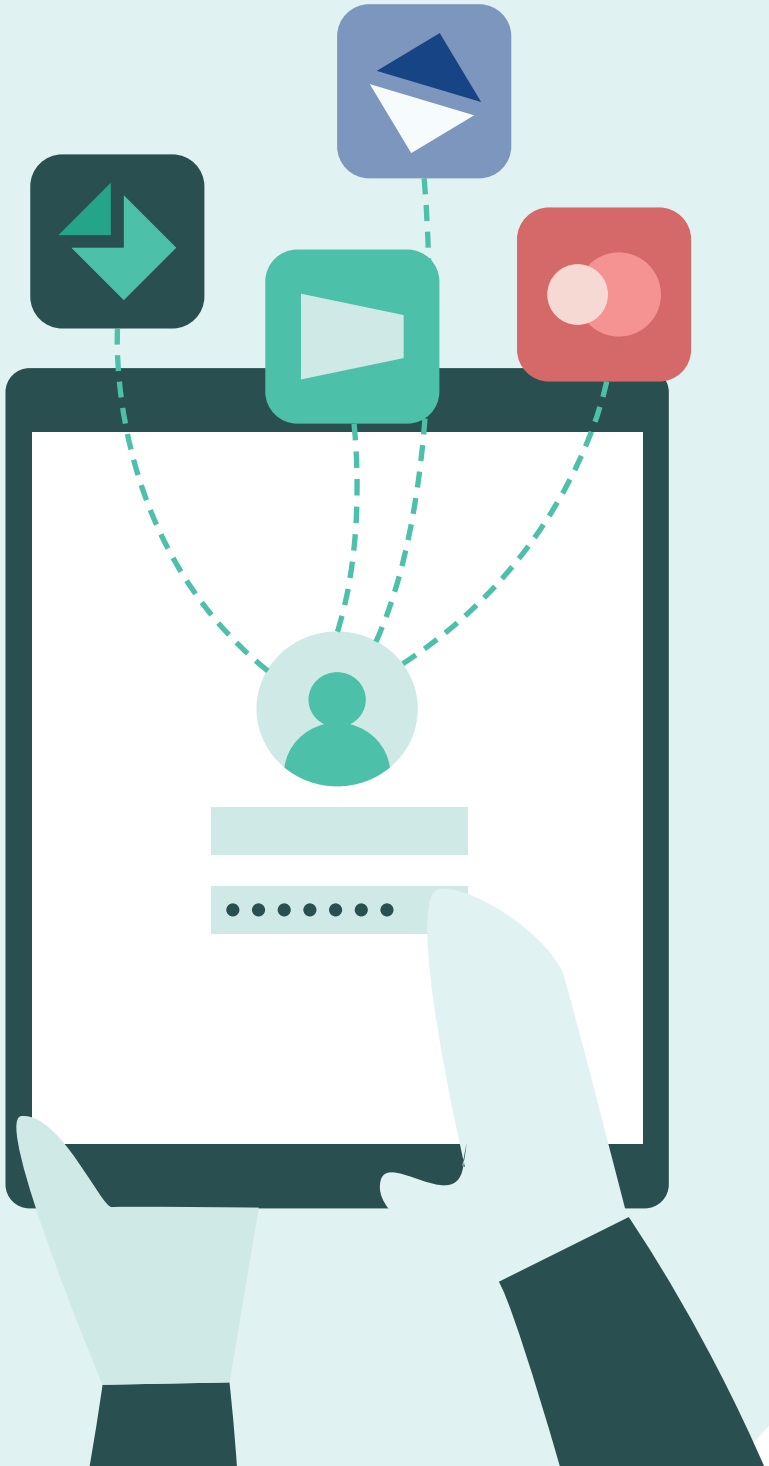
Jamf Connect und Cloud Identity Provider wie Okta und Microsoft Azure Active Directory bieten Unternehmen ein hohes Maß an Vertrauenswürdigkeit der Benutzer und der Geräte. Gleichzeitig sorgen sie dafür, dass die Mitarbeiter die Geräte nahtlos und ununterbrochen nutzen können.

Diese Ziele werden mittels der folgenden drei Bereiche realisiert:

Bereitstellung von Accounts und Authentifizierung

IT-Administratoren können auf einem Mac alle für die produktive Arbeit entscheidenden Apps allein anhand der Zugangsdaten des Mitarbeiters für die Cloud Identity bereitstellen. Damit geht die vollautomatische Implementierung noch einen Schritt weiter, denn der Benutzer kann sich mit denselben Zugangsdaten per Multi-Faktor-Authentifizierung anmelden. Somit weiß das Unternehmen, dass die richtige Person auf das richtige Gerät und die richtigen Ressourcen zugreift.

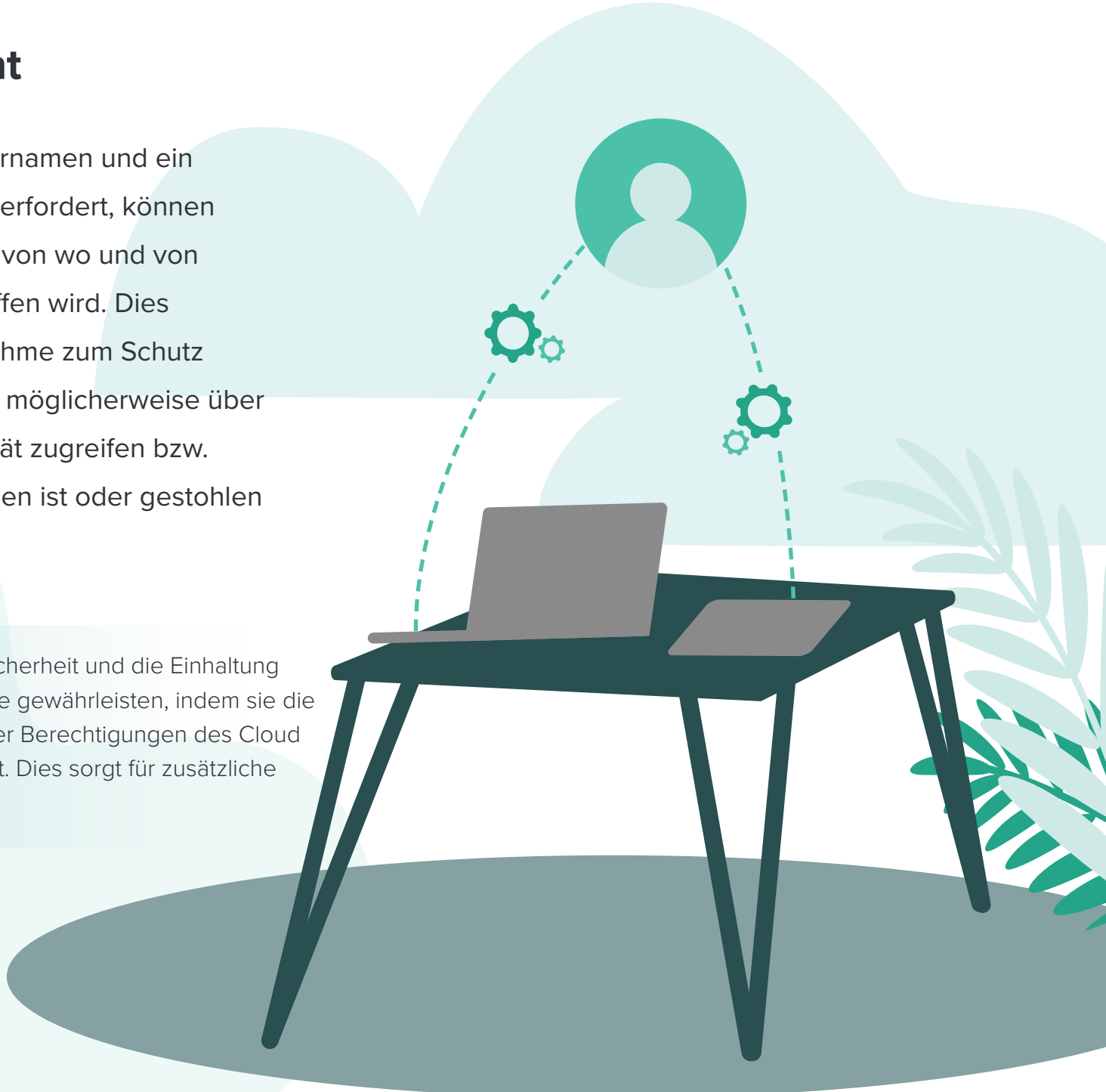
Im alltäglichen Betrieb kommt dieses einfache, doch sichere Anmeldeverfahren bei jeder Anmeldung eines Benutzers zur Anwendung.



Identity management

Da Jamf Connect einen Benutzernamen und ein Passwort für eine Cloud Identity erfordert, können IT-Administratoren überwachen, von wo und von wem auf welche Geräte zugegriffen wird. Dies ist eine starke Sicherheitsmaßnahme zum Schutz externer Mitarbeiter, wenn diese möglicherweise über unsichere Netzwerke auf ihr Gerät zugreifen bzw. wenn ein Gerät verloren gegangen ist oder gestohlen wurde.

Die IT-Abteilung kann die Sicherheit und die Einhaltung von Richtlinien für alle Geräte gewährleisten, indem sie die Passwortrichtlinien mittels der Berechtigungen des Cloud Identity-Anbieters durchsetzt. Dies sorgt für zusätzliche Sicherheit.



Synchronisierung der Benutzeridentitäten und der Gerätezugangsdaten

Mit Jamf Connect können die Mitarbeiter ihre betriebliche Identität (Cloud Identity) jederzeit mit dem Passwort ihres lokalen Mac Accounts synchronisieren. So können die Mitarbeiter auf alle nötigen Ressourcen zugreifen, ohne mehrmals ein Passwort eingeben zu müssen.

40% Laut Gartner machen Anfragen zum Zurücksetzen von Passwörtern 40 Prozent aller Helpdesk-Tickets aus[3]. Mit Jamf Connect sind diese Anträge nicht mehr erforderlich. Dies spart den IT-Mitarbeitern viel Zeit und hat den Effekt, dass die Mitarbeiter nicht unproduktiv auf die Lösung des Problems warten müssen.

Laufender Support für alle Mitarbeiter – egal wo.

Das Onboarding, also die Aufnahme und Integration der Mitarbeiter, sowie eine sofortige, sichere Verbindung zu den nötigen Ressourcen sind die ersten beiden Schritte um sicherzustellen, dass externe Mitarbeiter produktiv arbeiten können. Doch genau so wichtig ist die laufende Verwaltung der Geräte.

Jamf Pro und Jamf Now kommunizieren über den Apple Push Notification Service (APNs) mit den Geräten und geben ihnen entsprechende Anweisungen. So wird eine ständige Verbindung zu den Geräten gehalten, sodass sich die IT-Abteilung nicht mehr darum kümmern muss.

Wenn die IT-Abteilung ein (extern oder intern genutztes) Gerät ändern möchte, sendet sie einfach per APNs ein Konfigurationsprofil oder einen MDM-Befehl. VPN, E-Mail, WLAN und zahllose andere Einstellungen können automatisch auf die Geräte der Mitarbeiter angewendet werden, ohne dass die Mitarbeiter dabei tätig werden müssen.

Zielgerichtete Einstellungen auf mehreren Geräten

Mit der patentierten Technologie dynamischer Gruppen von Jamf Pro können Sie einzelne Geräte oder Gerätegruppen auf intelligente Weise zielgerichtet konfigurieren. Mit der intelligenten Zielgruppenorientierung von Jamf Pro erfassen Sie die Bestandsdaten aller verwalteten Geräte und lösen bei Bedarf automatisch Maßnahmen aus, die die ganze Gruppe oder eine Untergruppe betreffen. Wenn beispielsweise weitere Mitarbeiter künftig extern arbeiten, können Sie all diese Mitarbeiter einer intelligenten Gruppe zuweisen und jedem Gerät in der Gruppe automatisch ein VPN-Konfigurationsprofil bereitstellen, um einen nahtlosen Zugriff auf Unternehmensressourcen zu gewähren.

Sie haben alternativ die Möglichkeit, den Mitarbeitern Elemente per Self Service on-demand zur Verfügung zu stellen. Die IT-Mitarbeiter richten den Self Service App-Katalog mit freigegebenen Konfigurationen, Ressourcen, Skripts zur Behebung gängiger Probleme, Lesezeichen und vertrauenswürdigen Apps ein, die die Mitarbeiter dann eigenständig herunterladen und nutzen können. Die Benutzer sind so in der Lage, jederzeit und von jedem Standort aus auf alle Ressourcen zuzugreifen, ohne dass in der IT-Abteilung auch nur eine Helpdesk-Supportanfrage zu diesen Themen eintrifft.

Innovative App-Verwaltung

Die Wirtschaft stützt sich auf Apps. Die Verwaltungsstrategie des Unternehmens muss diese Tatsache auf angemessene Weise berücksichtigen. Durch die Integration mit Apple Business Manager können Apps über Jamf Pro im App Store gekauft (oder im App-Verzeichnis Ihres Unternehmens bestellt) und direkt auf den Geräten bereitgestellt werden. Auch diese Apps können im Push-Verfahren auf die Geräte übertragen oder per Self Service bereitgestellt werden.

Die Bereitstellung der aktuellsten Apps und Betriebssystemversionen ist für die Sicherheit des Geräts und des Unternehmens ebenfalls von großer Bedeutung. Mit Jamf Pro und Jamf Now kann die IT-Abteilung Apps und Betriebssysteme auf effiziente Weise bereitstellen und den Vorgang mithilfe von Bestandsmeldungen überwachen.

Sie können die Verfügbarkeit neuer Betriebssystemversionen auch hinauszögern, um den IT-Mitarbeitern Gelegenheit zu geben, neue Betriebssystemversionen zu prüfen, bevor diese für die Endanwender verfügbar gemacht werden. Dies ist eine weitere Möglichkeit, wie Jamf Pro den IT-Helpdesk entlasten kann und die Benutzer befähigt, auch ohne IT-Support erfolgreich zu arbeiten.

Besserer Schutz für Macs

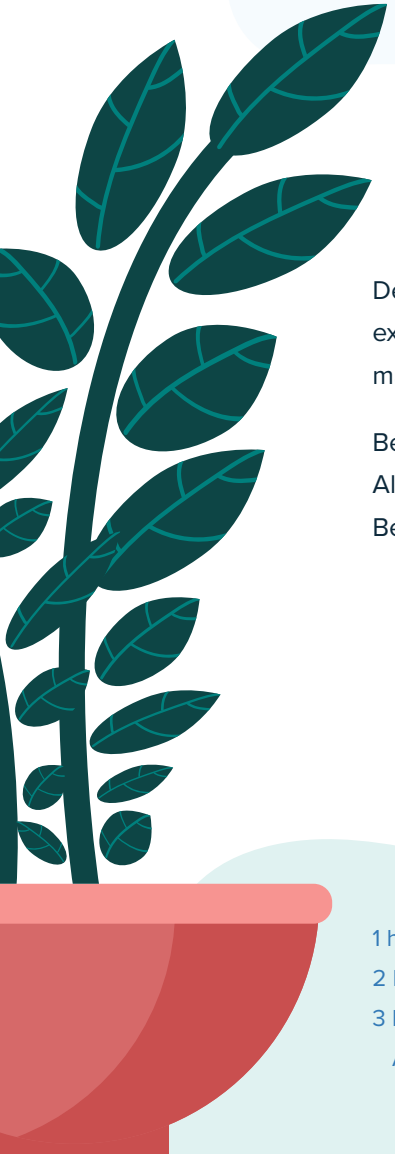
Wenn immer mehr Mitarbeiter Macs für die Arbeit nutzen, ist eine Sicherheitslösung speziell für Macs nötig. Nutzen die Mitarbeiter zuhause ihre eigenen Computer, entstehen dadurch neue Gefahren durch Angriffe auf Unternehmensressourcen. Mitarbeiter besuchen möglicherweise Websites, die sie in einem Unternehmensnetzwerk normalerweise nicht öffnen würden, nutzen die Geräte für private E-Mails oder gestatten es ihren Kindern, auf einer Website Spiele zu spielen. Wenn dadurch Malware auf ein Gerät gelangt, stehen die Mitarbeiter der Sicherheits- und IT-Abteilung vor der zusätzlichen Herausforderung, solche Angriffe ferngesteuert abzuwehren.

Durch die Nutzung von nativen Apple Sicherheitstools – wie beispielsweise dem neuen Endpoint Security Framework von Apple und der Analyse von macOS Systemereignissen auf dem Gerät – bietet Jamf Protect benutzerdefinierte Sicherheitsanalysen und Erkennungsfunktionen, die Spezialisten für Gerätesicherheit oder aber auch IT-Administratoren in Unternehmen unübertroffene Transparenz bei ihrem gesamten Bestand an Macs liefern, unabhängig vom Standort.

Mit Jamf Protect und Jamf Pro verfügen Sie über einige der besten Tools auf dem Markt, um Vorfälle mit Macs zu identifizieren und zu beheben, ohne dass die Geräte jemals in das Unternehmensnetzwerk eingebunden werden müssen:

- Empfangen Sie in Echtzeit Warnmeldungen über verdächtige Aktivitäten.
- Untersuchen Sie auf den Geräten erfolgte Aktivitäten.
- Richten Sie proaktiv Sperren gegen bekanntermaßen schädliche Apps ein.
- Isolieren Sie ein Gerät von kritischen Ressourcen.
- Entfernen Sie schädliche Dateien von den Geräten.
- Stellen Sie macOS und installierte Apps erneut bereit.

Schaffen Sie ein modernes Arbeitsumfeld für Mitarbeiter im Homeoffice



Die aktuelle Gesundheitskrise ist nur ein Grund von vielen, Workflows einzurichten, mit denen Sie sicherstellen können, dass Mitarbeiter ganz unabhängig von ihrem Standort sicher und produktiv arbeiten können.

Der Trend zum Homeoffice wird sich weiter fortsetzen. Um eine positive Unternehmenskultur aufrechtzuerhalten, müssen externe Mitarbeiter auf dieselbe Weise befähigt und gestärkt werden wie ihre internen Kolleginnen und Kollegen. Jamf macht dies möglich und bietet den Mitarbeitern gleichzeitig optimale Benutzerfreundlichkeit und maximale Sicherheit.

Bereiten Sie sich schon heute auf den massiven Umstieg in das Homeoffice vor und testen Sie Jamf am besten noch heute. Als Kunde profitieren Sie von mehr als 130 kostenlosen Online-Schulungsmodulen über die optimale Nutzung von Jamf zur Befähigung und Stärkung Ihres Personals.

Testversion

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

1 https://www.talentlms.com/blog/remote-work-statistics-survey/
2 https://b2b-assets.glassdoor.com/the-true-cost-of-a-bad-hire.pdf
3 https://342sv54cwf1w32bxz36tm0bv-wpengine.netdna-ssl.com/wp-content/uploads/2015/05/AD-Password-reset-tool.pdf