jamf

WHITE PAPER

Überlegungen zur Sicherheit in Bezug auf Apple im Unternehmen

Dieses Whitepaper befasst sich mit gängigen Sicherheitsdiskussionen und erläutert, was Unternehmen über die Apple Plattform wissen müssen, damit die Mitarbeiter interner Teams über Best Practices in puncto Sicherheit informiert sind, bevor sie Apple Geräte in ihre Umgebung integrieren.

Folgende Themen werden behandelt:

- Geräteverwaltungskonzept von Apple
- Sicherheitsmerkmale, die es nur bei Apple gibt
- Überlegungen bei der Einbindung neuer Apple Geräte
- Verfügbare Apple Integrationen für die Nutzung bereits vorhandener Ressourcen

Struktur des Apple Ökosystems

Herangehensweise an die Apple Geräteverwaltung
Apple entwickelte die iOS und macOS Plattformen mit einer integrierten Konzeption für Hardware, Software und Services. Diese sind von Grund auf zuverlässig und sicher. Sie erleichtern IT-Abteilungen die Konfiguration, Implementierung und Verwaltung. So wie Mitarbeiter eine einheitliche Benutzerführung beim Einsatz von iPhone, iPad und Mac bei der Arbeit erwarten, so sollten auch IT-Experten eine einheitliche Benutzerführung bei der Verwaltung der beiden Plattformen für die Mitarbeiter erwarten dürfen.

Apple bietet spezielle Programme für Unternehmen, die die Optimierung der Bereitstellung und der Sicherheit unterstützen und dafür sorgen, dass die Benutzer ihre Geräte sofort nach dem Auspacken einsetzen können. Das Programm zur Geräteregistrierung (DEP) und das Programm für Volumenlizenzen (VPP) von Apple ermöglichen in Verbindung mit Mobile Device Management (MDM) eine einheitliche, gesicherte Verwaltung von Mac, iPad, iPhone und Apple TV Geräten.

Viele Unternehmen setzen auf ein einziges Tool, um die Anforderungen aller ihrer Apple, Microsoft und Google Geräte zu erfüllen. Dies führt bei den Unternehmen zu Mängeln in Bezug auf die Verwaltung, Benutzerfreundlichkeit und Sicherheit. Wenn ein einziges Management-Tool zur Verwaltung mehrerer Plattformen verwendet wird, können die Sicherheitsfunktionen nicht ordnungsgemäß genutzt werden, und der Nutzen von Apples integrierter Vorgehensweise geht verloren.

Das Apple Framework

Um die Sicherheitskonzeption von Apple ausdrücken zu können, muss man zunächst die Grundlagen des Apple Framework kennen.

Apple Bereitstellungsprogramme

Management framework

Apple Sicherheitsfunktionen

Apple Betriebssysteme

Basis der Apple Betriebssysteme

UNIX

Unterschiede zwischen der Verwaltung unter Apple und unter Microsoft

Wie unterscheidet sich Apple von der herkömmlichen Microsoft Endgeräteverwaltung

Der Schlüssel zur Benutzerfreundlichkeit von Apple ist die integrierte Verwaltungsarchitektur, die als Mobile Device Management (MDM) bezeichnet wird. Mit MDM kann die IT-Abteilung Konfigurationsprofile erstellen, die verschiedene Betriebssystemeinstellungen definieren. Die Profile werden drahtlos über den Apple Push Notification Service (APNs) bereitgestellt. Der APNs hält ständige Verbindung zu den Apple Geräten, sodass sich die IT-Abteilung nicht darum kümmern muss. MDM erschließt Verwaltungsfunktionen, die Windows Administratoren nur ansatzweise durch Bindung oder Gruppenrichtlinienobjekte (GPO) zur Verfügung stehen.

Beeinflusst der APNs unsere Einstellung zur Sicherheit?

Bei APNs handelt es sich um einen stabilen, sehr effizienten Dienst für die Verbreitung von Informationen an iOS, watchOS, tvOS und macOS Geräte. APNs ist ein entscheidender Aspekt der Apple Bereitstellungsprogramme und anderer Sicherheitsfunktionen wie etwa Fernsperren und Fernlöschen. Die Programme und Services von Apple, also z. B. DEP, VPP oder MDM, funktionieren nur mit eingerichtetem APNs, da diese nicht über eine Proxy-Verbindung genutzt werden können. Der Zugriff auf die Programme muss über eine Direktverbindung zu Apple erfolgen, also über APNs.

Weitere Vorteile von APNs:

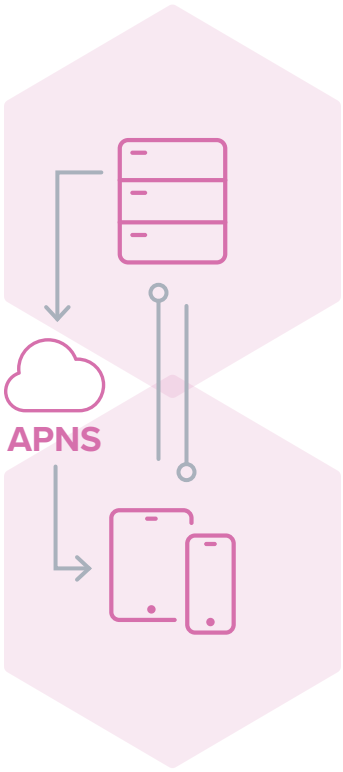
- Erweiterte Sicherheit bei der Verwaltung von unternehmenseigenen Apple Geräten. Dank APNs können Sie ein verloren gegangenes, gestohlenes bzw. angegriffenes Gerät drahtlos ferngesteuert sperren bzw. löschen.
- MDM nutzt APNs zum Senden wichtiger Befehle, z. B. für Softwareinstallationen oder Bestandsaktualisierungen.
- MDM-Konfigurationsprofil-Payloads können macOS zwar auch „offline“ bereitgestellt werden. Diese Methode ist jedoch wesentlich aufwändiger als die drahtlose Verwaltung.
- APNs veranlasst jedes Gerät, sich automatisch beim MDM-Server anzumelden

Diese einzigartige Technologie, die als Herausforderung in Sachen Sicherheit erscheint, bietet viele Vorteile.

Viele Dienste von Google und Microsoft verlangen mittlerweile dasselbe Maß an Vertrauenswürdigkeit und eine direkte Verbindung wie APNs. Die VOIP-Lösungen für iOS von Cisco nutzen APNs für Push-Meldungen und Callkit. APNs ist für die Sicherheit und die Benutzerfreundlichkeit entscheidend. Dienste wie App Store, iCloud Authentifizierung und Internet-Wiederherstellung funktionieren ohne APNs nur eingeschränkt oder überhaupt nicht. Wenn Sie die Ports gemäß den Spezifikationen von Apple öffnen, erledigt sich alles andere von selbst.

Weitere Informationen finden Sie auf der Apple Website: https://help.apple.com/deployment/macos/#/ior9d28751c0.

Architektur des Apple Push Notification Servers



Erfordert Apple Software anderer Anbieter?
Im Gegensatz zu Windows oder Android werden bei Apple Geräten zusätzliche Sicherheitsstufen oder Zusatztools anderer Hersteller seltener genutzt.

Windows-orientierte Sicherheitsunternehmen neigen üblicherweise dazu, hinter den Entwicklungszyklen von Apple zurückzubleiben, was die Gefahr birgt, die Übernahme neuer Betriebssysteme und Sicherheitssysteme zu verlangsamen. Wenn man Apple wie jede andere Plattform behandelt, hindert dies die Mitarbeiter oft daran, ihre Systeme mit maximaler Produktivität zu nutzen. Zudem schränkt dies die Benutzerfreundlichkeit ein, für die Apple bekannt ist. Darüber hinaus kommt es bei der Anpassung einer Windows Softwareversion an Apple Geräte fast immer zu einer mangelhaften Programmausführung, zu Speicherfressern und Fällen von KEXT-Panik (durch Kernel Extensions) – also zu endlosen IT- und Sicherheitsproblemen.

Die integrierte Verschlüsselung und der Virenschutz von Apple ermöglichen es vielen Unternehmen, ohne Produkte anderer Anbieter zu arbeiten. Einige suchen jedoch noch immer nach Lösungen für die Eindämmung von Datenlecks im Unternehmen. Datenlücken im Unternehmen können mithilfe von MDM überwacht werden; als Schutzvorkehrungen auf Netzwerkseite können zusätzliche Tools wie Cisco Security Connector eingesetzt werden.

Im Februar 2018 stellten Cisco, Apple, Aon und Allianz eine völlig neue Lösung für das Cyber Risk Management in Unternehmen vor. Diese umfasst die von Aon bereitgestellte Analyse der Widerstandsfähigkeit gegen Cyber-Angriffe, extrem sichere Technologie von Cisco und Apple sowie erweiterte Versicherungsschutzangebote von Allianz. Weitere Informationen zu dieser Partnerschaft finden Sie in der ungekürzten Ankündigung auf der Apple website.

Wie benutzerfreundlich ist die Verwaltung von Apple Geräten?
Im IT-Bereich galt bisher die Einstellung: „Die Qualität der von uns genutzten Tools für die Verwaltung von Apple reicht nicht an die Qualität der für unsere Windows Geräte genutzten Tools heran“. Diese Einstellung rührte von der falschen Vorstellung her, dass Apple schwieriger zu verwalten sei als andere Plattformen. Deshalb schreckten viele Unternehmen davor zurück, Apple Geräte anzubieten und zu unterstützen.

Umfragen haben jedoch gezeigt, dass die Verwaltung von Apple sogar einfacher ist als die anderer Plattformen. Laut einer Umfrage von Dimensional Research gaben 66 Prozent der Befragten an, dass Macs einfacher abzusichern sind als andere PCs. Zudem gaben 90 Prozent der Befragten an, dass iOS einfacher abzusichern ist als andere mobile Plattformen. Ähnliche Ergebnisse erbrachte die Frage, ob die Bereitstellung, Konfiguration und der Support von Apple Geräten einfacher sei.

Der Branchengigant IBM ist eines der vielen Unternehmen, die ein Employee Choice Programm für Mitarbeiter anbieten, das auch die Apple Plattform beinhaltet. Fletcher Previn, der jetzige CIO von IBM, hat nachgewiesen dass IBM mit jedem Mac, für den sich die Mitarbeiter anstatt eines PC entschieden haben, sogar Geld verdient und einspart.

Dies zeigt, dass im Unternehmen großer Bedarf an einer einheitlichen Bereitstellung und Benutzererfahrung herrscht. Apple bietet diese Einheitlichkeit und Sicherheit ganz ohne zusätzlichen Aufwand.

66%
der befragten Unternehmen gaben an, dass Macs einfacher abzusichern sind als PCs.

90%
der befragten Unternehmen gaben an, dass iOS einfacher abzusichern ist als andere mobile Plattformen.

Sicherheitsmerkmale, die es nur beim Apple Ökosystem gibt

Welche Sicherheitsmerkmale sind in macOS integriert?
Die Basis von macOS bildet eine integrierte, sichere Software.

Folgende Systemsicherheitsmerkmale sind in macOS integriert:

- **FileVault** iist eine zusätzliche Verschlüsselungsebene, die in macOS integriert ist und die Benutzerdaten bei Geräteverlust bzw. -diebstahl schützt.
- **Softwareaktualisierungen** cstammen direkt von Apple und werden von Apple digital signiert, sodass sich das Unternehmen und seine IT-Abteilung sicher sein können, dass sie vertrauenswürdig sind.
- Der **Systemintegritätsschutz (SIP)** schützt zentrale Betriebssystemdateien, die andernfalls das Ziel von Exploits durch Benutzer- und Anwendungszugriffe sein könnten.
- Die IT-Abteilung kann mithilfe von **Gatekeeper** definieren, von wo die Benutzer Apps laden dürfen. So wird verhindert, dass unsignierte Apps (oder Malware) ausgeführt werden können. Die Verbreitung von Malware wird daher im Zusammenspiel mit XProtect schnell unterbunden.
- **XProtect** ist ein automatisches Anti-Malware-Dienstprogramm, das von Apple immer auf dem neuesten Stand gehalten wird. Dies verhindert, dass Schadsoftware bzw. häufig veraltete, anfällige Plug-Ins wie Java und Flash auf dem Mac ausgeführt werden können.
- **Tool zur Entfernung von Malware**. Apple kann Malware entfernen, die dennoch auf das System gelangen konnte.
- Alle im **App Store** erhältlichen Apps werden von Apple geprüft; es sind nur von Apple zugelassene Ressourcen erhältlich. Apple kann die Verfügbarkeit von Apps sofort einstellen und Entwicklerzertifikate widerrufen.
- Durch **App Sandboxing** wird sichergestellt, dass Apps keine Daten aus dem System oder von anderen Apps weitergeben (oder unbefugt nutzen.
- Die Benutzer und die IT-Abteilung können die **Datenschutzeinstellungen** festlegen. Dabei handelt es sich um einen transparenten Prozess, der die Benutzer darüber informiert, dass Ortungsdienste genutzt werden, welche Apps Zugriff auf Kontakte oder Kalender haben und welche Informationen an Apple bzw. an App-Entwickler weitergeleitet werden.

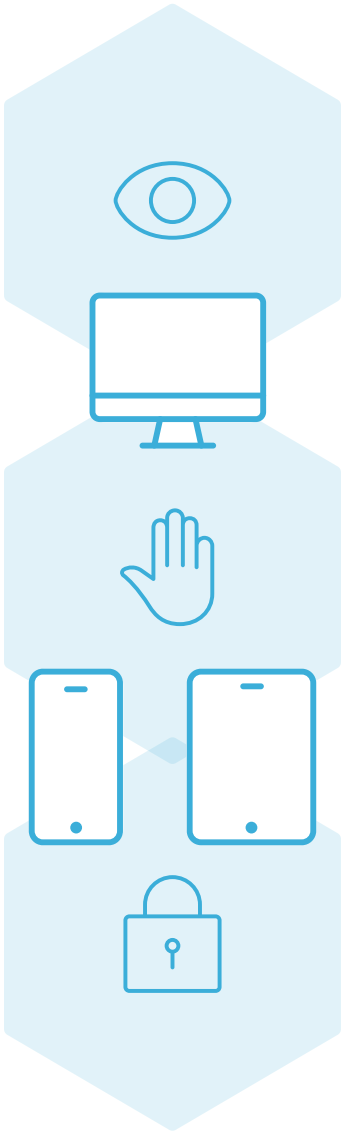
Eine ungekürzte Liste der Sicherheitsfunktionen des Mac finden Sie unter: https://www.apple.com/macos/security/.

Weshalb sollten wir FileVault zur Datenträgerverschlüsselung nutzen?
FileVault ist die integrierte Datenträgerverschlüsselung von macOS. Deshalb braucht die IT-Abteilung keine zusätzliche Software einzusetzen, um Datenträger zu verschlüsseln. Die Funktion kann manuell aktiviert werden, oder die IT-Abteilung kann diese ferngesteuert auf allen Macs aktivieren. Verschlüsselungscodes können zentral verwaltet werden, so dass die IT-Abteilung auf die erforderlichen Daten zugreifen kann, auch nachdem der betreffende Mitarbeiter das Unternehmen verlassen oder sein Passwort vergessen hat und Hilfe beim Einloggen benötigt. Verschlüsselungscodes lassen sich auch problemlos rotieren, um die Sicherheit zu erhöhen.

Welche Sicherheitsmerkmale sind in iOS integriert?
Viele der zentralen Sicherheitsfunktionen für Mac sind auch für iPad und iPhone verfügbar. Dies gewährleistet eine einheitliche, sichere Nutzung des gesamten Apple Ökosystems:

- Zu den Systemsicherheitsmerkmalen zählen unter anderem Secure Boot, Autorisierung der Systemsoftware und Secure Enclave. Sie gewährleisten, dass die Sicherheit des Betriebssystems nicht beeinträchtigt wird. Die IT-Abteilung ist auch in der Lage, das gesamte Betriebssystem iOS zu löschen und das Gerät komplett neu aufzusetzen.
- Bei Touch ID / Face ID wird mithilfe des Fingerabdrucksensors bzw. der Gesichtserkennung der Anmeldevorgang vereinfacht und sichergestellt, dass nur autorisierte Benutzer auf das Gerät zugreifen können.
- Durch Verschlüsselung und Datenschutz wird sichergestellt, dass private und geschäftliche Daten nicht gefährdet werden können, auch wenn andere Aspekte des Geräts durch Diebstahl oder Verlust gelöscht wurden.
- Der Betreuungsmodus ist ein zusätzliches Funktionsmerkmal, mit dem die IT-Abteilung in strenger kontrollierten Umgebungen zusätzliche Verwaltungsfunktionen nutzen kann.

Eine ungekürzte Liste der Sicherheitsfunktionen von iOS finden Sie unter: https://www.apple.com/business/docs/iOS_Security_Guide.pdf.



Überlegungen bei der Einbindung neuer Apple Geräte

Wie können wir die Sicherheit unserer Apple Geräte nachweisen?
Die Apple Geräteverwaltung basiert auf der Möglichkeit, Konfigurationsprofile zu erstellen. Durch die Erstellung von Konfigurationsprofilen mit einer MDM-Lösung (Mobile Device Management) wie Jamf Pro kann die IT-Abteilung die Nutzung von Passwörtern erzwingen, Einstellungen einschränken, Netzwerkprotokolle definieren, VPN-Einstellungen und E-Mail-Accounts konfigurieren und vieles mehr. Die IT-Abteilung kann dann alle diese Einstellungen auf den verwalteten Geräten bereitstellen.

Weshalb benötigen wir keine App-Container?
Apple-zentrierte Verwaltungstools wie Jamf Pro werden verwendet, um genehmigte Apps auf Geräten bereitzustellen und um zu verhindern, dass nicht genehmigte Apps auf Geräte gelangen. iOS unterstützt bereits die Verwaltung von unternehmenseigenen Apps über das native App-Management mithilfe von Lösungen wie Jamf Pro. Diese Verwaltungsmethode trennt Unternehmensdaten von privaten Daten und verwaltet den Datenfluss ohne Container-Apps, die die Leistung verlangsamen bzw. mit jeder neuen Betriebssystemversion unbrauchbar werden.

Welche Sicherheitsvorkehrungen für den Mac gibt es außerhalb des MDM-Frameworks?
Lösungen wie Jamf Pro gehen für macOS über die grundlegende Geräteverwaltung mit dem Jamf Agent hinaus. Der Jamf Agent ist eine Binärdatei, die installiert wird, nachdem ein Mac für die Verwaltung registriert wurde. Auf diese Weise kann die IT-Abteilung einen verborgenen Administrator-Account erstellen, der Remote-Root-Zugriff auf alle verwalteten Mac Geräte gewährt.

Mit installiertem Jamf Agent kann die IT-Abteilung erweiterte Richtlinien und Skripte ausführen, Software wie z. B. Adobe installieren, die nicht im App Store erhältlich ist, und vieles mehr. Dies erweitert die Anpassungs- und Verwaltungsmöglichkeiten über den Leistungsumfang von MDM hinaus.

Wie können wir die Compliance der Apple Geräte in unserer Umgebung prüfen, durchsetzen und melden?

In stark regulierten Branchen sind ggfs. regelmäßige zeitraubende Audits vorgeschrieben. Für Compliance-Prüfungen ist es daher wichtig, dass der Nachweis erbracht werden kann, dass die Geräte tatsächlich verwaltet werden und sicher sind.

Die Bestandserfassung ist der Schlüssel zur Erfüllung der gesetzlichen Vorschriften und der unternehmensinternen Sicherheitsanforderungen. Zu wissen, wie viele Geräte sich in der Unternehmensumgebung befinden, wer welches Gerät nutzt, welchen Status die Software-Updates haben, welche Profile und Einstellungen den einzelnen Geräten zugewiesen wurden, welcher Verschlüsselungsstatus und welche Einschränkungen und Konfigurationen angewendet werden, ist der Schlüssel zur Integrität und Sicherheit der Umgebung.

Lösungen wie Jamf Pro ermöglichen es der IT-Abteilung, Berichte über eine nahezu unbegrenzte Anzahl an Bestandskategorien zu erstellen, um Unternehmen dabei zu unterstützen, bessere Geschäftsentscheidungen zu treffen und die Einhaltung der Vorschriften nachzuweisen. Wenn ein Gerät nicht mehr den Vorschriften entspricht, kann dieses Problem durch die Bereitstellung von Konfigurationsprofilen für das entsprechende Gerät wieder behoben werden.

Wenn mehrere Geräte den Vorschriften nicht mehr entsprechen oder die gesamte Umgebung geprüft werden muss, können Sie mithilfe von Jamf Pro dynamische, smarte Gruppen von Geräten erstellen. Smarte Gruppen basieren auf erweiterten, von der IT-Abteilung definierten Bestandskriterien. Sie können ausgehend vom Bestandsbericht automatisierte Administrationsmaßnahmen auslösen.

Wie werden Patches für macOS Software anderer Anbieter implementiert?
Software kann schnell veraltet sein. In diesem Fall können das Gerät, die Daten und das Netzwerk anfällig für interne und externe Bedrohungen werden. Diese Schwachstellen können mithilfe des Patch-Managements schnell und effizient behoben werdent.

Die Patch-Verwaltungsfunktionalität Ihrer MDM-Lösung sollte es der IT-Abteilung ermöglichen, Patch-Warnungen zu empfangen, wenn aktualisierte Versionen der Software anderer

Anbieter verfügbar sind. In diesem Fall sollte es der IT-Abteilung möglich sein, Softwarepakete mit dem entsprechenden Patch (aktualisierte Softwareversion) zu erstellen, den Patch auf den entsprechenden Geräten bereitzustellen und dann einen Patch-Bericht über die Bestandsverwaltung zu empfangen, um sicherzustellen, dass der Patch korrekt installiert wurde.

Indem Unternehmen sofort darüber informiert werden, welche Apps und welche Software veraltet sind, und dann schnell Maßnahmen ergreifen können, um sicherzustellen, dass jeweils die aktuellste und sicherste Version installiert ist, können sie eine proaktive Herangehensweise an die Sicherheitsabläufe verfolgen.

Warum sollten wir unsere Apple Geräte nicht an Active Directory anbinden?
Für den Mac gilt eine andere Strategie als die herkömmliche 1-zu-1-Implementierung. Mit Tools wie Jamf Pro, Enterprise Connect und NoMAD gehört die Anbindung der Vergangenheit ein. Die Anbindung macht DEP-Workflows komplizierter, wenn die Domain-Controller einer Organisation nicht von außen zugänglich sind. Zudem verlieren Organisationen, die die Anbindung nutzen, die Möglichkeit, Macs außerhalb des Büros, z. B. durch DEP, automatisch aufzusetzen. Zwar stellt die Anbindung eine Option dar. Unternehmen, die eine Lösung wie Jamf Pro verwenden, können jedoch lokale Accounts verwalten, um dieselben Anforderungen an die Komplexität und den Ablauf von Kennwörtern umzusetzen, ohne sich Gedanken über Verbindungen oder eine unterbrochene Synchronisation mit AD machen zu müssen. Dies bedeutet weniger Passwortabfragen für die Endanwender und weniger Anrufe beim IT-Helpdesk..

Wie funktionieren Cloud-Dienste mit Apple Geräten?
Die Verlagerung in die Cloud nimmt zu. Beim Cloud-Hosting ist der Zugriff auf die Datenbank beschränkt. Wenn diese sich auf einem Server in Ihrem eigenen Netzwerk befindet, ist dies nicht der Fall. Seit Jahrzehnten haben Unternehmen „Mauern“ um sich herum errichtet und Netzwerk-Perimeter als erste Verteidigungslinie eingesetzt. Da die Arbeit immer mobiler wird und Daten nicht mehr nur hinter der Firewall anfallen, müssen Unternehmen zu einem moderneren, identitätsbasierten Sicherheitsmodell übergehen.

Microsoft verschiebt Unternehmensdaten mit Azure Active Directory in die Cloud. Um sicherzustellen, dass nur vertrauenswürdige Benutzer auf vertrauenswürdigen Geräten mit vertrauenswürdigen Apps auf die Unternehmensdaten in der Cloud zugreifen, bieten Microsoft und Jamf eine exklusive Integration für einen proxyfreien Conditional Access an.

Weitere Informationen finden Sie hier: https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/.

Die Zunahme mobiler Arbeitsplätze und die zunehmende Nutzung von Cloud-Computing-Modellen ist keine Modeerscheinung

85%
aller Organisationen speichern vertrauliche Informationen in der Cloud.

80%
aller Mitarbeiter nutzen nicht genehmigte SaaS-Apps bei der Arbeit.

41%
aller Mitarbeiter geben an, dass mobile Apps für Unternehmen ihre Arbeitsweise verändert haben.

Wie setzen wir branchenübliche Sicherheitsstandards durch?
Die Durchsetzung hängt davon ab, welche Sicherheitsstandards gelten und welche Compliance-Standards eingehalten werden müssen. SOC 2 unterscheidet sich von HIPAA, PCI von CIS. Zu wissen, woran man sich halten muss, ist ein wichtiger erster Schritt.

Jamf Pro bietet einen flexiblen Rahmen, der Sie dabei unterstützt, viele gängige Vorschriften einzuhalten. Die IT-Abteilung kann einfach die geltenden Richtlinien angeben, die entsprechenden Profile und Richtlinien erstellen und anwenden. In diesem Zusammenhang können beispielsweise Funktionen für Privatkunden wie iCloud Drive eingeschränkt werden; es kann festgelegt werden, dass Gatekeeper nur das Herunterladen abgesicherter Apps zulässt, dass Mac Computer mithilfe von FileVault verschlüsselt werden oder dass Apps eingeschränkt werden, indem auf allen verwalteten Apple Geräten (oder auch in macOS) nach einer eingeschränkten App gesucht und diese dann gelöscht wird. Die IT-Abteilung muss lediglich die Einstellungen definieren, anhand dieser Informationen Konfigurationsprofile und -richtlinien erstellen und diese auf die Geräte anwenden.

In diesem Whitepaper erfahren Sie, wie Sie die Richtlinien des Center for Internet Security (CIS) einhalten können: https://www.jamf.com/resources/white-papers/macos-security-checklist/.

Weshalb sollten wir Apple Bereitstellungsprogramme nutzen?

Die Apple Bereitstellungsprogramme für Unternehmen (DEP und VPP) sind kostenlos und nur bei Apple erhältlich. Diese Programme bieten nicht nur mehr Sicherheit, sondern bieten sie auch der IT-Abteilung die Möglichkeit zur Automatisierung und Personalisierung der Geräteeinrichtung in größeren Stückzahlen.

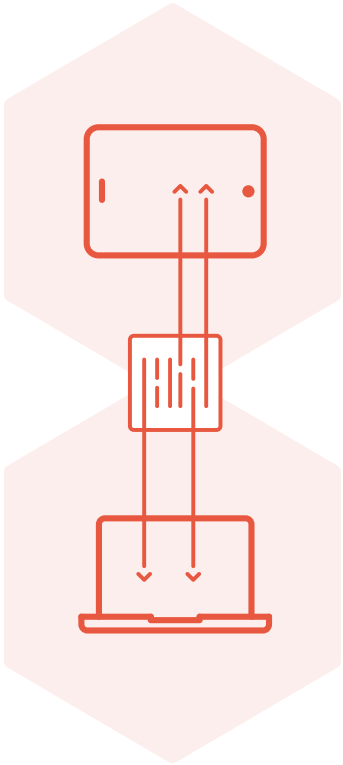
- DEP ist die bevorzugte Methode von Apple, um unternehmenseigene Apple Geräte abzusichern und zu verwalten. DEP ermöglicht die Implementierung ohne Benutzereingriff. Dadurch entfallen die herkömmliche Erstellung von Images oder auch die Notwendigkeit der manuellen IT-Konfiguration. Die Benutzer können sich schnell und nahtlos in der Umgebung registrieren, was die Einarbeitungszeit minimiert und die Endgeräte mit nur wenigen Klicks absichert. Direkt bei Apple oder bei autorisierten Apple Händlern bestellte Geräte können am DEP-Programm zur Geräteregistrierung teilnehmen. Sie werden dann bei der Ersteinrichtung automatisch für die Verwaltung registriert.
- Bei macOS, iOS und tvOS Geräten ermöglicht DEP die Nutzung zusätzlicher Kontrollmechanismen, die eine noch detailliertere Verwaltung ermöglichen.
- In Verbindung mit MDM (Mobile Device Management), der integrierten Verwaltungsarchitektur von Apple, wird der Endzustand der Geräte der jeweiligen Benutzer durch eine dynamische Methode erzielt, die deren Anforderungen erfüllt. Es wird kein undifferenziertes Einheits-Image erstellt.
- Mithilfe von VPP kann die IT-Abteilung Lizenzen für Apps aus dem App Store erwerben und die Software dann an Einzelpersonen oder an Geräte verteilen. Wenn Apps direkt an die Geräte verteilt werden, sind keine Apple IDs erforderlich. Apple IDs dienen der Identifizierung von Benutzern. Mit ihrer Hilfe können Benutzer auf Apple Services wie iCloud, iTunes und den App Store zugreifen.
- Die IT-Abteilung kann gekaufte VPP-Apps verwalten und zur erneuten Nutzung zurückfordern, wenn Mitarbeiter das Unternehmen verlassen oder eine bestimmte App nicht mehr benötigen.

"Not every Apple device management solution supports Apple's programs and services. Check with your vendor to ensure they support these programs, as well as the incremental changes."

Verfügbare Apple Integrationen für die Nutzung bereits vorhandener Ressourcen

Wie lässt sich Apple (und Jamf) in unsere bereits vorhandene IT-Technologieinfrastruktur integrieren

Organisationen, IT-Abteilungen und Mitarbeiter agieren nicht in einer geschlossenen Blase. Apple hat sein Engagement für Unternehmen durch die Zusammenarbeit mit Technologieunternehmen wie Cisco unter Beweis gestellt, um moderne und sichere Business Services bereitzustellen.



Viele Unternehmen benötigen Serviceleistungen außerhalb des Apple Ökosystems. Dank sicherer, kompatibler Integrationen können Organisationen alle Aspekte ihrer Umgebung nutzen und vielfältige Dienste nutzen, um das Unternehmen voranzubringen.

Einige Beispiele hierfür:

- Die API von Jamf bietet die Flexibilität, Integrationen für vorhandene IT-Tools zu entwickeln.
- Microsoft EMS Integration mit Jamf bietet eine exklusive, proxylose Integration für den Conditional Access auf dem Mac.
- Cisco ISE dient dazu, Sicherheits- und Zugriffsrichtlinien für Geräte zu entwickeln und durchzusetzen, die mit dem Netzwerk eines Unternehmens verbunden sind.
- Cisco Fast Lane spart Netzwerkbandbreite durch Priorisierung von Apps und durch automatische Konfiguration der Dienstgüte.
- ServiceNow automatisiert IT- und Geschäftsabläufe für die Betriebsführung

Moderne Organisationen steigen auf Unternehmenstools wie Cisco um. Dabei bietet der Einsatz von Jamf für die Mac Verwaltung eine vollständig integrierte Lösung, ohne an einer unterstützten Plattform zu sparen.

Zudem hat das im Bereich der Identitätsverwaltung tätige Unternehmen Okta Inc. in dem vor kurzem erschienenen Sicherheitsdatenbericht verschiedene Erkenntnisse veröffentlicht, die klar auf eine zunehmende Verbreitung von Cybersicherheitsanwendungen in Unternehmen hindeuten. Alle mit Jamf vergleichbaren Sicherheitstools befanden sich erstmalig in diesem Jahr unter den ersten 15 Apps mit den schnellsten Zuwächsen.

Apple + Jamf = unübertroffene Geräteverwaltung und Sicherheit
Die sicherste Plattform erfordert die robusteste Verwaltungslösung, um sicherzustellen, dass alle möglichen Sicherheitsfunktionen durchgesetzt und installiert werden. Kein anderes MDM-Unternehmen ermöglicht eine so gute Integration mit Apple und den Apple Services wie Jamf, und kein Anbieter ist so gut aufgestellt, um den Erfolg beim Einsatz von Apple Geräten sicherzustellen.

Aus diesem Grund vertrauen sicherheitsbewusste Unternehmen wie beispielsweise 15 der 25 größten Fortune 500-Unternehmen und acht der zehn führenden Technologieunternehmen bei der Verwaltung ihrer Apple Umgebung auf Jamf.

Jamf bietet Support für alle Apple Betriebssysteme und Funktionen ab dem allerersten Tag. Unternehmen, die ihre Mitarbeiter mit Apple unterstützen wollen, vertrauen auf Jamf als Produkt erster Wahl.

Jamf bietet die notwendigen Tools, um 100 oder auch 100.000 Apple Geräte abzusichern. Gleichzeitig haben Unternehmen die Freiheit, sich auf ihre strategischen Aufgaben zu konzentrieren, die Zeit sparen, die Benutzerfreundlichkeit verbessern und den Erfolg des Unternehmens voranbringen.

96 Prozent der Kunden von Jamf verlängern ihre Verträge Jahr für Jahr. Weitere Informationen darüber, wie Sie Jamf Pro für die Apple Geräteverwaltung nutzen können, finden Sie unter jamf.com/de/produkte/jamf-Pro

jamf

www.jamf.com

Um mehr darüber zu erfahren, wie sie Jamf Pro für die Verwaltung Ihrer Macs oder iOS nutzen können, besuchen Sie **jamf.com/de/produkte/jamf-pro**