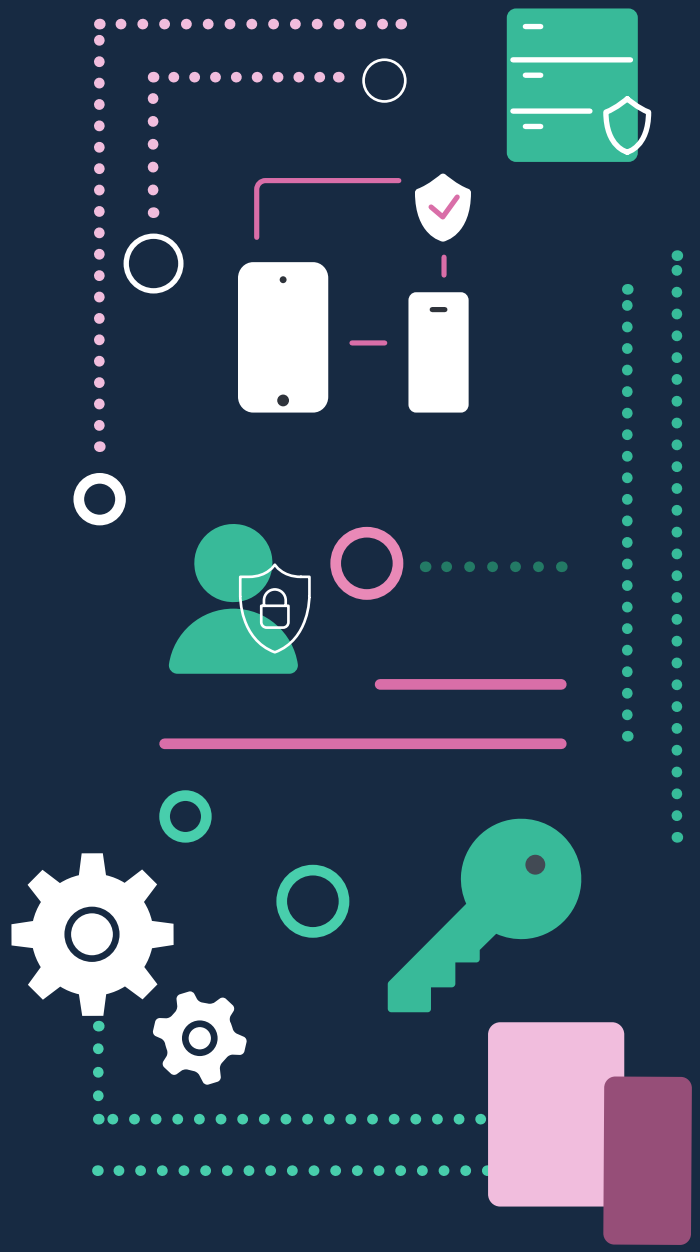


jamf

Identität Verwaltung und Sicherheit

Ein erweiterter Leitfaden

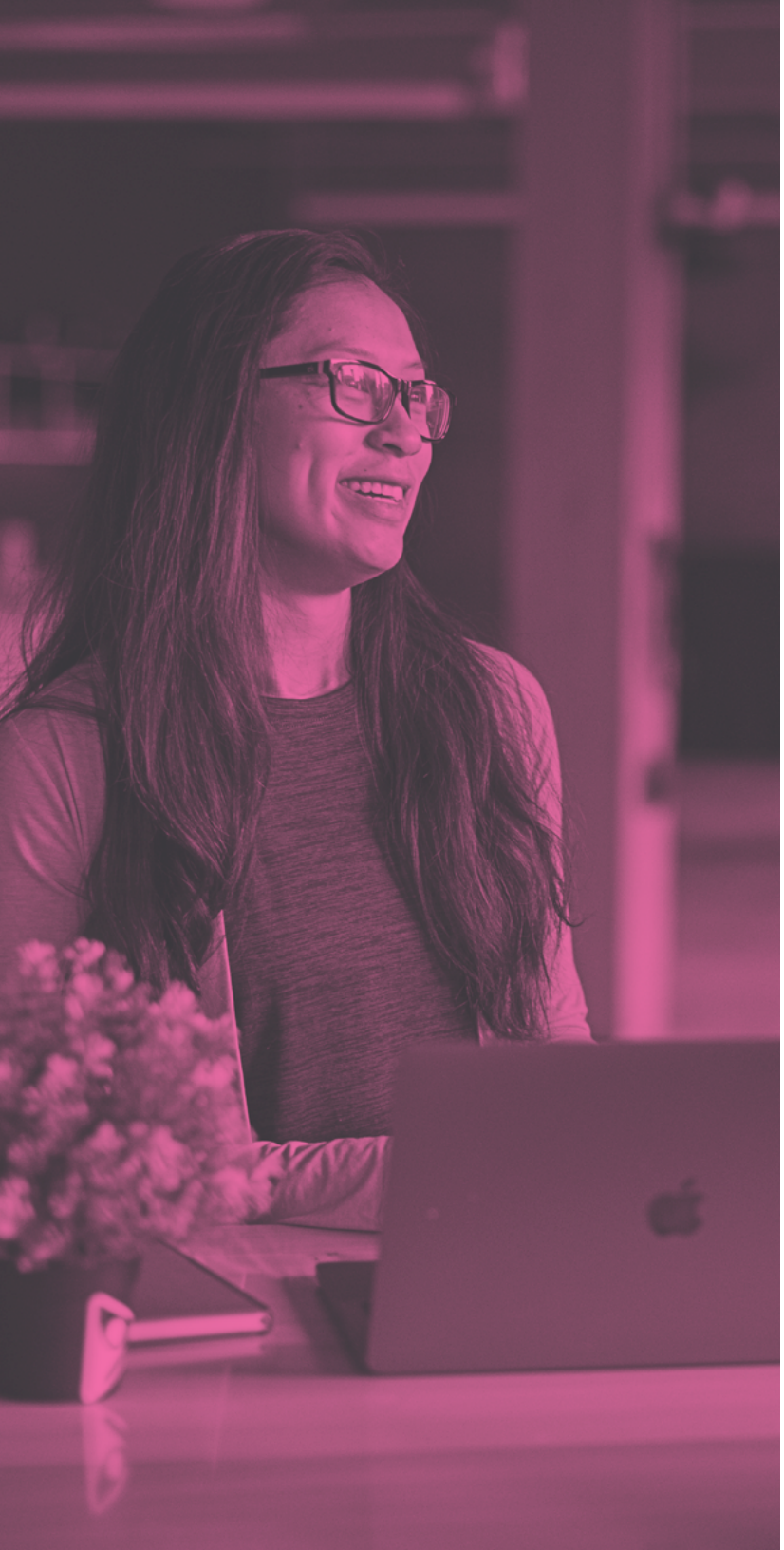
JEDER ARBEITNEHMER HAT SEINE EIGENE IDENTITÄT

Im Laufe des letzten Jahrzehnts ist die Bedeutung der Identitätsverwaltung ganz deutlich geworden, da Organisationen zunehmend die Anforderung von Telearbeiter*innen erfüllen müssen. Eine Migration von Systemen vor Ort zur Cloud hat viele Organisationen der modernen Identitätsverwaltung einen Schritt näher gebracht – ein Thema, das wir in „Identitätsverwaltung für Anfänger“ behandelt haben. Identitätsmanagement geht jedoch weit über Authentifizierung und Autorisierung hinaus, da Unternehmen auf dem Weg zum Erreichen ihrer Zero-Trust-Sicherheitsziele Benutzeridentitäten nutzen.

Ein wichtiger Punkt des Zero-Trust-Konzepts besteht darin, dass man den zahlreichen Komponenten nicht vertraut, die zusammen die Verbindung zwischen Ihren Benutzer*innen und Ihren Diensten herstellen. Eine der größten Komponenten, der Sie nicht vertrauen (und nicht vertrauen sollten) ist das Netzwerk. Um Ihnen Schritt für Schritt zu helfen, werden wir einige Aspekte der Technologien und Details behandeln, an die Sie beim Planen der Identitäts- und Sicherheitsverwaltung denken sollten. Wenn Sie unsere Einführung in Zero Trust mit dem Vertrauen in Zero-Trust-Asset noch nicht gelesen haben, sollten Sie das vielleicht vorher tun. Dieses E-Book wird die in den oben genannten Texten erwähnten Konzepte detaillierter behandeln und Sie auf eine fortgeschrittene Stufe bringen.

IN DIESEM LEITFADEN BESPRECHEN WIR FOLGENDES:

- Wie moderne Authentifizierung funktioniert
- Methoden zur Sicherung des Netzwerkverkehrs
- Hinzufügen von Workflows mit bedingtem Zugriff
- Wie Jamf das alles zusammenbringt



MODERNE AUTHENTIFIZIERUNG FÜR DIE UNGEDULDIGEN

In unserem vorherigen E-Book „Identitätsverwaltung für Anfänger“ haben wir die Unterschiede zwischen Autorisierung und Authentifizierung abgedeckt. Jetzt sprechen wir darüber, wie das mit modernen Services ausgeführt wird, um ein Single-Sign-On (SSO) zu ermöglichen.

Es gibt zwar viele Methoden zur Validierung eines Benutzers/einer Benutzerin, aber die gängigsten sind SAML (Security Assertion Markup Language) und OAuth in Kombination mit OIDC (OpenID Connect). Beide Systeme verfolgen sehr ähnliche Ziele, nämlich die Authentifizierung eines Benutzers/einer Benutzerin gegenüber einer Wahrheitsquelle, die in der Regel als IdP (Identity Provider) bezeichnet wird, und die anschließende Generierung eines Codes, der mit anderen Diensten geteilt werden kann, um zu beweisen, wer Sie sind. Wenn Sie mit Kerberos aus der Arbeit mit Active Directory vertraut sind, werden Sie viele Ähnlichkeiten feststellen.

MODERNE AUTHENTIFIZIERUNG FÜR DIE UNGEDULDIGEN

HIER SIND DIE FÜR ADMINISTRATOR*INNEN WICHTIGEN PUNKTE:

- Die SAML-Authentifizierung generiert Assertions, das sind signierte XML-Blöcke, die Sie identifizieren und es anderen Diensten ermöglichen, darauf zu vertrauen, dass Sie authentifiziert worden sind.
- SAML erfordert, dass alle Dienste individuelle Zertifikate für die Kommunikation mit dem SAML-Authentifizierungsanbieter verwenden, was die Verwendung nativer Anwendungen oder von Anwendungen, die auf den Geräten der Benutzer*innen laufen, erschwert.
- OIDC arbeitet mit OAuth zusammen, um signierte JWT (JSON Web Tokens) zu generieren, die aus JSON und nicht aus XML bestehen, aber ansonsten funktional ähnlich wie SAML-Assertions sind.
- OIDC hat den zusätzlichen Vorteil eines ID-Tokens, das immer ein JWT ist. Es handelt sich um einen tragbaren Benutzerdatensatz, der zum Nachweis seiner Gültigkeit auch signiert ist.

Während der Authentifizierung bei einem Service über SAML oder OIDC/OAuth, erhält der Service nie das Passwort des Benutzers/der Benutzerin, da das nur von Ihrem IdP gehandhabt wird. Stattdessen erhält der Service entweder eine SAML-Assertion oder ein OAuth-Token, das vom IdP signiert ist, damit der Service ihm vertrauen kann. Es gibt zwar unterschiedliche Implementierungsdetails, aber sowohl SAML als auch OIDC/OAuth bieten sehr sichere, moderne und erweiterbare Möglichkeiten zur Authentifizierung eines Benutzers/einer Benutzerin bei Services.

MODERNE AUTHENTIFIZIERUNG FÜR UNGEDULDIGE

Hier ist ein Beispiel für eine SAML Assertion:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                     AssertionConsumerServiceURL="https://[servername].jamfcloud.com/saml/SSO"
                     Destination="https://login.microsoftonline.com/[tenant]/saml2"
                     ForceAuthn="false"
                     ID="a4a9efd7a384732928bf1bdbg2afab3"
                     IsPassive="false"
                     IssueInstant="2021-04-02T16:30:58.826Z"
                     ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                     Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://[servername].jamfcloud.com/saml/metadata</saml2:Issuer>
</saml2p:AuthnRequest>
```

Zum Vergleich hier ein Beispiel eines OAuth Tokens:

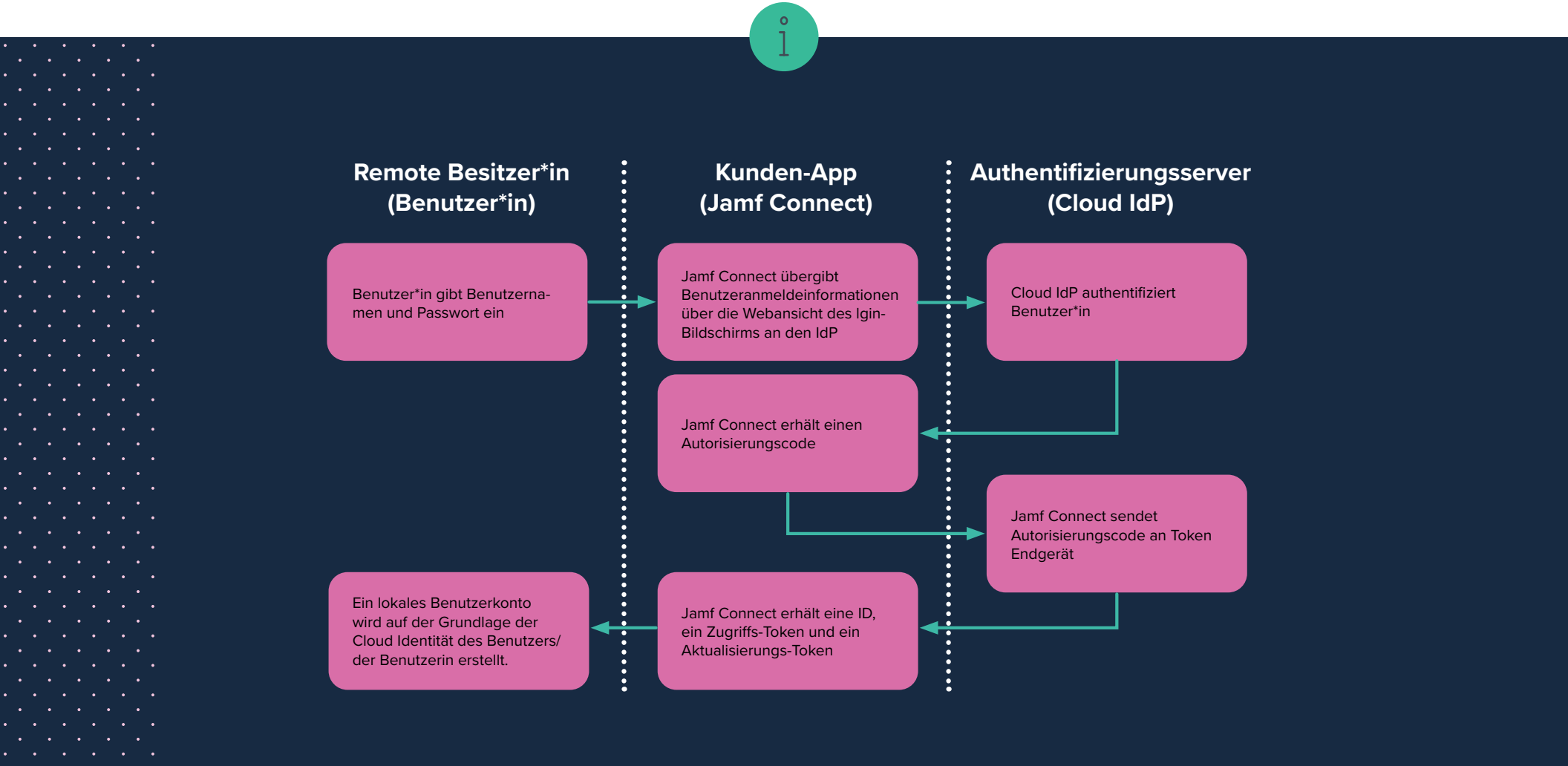
```
"app_displayname": "My Sample OIDC App Name",
  "appid": "2520beb2-535e-4e42-bf70-1d4cd5429551",
  "appidacr": "0",
  "family_name": "Lastname",
  "given_name": "Firstname",
  "idtyp": "user",
  "ipaddr": "52.205.5.180",
  "name": "Firstname Lastname",
  "oid": "0fa4b783-1c00-4765-b40d-c2b72de03079",
  "onprem_sid": "S-1-5-21-1861720204-2608728089-2580082577-1523",
  "platf": "5",
  "puid": "100320004CDFC4DB",
  "rh": "0.AQ4A2rA-GiB-Uuy8iVxxpwQALK-ICVeU0JOy3AdTNVClVFQAQ8.",
```

*Hinweis: Dies ist eine Teildarstellung des Tokens, kein vollständiges Token-Muster.

SAML UND OIDC/OAUTH MIT JAMF

Jamf Pro verwendet SAML, während Jamf Connect und Jamf Protect OIDC/OAuth verwenden. Für Jamf Connect ist SAML nicht anwendbar, da Zertifikate erforderlich sind und Zertifikate und private Schlüssel an Benutzergeräte gesendet werden müssen, von denen man nicht weiß, ob man ihnen vertrauen kann. Das Endergebnis ist die Fähigkeit von Jamf, die Multi-Faktor-Authentifizierung von Ihrem Cloud-IdP zu unterstützen, ohne dass Sie die Benutzer*innen bei jedem Dienst im Detail überwachen müssen.

Hier ist ein Beispiel dafür, wie Jamf Connect einen OIDC Authorization Code Grant verwendet, um den Cloud-Benutzernamen und das Passwort des Benutzers/der Benutzerin im Austausch für einen Autorisierungscode zu authentifizieren, den Jamf Connect an Ihren IdP-Token-Endpunkt sendet.



MODERNE AUTHENTIFIZIERUNG UND IDP FÖDERATION

Man kann nicht über moderne Authentifizierung sprechen, ohne auf das Thema IdP Föderation einzugehen. Hier können Sie Azure AD mit Microsoft Office 365 verwenden, aber die Identität ist wirklich mit Okta föderiert, da dies Ihr IdP ist, der die „Wahrheit" über das Passwort eines Benutzers/einer Benutzerin hat. Die Föderation kann zwar sehr kompliziert werden und mehrere Ebenen der Umleitung umfassen, aber das Grundkonzept besteht darin, dass ein IdP die Authentifizierung an einen anderen IdP weitergeben kann.

In den meisten Fällen sollten Dienste, die sich über SAML oder OIDC in einen IdP integrieren können, nicht wissen oder sich darum kümmern müssen, ob Sie mit einem anderen Anbieter/einer anderen Anbieterin föderiert sind. Die meisten dieser Details werden aus der ursprünglichen Verbindung abstrahiert.

MULTI-FAKTOR-AUTHENTIFIZIERUNG

Da wir über die Authentifizierungsmethoden gesprochen haben, sollten wir auch die Multi-Faktor-Authentifizierung (MFA) und die passwortlose Authentifizierung erwähnen.

Gestohlene Anmeldedaten stellen heutzutage eines der größten Sicherheitsprobleme dar, denen Organisationen gegenüberstehen. Tatsächlich gehen 80% aller Datenverletzungen auf gestohlene oder schwache Passwörter zurück, aber laut Weltwirtschaftsforum werden weniger als 10% der Mittel für die Eliminierung von kompromittierten Anmeldedaten ausgegeben. Als Reaktion darauf nutzen viele Organisationen ihren Identitätsanbieter, um MFA und passwortlose Sicherheit einzuführen.

IdPs können ein weites Spektrum an MFA unterstützen, und in geringerem Umfang auch passwortlose Lösungen. Herkömmliche MFA-Typen basierten auf Einmalpasswörtern (OTP), bei denen der Benutzer/die Benutzerin zusätzlich zu seinem Passwort eine sich ständig ändernde Zahl eingeben musste. Die Nummer wurde entweder auf einem kleinen Schlüsselanhänger mit einem LCD-Bildschirm oder einer App auf einem ihrer Geräte generiert.

Um es den Nutzer*innen leichter zu machen, haben viele IdPs jetzt ihre eigene App für Mobilgeräte, bei der der Nutzer/die Nutzerin nach der Eingabe eines Passworts eine Push-Benachrichtigung auf dem Gerät erhält und darauf reagieren muss, in der Regel mit einer Form der biometrischen Authentifizierung, wie Face ID oder Touch ID, um sicherzustellen, dass die richtige Person auf den Push reagiert.

Ein weiterer MFA-Typ, der sich immer mehr durchsetzt, ist FIDO (Fast Identity Online), eine auf Datenschutz und Sicherheit ausgerichtete Authentifizierungsmethode, die in die meisten modernen Webbrowser integriert ist und auch die Form eines externen Sicherheitsschlüssels annehmen kann. FIDO und andere Formen der MFA können auch für die passwortlose Authentifizierung verwendet werden, bei der der Benutzer/die Benutzerin kein Passwort eingeben muss. Stattdessen wird die MFA für den gesamten Prozess verwendet.

Jamf Produkte unterstützen zahlreiche MFA-Optionen. Da die meisten IdP Authentifizierungen über eine Webansicht abgewickelt werden, werden die gesamte Konfiguration und Einrichtung der MFA Spezifikationen vom IdP selbst vorgenommen.

Jamf Connect kann beispielsweise die Okta Authentication API verwenden, um primäre Jamf Connect Aufgaben für Benutzer*innen zu konfigurieren, wie etwa:

- Cloud Authentifizierung auf einem lokalen Account
- Passwort-Synchronisierung
- Anmeldung von Benutzer*innen bei Okta

Lesen Sie die Entwicklerdokumentation von Okta, um mehr über diese API zu erfahren.

MEHR ALS VPNS

Wenn Sie vor der Einführung von Zero Trust den Datenverkehr zwischen den Geräten Ihrer Benutzer*innen und den von Ihnen angebotenen Diensten schützen wollten, haben Sie höchstwahrscheinlich ein VPN (Virtual Private Network) verwendet, um die gesamte Kommunikation mit Ihren Benutzern zu sichern. VPNs sind zwar immer noch ein sehr nützliches Instrument für IT-Abteilungen, haben aber auch einige Nachteile:

- Für die meisten VPNs ist eine Kunden Software erforderlich
- Unterstützt möglicherweise keine Cloud Authentifizierung
- Erfordert in der Regel spezielle Hardware in Ihrem Netzwerk, die Cloud basierte Dienste möglicherweise nicht schützt
- Bietet den Benutzer*innen oft eine schlechte Benutzererfahrung mit Mobilgeräten
- Schlechte Benutzererfahrung auf Mobilgeräten

Da die meisten Nutzer*innen zu Hause über eine immer schnellere Bandbreite verfügen, kann die Unterstützung eines VPN, das den von Ihren Nutzer*innen erzeugten Datenverkehr bewältigen kann, schnell sehr teuer werden.

ZERO-TRUST NETZWERKZUGRIFF

Eine neuere Philosophie zur sicheren Anbindung von Kund*innen an Dienste ist ZTNA (Zero Trust Network Access). Bei ZTNA wird kein VPN benötigt, und in den meisten Fällen nicht einmal Kunden Software. Stattdessen stellen die Nutzer über einen Webbrowser eine Verbindung zu einem ZTNA-Dienst her, der eine moderne Authentifizierung verlangen kann, die dann die Verbindung des Nutzers/der Nutzerin vermittelt oder anderweitig sichert.

Während ZTNA-Lösungen ursprünglich für den Schutz älterer On-Premise-Dienste entwickelt wurden, bei denen die Hinzufügung einer modernen Authentifizierung ansonsten unerschwinglich gewesen wäre, schützen viele von ihnen jetzt auch Cloud basierte Dienste, wenn dies gewünscht wird. Sie können ZTNA-Lösungen finden, die selbst Cloud basiert sind oder für den Betrieb in Ihrem eigenen Rechenzentrum konzipiert sind, wenn Sie mehr Kontrolle wünschen. Da ZTNA-Lösungen immer robuster werden, können Sie mehr als nur den Webverkehr sichern, was es Ihnen ermöglichen könnte, von einem VPN zur Sicherung des Zugangs zu Ihrem Netzwerk wegzukommen.

Erfahren Sie mehr über ZTNA mit Jamf.

Die ZTNA-Lösung von Jamf Connect wurde mit Blick auf die moderne Datenverarbeitung entwickelt, indem ein identitätszentriertes Sicherheits-modell mit risikobewusstem Richtli-nienmanagement und applikations-spezifischen Mikrotunneln integriert wurde.

BEDINGTER ZUGRIFF

Eine robuste Zero-Trust-Architektur umfasst oft Elemente des bedingten Zugriffs oder Gerätevertrauens. In diesen Situationen wird der Zustand des Geräts selbst Teil der Entscheidung darüber, wie sehr man der Verbindung trauen kann (falls überhaupt). Verwaltete Geräte helfen Unternehmen dabei, das Geräterisiko besser zu verstehen und zu entscheiden, welche vertrauenswürdigen Benutzer*innen auf vertrauenswürdigen Geräten und mit vertrauenswürdigem App Zugriff auf Daten und Ressourcen erhalten können.

Der bedingte Zugriff ist in der Regel eine Kombination aus der Zusammenarbeit Ihres IdP mit einem lokalen Agenten/einer lokalen Agentin oder Ihrer Gerätemanagementlösung, um festzustellen, welche Version des Betriebssystems auf dem Gerät läuft, welche Sicherheitsrichtlinien vorhanden sind oder eine Reihe anderer Attribute, die dazu beitragen, den Zustand des Geräts zu bestimmen Der IdP kann dann die Verbindung zulassen oder in einigen Fällen eine weitere Authentifizierung, z. B. eine zusätzliche MFA, verlangen, bevor er den Benutzer/die Benutzerin vollständig authentifiziert.

Ein bedingter Zugriff basiert darauf, was ein App-Benutzer/eine App-Benutzerin tun will. Möglicherweise benötigen Sie überhaupt keine MFA oder Dienste mit geringerer Sicherheit, wie z. B. den Zugriff auf ein IT-Ticketsystem. Der Zugriff auf ein Quellcode-Repository kann jedoch erfordern, dass der Benutzer/die Benutzerin nicht nur eine MFA-Prüfung besteht, sondern sich auch auf einem unternehmenseigenen und verwalteten Gerät befindet.

Es gibt eine Reihe von Anbieter*innen, die bei der Verwaltung von Identität und Zugang zu Diensten helfen, darunter Centrify, Duo Security, Microsoft, Ping Identity, Okta und Salesforce. Viele dieser Tools funktionieren mit vorhandener Authentifizierungsinfrastruktur wie Ihrem Cloud Identity Provider und erweitern diese Identitäten mithilfe der bereits erwähnten Protokolle OIDC und SAML auf Cloud-Services.

Sehen wir uns ein Beispiel dafür an, wie Jamf mit Microsoft zusammenarbeitet, um bedingten Zugriff zu ermöglichen. Jamf Pro kann Richtlinien auf Geräten erzwingen, um auf Microsoft Office 365 zugreifen zu können, indem der bedingte Zugriff mit Enterprise Mobility + Security (EMS) genutzt wird. Von Jamf verwaltete Macs erhalten jetzt Zugriff auf Microsoft Apps, sofern sie die von Microsoft Endpoint Manager vorgegebenen Richtlinien bezüglich der Geräte-Compliance erfüllen. Sobald die Daten des Mac in der Cloud sind, können Endpoint Manager und EMS vollständig in Jamf integriert werden, um Verwaltungsfunktionen auf dem Gerät wahrzunehmen. Wenn ein nicht verwalteter Mac den Zugriff auf E-Mail oder andere Cloud Dienste anfordert, kann die IT-Abteilung einen benutzerinitiierten Anmeldeprozess von Jamf Pro aus aktivieren und sicherstellen, dass nicht sichere oder nicht verwaltete Geräte unter der Verwaltung angemeldet werden, bevor der Zugriff gewährt wird.

DER BEDINGTE ZUGRIFF VON JAMF UNTERSTÜTZT NICHT NUR MICROSOFT, SONDERN AUCH WICHTIGE FÜHRUNGSKRÄFTE DER BRANCHE WIE GOOGLE UND AWS.

Wenn die Benutzeranmeldeinformationen von Microsoft und die Geräteanmeldeinformationen von Jamf überprüft werden, wird eine Analyse des Benutzerrisikos, des Geräterisikos (entspricht das Gerät den Unternehmensrichtlinien oder nicht) und des Anwendungsrisikos (welche Apps wird verwendet) durchgeführt, um zu entscheiden, ob der Zugriff auf Cloud-Ressourcen gewährt oder gesperrt werden soll - und das alles in Echtzeit.

Jetzt erhalten Organisationen eine Erweiterung der Multi-Faktor-Authentifizierung durch verifizierte Compliance:

1. Benutzername und Passwort
2. Code und Token
3. Geräte-Compliance

Auf diese Weise können Unternehmen kontextabhängig und dynamisch den richtigen Zugang auf der Grundlage eines Benutzers/einer Benutzerin, eines Geräts und des Kontexts des jeweiligen Anwendungsfalls bereitstellen und so den adaptiven und flexiblen Perimeter bereitstellen, der von den heutigen Mitarbeiter*innen mit mehreren Geräten und an mehreren Standorten gefordert wird.

ENDPUNKT-SICHERHEIT

Die durch das Identitätsmanagement implementierten Sicherheitsmaßnahmen betreffen sowohl die Endbenutzer*innen als auch die IT-Abteilung während des gesamten Lebenszyklus der Mitarbeiter*innen, unabhängig davon, ob sie vor Ort oder an einem anderen Ort arbeiten. SaaS-Apps und die Verbindung von Mitarbeiter*innen mit Unternehmensressourcen bieten Möglichkeiten, Risiken für Ihre Endgeräte, Ihre Benutzer*innen und Unternehmensdaten zu mindern.

Endgerätesicherheit ist die Praxis, für Geräte oder Endgeräte von Benutzer*innen das Risiko zu mindern, von bösartigen Akteur*innen genutzt zu werden. Es ist zunehmend wichtig, dass Geräte und Daten von autorisierten Benutzer*innen für legitime Zwecke verwendet werden, besonders wenn Daten in verschiedenen SaaS-Apps verteilt sind. Um dieses Ziel zu erreichen, müssen verschieden Faktoren zusammenarbeiten – darunter die Identitätsverwaltung, aber auch Virenschutz (AV), Sicherheits-Konfigurationsmanagement, Endgeräte-Entdeckung und Reaktion.

Unternehmen können nicht warten, bis Malware, Adware oder andere unerwünschte Softwareprobleme auftreten, und Sicherheitstools, die das Gerät mehr beeinträchtigen als schützen, verhindern nur die Produktivität der Endbenutzer*innen. Sie müssen über die Implementierung eines Virenschutzes nachdenken, der Mac-spezifische Angriffe effektiv identifiziert und behebt, ohne Ressourcen für die Suche nach Bedrohungen für Windows auf einem Mac aufzuwenden. Es gibt eine Menge zu bedenken, wenn es um Sicherheit geht, aber die gute Nachricht ist, dass Jamf bei all dem helfen kann.

Zusätzlich zu den Identitätsmanagement-Funktionen von Jamf Connect und den integrierten Sicherheitstools von Jamf Pro ist Jamf Protect so konzipiert, dass es sich nahtlos in die Sicherheitslandschaft Ihres Unternehmens einfügt, um Malware zu verhindern, vor Apple spezifischen Bedrohungen zu schützen und Endpunkte auf die Einhaltung von zu überwachen.

Für Unternehmen, die komplexere Umgebungen mit einer Vielzahl von Sicherheitstools haben, können wir die Fähigkeiten von Microsoft und Jamf kombinieren. IT-Administrator*innen und Sicherheitsteams haben von ihrer gewohnten Oberfläche aus einen vollständigen Überblick über die Sicherheitsaktivitäten in ihrer Mac Fleet. Jamf Protect überträgt alle Mac spezifischen Sicherheitsdaten und -warnungen direkt in Azure Sentinel mit minimaler Konfiguration. Alle bösartigen oder verdächtigen Mac Aktivitäten sowie Malware-Benachrichtigungen können einfach in vorhandene Workflows integriert werden, was wenig Mühe und Zeit vom Sicherheits- und IT-Personal erfordert. Mit den Angriffserkennungs- und Protokollinformationen von Jamf Protect kann Azure Sentinel seine Funktionen erweitern, um breit angelegte Angriffe auf alle Mac Geräte zu erkennen und zu beheben und gleichzeitig die Sicherheit des gesamten Unternehmens zu verbessern.

NEUAUSRICHTUNG IHRES SICHERHEITSSTATUS MIT IDENTITÄT

Es ist an der Zeit, das traditionelle, perimeterbasierte Sicherheitsmodell zu überdenken. Indem sie viele der gleichen Partner*innen nutzen, die bei der Bereitstellung der Identität helfen, können Unternehmen gleichzeitig moderne Sicherheit und sogar Nullvertrauen erreichen. Menschen und Daten sind in Bewegung und Organisationen benötigen moderne Lösungen, um auf diese Änderungen zu reagieren. Sie müssen über Gerätesicherheit, benutzerbasierte Sicherheit, Multi-Faktor-Authentifizierung und darüber hinaus führende Lösungen nachdenken. Sie müssen ihre Endgeräte sichern.

Jamf bietet eine Möglichkeit, das alles zu vereinen. Bessere Sicherheit beginnt hier.

Starten Sie mit einer kostenlosen Testversion

oder kontaktieren Sie Ihren bevorzugten Reseller, um loszulegen.