Der Leitfaden für Fortgeschrittene zum iOS/iPadOS Management

Die Sicherheitslandschaft

Die Cybersicherheit wird weiter verbessert.
Laut dem kürzlich veröffentlichten PwC-Bericht „ 2023 Global Digital Trust Insights" hat sich die Cybersicherheit seit 2020 in vielerlei Hinsicht verbessert: Mehr als 70 % der 3.522 C-Suite-Führungskräfte aus einem breiten Spektrum von Branchen und globalen Standorten haben 2021 Verbesserungen der Cybersicherheit eingeleitet.

Wir haben noch einen langen Weg vor uns.
38 % der Befragten glaubten, dass sie die Risiken im Zusammenhang mit der Ermöglichung von Remote- und Hybridarbeit vollständig gemindert haben, während 48 % der Meinung waren, dass sie diese Risiken vollständig gemindert haben. 35 % berichteten von einer vollständigen Entschärfung der Probleme im Zusammenhang mit einer rasch beschleunigten Cloud-Einführung.

Allerdings geben **nur drei Prozent an, dass sie aufkommende Cyber-Risiken** vollständig abgemildert haben. Nur fünf Prozent gaben an, dass sie alle fünf Aspekte des Sicherheits-Workflows - Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen - optimiert haben.

Und die Besorgnis nimmt mit der mobilen Technologie noch zu, da Malware, die in scheinbar harmlosen Apps versteckt ist, Schlagzeilen gemacht hat. Herkömmliche Firewall-basierte Sicherheits- und Verwaltungssysteme kommen mit mobilen Geräten einfach nicht zurecht, da es zum Wesen mobiler Geräte gehört, dass sie von entfernten Standorten aus auf Arbeitstools zugreifen können. Und wenn man die jüngste BYOD-Welle in Unternehmen hinzunimmt, gibt es eine Menge zu bedenken.

Wie können InfoSec- und IT-Administrator*innen also sicherstellen, dass alle Sicherheitsprotokolle in allen Bereichen der digitalen Umgebung, einschließlich und insbesondere iOS und iPadOS, vorhanden sind?

Nur

3%

berichten, dass sie neu auftretende Cyber-Risiken vollständig abgemildert haben

Richtige iOS Verwaltung ist sichere iOS Verwaltung

Dieser 201 Leitfaden zur Verwaltung von iOS und iPadOS Geräten, eine Fortsetzung unseres E-Books iPhone und iPad Verwaltung für Einsteiger, beschreibt, wie die Verwaltung von iOS und iPadOS Geräten der Schlüssel zur Sicherung Ihrer Apple Flotte ist. Eine ordnungsgemäße Verwaltung ist nicht das gesamte Bild der Sicherheitslandschaft, aber sie ist die Grundlage, auf der alle Unternehmen aufbauen müssen.

Lesen Sie weiter, um mehr darüber zu erfahren, wie eine ordnungsgemäße Verwaltung Sicherheit bedeutet. Außerdem werden wir die wichtigsten Funktionen, Arbeitsabläufe und Einstellungen behandeln, die für die sichere Verwaltung Ihrer iOS und iPadOS Flotte erforderlich sind, und alle Grundlagen abdecken.

PKI und Push-Zertifikate

PKI Zertifikate
Ein PKI-Zertifikat ist eine Textdatei, die Daten zur Identifizierung von Benutzer*innen und Geräten enthält. Im Grunde bestätigt es die Sicherheit des Mobilgeräts und sichert die Informationen, die von einem Ort zum anderen gehen, durch Verschlüsselung.

Die Verschlüsselung mit Zertifikaten sichert nicht nur die gesamte Kommunikation, sondern ermöglicht auch den sofortigen Entzug des Zugriffs durch Personen, die das Unternehmen verlassen, oder durch Geräte, die nicht mehr den Vorschriften entsprechen.

Zertifizierungen können für Single Sign-On (SSO), Anmeldeprofile, Geräteverwaltung mit Jamf Binary, Konfigurationsprofile und mehr verwendet werden. Administrator*innen können sie manuell über ein Webportal, durch Automatisierung mit einem Drittanbieter wie Jamf Connect oder durch eine direkte Zertifikatsanforderung bereitstellen: ein automatisierter Prozess, bei dem das Gerät über Jamf Pro mit dem Server kommuniziert.

Sie können das integrierte Zertifikat der Zertifizierungsstelle (CA) herunterladen, widerrufen und erneuern, ein integriertes Zertifikat aus einer Zertifikatsignierungsanforderung (CSR) erstellen und ein Backup erstellen.

Push-Zertifikate

Ein Push-Zertifikat ist eine verschlüsselte Datei, die von Apple generiert wird und die das Vertrauen zwischen einem Drittanbieterdienst wie Jamf Pro und dem Apple Push Notification Service (APNs) herstellt. Ein Push-Zertifikat wird von Apple erstellt, benötigt aber einen Dritten Service, wie Jamf, und APNs. Sie verwenden eine Apple ID, die einer Organisation gehört, und nicht eine persönliche Apple ID.

Push-Zertifikate ermöglichen die Kommunikation zwischen dem Jamf Pro Server und den APNs. APNs kontrollieren Informationen, insbesondere Informationen von Anwendungen, die an und von Geräten gesendet werden. Push-Benachrichtigungen sind die Art und Weise, wie Anwendungen auf Geräten Kommunikation erhalten.

Da es sich um eine von Apple verschlüsselte Datei handelt, können Sie eine App aus der Ferne auf der Grundlage dieser Sicherheitsinformationen deinstallieren.

Wie man Zertifikate findet

Unter iOS werden die Zertifikate im Schlüsselbund des Herausgebers gespeichert. Sie können eine Liste von Zertifikaten anzeigen, indem Sie sie in .csv-, .txt- oder XML-Dateien exportieren. Jamf Pro erleichtert dieses Verfahren, indem es einen IT-Administrator*in durch das Verfahren zur Erstellung eines Push-Zertifikats (.pem) und zum Hochladen in Jamf Pro führt. Sie benötigen eine gültige Jamf ID und Apple ID, und es ist wichtig, dass Administrator*innen diese Zertifikate auf dem neuesten Stand halten. Wenn sie verfallen, verlieren APNs die Konnektivität zu den Servern/Endgeräten der Mobilgeräteverwaltung (MDM).

Bedingter Zugriff

Wie bereits erwähnt, können die meisten Unternehmen kein Netzwerk mehr einrichten und Geräte und Benutzer über eine Firewall schützen - insbesondere mobile Geräte, die Mitarbeiter*innen häufig von zu Hause, unterwegs und auf Flügen nutzen.

Conditional Access ist eine Komponente in Microsofts Cloud, die es einem Unternehmen ermöglicht, Parameter für die Sicherung von Unternehmensdaten an mehreren Standorten festzulegen. Es kann den Zugang zu Unternehmensdaten wie E-Mail, OneDrive, Word und Excel sowie zu Cloud-Apps wie Jamf Pro sperren, indem es das Risiko zu diesem Zeitpunkt bewertet.

Die Anforderung eines vertrauenswürdigen Geräts und eines vertrauenswürdigen Benutzers für den Zugriff verbessert die Verwaltung und die Sicherheit, unabhängig davon, wo jemand arbeitet.

Organisatorische iPhones und iPads werden von Jamf verwaltet und über einen Cloud Connector oder einen manuellen Connector bei Microsoft Intune registriert. Die starke Partnerschaft zwischen Jamf und Microsoft stellt sicher, dass dies nahtlos funktioniert: Jamf sendet iOS und iPadOS Geräteinventar an Intune. Intune bewertet die Compliance und erstellt einen Compliancebericht. Azure AD erzwingt Zugriffskontrollen.

Geräte-Compliance

Bei der Geräte-Compliance gibt es viele bewegliche Teile, aber keinen, der mehr als Mobilgeräte ist. Erstens können diese Geräte auf verschiedene Weise erworben werden, z. B. direkt von Apple, über autorisierte Händler oder persönliche Geräte, die in einem BYO-Programm angemeldet sind. Zweitens bedeutet die Art der Personen, die iPads und iPhones im Unternehmen für die tägliche Arbeit nutzen, dass diese Organisationen eine zusätzliche Ebene von Compliance-Vorschriften haben. Aus diesem Grund sind für die Geräte innerhalb Ihres Unternehmens unterschiedliche Schritte erforderlich, die den Anforderungen Ihres Unternehmens entsprechen.

Organisationen des Gesundheitswesens, die im klinischen Bereich häufig iPhones und iPads verwenden, müssen den HIPAA befolgen. Hochschuleinrichtungen müssen FERPA einhalten, und K-12-Schulen haben strenge, vom Bund vorgeschriebene Sicherheitsanforderungen zu erfüllen.

Ein gründliches und gut durchdachtes Programm zur Verwaltung der Geräte-Compliance ist für die Cybersicherheit, die Daten- und die Benutzersicherheit unerlässlich. Und eine Führungskraft in der Branche für die Verwaltung von Mobilgeräten, die bei der Durchsetzung dieser Richtlinien hilft, ist ein Muss. Wenn Sie mehr über die Erstellung einer umfassenden Compliance-Richtlinie erfahren möchten, die die Sicherheit Ihrer Geräte, Benutzer*innen und Unternehmensdaten gewährleistet, lesen Sie bitte Compliance Verwaltung für Einsteiger.

Skripting, Konfigurationsprofile und Verschlüsselung: Zusammenarbeit

Skripting

Die Automatisierung allgemeiner Aufgaben erhöht die Sicherheit um das Zehnfache: Es gibt keine menschlichen Fehler mehr bei der Implementierung und es besteht auch keine Gefahr mehr, dass ein Administrator eine wichtige Aufgabe vergisst. Dies kann durch Skripting geschehen. Mit Skripten lassen sich viele Aufgaben automatisieren, und Administratoren erhalten mehr Kontrolle über ihre Anwendungen.

Beim Skripting geht es um Übung und darum, klein anzufangen. Sie haben eine Aufgabe, die Sie gerne automatisieren würden? Nutzen Sie Jamf Nation und andere Mac Admin-Boards, um nach Skripten zu suchen, die andere für diesen Zweck bereits erstellt haben.

Möchten Sie mit spezifischen Skripten und Aufgaben einsteigen? Lesen Sie Automatisierung allgemeiner Aufgaben mit Apple Skripten und Jamf.

Konfigurationsprofile

Eine wichtige Möglichkeit, die Kontrolle eines Administrators durch Skripte zu erweitern und zu sichern, ist die Implementierung von Konfigurationsprofilen. Häufige Anwendungsfälle für Konfigurationsprofile sind die Durchsetzung von Passcode-Anforderungen, die Konfiguration gespeicherter Wi-Fi-Netzwerke und mehr.

Konfigurationsprofile sind XML-Dateien mit der Erweiterung .mobileconfig, die eine einfache Möglichkeit bieten, Einstellungen und Einschränkungen für Geräte und Benutzer*innen zu definieren. Sie verwenden in der Regel den Apple Push-Benachrichtigung Service (APNs.)

Konfigurationsprofile können die Sicherheit an sich verstärken und verbessern, indem sie Sicherheitsprotokolle in Passcodes, Verhalten und mehr durchsetzen.

Konfigurationsprofile sind in Apple Configurator 2, Profile Manager und Ihrem MDM-Anbieter*innen integriert und können für Geräte und Benutzer*innen bereitgestellt werden, die im MDM angemeldet sind.

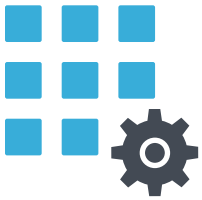
Administrator*innen können Anwendungen auch auf der Grundlage detaillierter Informationen und Sicherheitsprotokolle konfigurieren.

Verschlüsselung

Skripting und Konfigurationsprofile sind zwar leistungsfähige Werkzeuge, aber alles, was die Aktionen eines Geräts steuern kann, muss absolut sicher sein. Die Festplattenverschlüsselung garantiert die Sicherheit der Informationen. Es verschlüsselt Code und Skripte, indem es sie in einen unlesbaren Zustand versetzt, der schwer zu entschlüsseln ist.

Apple verwendet für die Verschlüsselung eine Technologie namens Data Protection. Bestimmte Systemanwendungen (z. B. Nachrichten, Mail, Kalender, Kontakte, Fotos) und Gesundheitsdatenwerte verwenden standardmäßig den Datenschutz. Anwendungen von Drittanbieter*innen erhalten diesen Schutz automatisch.

App-Verwaltung



Da Anwendungen weiterhin der wichtigste Teil der Endbenutzererfahrung sind, ist die Anwendungsverwaltung ein wesentliches Element bei der Verwaltung und Sicherung von Geräten. Von der Beschaffung und dem Hosting bis hin zur Aktualisierung und Bereitstellung ist eine ordnungsgemäße App-Verwaltung von entscheidender Bedeutung für die Sicherung einer Apple-Flotte und gleichzeitig für die Produktivität der Endbenutzer*innen.

Verwaltete Apps-Konfiguration
App Config erlaubt es Unternehmen mit MDM-Lösungen, Daten per Fernzugriff auf ein verwaltetes Gerät zu übertragen, die von der App verwendet werden können, um das Benutzererlebnis oder das App-Verhalten anzupassen.

Die Entwicklung einer einzigen App, die bereitgestellt und an die Bedürfnisse all Ihrer Kund*innen angepasst werden kann, reduziert die langfristigen Kosten und die Wartung der App-Entwicklung.

Apps, die App Config unterstützen, funktionieren weiterhin so, wie sie ursprünglich für allgemeine Verbraucheranwendungen konzipiert wurden, während sie in Unternehmensumgebungen so erweitert werden können, dass sie individuellere Workflows oder Umgebungen unterstützen. Und mit App Config werden UI-Anpassungen möglich, sodass IT-Administrator*innen eine einfache UI zur Verfügung haben, um eine App nach ihren Bedürfnissen zu konfigurieren. Bietet auch Zugang zu Benutzer*innen- und Geräteinformationen

Apps und Bücher
Apps und Bücher ist eine Möglichkeit, iOS Apps oder Bücher über den Apple Business Manager oder den Apple School Manager massenhaft an Endbenutzer zu verteilen oder zu widerrufen (Unternehmen müssen den Apple Business Manager oder den Apple School Manager verwenden, um Apps und Bücher nutzen zu können).

Kauf und Lizenzierung von Apps und Büchern in großen Mengen bei Apple

Die Verteilung von App Store-Apps über den verwalteten und einfachen Workflow ermöglicht es IT-Administratoren, den Benutzern Apps in großen Mengen und auf der Grundlage von Kriterien zuzuweisen, die in Ihrem MDM festgelegt wurden.

Verteilen Sie sie an Einzelpersonen über die Apple ID oder direkt an Geräte ohne Apple ID

iOS Apps müssen die App-Standards von Apple erfüllen, um über den App Store erhältlich zu sein, was bedeutet, dass sie von Natur aus sicherer sind als andere Apps von Drittanbieter*innen außerhalb des App Store. Als Teil Ihrer Sicherheitsvorkehrungen ist es wichtig, dass:

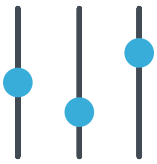
Sie können ein Token (das Sie von Apple erhalten haben) mit Ihrer MDM-Lösung verknüpfen, um es zuzuweisen und zu verteilen, sodass Sie die richtigen Benutzer*innen auswählen und ansprechen können.

Bei der gerätezugewiesenen verwalteten Verteilung ermöglichen verwaltete IDs die Verteilung von Inhalten an verwaltete Geräte, ohne dass die Verwendung von Apple IDs erforderlich ist. Die gerätezugeordnete verwaltete Verteilung wird für vom Benutzer registrierte Geräte empfohlen und verhindert, dass Apps im persönlichen App Store-Konto des Benutzers angezeigt werden.

Bei der benutzerzugewiesenen verwalteten Verteilung werden die Inhalte an das verwaltete Gerät verteilt, aber die Inhaltslizenz wird dem Benutzer direkt über eine verwaltete oder persönliche Apple ID zugewiesen. Dies erfordert die Registrierung von Nutzer*innen mit Volumeneinkauf und die Zuweisung von Inhaltslizenzen an Nutzer*innen, bevor Sie Inhalte verteilen. Auf diese Weise können Sie:

Automatische Apps-Updates planen

Apps automatisch zur Aktualisierung von iOS zwingen



Manuelles Erzwingen von iOS Updates für Apps

Verteilen eines App-Updates (nur für einzelne Apps)

Workflows für die Patch-Richtlinien
Die meisten Administrator*innen von Apple sind mit dem manuellen Verfahren zur Bereitstellung von Patches vertraut. Jamf bietet Workflows für diese Aktionen an, die sich um Fehlerbehebungen kümmern — wichtig für die Netzwerksicherheit, da Fehler in Anwendungen von Drittanbietern eine der am häufigsten genutzten Möglichkeiten sind, in ansonsten sichere Umgebungen einzudringen.

Ein vollständiges Verständnis Ihrer App-Umgebung gibt Ihnen Aufschluss darüber, welche Apps auf welchen Computern veraltet sind. Dieses Verfahren wird mit App-Installern automatisiert und kann im Hintergrund ablaufen.

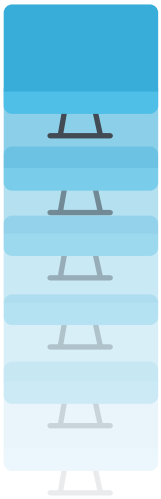
Was ist mit BYOD?

Die Kombination von profil- oder kontengesteuerter Benutzerregistrierung mit der Verwaltung mobiler Geräte von Jamf bedeutet, dass Sie jedes beliebige Gerät im Besitz von Mitarbeiter*innen sichern und verwalten können. Mit identitätsbasiertem Zugriff können Administrator*innen Geräte verwalten und schützen, je nachdem, wer sie benutzt.

Wenn Sie mehr über die Erstellung eines sicheren und gut verwalteten BYOD- Programms erfahren möchten, lesen Sie bitte Jamf und Apple: Besser gemachte BYOD-Programme.

Massenaktionen

Eine weitere Möglichkeit, mehrere lästige Aufgaben auf vielen Geräten gleichzeitig auszuführen, sind Massenaktionen. Mit Jamf Pro können Administrator*innen Massenaktionen für jede Smart Group oder statische Gruppe, Geräte-Suchergebnisse oder Listen mit Übereinstimmungen bei der Lizenznutzung erstellen. Massenaktionen können alles Mögliche sein. Einige Beispiele: Befehle aus der Ferne, Bearbeitung eines Seitenfensters oder E-Mails an Benutzer*innen.



Dies erhöht die Sicherheit von Umgebungen. Egal, ob fünf oder 5.000 Geräte verwaltet werden, durch Massenaktionen wird sichergestellt, dass praktisch kein Gerät übersehen wird, das eine Sicherheitsverletzung verursachen könnte.

Jamf Sicherheitslösungen für iOS und iPadOS

Es ist zwar klar, dass eine sorgfältige Verwaltung von iPadOS und iOS Geräten für die Sicherheit unerlässlich ist, aber es ist auch wichtig, daran zu denken, dass die Geräteverwaltung die Grundlage für die Sicherheit ist. Der Einsatz sicherheitsspezifischer Tools auf dieser soliden Grundlage ist das letzte Teil des Sicherheitspuzzles. Für einen grundlegenden Überblick lesen Sie bitte Abwehr von Bedrohungen für Anfänger.

Abwehr und Schutz vor mobilen Bedrohungen

Die Sicherheitslösungen von Jamf für die Abwehr von Bedrohungen und den Schutz von Endgeräten gehen über einen einfachen Virenschutz für Malware hinaus. Jamf, die Komplettlösung zur Abwehr mobiler Bedrohungen, nutzt das fortschrittliche maschinelle Lernen und die Bedrohungsintelligenz-Engine MI:RIAM, um neuartige Bedrohungen zu erkennen und abzuwehren, bietet netzwerkinternen Schutz, sammelt Erkenntnisse in Echtzeit und ermöglicht einen starken Schutz der Privatsphäre der Benutzer*innen.

Außerdem erfahren Sie, wie wichtig andere Sicherheitssysteme wie Identitäts- und Zugriffsmanagement, Bedrohungsabwehr und -beseitigung, Inhaltsfilterung und Zero Trust Network Access (ZTNA) für die Sicherheit von Benutzer*innen, Geräten und Unternehmensdaten sind.

Wie Jamf helfen kann

Jamf Pro und Jamf School

Eine solide und sichere Grundlage bietet Jamf Pro — der Standard für die Apple Geräteverwaltung — oder Jamf School (MDM) für Schulen und Bezirke. Sie können mehr erfahren und eine Testversion direkt bei uns anfordern oder sich an Ihren bevorzugten Wiederverkäufer wenden, um loszulegen.

Sicherheit über die Geräteverwaltung hinaus

Lesen Sie unseren Bericht über den Stand der Apple Sicherheit in Unternehmen, für den 1.500 IT- und InfoSec-Expert*innen befragt wurden. Er umfasst die aktuelle Gerätenutzung und -ansätze, Herausforderungen für die Gerätesicherheit und den zukünftigen Stand der Endgerätesicherheit.

Trusted Access

Trusted Access ist die Lösung von Jamf für Sicherheit jenseits des Sicherheitsmanagements. Trusted Access ist ein einzigartiger Arbeitsablauf, der Gerätemanagement, Benutzeridentität und Endgeräteschutz zusammenführt, um Unternehmen dabei zu helfen, eine Arbeitsumgebung zu schaffen, die von den Benutzer*innen geschätzt wird, und einen sicheren Arbeitsplatz zu schaffen, dem Unternehmen vertrauen.

Trusted Access mit Jamf stellt sicher, dass nur vertrauenswürdige Benutzer*innen mit registrierten, sicheren Geräten auf Unternehmensdaten zugreifen können. Dadurch wird die Sicherheit Ihres modernen Arbeitsplatzes erheblich erhöht und gleichzeitig die Arbeit für Ihre Benutzer rationalisiert - unabhängig davon, wo die Arbeit stattfindet.

Erfahren Sie mehr über die hochmodernen, auf den Mac zugeschnittenen Sicherheitsangebote von Jamf, um zu sehen, wie wir Ihnen helfen können, Ihre Mac Flotte zu verwalten und zu schützen!

Unter jamf.com/de/loesungen erfahren Sie mehr darüber:

Identitäts- und Zugriffsverwaltung

Geräteverwaltung

Endgerätesicherheit

Angriffe vorbeugen und beheben

Inhaltsfilter für sicheres Internet

Zero-Trust Netzwerkzugang (ZTNA)

Gerätesicherheit und Compliance

Und wenn Sie bereit sind, mit Jamf in die Verwaltung und Sicherheit Ihrer Macs einzusteigen, fordern **Sie noch heute eine kostenlose Testversion an!**

Quelle:1. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (auf Englisch)