jamf

Sicherheit ohne Passwörter

Passwörter, P@sswörter1, P@$$wörter$1234!

Das Passwort dient schon lange als Barriere, die alle Personen fernhält, die keinen Zugriff haben sollten und jene hereinlässt, die Zugang haben sollten. Es ist der Türsteher für Ihr Gerät und Ihre Daten. Passwörter standen bewundernswert am Eingang Ihrer Geräte und haben diese mit der Macht verteidigt, die mindestens acht Buchstaben, eine Ziffer und ein Sonderzeichen ihnen verliehen haben.

In dem Maße, wie unser digitaler Fußabdruck weiter wächst und das Geräte-Ökosystem zunimmt, steigen auch die Anforderungen mobiler Benutzer, was den Wert und die Benutzerfreundlichkeit des Passworts zunehmend verringert. Benutzer interagieren jetzt mit mehr Geräten und Apps als je zuvor, und das jeden Tag häufiger – wodurch jedes Mal ein Sicherheitsrisiko besteht, falls das Passwort kompromittiert wurde.

Jeder IT-Administrator hat die schreckliche Liste der am häufigsten verwendeten Passwörter gesehen – und sie ist schrecklich – denn praktisch jede Interaktion von Benutzern mit Geräten und den Daten auf diesen Geräten erfordert, dass sie ihre Identität beweisen müssen.

Die 10 am häufigsten verwendeten Passwörter[1]

1. 123456
2. 123456789
3. qwertz
4. Passwort
5. 12345
6. qwertz123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

1. Laut Cybernews.com

In diesem Dokument besprechen wir Folgendes:

- Gesteigerte Sicherheit im Vergleich mit Benutzerfreundlichkeit
- Was passwortlos bedeutet
- Warum Organisationen sich für passwortlose Workflows interessieren sollten
- Jamfs Antwort auf Passwortprobleme

Gesteigerte Sicherheit im Vergleich mit Bneutzerfreund-lichkeit

Das größte Sicherheitsproblem für Organisationen heute? **Gestohlene Anmeldedaten.** Überrascht? ... dass **80% aller Datensicherheitsverstöße mit gestohlenen oder schwachen Passwörtern verbunden sind**? Selbst bei Durchsetzung stärkerer Passwortrichtlinien können Server-Sicherheitslücken Passwörter und dadurch Informationen über Unternehmen und Mitarbeiter freilegen. Zudem werden InfoSec-Gegenspieler in ihrer Methodik und den Arten der Angriffe immer komplexer. Phishing-Angriffe, Push-Benachrichtigungen und betrügerische Aktionen zur Übernahme von Accounts sind alle auf anfällige Benutzer ausgerichtet und versuchen, einen direkten Zugriff auf Geräte und wichtige Daten zu erhalten.

Im Laufe der Zeit führte die Notwendigkeit einer erhöhten Sicherheit die IT-Abteilung dazu, als Lösung mehr Passwortkomplexität und Passwortwechsel zu erfordern. Während diese zusätzlichen Maßnahmen halfen und als “Best Practices” betrachtet werden sollten, wurden sie auch ein Problem bei der Benutzererfahrung. Viele Benutzer reduzierten einfach ihre Last, indem sie schwächere Passwörter erstellen, indem sie das Passwort auf Papier oder digital notieren und sogar indem sie den Zettel unter die Tastatur legen, wo jeder ihn finden kann. Diejenigen, die beschlossen, komplexe Passwörter zu erschaffen und zu verwenden, hatten ihre eigenen Probleme – Helpdesk-Tickets weil sie diese zufälligen Zeichenfolgen mit Buchstaben, Zahlen und Schriftzeichen vergessen haben.

Während ein Passwort-Zurücksetzen möglicherweise nicht die komplexesten Helpdesk-Tickets darstellt, werden sie für jeden IT-Administrator mühselig, der eigentlich für höhere Aufgaben eingestellt wurde, als Passwörter zurückzusetzen. Um einen Schritt weiter zu gehen, kostet es Geld, wenn Ihr IT-Team seine kostbare Zeit für die Behebung von trivialen Tickets verschwendet. **Die Zurücksetzung eines einzelnen Passworts kostet Unternehmen im Durchschnitt 70 US-Dollar**. Wenn Sie die ganze Zeit hinzuzählen, die für diese Tickets verschwendet wird, ist das in manchen Unternehmen ein schockierend hoher Betrag. Für Endnutzer bedeutet das Vergessen eines Passworts und das Warten auf die Rücksetzung eine Blockade der Arbeit und Produktivität. Dennoch reicht dieser Zeit- und Geldaufwand nicht immer, damit Passwörter die Aufmerksamkeit von Sicherheitsteams und Benutzern erhalten, die sie verdienen.

Die steigenden Sicherheitsanforderungen zur Verhinderung von Angriffen auf Unternehmen und zum Schutz von Firmen- und Kundendaten haben die Sicherheitsbudgets in Unternehmen erhöht. Doch die Sicherheitsverstöße nehmen auch zu, und die Zuweisung von Mitteln zur Verhinderung von kompromittierten Passwörtern entspricht nicht dem dadurch verursachten Problem. Tatsächlich **werden weniger als 10% für die Beseitigung von kompromittierten Anmeldedaten ausgegeben, aber das führt zu mehr als 80% aller Sicherheitsverstöße**. Hier können passwortlose Workflows helfen.

Was bedeutet passwortlos eigentlich?

Gartner prognostiziert, dass bis 2022 60% der großen und weltweit tätigen Unternehmen sowie 90% der mittelgroßen Unternehmen passwortlose Methoden in mehr als 50% der Anwendungsfälle implementieren werden.

Warum? Ein passwortloser Workflow für die Authentifizierung von Benutzern eliminiert von sich aus das Problem schwacher Passwörter. Zudem wird die Passwortmüdigkeit der Benutzer gelindert und Organisationen müssen keine Passwörter mehr speichern, die exponiert und kompromittiert werden könnten. Anders gesagt vermeidet das praktisch jedes Problem physischer Passwörter, die zu Beginn dieses Dokuments erwähnt wurden.

Um passwortlose Workflows erfolgreich einzuführen, muss eine Organisation ihren Benutzern die Möglichkeit bieten, ihre Identität während der Anmeldung bei Ressourcen, Daten oder Software zu authentifizieren oder zu bestätigen, für deren Zugriff und Nutzung sie von der IT-Abteilung eine Genehmigung erhalten haben. Führungspersonal in den Bereichen Sicherheit und Identitäts- und Zugriffsverwaltung (IAM) sollte mit wesentlichen Authentifizierungs- und Autorisierungskonzepten der Identitätsverwaltung vertraut sein.

Ein Beispiel für eine Authentifizierungsmethode ist ein Smartcard-System. Eine Smartcard ist eine physische Karte, die einer Kreditkarte ähnelt und kryptographische Schlüssel enthält, die direkt mit einem Benutzer verbunden sind. Sie wird als sichere Methode zur Authentifizierung verwendet.

Was ist passwortlose Authentifizierung?

Passwortlose Authentifizierung ist eine Authentifizierungsmethode, bei der Benutzer sich bei einem Computersystem anmelden können, ohne ein Passwort oder ein anderes wissensbasiertes Geheimnis einzugeben.

Was ist zertifikatbasierte Authentifizierung?

Zertifikatbasierte Authentifizierung ist die Verwendung eines digitalen Zertifikats zur Identifizierung eines Benutzers, einer Maschine oder eines Geräts, bevor Zugriff auf eine Ressource, ein Netzwerk, eine App usw. gewährt wird.

Was ist die Multi-Faktor-Authentifizierung (MFA)?

Die Multi-Faktor-Authentifizierung (MFA) ist ein Authentifizierungsverfahren, die Benutzer zwingt, zwei oder mehr Verifizierungsfaktoren bereitzustellen, um Zugriff auf eine Ressource zu erhalten. Das könnte eine PIN auf dem Smartphone des Benutzers sein, **Face ID**, Fingerabdruckverifizierung oder einige anderen Optionen.

Das Problem ist, dass die Implementierung dieser Systeme zeitraubend und sehr teuer ist, sowie dass der Endnutzer mit zusätzlicher Hardware umgehen muss. Solange Ihre Organisation kein Anwendungsfall mit hohem Risiko ist, überwiegen die Kosten und die Möglichkeit des Verlusts durch den Endbenutzer oder eines Defekts der Smartcard oft die potenzielle Bedrohung und machen diese Sicherheitsstufe klar überflüssig.

Das Beispiel, das die meisten Menschen kennen, wenn es um passwortlose Anmeldung geht, ist die Verwendung der Biometrie. Face ID und Touch ID sind Beispiele, die jeder Apple Benutzer kennt. Die Biometrie ermöglicht es einem Benutzer, sich zu authentifizieren, ohne ein Passwort zu eingeben oder eine geheime Frage zu beantworten, die gestohlen oder erraten werden kann. Ihr Gesicht ist Ihr Gesicht, und Ihr Daumen ist Ihr Daumen – das lässt sich kaum stehlen. Wenn man noch die Forderung einer wechselnden PIN hinzufügt, verdoppelt das die Effektivität der Sicherheit.

Wir haben darüber gesprochen, wie Passwörter nicht mehr die sicherste Methode für Organisationen darstellen, Benutzern Zugriff auf ihre Geräte und Ressourcen zu ermöglichen, noch bieten sie Mitarbeitern, die tagtäglich immer wieder Passwörter eingeben müssen, ein optimales Erlebnis. Aufgrund der sich ändernden Situation bezüglich der Tele- und Hybridarbeit müssen Organisationen jetzt bessere Sicherheitsmaßnahmen einführen, die auch die Benutzererfahrung berücksichtigen. Sehen wir uns einmal an, wie die digitale Transformation Organisationen zunehmend dazu bringt, passwortlose Workflows zu implementieren.

Warum sollten sich Organisationen für passwortlose Methoden interessieren?

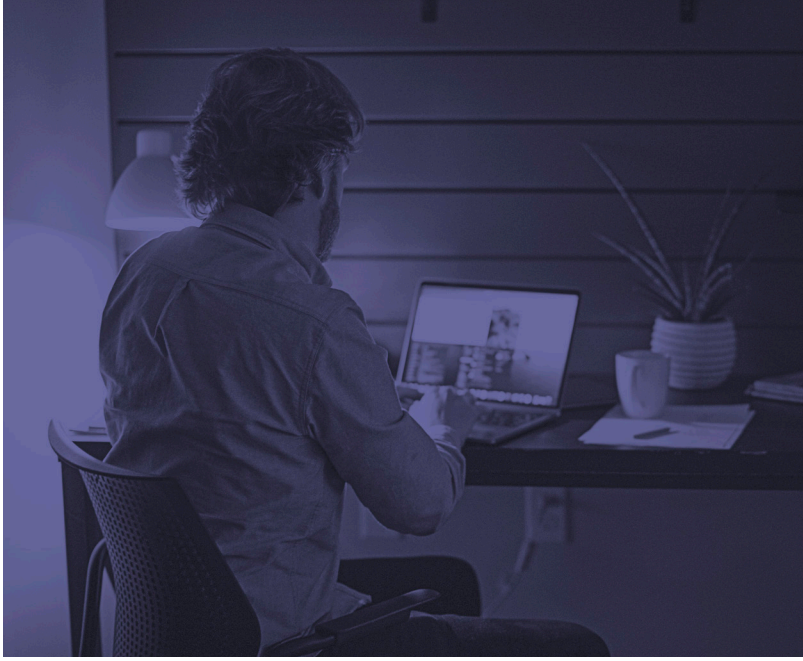
Wenn die zu Beginn dieses Dokuments kurz beschriebenen Schwachstellen noch nicht ausreichten, um Sie zu überzeugen, auf passwortlose Workflows umzusteigen, sollten wir uns die Digitalisierung und deren Auswirkungen auf Passwörter genauer ansehen.

Telearbeiter

Der Wechsel zur Tele- und Hybridarbeit hat die Dringlichkeit für passwortlose Authentifizierung beschleunigt, da eine hervorragende Benutzererfahrung und Fernsicherheit noch wichtiger werden. Dabei spielt die Tatsache eine wichtige Rolle, dass Endbenutzer sich aus der Ferne anmelden. Benutzer können auf ihre Geräte und Ressourcen von überall aus – zuhause, im Büro, in einem Café, im Park – zugreifen, was flexibel und bequem ist, aber auch das Risiko bringt, außerhalb der Unternehmenszentrale zu sein. Benutzer können sich auf ungesicherten Netzwerken befinden, die Löcher in die Sicherheitsebene bohren und Angriffe wahrscheinlicher machen. Eine einfache Methode zur Reduzierung des Bedrohungsrisikos ist ein sauberer und zuverlässiger passwortloser Workflow, mit dem Benutzer auf alles zugreifen können, was sie benötigen. Es gibt keine Passwörter mehr, die gestohlen werden können, und es gibt weniger Helpdesk-Tickets. Dadurch wird auch die Passwortmüdigkeit umgangen.

Die Arbeit befindet sich in der Cloud

Das Cloud Computing hat die Welt verändert, und der Übergang dazu stellt zweifellos eine wichtige Komponente in einem Großteil der modernen IT-Infrastruktur dar.
Da der lokale Unternehmensperimeter verschwindet und Organisationen in die Cloud wechseln, sollte ihre Strategie für die Identitätsverwaltung dem folgen. Apps und Ressourcen befinden sich überall in der Cloud. Die IT-Abteilung muss den Mitarbeitern eine sichere Methode bieten, um Zugriff zu erhalten und produktiv zu bleiben. Ein passwortloses System kann dabei helfen, sicheren und nahtlosen Zugriff auf die Cloud und alle Apps darin zu bekommen.



Senkung der Kosten für die Passwortverwaltung

Laut **dem Weltwirtschaftsforum** verbringen Mitarbeiter weltweit durchschnittlich 11 Stunden pro Jahr mit der Eingabe oder Zurücksetzung von Passwörtern. Wenn man das mit der Anzahl der Mitarbeiter in Ihrer Organisation multipliziert, stellt das eine enorme Zeitspanne dar, die für die Passwortverwaltung verschwendet wird. Auch wenn die Implementierung einer neuen Lösung etwas kostet, ist das viel weniger als die Verschwendung von Stunden auf mühselige Passwort-Zurücksetzungen und eine nicht konzentrierte Belegschaft.

Unterstützt erhöhte Produktivität

Weniger Zeit für die Passwortverwaltung führt dazu, dass Mitarbeiter mehr Zeit haben, sich auf ihre Aufgaben zu konzentrieren. Dabei haben sie ungestörten Zugriff auf die zulässigen Ressourcen und erleben einen produktiveren Arbeitstag. Dabei werden nicht nur die Kosten durch verringerte Passwortverwaltung reduziert, ebenso wie die sicherheitsrelevanten Probleme in Bezug auf die Risiken von Passwörtern – die erhöhte Produktivität der Mitarbeiter führt auch zu gesteigerten Einnahmen.

Das sind nur einige weitere Beispiele, wie etwas wie Passwörter – ein Aspekt, den man viele Jahre übersehen hat oder als “gut genug” betrachtet hat – optimiert werden kann, um die allgemeine Sicherheitsstrategie, den Umsatz und das finanzielle Wohlergehen des Unternehmens zu unterstützen. Man sieht klar, warum viele passwortlose Workflows als wichtige Komponente ihrer Pläne zur digitalen Transformierung betrachten.

Jamfs Antwort auf Passwortprobleme: Jamf Unlock

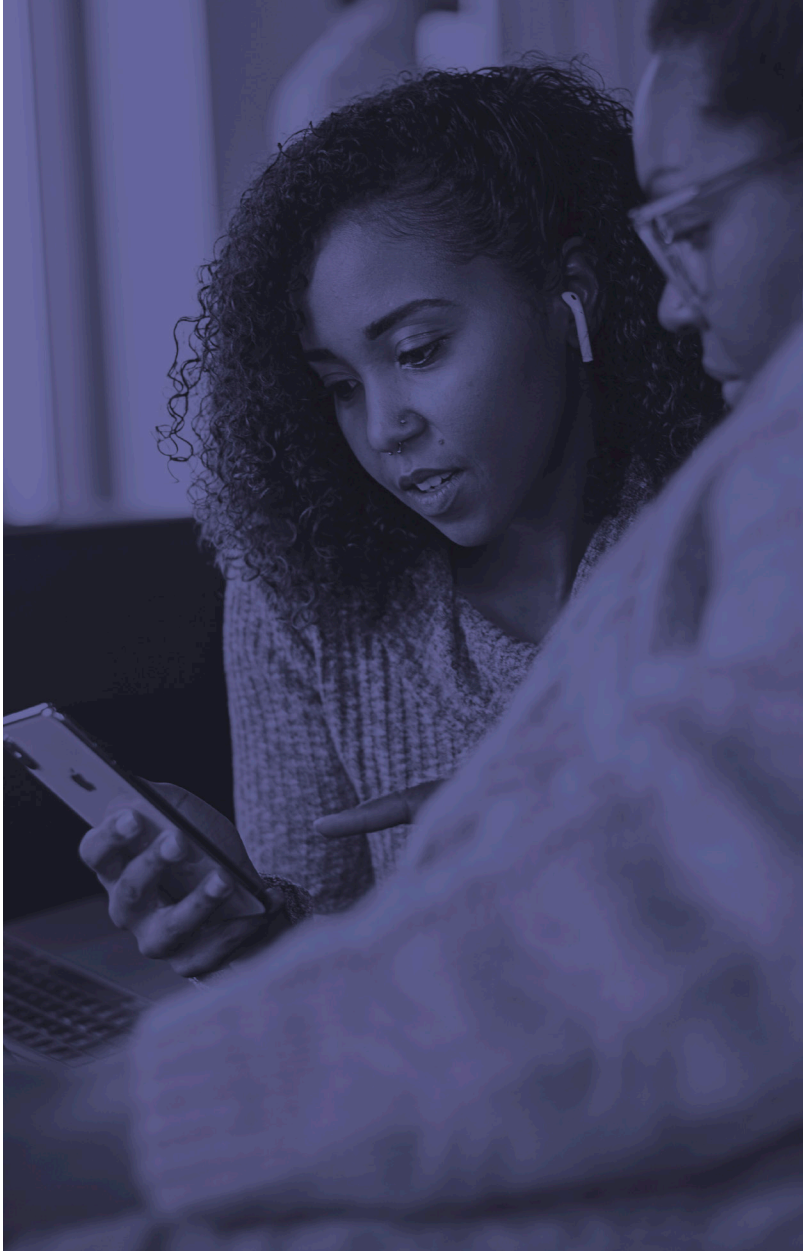
Statt sich auf unverwaltete, kostspielige Hardware wie Smartcards zu verlassen, bietet Jamf Unlock – eine integrierte Funktion von Jamf Connect – einen passwortlosen Workflow auf dem Gerät, das Benutzer immer eingeschaltet haben (ihr iPhone), um ihren Mac sicher zu entsperren und einen sichereren Anmelde- und Authentifizierungsprozess mit einer nahtlosen Endbenutzererfahrung zu ermöglichen. Der Jamf Unlock Workflow erfüllt die Anforderungen der Mac Systemauthentifizierung mit einem Authentifizierer, der auf dem iOS Gerät eines Benutzers läuft, statt einer Passworteingabe auf ihrem Mac.

1. Benutzer öffnen die iOS App Jamf Unlock auf ihrem iPhone und melden sich erstmalig mit ihren cloudbasierten ID-Anmeldeinformationen an.
2. Dann koppeln Benutzer ihr iPhone mit einem QR-Code mit ihrem Mac.
3. Auf dem Mac geben Benutzer auf Aufforderung ihr lokales Passwort ein, um die Gerätekopplung zu ermöglichen.
4. Sobald die Kopplung abgeschlossen ist, können Benutzer die App verwenden, um den Mac sicher mit der von der IT-Abteilung festgelegten Methode zu entsperren – Biometrie mit oder ohne eine wechselnde PIN.

Jamf Unlock nutzt die Multipeer Connectivity, CryptoTokenKit und das Core Bluetooth Framework von Apple, um drahtlos eine zertifikatbasierte Authentifizierung zwischen dem Mobilgerät eines Benutzers und dem Mac zu ermöglichen.

Verbessern Sie Ihre Sicherheit und gehen Sie mit Private Access einen Schritt weiter: Entsperren ist nur ein Teil der Sicherung von Daten und Ressourcen. Jamf Private Access – eine echte Zero-Trust-Netzwerk-Access Plattform – sorgt dafür, dass die Unternehmensverbindungen sicher sind, nachdem sich Benutzer auf Geräten authentifiziert haben.

Weitere Informationen über Private Access



Passwortlose Workflows werden zweifellos weiterentwickelt, sollten aber nur eine Komponente einer modernen Identitäts- und Sicherheitsstrategie sein. Jamf Unlock ist eine Komponente von Jamf Connect für Mac, die Organisationen sofortige Kontobereitstellung, Identitätsverwaltungsfunktionen und eine einzige Cloud-Identität für den Zugriff auf den Mac und Ressourcen bietet. Durch die Integration in einen Cloud-Identitätsanbieter ermöglicht es Jamf Connect der IT-Abteilung, die mit der Identität der Endbenutzer verbundenen Daten und die für ihre Accounts autorisierten Programme und Ressourcen aus der Ferne zu verwalten. Das erhöht nicht nur die Sicherheit, sondern optimiert auf die Kontobereitstellung und ermöglicht es Benutzern, ihren Mac zu öffnen und sofort sicheren Zugriff auf alles zu erhalten.

Werden Sie noch heute sicherer

Natürlich verändert sich die Arbeitsumgebung ständig, aber diese Entwicklung bringt sowohl Herausforderungen als auch Chancen mit sich. Fortschritte wie mobile und aus der Ferne arbeitende Arbeitskräfte öffnen die Tür für Angreifer und Hacker, die dies ausnutzen. Aber das führt auch zu kreativen Workflows und Lösungen für IT-Administratoren, InfoSec und Benutzer.

Auch wenn InfoSec-Teams immer zuerst an die Sicherheit denkent, werden sie ständig herausgefordert, diese Priorität mit den Wünschen und Bedürfnissen der Endbenutzer abzugleichen, die sich viel mehr auf den täglichen Umgang mit ihren Geräten konzentrieren. Benutzer wollen keine mühsamen Workflows oder Sicherheitsmaßnahmen, die sie extrem verlangsamen. Auch wenn die meisten Benutzer die Bedeutung der Datensicherheit verstehen, geht das nur bis zu einem gewissen Punkt.

Da Jamf Unlock mühelos in existierende Workflows integriert werden kann, nutzt das in dieser Hinsicht sowohl dem Endnutzer als auch den InfoSec/IT-Teams Auch wenn böswillige Akteure immer versuchen, in ihre Daten einzubrechen, bietet die Umsetzung eines passwortlosen Workflows mit Jamf Unlock und Jamf Connect einen deutlichen Gewinn. Dies liefert eine zusätzliche Sicherheitsstufe und eine hervorragende Endbenutzererfahrung, welche die Risiken durch vorgetäuschte Identitäten reduziert.

Die Implementierung einer passwortlosen Umgebung sollte ein gut durchdachtes Verfahren für jede Organisation sein. Das gilt für die meisten Sicherheitspläne – aber dies ist eine Erweiterung, die jede Organisation voranbringt und die Wachstumsmöglichkeiten bietet. Der Schwerpunkt sollte auf der Optimierung Ihres Verfahrens und der Einsparung von indirekten Kosten liegen, statt auf der Einführung unnötiger Hardware und weiteren Kosten. Genau das bietet Jamf Unlock, und daher ist das die beste Methode für die Sicherung der Macs in Ihrer Organisation.

Kontaktieren Sie uns oder kontaktieren Sie Ihren Apple Partner, um die Identitätsverwaltung und die passwortlosen Fähigkeiten von Jamf Connect in Ihrer Organisation zu nutzen.