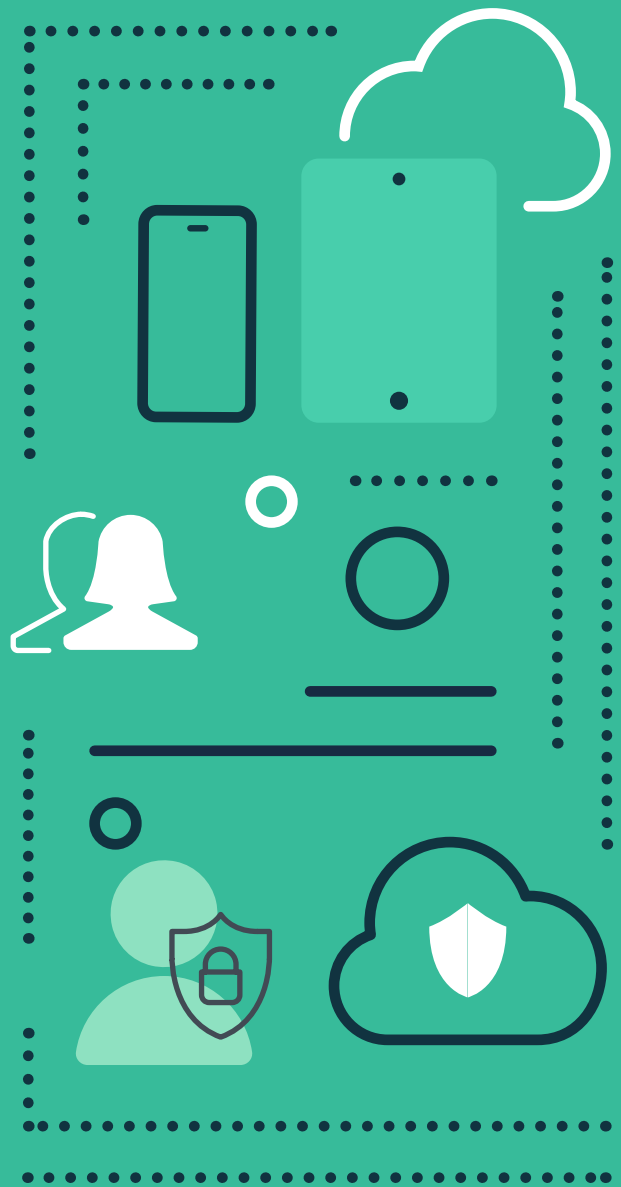

jamf

Identitäts-verwaltung

für Beginner

JEDER ARBEITNEHMER/JEDE ARBEITNEHMERIN HAT SEINE/ IHRE EIGENE IDENTITÄT

Traditionell gingen die Mitarbeiter*innen in ein Bürogebäude, hatten einen Desktop-Computer an ihrem Schreibtisch und die Hardware verließ diesen Standort nie. Multipliziert mit der Anzahl der Mitarbeiter*innen einer Organisation ergibt sich ein Bild der Geräte und Zugriffe, die die IT-Abteilung verwalten muss. Die heutige Arbeitsumgebung sieht ganz anders aus. Der moderne Arbeitnehmer ist mobil, wechselt im Laufe des Tages nahtlos von Laptop zu Tablet zu Telefon und braucht überall Zugang zu seinen Informationen und Daten.

Der digitale Fußabdruck von Arbeitnehmern hat sich vergrößert und verschlimmert, sowohl in Bezug auf die Zeit, die sie mit Geräten verbringen, als auch in Bezug auf das reine Datenvolumen, auf das sie zugreifen möchten. Eine der wichtigsten Taktiken, die Unternehmen zum Schutz dieser Informationen anwenden, ist die Kontrolle darüber, wer Zugang zu bestimmten Dateien, Software und Daten hat und wie sie darauf zugreifen. Dies ist eine einfache Methode, um die Erfahrung der Endbenutzer zu verbessern, indem man ihnen das gibt, was sie brauchen, wenn sie es brauchen, nicht mehr und nicht weniger.

Es ist ein Aspekt der IT, der immer alltäglicher wird, aber da die technologische Welt voranschreitet und die Bedürfnisse der Mitarbeiter*innen sich mit ihr verändern, ist es wichtig, dass Unternehmen ihre Arbeitsabläufe so gestalten, dass sie sowohl modern als auch anpassungsfähig sind. Eine davon ist die Identitäts- und Zugriffsverwaltung, die oberste Priorität genießt.

IN DIESEM LEITFADEN BESPRECHEN WIR FOLGENDES:

- Grundlagen der Identitätsverwaltung
- Workflows für moderne Identitäts- und Zugangsverwaltug
- Warum die Cloud für den Erfolg von heute entscheidend ist
- Wie alles mit Jamf zusammenkommt

GRUNDLAGEN DER IDENTITÄTSVERWALTUNG

Identitäts- und Zugnagsverwaltung (IAM) ist die übergreifende Disziplin zur Überprüfung der Identität eines Benutzers/einer Benutzerin und seiner Zugriffsberechtigung auf ein bestimmtes System. **Dazu müssen die Benutzer*innen authentifiziert und autorisiert werden.**

Die **Authentifizierung** ist im Allgemeinen mit dem Akt des „Einloggens“ verbunden und ist der Teil, in dem Ihre Identifikation authentifiziert oder als echt festgestellt wird. In den meisten Fällen handelt es sich dabei um einen Benutzernamen und ein Passwort.

Im Identitätsmanagement bedeutet Authentifizierung jedoch nicht, dass Sie tatsächlich Zugang zu etwas haben, sondern es bezieht sich einfach auf die Fähigkeit eines Benutzers, sich zu verifizieren. Für den Zugriff auf Daten-, Software und Dateien benötigen Sie eine Autorisierung. Die **Autorisierung** bezieht sich auf die Ressourcen, Software, Daten usw. zu denen Sie Zugang erhalten, um sich zu authentifizieren.

Authentifizierung = wer Sie sind
Autorisierung = was Sie tun können

GRUNDLAGEN DER IDENTITÄTSVERWALTUNG

Um dieses Konzept der Authentifizierung und Autorisierung mit Leben zu erfüllen, erstellten die Unternehmen ein Verzeichnis, das im Wesentlichen ein Katalog der technischen Daten ihrer Mitarbeiter*innen war. Zum Beispiel: Name, Gerätetyp, Berufsbezeichnung, Abteilung, Benutzernamen, Kennwörter und die Software und Dateien, auf die sie zugreifen mussten. Damit wurde die Grundlage für die Verwaltung von Identitäten geschaffen. Dies wird manchmal auch als Legacy IT bezeichnet.

Vor 15 Jahren war die Identitätsverwaltung noch einigermaßen einheitlich. Sie hattenLightweight Directory Access Protocol (LDAP) für die Katalogisierung der Identifikation und der Details Ihrer Benutzer*innen, Kerberos für die Benutzerauthentifizierung, und wenn man beides zusammenfügte, erhielt man Active Directory (AD), das im Kern das Ausmaß des Identitätsmanagements darstellte. In den letzten zehn Jahren hat sich dieser Prozess jedoch weiterentwickelt.

Die herkömmliche IT verlässt sich auf Verzeichnisdienste als "Quelle der Wahrheit", aber da sich die Sicherheits- und Bereitstellungsanforderungen weiterentwickeln, müssen Unternehmen einen neuen Ansatz für die Identität als Teil ihrer Unternehmensstrategie wählen. Mit einem vollständigen Identitätsstack können Unternehmen die Identität über Hardware und Software hinweg vereinheitlichen, um Funktionen und erweiterte Arbeitsabläufe freizuschalten und letztendlich das Geschäft zu transformieren.

GRUNDLAGEN DER IDENTITÄTSVERWALTUNG

Identitätsverwaltung geht über die Authentifizierung und Autorisierung von Benutzer*innen hinaus. Sie bestimmt auch, wie die Benutzer*innen auf organisatorische Ressourcen zugreifen.

Für entfernte und mobile Mitarbeiter*innen ist die herkömmliche IT-Version für den Zugriff auf Ressourcen über virtuelle private Netzwerke (VPNs). Bei der Verwendung eines VPN wird der Zugang ganzheitlich gewährt und ermöglicht den Benutzer*innen den Zugriff auf das gesamte Ressourcennetz, was ein erhebliches Sicherheitsrisiko darstellt. Wenn böswillige Akteure über das VPN vollständigen Netzwerkzugang erhalten, können sie sich seitlich bewegen, um auf alle Inhalte innerhalb dieses Netzwerks zuzugreifen.

Historisch gesehen sind VPNs weder benutzer- noch mobilitätsfreundlich. In der modernen Arbeitswelt müssen Benutzer*innen in der Lage sein, jederzeit und von jedem Ort aus Zugriff zu haben.

MODERNE IDENTITÄTS- UND ZUGANGSVERWALTUNG

Bei der Umstellung von der alten auf die moderne IT geht es nicht nur um die Technologie, sondern auch darum, wie die Technologie eingesetzt wird, um die Produktivität der Endbenutzer zu steigern und das Unternehmen zu verändern.

DER IDENTITÄTSSTAPEL

Verzeichnisdienste

Dient als zentraler Datensatz für Mitarbeiter*innen, z. B. Name und Abteilung. Wird häufig bei der Integration mit Verwaltungsplattformen wie Jamf Pro genutzt, um angepasste Geräte für Endbenutzer*innen bereitzustellen.

Altlasten: Active Directory vor Ort

Modern: Cloud-Directory.

Cloud SSO

Cloud-SSO baut auf Informationen aus Verzeichnisdiensten auf und stellt sicher, dass Endbenutzer sichere Anmeldeinformationen eingeben, um auf Unternehmensressourcen zuzugreifen.

Altlasten: Benutzer*innen müssen sich jedes Mal authentifizieren, wenn sie auf Cloud-basierte Apps oder Ressourcen zugreifen.

Modern: Benutzer genießen Zugriff auf Cloud-basierte Apps wie Microsoft Outlook und Slack bei weniger Authentifizierungs-Aufforderungen.

Jamf Connect

Mit Verzeichnisdiensten und Cloud SSO vereinheitlicht Jamf Connect die Identität in allen Unternehmensapps und auf den Geräten der Benutzer*innen, ohne das Vertrauen zu beeinträchtigen. Endbenutzer nutzen eine einzige Cloud-Identität, um einfach und schnell Zugang zu den Ressourcen zu erhalten, die sie für ihre Produktivität benötigen.

Modern:

- Optimieren Sie die Bereitstellung und Authentifizierung für die vollständige Unterstützung von Mitarbeitern an entfernten Standorten.
- Automatische Synchronisierung von Benutzeridentitäten und Geräteanmeldeinformationen.
- Sicherstellen, dass die IT-Abteilung über umfassende Identitätsmanagement-Funktionen verfügt.
- Sicherer Zugriff auf Unternehmensressourcen und Apps mit VPN der nächsten Generation

Verzeichnisdienste

Verzeichnisdienste + Cloud SSO

Verzeichnisdienste + Cloud SSO + Jamf Connect

MODERNE IDENTITÄTSVERWALTUNG

Der moderne Identitätsstapel besteht heute aus drei Komponenten:

1. **Verzeichnisdienste und Cloud basiertes Single Sign-On (SSO) von einem Cloud Identitätsanbieter (Cloud IdP), in der Regel Azure oder Okta**
2. **Jamf für die Verwaltung mobiler Geräte**
3. **Jamf Connect zur Vereinheitlichung von Cloud IdP, Hardware und Software, mit sicherem Zugriff auf Geschäftsapps**

Alle Komponenten arbeiten zusammen, um die Erfahrung der Endbenutzer*innen für mobile Mitarbeiter*innen zu verbessern und das allgemeine Sicherheitsniveau für die gesamte Bereitstellung zu erhöhen.

Was ist ein Identity Provider?
Ein Identity Provider (IdP) ist ein Service, der digitale Identitäten speichert und verwaltet. Unternehmen nutzen diese Services, um ihren Mitarbeiter*innen oder Benutzern die Verbindung zu den von ihnen benötigten Ressourcen zu ermöglichen. Sie bieten eine Möglichkeit, den Zugang zu verwalten und Privilegien hinzuzufügen oder zu entfernen, während die Sicherheit gewährleistet bleibt.

Was ist Single-Sign-On (SSO)?
Single Sign-On (SSO) ist ein Authentifizierungsverfahren, das es Benutzer*innen ermöglicht, sich mit einem einzigen Satz von Anmeldedaten sicher bei mehreren Apps und Websites zu authentifizieren.

MODERNE IDENTITÄTS - UND ZUGANGS VERWALTUNG

Da sich alle Mitarbeiter*innen an einem Standort befanden und nur die verfügbare Technologie nutzten, um einen kleineren digitalen Fußabdruck zu hinterlassen, waren die grundlegenden Identitätsmanagementverfahren ausreichend. Das Problem ist, dass sich die Technologie verändert hat, dass Ihre Mitarbeiter*innen täglich mehr Geräte benutzen, um auf viel mehr Daten und Software zuzugreifen, dass die Sicherheitsrisiken gestiegen sind und dass Ihre Mitarbeiter*innen nicht mehr statisch, sondern dynamisch sind.

Wie bei vielen Aspekten der Technologie und der IT-Infrastruktur musste sich das Spiel ändern, als die Mitarbeiter*innen mobil wurden. Bei der Identitätsverwaltung war das nicht anders. Um AD und LDAP zu verwenden, bindet ein Benutzer/eine Benutzerin sein/ihr Gerät an ein lokales AD. Aber wie bereits erwähnt, waren die Mitarbeiter*innen nicht mehr durchgängig vor Ort, was zu Problemen führte:

- Benutzer*innen können ihre Passwörter nur vor Ort ändern, wenn AD erreichbar ist. Dies führt sowohl zu Verwirrung als auch zu kostspieligen Helpdesk-Tickets, wenn ein Benutzer/eine Benutzerin sein/ihr Passwort vergisst oder es ganz ändern muss.
- Da AD für Windows entwickelt wurde, werden durch die Nutzung von AD als primärem Identity Provider die Verwaltungsfunktionen für Macs eingeschränkt. Dies erfordert den Einsatz von Add-ons Dritter, was die Verwaltung der Benutzer*innen komplexer macht und höhere Kosten verursacht.
- Benutzer*innen aus der Ferne müssen sich im lokalen Netzwerk (LAN) befinden oder ein virtuelles privates Netzwerk (VPN) verwenden, um auf interne Ressourcen zuzugreifen. Das ruiniert die Benutzererfahrung und steigert die Frustration.

Diese und andere Gründe führen dazu, dass die Einführung von Cloud IdPs zu einem Kernstück der modernen Identitäts- und Zugangsverwaltung wird.

WARUM DIE CLOUD FÜR DEN ERFOLG VON HEUTE ENTSCHEIDEND IST

Mit Cloud Identity kann die IT-Abteilung Benutzer, Gruppen, Passwörter und den Zugang zu Unternehmensanwendungen und Cloud-Ressourcen zentral und aus der Ferne verwalten. Cloud IdPs wie Microsoft, Google und Okta bieten allen Mitarbeiter*innen — ob vor Ort oder aus der Ferne — sicheren Zugriff auf die Ressourcen, die sie für ihre Produktivität benötigen.

Identität des Erbes	Moderne Identität
• Active Directory	• Azure
• Open Directory	• Okta
• LDAP	• Google Suite

Die Zusammenarbeit mit einem Cloud Identitätsanbieter ermöglicht es Unternehmen, über die Grenzen ihres Büros hinauszugehen und eine nahtlose Benutzererfahrung zu bieten, während ihre Daten und Geräte sicher bleiben.

WARUM DIE CLOUD FÜR DEN ERFOLG VON HEUTE ENTSCHEIDEND IST

Ihr IdP — Okta, Azurblau, G Suite usw. — wird als Ihr Directory Service fungieren (d.h. das „Telefonbuch“ für Mitarbeiter*innen). Dazu gehören ihre persönlichen Daten, die Abteilung, in der sie arbeiten, ihre Berufsbezeichnung und vor allem, welche Apps/Ressourcen für sie bestimmt sind. Wenn sich ein*e Benutzer*in beim Cloud-IdP anmeldet und seine/ihre Identität validiert, hat er/sie Zugriff auf alles, was im Cloud-Verzeichnis für ihn/sie vorgesehen ist. **Authentifizierung und Autorisierung in Aktion!**

Mit diesem Cloud IdP können Sie auch die Vorteile von SSO nutzen, um die Sicherheit Ihrer mobilen Geräte zu erhöhen und die Benutzerfreundlichkeit auf einen Schlag zu verbessern. Anstatt dass Ihre Benutzer sich selbst authentifizieren und bei jeder einzelnen Plattform, Anwendung und jedem Dienst anmelden müssen, den Sie anbieten, können sie dies mit SSO einmalig und sicher tun und erhalten dann Zugang zu allem, was sie benötigen.

WARUM DIE CLOUD FÜR DEN ERFOLG VON HEUTE ENTSCHEIDEND IST

Um diese Sicherheit einen Schritt weiterzubringen, können Unternehmen die Multi-Faktor-Authentifizierung (MFA) nutzen. Durch das Hinzufügen von MFA fügen Sie einen einfachen, zusätzlichen Schritt hinzu, bei dem Ihr Endbenutzer/Ihre Endbenutzerin seine/ihre Identität über einen anfälligen Benutzernamen und ein Passwort hinaus bestätigen muss, bevor er Zugriff auf die benötigten Ressourcen erhält.

Um dies zum Leben zu erwecken und Ihren Cloud IdP mit Ihren Geräten zu vereinen, kommt Jamf Connect ins Spiel.

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

Die Multi-Faktor-Authentifizierung (MFA) ist ein Authentifizierungsverfahren, bei dem der Benutzer*innen zwei oder mehr Verifizierungsfaktoren angeben muss, um Zugang zu einer Ressource zu erhalten. Dies kann eine PIN auf dem Telefon des Nutzers/der Nutzerin, FaceID, eine Verifizierung per Fingerabdruck oder eine Reihe anderer Optionen sein.

JAMF CONNECT BRINGT ALLES NAHTLOS ZUSAMMEN.

Active Directory wurde für Windows entwickelt, was bedeutete, dass Apple Nutzer*innen keine andere Möglichkeit als die Anbindung an AD hatten, bevor Jamf Connect dies änderte.
Da Unternehmen sich von AD abwenden und mehr Mac Geräte einsetzen, um der wachsenden Nachfrage gerecht zu werden, müssen sie Arbeitsabläufe einrichten, um die Unternehmensdaten zu schützen und gleichzeitig eine ideale Benutzererfahrung zu bieten.

Mit Jamf Connect integrierte Cloud IdPs ermöglichen der IT-Abteilung die Fernverwaltung von Benutzerpasswörtern und den Zugriff auf Unternehmensapps. Mit einer automatisierten MDM-Registrierung ist der Prozess einfach und sicher:

1. **Ein Benutzer wird eingeladen, sich für die automatische MDM-Registrierung anzumelden.**
2. **Während der Registrierung wird Jamf Connect vom MDM Server heruntergeladen und installiert.**
3. **Benutzer*innen werden direkt zum Jamf Connect Login-Fenster weitergeleitet und geben ihre Cloud Identity Anmeldedaten ein, anstatt ihren eigenen Benutzernamen und ihr eigenes Passwort zu erstellen.**

JAMF CONNECT BRINGT ALLES NAHTLOS ZUSAMMEN.

Der Benutzer/die Benutzerin hat für alles denselben Benutzernamen und dasselbe Passwort, was ein unglaubliches Erlebnis schafft und gleichzeitig die Sicherheit des Kontos gewährleistet.

Zu den Vorteilen gehören:

Erstellung von Konten: Erstellen Sie lokale Mac Accounts auf der Grundlage von Okta, Microsoft Azure, Google Cloud und Identitäten, was zu einer verbesserten Anmeldeerfahrung für Benutzer*innen und einer organisierten Mac Fleet für die IT-Abteilung führt.

Sicheres Enrollment: Nutzen Sie die moderne Authentifizierung, um zu überwachen, auf welche Geräte von wo und von wem aus zugegriffen wird, und stellen Sie sicher, dass sich der richtige Benutzer auf dem Gerät befindet, bevor Sie sensible Daten bereitstellen.

Eliminieren Sie gemeinsam genutzte Administratorkonten: Erstellen Sie mehrere IT-Administratorkonten, die die Berechtigungen des Cloud IdP nutzen, ohne dass gemeinsame Servicekonten erforderlich sind.

Durchsetzung von Kennwortrichtlinien: Administrator*innen können Passwortrichtlinien über den IdP durchsetzen, um die Konsistenz und Sicherheit für alle Benutzer*innen zu gewährleisten.

Passwort-Synchronisierung: Synchronisieren Sie den Mac Benutzernamen und das Kennwort mit den Cloud Identitätsdaten und nutzen Sie eine einzige Identität für alles, was Sie für die Produktivität benötigen.

*Die Synchronisierung von Passwörtern ist für Google Cloud derzeit nicht verfügbar.

JAMF CONNECT BRINGT ALLES NAHTLOS ZUSAMMEN

Moderne Identitäts- und Zugangsverwaltung und eine Zero Trust Network Access (ZTNA)-Lösung aus einer Hand.

Wenn Unternehmen ZTNA implementieren, werden ihre Benutzer*innen authentifiziert und autorisiert, und die Geräte werden jedes Mal überprüft, wenn ein Benutzer/eine Benutzerin auf Daten oder Ressourcen zugreift. Least-Privilege-Durchsetzung und Geräteprüfungen in Echtzeit ermöglichen den Zugriff auf jede App nur für bestimmte, autorisierte Benutzer*innen auf vertrauenswürdigen Geräten.

ZTNA ermöglicht die Benutzerauthentifizierung mittels SSO über Ihren bevorzugten Cloud basierten IdP. Die Integration mit bestehenden Cloud basierten IdPs ermöglicht eine schnelle Bereitstellung und Verwaltung von Richtlinien. Eine Verbindung kann nur dann hergestellt werden, wenn der Benutzer/die Benutzerin über die entsprechenden Berechtigungen für die angegebene App verfügt.

Weitere Informationen über ZTNA finden Sie in unserem E-Book.

IDENTITÄTS- UND ZUGANGS-VERWALTUNG IST HIER.

Die steigende Nachfrage nach Remote-Belegschaften, mobilen Mitarbeiter*innen und dem ständigen Zugang zu Arbeitsmaterialien macht dies zu einer Notwendigkeit. Jamf führt Ihre gesamte Infrastruktur in einer nahtlosen Erfahrung für Benutzer*innen und IT zusammen.

Testversion anfordern

oder kontaktieren Sie Ihren bevorzugten Reseller, um loszulegen.