Der erweiterte Leitfaden zur Mac Verwaltung

Die Sicherheitslandschaft

Die Cybersicherheit nimmt weiter zu.
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 waren der Ansicht, dass sie die Risiken im Zusammenhang mit der Ermöglichung von Remote- und Hybridarbeit vollständig gemindert haben, während 48 % glaubten, dass sie diese Risiken mäßig gemindert haben. 35 % berichteten von einer vollständigen Entschärfung der Probleme im Zusammenhang mit einer rasch beschleunigten Cloud-Einführung.

Allerdings berichten **nur drei Prozent, 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.

Leider brauchen Cyberkriminelle nur einen Weg, um Schaden anzurichten.
Wie können InfoSec und Mac Administrator*innen sicherstellen, dass **alle Sicherheitsprotokollein allen Bereichen** der digitalen Umgebung vorhanden sind?

Nur

38%

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

Richtige Mac Verwaltung ist sichere Mac Verwaltung

In diesem 201 Leitfaden zur Mac Verwaltung, einer Fortsetzung unseres E-Books Mac Verwaltung für Einsteiger, wird erörtert, wie die Verwaltung von macOS 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 Organisationen aufbauen müssen.

Lesen Sie weiter, um mehr darüber zu erfahren, wie richtige Verwaltung Sicherheit bedeutet. Wir werden auch die wichtigsten Funktionen, Workflows und Einstellungen behandeln, die für die sichere Verwaltung Ihrer Mac Flotte erforderlich sind und alle Grundlagen abdecken.

PKI und Push-Zertifikate

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

In Jamf Pro können Sie eine integrierte Zertifizierungsstelle (CA) verwenden, eine vertrauenswürdige Drittanbieter-CA (DigiCert, Venafi oder Active Directory Certificate Services) integrieren oder Ihre eigene PKI konfigurieren, wenn Sie Zugang zu einer externen CA haben, die das Simple Certificate Enrollment Protocol (SCEP) unterstützt. Die CA kann zur Ausstellung von Zertifikaten für Computer und Mobilgeräte verwendet werden. Bei der Verwendung von Jamf Pro, dem eingebauten CA-Zertifikat; widerrufen und erneuern, ein eingebautes Zertifikat aus einer Zertifikatsignierungsanforderung (CSR) erstellen und ein Backup erstellen.

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

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.

Push-Zertifikate

Ein Push-Zertifikat ist eine verschlüsselte Datei, die von Apple erstellt wird und das Vertrauen zwischen einem dritten Service wie Jamf Pro und dem Apple Push-Benachrichtigungsdienst (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 keine persönliche Apple IDs.

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

Da es sich bei der Datei um eine verschlüsselte Datei handelt, die von Apple generiert wurde, können Sie eine App auf der Grundlage dieser Sicherheitsinformationen aus der Ferne deinstallieren. Push-Zertifizierungen sind ein Jahr lang gültig und müssen mit der gleichen Apple ID erneuert werden, mit der sie ursprünglich erstellt wurden.

Wie man Zertifikate findet

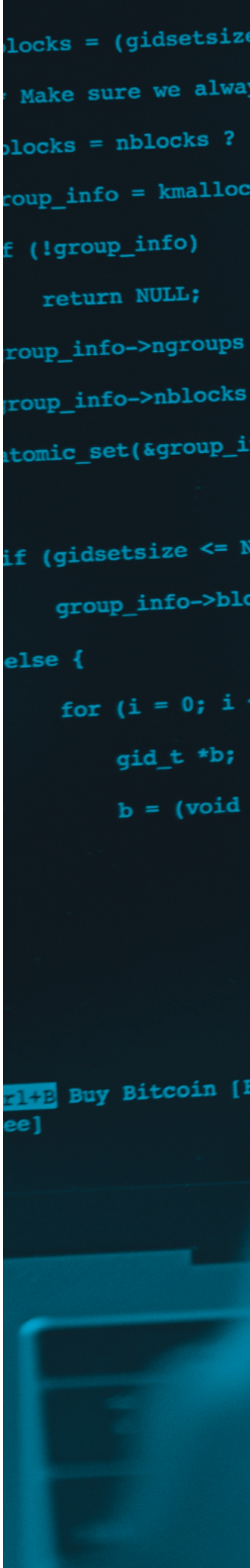
Sie können eine Liste von Zertifikaten anzeigen, indem Sie sie in .csv-, .txt- oder XML-Dateien exportieren. Jamf Pro erleichtert dieses Verfahren, indem es einen IT-Administrator*in durch das Verfahren zur Erstellung eines Push-Zertifikats (.pem) und zum Hochladen in Jamf Pro führt. Sie benötigen eine gültige Jamf ID und Apple ID, und es ist wichtig, dass Mac Administrator*innen diese Zertifikate auf dem neuesten Stand halten. Wenn sie verfallen, verlieren APNs die Konnektivität zu Ihrem Mobile Device Management (MDM) Server/Endgeräten.

Bedingter Zugriff

Aufgrund der neuen Normalität der Fernarbeit von zu Hause, in Cafés oder sogar auf Flügen können Unternehmen nicht mehr ein Netzwerk einrichten und Geräte und Benutzer durch eine Firewall schützen.

Bedingter Zugriff ermöglicht es einer Organisation, Parameter für die Sicherheit der Daten einer Organisation an mehreren Standorten festzulegen. Es kann den Zugriff auf Unternehmensdaten wie E-Mails, OneDrive, Word und Excel- und Cloud Apps wie Jamf Pro durch eine Risikobewertung zu diesem Zeitpunkt verhindern.

Das Erfordernis eines vertrauenswürdigen Geräts und eines vertrauenswürdigen Benutzers/Benutzerin für den Zugriff verbessert die Verwaltung und die Sicherheit, egal wo jemand arbeitet.



Organisatorische Macs werden von Jamf verwaltet und bei Microsoft Intune über einen Cloud-Connector oder einen manuellen Connector registriert. Die starke Partnerschaft von Jamf und Microsoft sorgt dafür, dass dies nahtlos funktioniert: Jamf sendet den Bestand der macOS Geräte an Intune. Intune bewertet die Compliance und erstellt einen Compliance-Bericht. Azure AD erzwingt Zugriffskontrollen.

Wenn Sie mehr über die Erstellung einer umfassenden Compliance-Richtlinie für Mac erfahren möchten, die die Sicherheit Ihrer Geräte, Benutzer und Unternehmensdaten gewährleistet, lesen Sie bitte Compliance Management für Anfänger*innen.

TeamViewer: Mac Admin-Zugriff aus der Ferne

TeamViewer ist eine schnelle und sichere Lösung für den Zugriff auf Computer und Netzwerke aus der Ferne. Es stellt eine Konnektivität aus der Ferne zwischen einem Jamf Pro Administrator/einer Jamf Pro Administratorin und dem Computer eines Endnutzers/einer Endbenutzerin her.

Dies verbessert die Sicherheit und Compliance, da Administrator*innen Probleme schnell einsehen, bewerten und lösen können, ohne dass Informationen in der Übersetzung verloren gehen. Und es beschleunigt die Problemlösung. Wenn sich diese Probleme auf die Sicherheit auswirken, kommt es auf Geschwindigkeit an.

Um auf diese Funktion zugreifen zu können, müssen Sie Ihrer Jamf Pro-Instanz eine Konfiguration für die TeamViewer Integration hinzufügen.

Jamf API

Die Jamf API soll den Zugang zu Jamf erleichtern. Es ermöglicht Unternehmen, Jamf Pro in ihr technisches System zu integrieren und so ein zusammenhängendes System zu schaffen, in das die Mac Verwaltung integriert ist. Dies ermöglicht die Konnektivität zwischen Jamf und anderen Anbieter*innen und lässt Integrationen wie Jamf Protect/Jamf Connect, die Jamf School Parent App, die Jamf Teacher App und vieles mehr zu.

Das Token-basierte Authentifizierungsschema der Jamf APIs erhöht den Sicherheitsstatus von Geräten, die mit Apps und Integrationen von Dritten verbunden sind. Es handelt sich um eine RESTful-Schnittstelle, d. h. sie folgt den Standards für sichere Software-Kommunikation.

Workflow

1. Fordern Sie mit der Basisauthentifizierung ein Bearer Token an, indem Sie einen POST an `/v1/auth/tokensenden.`

2. Sie sollten eine Antwort erhalten, die ein Token und ein Ablaufdatum enthält, ähnlich dem folgenden Beispiel:

```
{
    "token": "eyJhbGciOiJIUzUxMiJ9...",
    "expires": "2022-01-24T21:35:20.373Z"
}
```

3. Sie können das zuvor generierte Token verwenden, um jedes andere Jamf Pro API Endgerät aufzurufen, indem Sie es in einen Header mit dem Format Authorization einfügen: `Überbringer TOKEN VALUE.`

Integrationen ermöglichen eine ganzheitlichere Sicht auf die Fähigkeiten von Jamf und eine enge Verbindung mit Jamf Protect, Endpunktschutzfunktionen mit Netzwerkbedrohungsschutz für Mac. Dies lässt Administrator*innen zu, macOS Malware zu verhindern, vor bestimmten Ereignissen zu schützen, Endgeräte zu überwachen und Probleme schnell zu beheben.

Webhooks

Webhooks ermöglichen es einem Mac Admin, ein bestimmtes Ereignis auf einer Jamf Pro-Instanz zu abonnieren. Wenn das Ereignis eintritt, wird ein HTTP-POST-Payload an eine bestimmte URL gesendet. Sie erlauben es Administrator*innen, Echtzeit-Ereignisse von Jamf Pro zu nutzen, um benutzerdefinierte Workflows on-demand zu erstellen - unter Verwendung der Programmiersprache ihrer Wahl.

Webhooks unterstützen die Cybersicherheit, indem sie IT Administrator*innen über Echtzeit-Ereignisse in ihren Instanzen auf dem Laufenden halten, die als XML oder JSON gesendet werden. Außerdem können Administrator*innen generische Nutzdaten wie ComputerAdded (neuer Computer registriert), ComputerCheckin (Prüfung auf Aufgaben) oder ComputerPatchPolicyCompleted (Abschluss einer Patch-Richtlinie) erstellen.

Verteilungspunkte

Verteilungspunkte sind Server, auf denen Dateien zur Verteilung an Computer (und Mobilgeräte) gehostet werden. Pakete, Skripte und hauseigene Apps und Bücher können über eine Verteilerstelle verteilt werden.

Jamf Pro unterstützt Dateifreigabe-Verteilungspunkte und einen Cloud-Verteilungspunkt. Jamf wendet sich an lokale Vertriebsstellen, um Apps zu finden und sie für Geräte/Benutzer*innen mit Dateifreigabe bereitzustellen. Administrator*innen können Apps auch über den in der Cloud gehosteten Verteilungspunkt von Jamf verteilen: Jamf Cloud Distribution Service (JCDS).

Verteilungspunkte können eine Schwachstelle in der organisatorischen Sicherheit sein, da sie sich häufig in der Cloud befinden und die Benutzer*innen weltweit verteilt sind. Die Verteilung von Dateien an Macs über einen absolut sicheren Verteilungspunkt ist entscheidend.

Wie Verteilungspunkte mit Jamf funktionieren

Standardmäßig ist der erste Verteilerpunkt, den Sie zu Jamf Pro hinzufügen, der Hauptverteilerpunkt. Alle anderen Verteilungspunkte hängen von der ersten Quelle ab, die während der Replikation die maßgebliche Quelle für alle Dateien ist. Verteilungspunkte garantieren, dass die Dateien auf die richtige Weise an das richtige Gerät/den richtigen Benutzer*innen gesendet werden.

Skripte, Konfigurationsprofile und Festplattenverschlüsselung: Zusammenarbeiten

Skripting
Die Automatisierung gängiger 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 Skripte geschehen. Mit Skripten lassen sich viele Aufgaben automatisieren, und Administrator*innen haben mehr Kontrolle über ihre Mac Apps.

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

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

Konfigurationsprofile
Eine wichtige Möglichkeit, wie Skripte die Kontrolle eines Admins verstärken und sichern können, ist die Implementierung von Konfigurationsprofilen.

Konfigurationsprofile sind XML-Dateien (.mobileconfig), die eine einfache Möglichkeit bieten, Einstellungen und Einschränkungen für Geräte und Benutzer*innen zu definieren. Sie verwenden in der Regel APNs. Beim Erstellen eines Computerkonfigurationsprofils müssen Administrator*innen die Ebene angeben, auf der das Profil angewendet werden soll - Computerebene oder Benutzerebene. Jede Ebene hat eine eigene Reihe von Nutzlasten und einige wenige, die für beide gleich sind.

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 Jamf Pro integriert und können für Geräte und Benutzer*innen mit aktiviertem MDM bereitgestellt werden. Es gibt zwei Möglichkeiten, ein Konfigurationsprofil zu verteilen: es automatisch zu installieren (ohne Benutzerinteraktion) oder es im Self Service verfügbar zu machen.

Festplattenverschlüsselung
Skripte und Konfigurationsprofile sind zwar leistungsstarke Tools, aber alles, was die Aktionen eines Geräts steuern kann, muss absolut sicher sein. Die Verschlüsselung der Festplatte garantiert, dass die Informationen hinter einem Passwort sicher sind. Es verschlüsselt Code und Skripte, indem es sie in einen unlesbaren Zustand versetzt, der nur schwer zu entschlüsseln ist. Und es ist in den Mac integriert.

Die Festplattenverschlüsselung erlaubt es Mac Administrator*innen auch, FileVault auf Computern zu verwalten und zu aktivieren. FileVault verschlüsselt Informationen auf Macs und verhindert, dass jemand die Informationen ohne Passwort lesen kann).

Erweiterungsattribute

Erweiterungsattribute sind benutzerdefinierte Felder, die Sie erstellen können, um nahezu alle Arten von Bestandsdaten von Geräten zu erfassen. Sie können benutzerdefinierte LDAP-Attribute verwenden, um Erweiterungsattribute zu erstellen. Und wenn Sie möchten, können Sie mit Skripten sogar noch weitergehende Erweiterungsattribute erhalten.

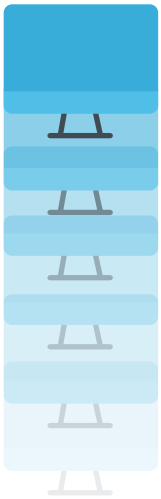
Wie man sie verwendet
Sobald die Daten aus den Erweiterungsattributen im Inventarisierungsdatensatz enthalten sind, können Administratoren mit Smart Groups in Jamf Pro aktiv werden: Gruppierung von Geräten und/oder Benutzer*innen in Gruppen auf der Grundlage von einem oder mehreren Inventarattributen. IT-Administrator*innen können nicht nur manuell Erweiterungsattribute erstellen, die ihren Anforderungen entsprechen, sondern auch die vorgefertigten Jamf Pro-Erweiterungsattribute für eine einfache und effiziente Erstellung von Erweiterungsattributen nutzen.

Die Verwendung von Erweiterungsattributen mit den intelligenten Gruppen von Jamf Pro ermöglicht es Ihnen, Ihre Flotte mit Gruppenaktionen auf Geräten mit beliebigen Betriebssystemen, die aktualisiert werden müssen, und mehr zu sichern. Die Implementierung von Erweiterungsattributen ermöglicht auch ein kohärenteres Verständnis der Daten in Ihrer Instanz, sodass Sie besser erkennen können, was gegen die Vorschriften verstößt oder Schwachstellen im System aufweist.

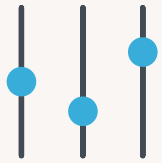
Massenaktionen

Eine weitere Möglichkeit, mehrere lästige Aufgaben auf vielen Computern gleichzeitig auszuführen, sind Massenaktionen. Mit Jamf Pro können Administrator*innen Massenaktionen für jede Smart Group oder statische Gruppe, Computersuchergebnisse 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. Ob fünf oder 5.000 Computer verwaltet werden, durch Massenaktionen wird sichergestellt, dass praktisch kein Gerät übersehen wird, das eine Sicherheitsverletzung verursachen könnte.



App-Verwaltung



Da Apps nach wie vor den größten Teil der Endbenutzererfahrung ausmachen, ist die Verwaltung von Apps auf Mac ein wichtiges 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.

Viele der heute am häufigsten genutzten Anwendungen sind nicht im Mac App Store zu finden. App Installers bietet Mac Administrator*innen eine bessere Möglichkeit, Anwendungen automatisch zu beschaffen, zu hosten, zu aktualisieren und auf ihren Computern oder für ihre Benutzer bereitzustellen. Veraltete Apps sind ein großes Sicherheitsproblem.

Deshalb bietet Jamf Angebote, mit denen man über die Aktualisierungen von Apps auf dem Laufenden bleibt:

App Installers
App Installers ist eine kuratierte Sammlung von Jamf-verwalteten und Jamf-bereitgestellten Installationspaketen, die die Bereitstellung rationalisieren und eine optimierte Alternative zu komplexen Arbeitsabläufen bieten, die für das Patchen von Drittanbieteranwendungen erforderlich sind.

Um die Sicherheit zu gewährleisten, validieren sie auch die Integrität der Patch-Definitionen, bevor sie die Bereitstellung erlauben. Nach der Überprüfung wird die neue App-Version automatisch auf allen kompatiblen Macs bereitgestellt.

Dies sind die Pakete, die Jamf als Quelle verwendet, neu paketiert und hostet. Dieser Jamf-App-Katalog ist eine Sammlung von Softwaretiteln, einschließlich einer Liste von mehr als 1.000 macOS Softwaretiteln von Drittanbietern, die in Jamf Pro unterstützt werden.

App-Installer müssen sich in einer intelligenten Computergruppe in Jamf Pro befinden. Wenn auf einem Zielcomputer in einer intelligenten Gruppe der Softwaretitel installiert ist, stellt der App Installer das Update bereit, wenn eine neue Version veröffentlicht wird.

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

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

Titel-Editor
Titel-Editor ist ein von Jamf gehosteter Dienst, der die Patch-Verwaltung erweitert, indem er benutzerdefinierte Softwaretitel bereitstellt, vorhandene Patch-Definitionen überschreibt und die Möglichkeit bietet, benutzerdefinierte Patch-Definitionen zu erstellen.

Jamf Sicherheitslösungen für Macs

Es ist zwar klar, dass eine sorgfältige Verwaltung von Mac-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 allgemeinen Überblick lesen Sie bitte Mac Endgeräteschutz für Einsteiger.

Jamf Protect Endgerätesicherheit

Jamf Protect geht über ein einfaches Antivirus-Tool für Malware hinaus. Es handelt sich um eine umfassende Sicherheitslösung für Endgeräte mit verhaltensbasierter Erkennung, die Verhaltensweisen, die häufig für Angriffe verwendet werden, vorhersieht und erkennt.

Sie erfahren auch, 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

Für eine solide und sichere Grundlage sollten Sie Jamf Pro ausprobieren — den Standard für die Verwaltung von Apple Geräten. Sie können mehr erfahren und eine Testversion direkt bei uns anfordern oder sich an Ihren bevorzugten Wiederverkäufer wenden, um loszulegen.

Sicherheit über das Gerätemanagement hinaus

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

Vertrauenswürdiger Zugriff

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

Trusted Access mit Jamf stellt sicher, dass nur vertrauenswürdige Benutzer 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**
- **Inhaltsfilter für sicheres Internet**
- **Endpunktesicherheit**
- **Zero-Trust Netzwerkzugang (ZTNA)**
- **Vorbeugung und Beseitigung von Bedrohungen**
- **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)