jamf

# Identitätsverwaltung und Sicherheit

ein erweiterter Leitfaden

# Jeder Arbeitnehmer hat seine eigene Identität

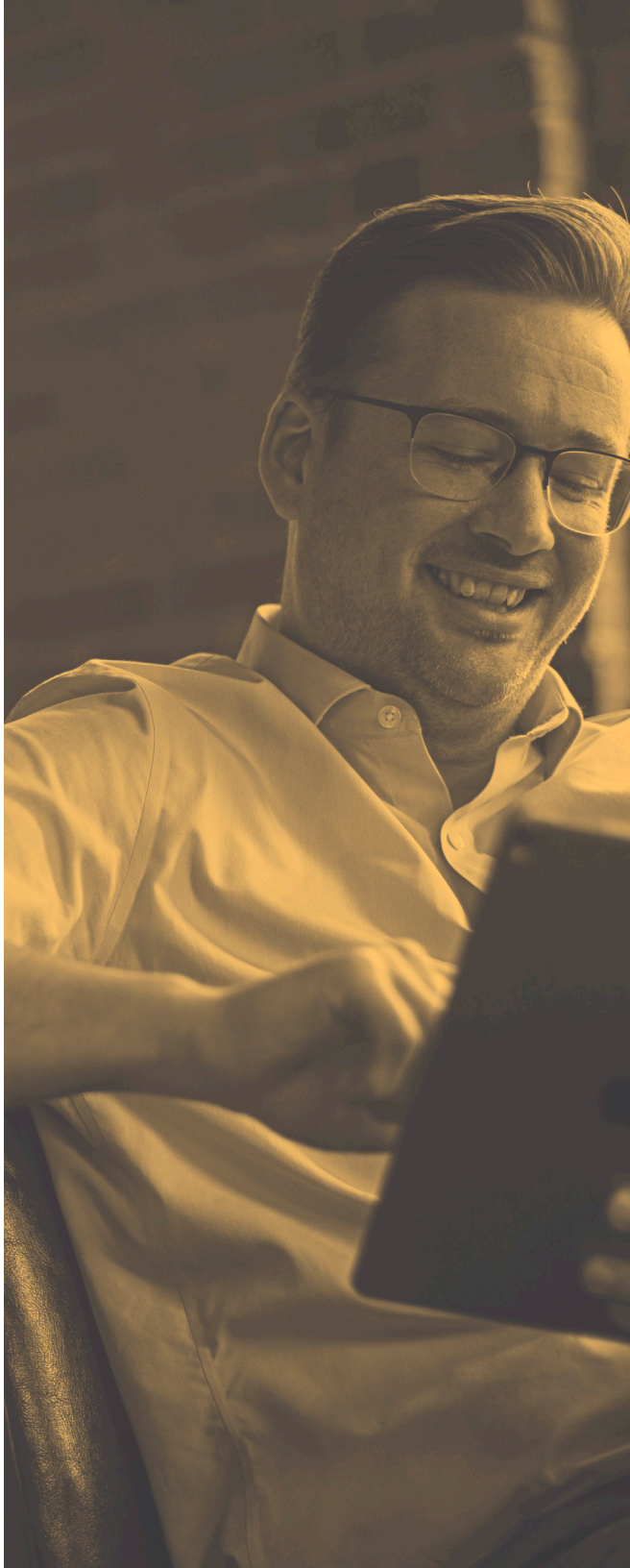
Im Laufe des letzten Jahrzehnts ist die Bedeutung der Identitätsverwaltung ganz deutlich geworden, da Organisationen zunehmend die Anforderung von Telearbeitern erfüllen müssen. Eine Migration von Systemen vor Ort zur Cloud hat viele Organisationen der modernen Identitätsverwaltung einen Schritt näher gebracht – ein Thema, das wir in „Identitätsverwaltung für Anfänger“ behandelt haben. Allerdings geht die Identitätsverwaltung weit über Authentifizierung und Autorisierung hinaus, da Organisationen Benutzeridentitäten nutzen wollen, um ihre Zero-Trust-Sicherheitsziele zu erreichen.

Ein wichtiger Punkt des Zero-Trust-Konzepts besteht darin, dass man den zahlreichen Komponenten nicht vertraut, die zusammen die Verbindung zwischen Ihren Benutzern 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 Putting Trust 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.

## Wir behandeln Folgendes:

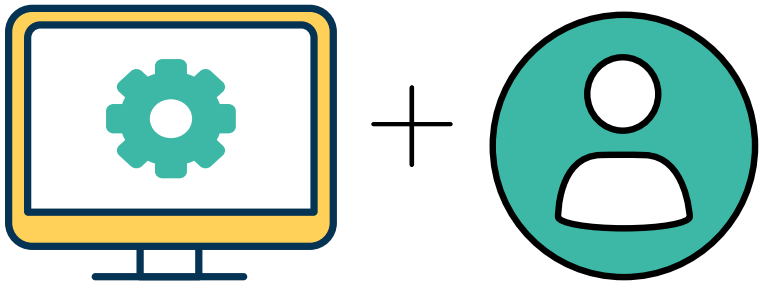
- Funktionsweise der modernen Authentifizierung
- Methoden zur Sicherung des Netzwerkverkehrs
- Workflows, um bedingten Zugriff zu implementieren
- die Verbindung durch Jamf

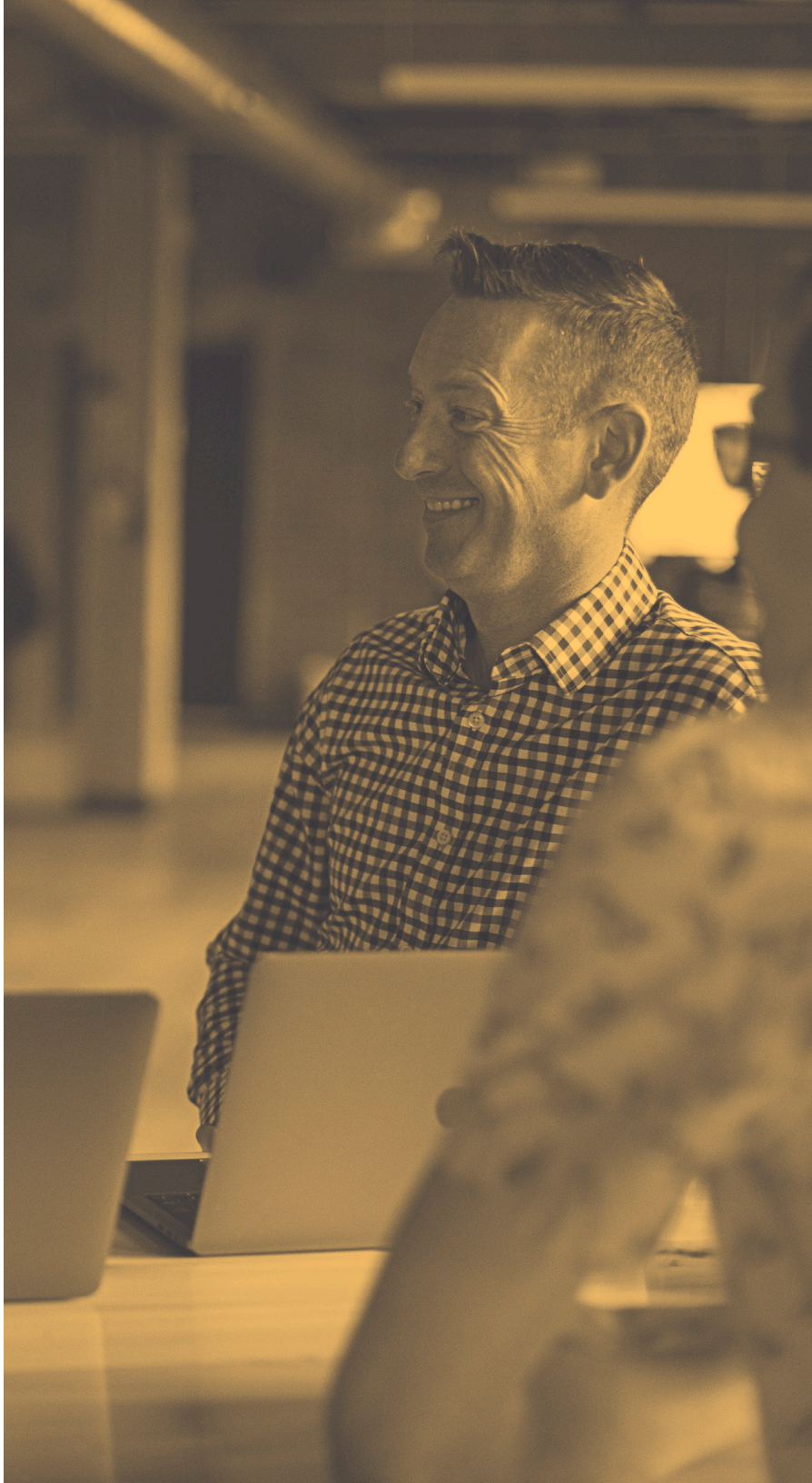


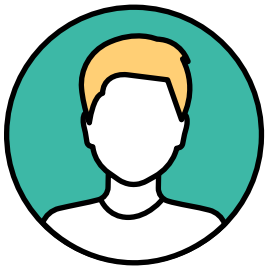
# Moderne Authentifizierung für Ungeduldige

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.

Während es viele Methoden gibt, um Benutzer zu validieren, werden heute SAML (Security Assertion Markup Language) und OAuth in Kombination mit OIDC (OpenID Connect) am häufigsten verwendet. Beide Systeme erfüllen sehr ähnliche Ziele, nämlich einen Benutzer anhand einer Quelle der Wahrheit zu authentifizieren, normalerweise als IdP (Identity Provider) bezeichnet, und dann einen Code zu generieren, der mit anderen Services geteilt werden kann, um nachzuweisen, wer Sie sind. Wenn Sie Kerberos von Ihrer Arbeit mit Active Directory her kennen, finden Sie hier viele Ähnlichkeiten.







# Moderne Authentifizierung für Ungeduldige

## Hier sind die für Administratoren wichtigen Punkte:

- Die SAML-Authentifizierung generiert sogenannte Assertions, signierte XML-Blöcke, die Sie identifizieren und anderen Services erlauben, auf Ihre Authentifizierung zu vertrauen.
- SAML erfordert, dass einzelne Services individuelle Zertifikate bei der Kommunikation mit dem SAML Authentifizierungsanbieter verwenden, was die Nutzung von nativen Apps oder Anwendungen, die auf den Geräten der Benutzer laufen, komplizierter macht.
- OIDC arbeitet mit OAuth zusammen, um signierte JWT (JSON Web Tokens) zu generieren, die JSON verwenden, nicht XML, aber sonst ähnlich wie SAML Assertions funktionieren.
- OIDC hat den zusätzlichen Vorteil eines ID Tokens, im Grunde ein portabler Nutzerdatensatz, der auch signiert ist, um seine Gültigkeit zu bestätigen.

Während der Authentifizierung bei einem Service über SAML oder OIDC/OAuth erhält der Service nie das Passwort des Benutzers, da das nur von Ihrem IdP gehandhabt wird. Stattdessen erhält der Service entweder eine SAML Assertion oder ein OAuth Token, die vom IdP signiert sind, damit der Service ihm vertrauen kann. Auch wenn sich die Implementierung in Details unterscheidet, bieten sowohl SAML als auch OIDC/OAuth sehr sichere, moderne und erweiterbare Methoden, um einen Benutzer bei Services zu authentifizieren.

# Moderne Authentifizierung für Ungeduldige

Hier ist ein Beispiel für eine SAML Assertion:

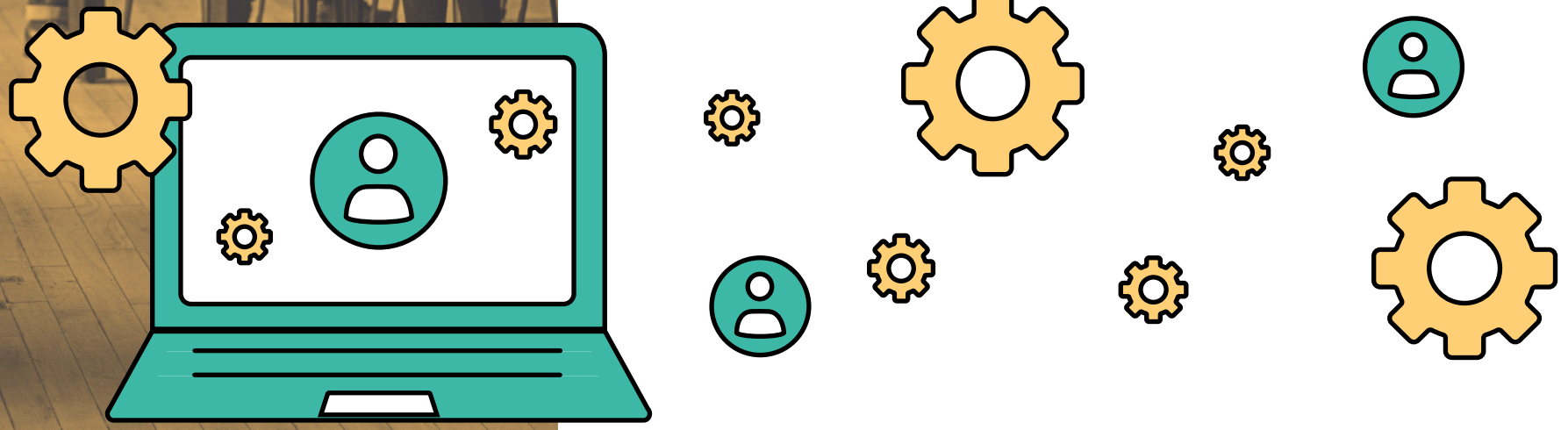
```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                     AssertionConsumerServiceURL="https://[servername].jamfcloud.com/saml/SSO"
                     Destination="https://login.microsoftonline.com/[tenant]/saml2"
                     ForceAuthn="false"
                     ID="a4a0efd7a384732928bf1bdbg2afab3"
                     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": "0fa4b783-1c80-4765-b40d-c2b72de03079",
  "onprem_sid": "S-1-5-21-1861720204-2608728089-2580082577-1523",
  "platf": "5",
  "puid": "100320004CDFC4D8",
  "rh": "0.AQ4A2rA_-GiB-UuvBjVxxpwQALK-ICVeU0JOv3AdTNVClVEOAO8.",
  "scp": "User.Read profile openid email",
```

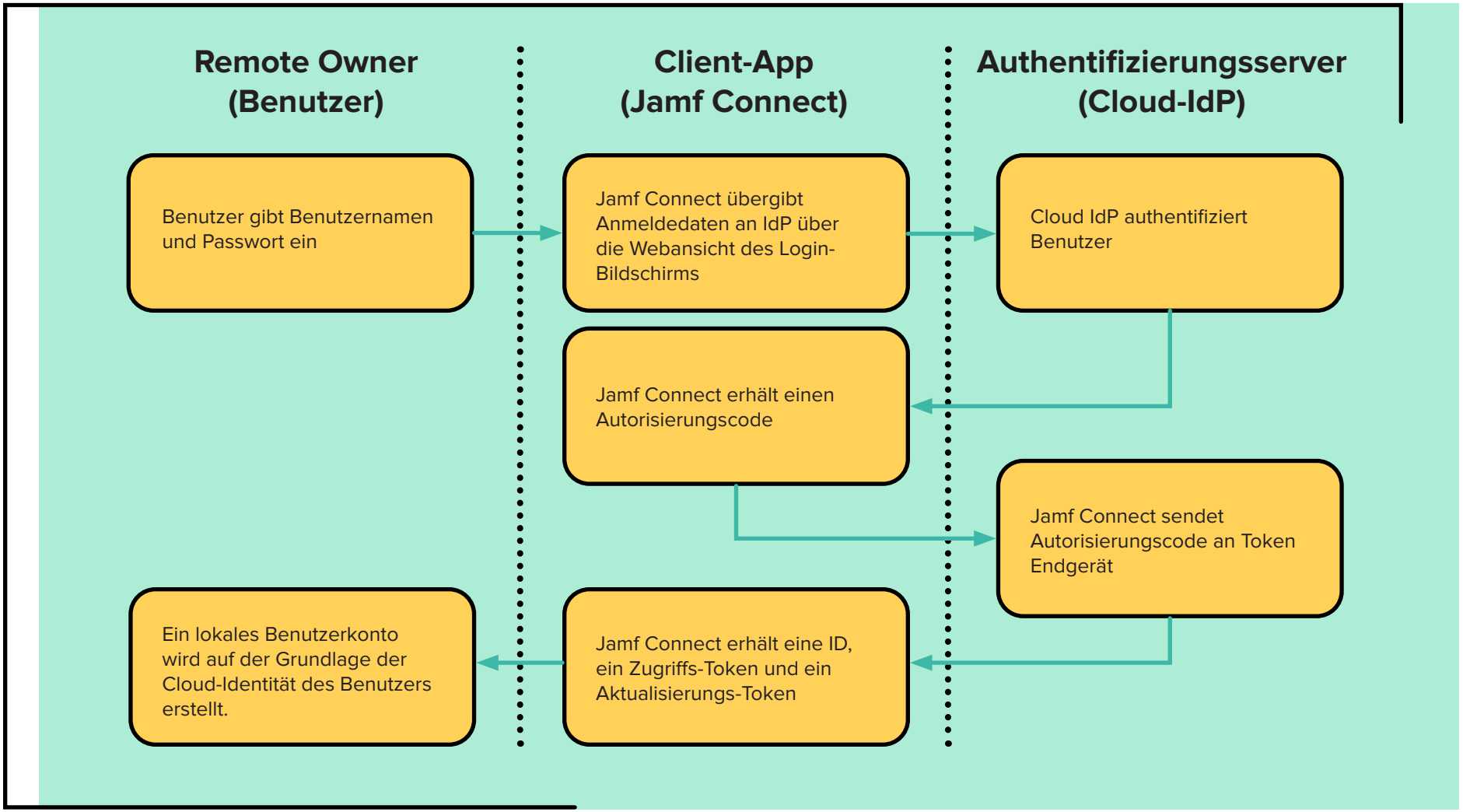
# SAML und OIDC/OAuth mit Jamf

Jamf Pro verwendet SAML, während Jamf Connect und Jamf Protect OIDC/OAuth verwenden. Für Jamf Connect ist SAML nicht anwendbar, da es Zertifikate benötigt und Zertifikate und private Schlüssel per Push-Nachricht an Benutzergeräte überträgt, deren Vertrauenswürdigkeit nicht bekannt ist. Das Endergebnis ist, dass Jamf ganz einfach eine Multi-Faktor-Authentifizierung Ihres Cloud-IdP unterstützt, ohne Benutzer auf jedem Service ins kleinste Detail überwachen zu müssen.



# SAML und OIDC/OAuth mit Jamf

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

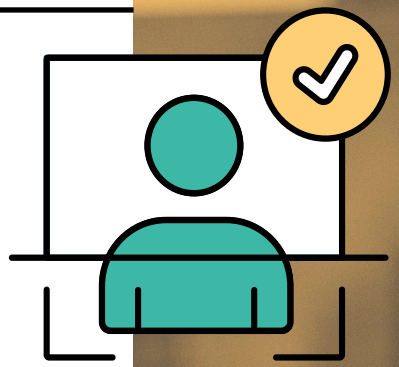


# Moderne Authentifizierung und IdP-Föderation

Man kann nicht über moderne Authentifizierung sprechen, ohne das Thema der IdP-Föderation zu behandeln. Sie verwenden vielleicht Azure AD mit Microsoft Office 365, aber die Identität wird wirklich mit Okta föderiert, da dies Ihr IdP ist, der die „Wahrheit“ über das Passwort eines Benutzers besitzt. Auch wenn die Föderation sehr kompliziert werden und mehrere Schichten der Umlenkung enthalten kann, besteht das Grundkonzept darin, dass ein IdP die Authentifizierung auf einen anderen IdP übertragen kann.

Meistens müssen Services, die über SAML oder OIDC in einen IdP integriert werden können, nicht wissen, ob Sie mit einem anderen Anbieter föderiert sind, oder es sollte ihnen gleichgültig sein. 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. Traditionelle Arten von MFA basierten auf einmaligen Passwörtern (One Time Password, OTP), wobei Benutzer zusätzlich zum Passwort eine sich ständig ändernde Zahl eingeben mussten. Diese Zahl wurde entweder von einem kleinen Schlüsselanhänger mit LCD-Bildschirm oder einer Anwendung auf einem ihrer Geräte generiert.

Um es den Benutzern einfacher zu machen, haben viele IdPs jetzt eine eigene App für Mobilgeräte, auf denen Benutzer nach der Eingabe des Passworts eine Push-Benachrichtigung erhalten. Dann müssen sie darauf reagieren, meist mit einer Form der biometrischen Authentifizierung wie Face ID oder Touch ID, um sicherzustellen, dass die richtige Person auf die Push-Benachrichtigung reagiert.

# Multi-Faktor-Authentifizierung

Ein weiterer Typ des MFA, der zunehmend populär wird, ist FIDO (Fast Identity Online). Diese auf den Datenschutz und Sicherheit ausgerichtete Authentifizierungsmethode ist in die meisten modernen Webbrowser integriert und kann auch die Form eines externen Sicherheitsschlüssels annehmen. FIDO und andere Formen von MFA können auch für passwortlose Authentifizierung verwendet werden, wobei Benutzer kein Passwort eingeben müssen. Stattdessen wird die MFA für den gesamten Prozess verwendet.

Jamf Produkte unterstützen zahlreiche MFA-Optionen. Da ein Großteil der IdP-Authentifizierung in einer Webansicht verarbeitet wird, werden die Konfiguration und Einrichtung der MFA-Details vom IdP selbst übernommen.

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

- Cloud-Authentifizierung auf einem lokalen Account
- Passwortsynchronisierung
- Anmeldung von Benutzern bei Okta

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

# Jenseits von VPNs

Vor der Verwendung von Zero Trust wurde primär ein VPN (Virtual Private Network) zur Sicherung der gesamten Kommunikation mit Benutzern verwendet, wenn man den Datenverkehr zwischen Benutzergeräten und angebotenen Services schützen wollte. Auch wenn VPNs immer noch ein sehr nützliches Tool für IT-Abteilungen darstellen, bieten sie doch einige Nachteile. Die meisten VPNs benötigen eine Client-Software, unterstützen eventuell die Cloud-Authentifizierung nicht, erfordern spezielle Hardware in Ihrem Netzwerk und – was angesichts der heutigen Trends der wichtigste Faktor ist – können Services in der Cloud nur schwer schützen.

Da die meisten Benutzer zu Hause eine immer größere Bandbreite haben, kann die Unterstützung eines VPNs, das den Datenverkehr ihrer Benutzer unterstützt, bald sehr kostspielig werden.

# Zero-Trust Network Access

Eine neuere Methode der sicheren Verbindung von Kunden mit Services ist ZTNA (Zero-Trust Network Access). Bei ZTNA wird kein VPN benötigt, und in den meisten Fällen nicht einmal Client-Software. Stattdessen verbinden sich Benutzer über einen Webbrowser mit einem ZTNA-Serice, der moderne Authentifizierung erfordern kann und dann die Verbindung des Benutzers per Proxy oder sonstigen Methoden sichert.

Während ZTNA-Lösungen ursprünglich für den Schutz von älteren Services vor Ort gedacht waren, bei denen die Verwendung moderner Authentifizierung zu kostspielig gewesen wäre, können jetzt viele auf Wunsch auch Cloud-Services schützen. Es gibt ZTNA-Lösungen, die selbst cloudbasiert sind oder in Ihrem eigenen Rechenzentrum existieren, wenn Sie mehr Kontrolle wünschen. In dem Maße, wie ZTNA-Lösungen robuster werden, können Sie mehr als nur den Web-Datenverkehr sichern, so dass Sie beim Schutz des Zugriffs auf Ihr Netzwerk VPNs ganz hinter sich lassen können.

# 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 Organisationen dabei, mit Geräten verbundene Risiken besser zu verstehen und zu entscheiden, welche vertrauenswürdigen Benutzer auf vertrauenswürdigen Geräten, die vertrauenswürdige Anwendungen verwenden, Zugriff auf Daten und Ressourcen erhalten.

Beim bedingten Zugriff arbeitet Ihr IdP meistens mit einem lokalen Agenten oder Ihrer Geräteverwaltungslösung zusammen. Dadurch wird bestimmt, welche Version des Betriebssystems das Gerät verwendet, welche Sicherheitsrichtlinien vorhanden sind, sowie eine Reihe anderer Attribute, welche den Sicherheitsstatus des Geräts beeinflussen. Das IdP kann dann die Verbindung erlauben oder in einigen Fällen mehr Authentifizierung wie zusätzliche MFA erfordern, bevor der Benutzer vollständig authentifiziert wird.

Ein bedingter Zugriff basiert darauf, was ein App-Benutzer tun will. Für Services mit geringeren Sicherheitsanforderungen, wie ein IT-Ticketingsystem, benötigen Sie möglicherweise keine MFA. Allerdings wäre bei einem Quellcode Repository erforderlich, dass der Benutzer nicht nur eine MFA-Prüfung besteht, sondern auch, dass es sich auf einem Gerät befindet, das dem Unternehmen gehört und von diesem verwaltet wird.

# Bedingter Zugriff

Es gibt eine Reihe von Anbietern, die Sie bei der Verwaltung der Identität und des Zugriffs auf Services unterstützen, 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 Anwendungen, 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 Zugriff auf E-Mail oder andere Cloud-Services beantragt, kann die IT-Abteilung einen vom Benutzer eingeleiteten Registrierungsprozess von Jamf Pro ermöglichen und sicherstellen, dass nicht sichere und nicht verwaltete Geräte verwaltet und angemeldet werden, bevor sie Zugriff erhalten.

# Bedingter Zugriff

Wenn Benutzerdaten von Microsoft und Gerätedaten von Jamf verifiziert werden, wird eine Analyse des Benutzerrisikos, des Geräterisikos (ob dies der Richtlinie der Organisation entspricht oder nicht) und des Anwendungsrisikos (welche Anwendung verwendet wird) durchgeführt, um zu entscheiden, ob Zugriff auf Cloud-Ressourcen gewährt oder blockiert wird, all das 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

So können Organisationen kontextbedingt und dynamisch den richtigen Zugriff auf der Grundlage von Benutzer, Gerät und Kontext des Anwendungsfalls bieten. Dadurch bieten sie einen anpassbaren und flexiblen Perimeter, wie ihn die heute mit mehreren Geräten und an mehreren Standorten arbeitende Belegschaft benötigt.

# Endgerätesicherheit

Sicherheitsmaßnahmen, die durch die Identitätsverwaltung umgesetzt werden, beeinflussen sowohl Endbenutzer als auch IT im gesamten Lebenszyklus von Mitarbeitern, unabhängig davon, ob vor Ort oder aus der Ferne gearbeitet wird. SaaS-Apps und die Verbindung von Mitarbeitern mit Unternehmensressourcen bieten Möglichkeiten, Risiken für Ihre Endgeräte, Ihre Benutzer und Unternehmensdaten zu mindern.

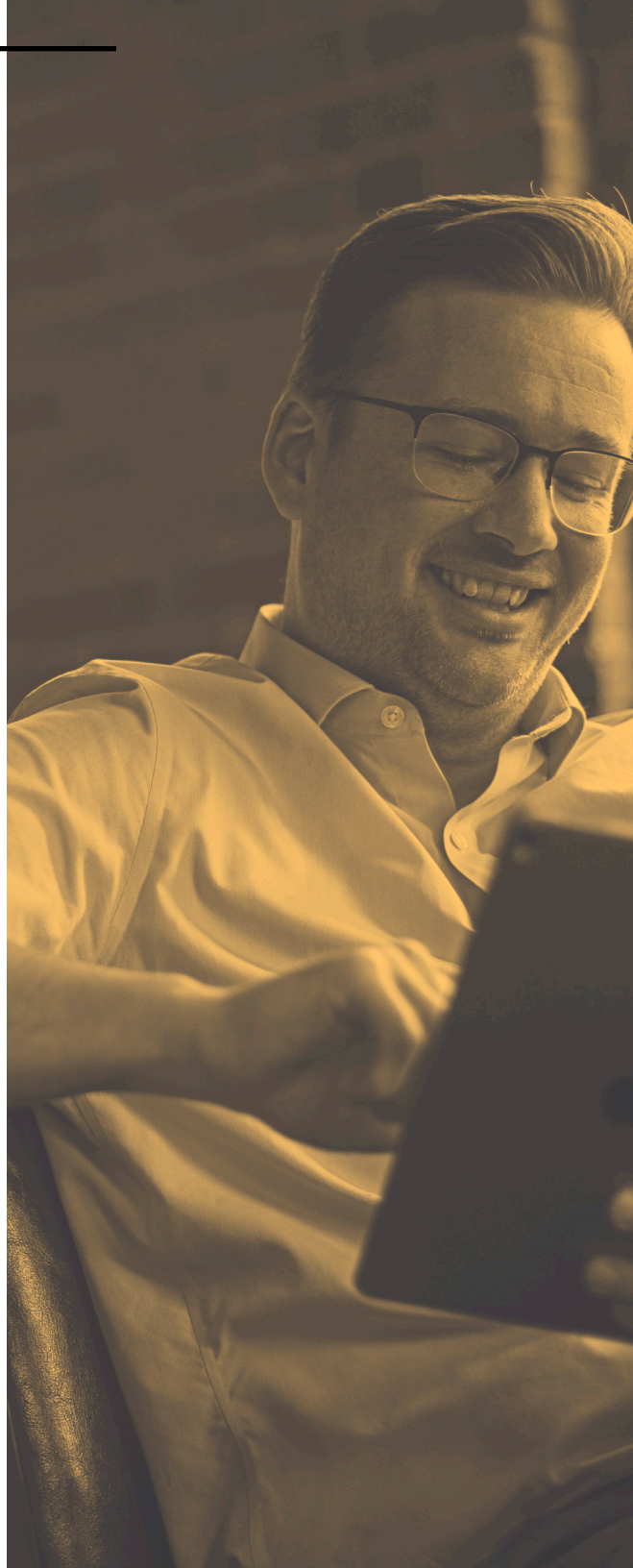
Endgerätesicherheit ist die Praxis, für Geräte oder Endgeräte von Benutzern das Risiko zu mindern, von bösartigen Akteuren genutzt zu werden. Es ist zunehmend wichtig, dass Geräte und Daten von autorisierten Benutzern für legitime Zwecke verwendet werden, besonders wenn Daten in verschiedenen SaaS-Anwendungen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

# Endgerätesicherheit

Organisationen können nicht warten, bis Malware oder andere unerwünschte Softwareprobleme entstehen, und Sicherheitstools, die Geräte eher verlangsamen als schützen, schaden nur der Produktivität der Endbenutzer. Sie müssen ein Antivirus-Programm implementieren, das Mac spezifische Angriffe effektiv identifiziert und behebt, ohne wertvolle Ressourcen mit der Suche nach Bedrohungen für Windows auf einem Mac zu verschwenden. Bei der Sicherheit muss man viel in Betracht ziehen, aber die gute Nachricht ist, dass Jamf bei all diesen Problemen helfen kann.

Neben den Identitätsverwaltungsfunktionen in Jamf Connect und den integrierten Sicherheits-Tools in Jamf Pro kann sich Jamf Protect nahtlos in das Sicherheitsprogramm Ihrer Organisation einfügen, um macOS Malware zu verhindern, vor Mac spezifischen Bedrohungen zu schützen und Endgeräte auf die Compliance zu überwachen.

Für Organisationen, die komplexere Umgebungen mit einer Vielzahl von Sicherheits-Tools besitzen, empfiehlt es sich, eine Kombination der Fähigkeiten von Microsoft und Jamf zu erwägen. IT-Administratoren und Sicherheitsteams können von einem vertrauten Interface aus die sicherheitsrelevanten Aktivitäten ihres Mac Bestands voll einsehen. Jamf Protect überträgt nativ alle Mac spezifischen Sicherheitsdaten und Warnungen direkt an Azure Sentinel, wobei ein Minimum an Konfiguration erforderlich ist. 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. Dank der Fähigkeiten von Jamf Protect zur Entdeckung und Protokollierung von Angriffen kann Azure Sentinel seine Fähigkeiten zur Identifizierung und Behebung von breitgefächerten Angriffen auf alle Mac Geräte erweitern und der Organisation als Ganzes eine bessere Sicherheit bieten.



# Identitäts-verwaltung entwickelt sich weiter

Es ist an der Zeit, das traditionelle, perimeterbasierte Sicherheitsmodell zu überdenken. Durch die Nutzung vieler der gleichen Partner bei der Bereitstellung von Identitäten können Organisationen gleichzeitig eine moderne Sicherheit und Zero Trust 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 hinausführende Lösungen nachdenken. Sie müssen ihre Endgeräte sichern.

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

**Erste Schritte**