jamf

Identity Management and Security

an advanced guide

Each worker has their own identity

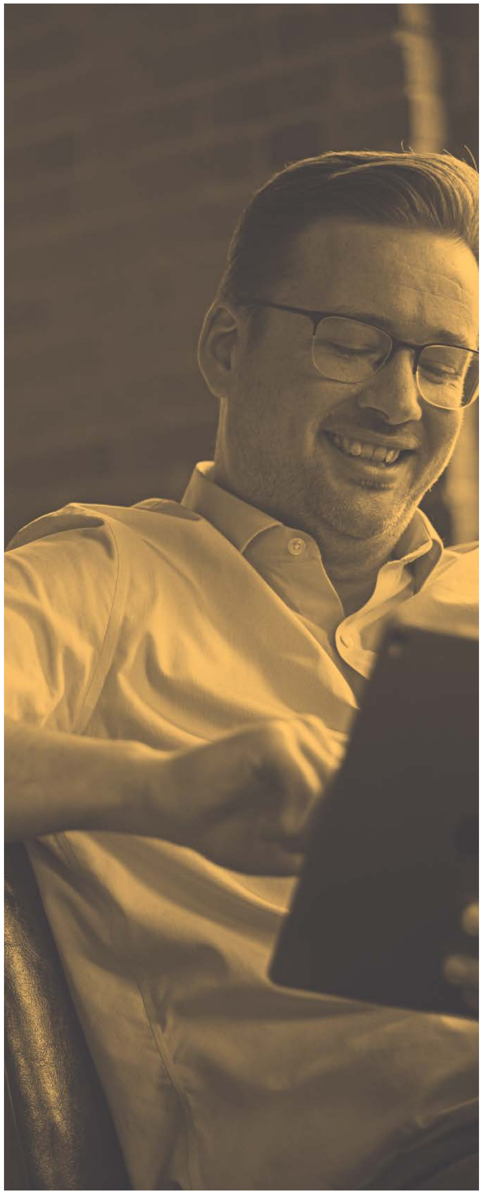
The importance of identity management has become abundantly clear in the past decade as organizations looked to accommodate remote workforce demands. A migration from on-premises setups to the cloud has taken countless organizations a step closer to modern identity management, a topic we dove into in **Identity Management for Beginners.** However, identity management goes well beyond authentication and authorization as organizations look to leverage user identities as a path to reaching their zero-trust security goals.

A major precept of zero trust is that you, in fact, don't trust many of the components that make up the connection between your users and your services. One of the largest components that you won't and shouldn't trust is the network.

To help you through this journey, we're going to cover a few aspects of technologies and details you may want to think about as you begin your identity and security planning. If you haven't already read our intro to zero trust with the **Putting Trust in Zero Trust asset**, you may want to start with that. This e-book will dive deeper into the concepts discussed in the two pieces mentioned earlier and take those beginning concepts to a more advanced level.

We'll cover:

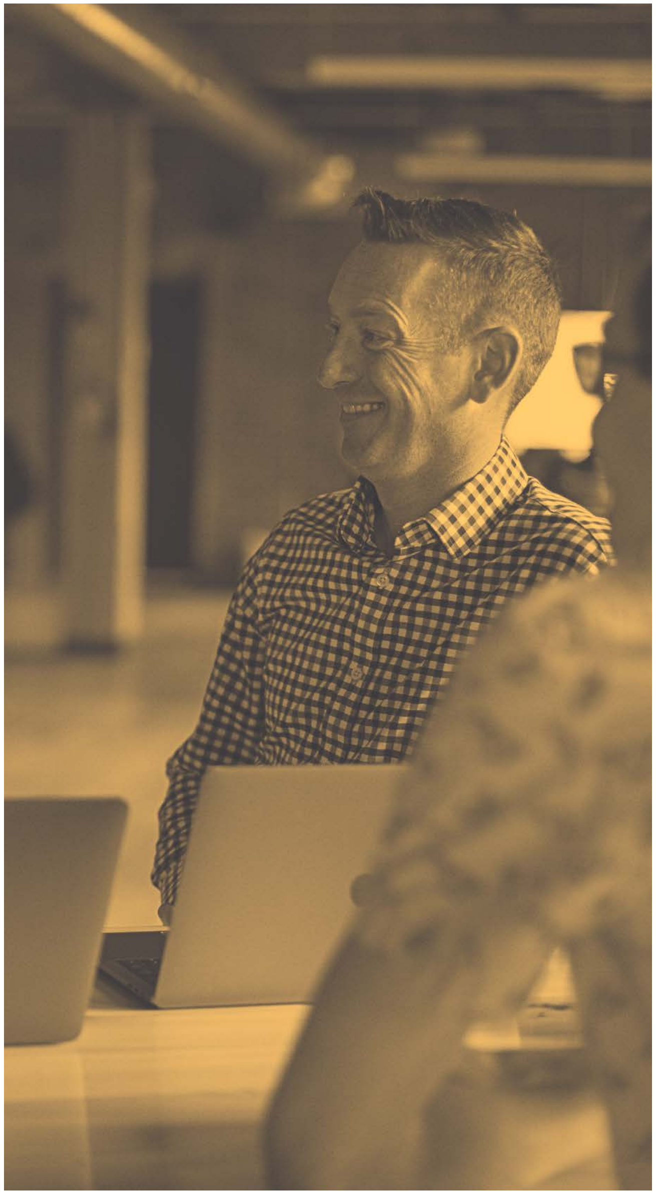
- How modern authentication works
- Techniques for securing network traffic
- How to add conditional access workflows
- How Jamf brings it all together



Modern Authentication for the Impatient

In our previous **Identity Management for Beginners e-book** we covered the differences between authorization and authentication, now let's talk about how that's actually done with modern services to enable single sign-on (SSO).

While there are a lot of methods to validate a user, the most common ones today are SAML (Security Assertion Markup Language) and OAuth combined with OIDC (OpenID Connect). Both systems accomplish very similar goals which is to authenticate a user to some source of truth, typically referred to as an IdP (Identity Provider), and then generate a code that can be shared with other services to prove who you are. If you're familiar with Kerberos from working with Active Directory, you'll find many of similarities.



Modern Authentication for the Impatient

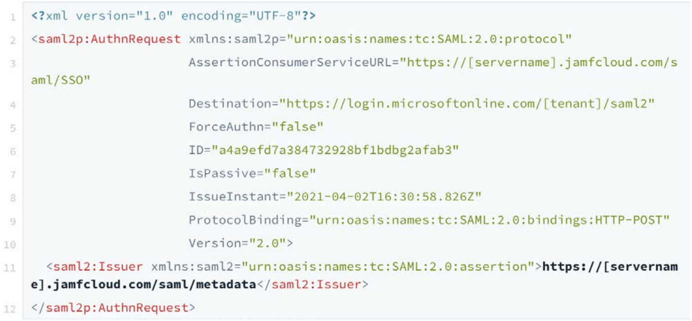
As an admin, here are the salient points that matter for you:

- SAML authentication generates assertions that are signed blocks of XML that identify you and allow other services to trust that you've been authenticated.
- SAML requires any services to have individual certificates to use when communicating with the SAML auth provider, as such it makes it more complicated for using native apps, or applications that run on the users' devices.
- OIDC works with OAuth to generate signed JWT (JSON Web Tokens) that are JSON not XML but otherwise are functionally similar to SAML assertions.
- OIDC has the added benefit of an ID Token which is effectively a portable user record that is also signed to prove that it's valid.

When authenticating to a service via SAML or OIDC/OAuth, the service never actually gets the user's password, as that is only handled by your IdP. Instead, the service gets either a SAML assertion or an OAuth token that is signed by the IdP so the service can trust it. While there are implementation details between the two, both SAML and OIDC/OAuth provide very safe, modern and extensible ways of authenticating a user to services.

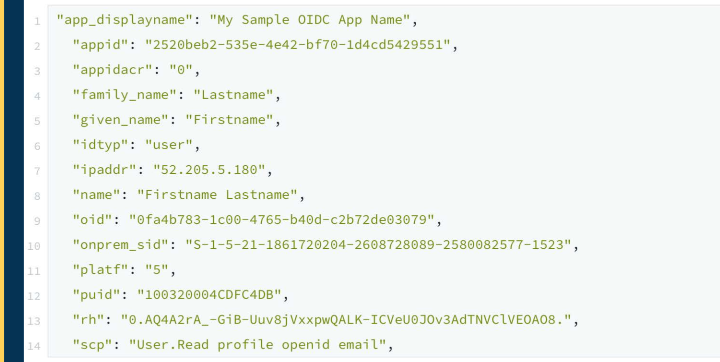
Modern Authentication for the Impatient

Here's a sample of what a SAML assertion looks like:



```
<?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>
```

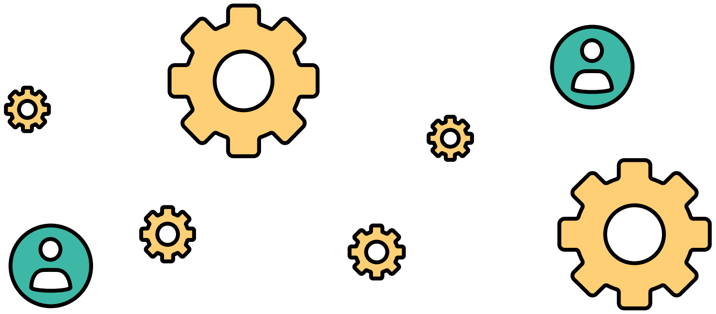
For comparison, this is an example of an OAuth token:



```
"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-Uuv8jVxxpwQALK-ICVeU0JOv3AdTNVClVEOAO8.",
  "scp": "User.Read profile openid email",
```

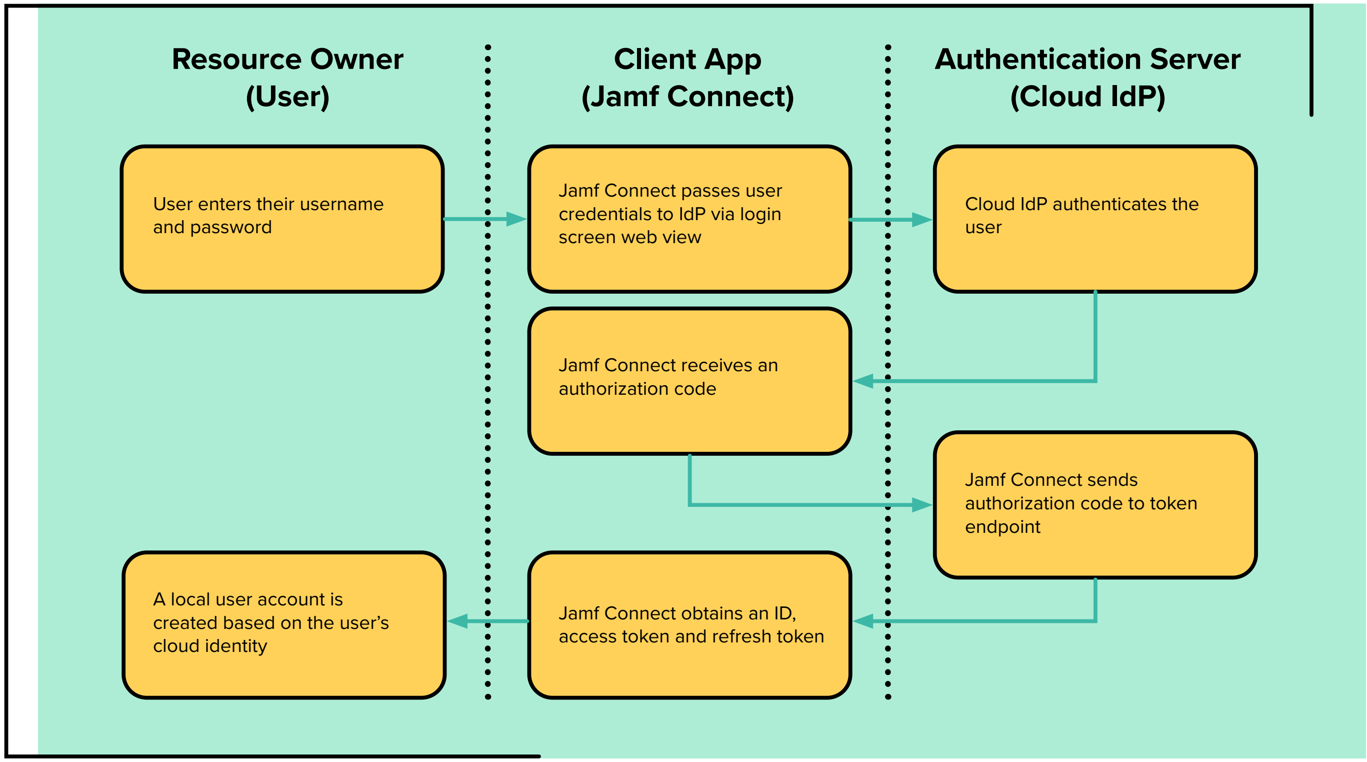
SAML and OIDC/OAuth with Jamf

Jamf Pro uses SAML, while **Jamf Connect** and **Jamf Protect** use OIDC/OAuth. For Jamf Connect, SAML isn't applicable because of the need for certificates and pushing certificates and private keys to user devices that you don't know if you can trust. The end result is Jamf's ability to easily support multi-factor authentication from your cloud IdP, without having to micromanage users on each service.



SAML and OIDC/OAuth with Jamf

Here is an example of how Jamf Connect uses an OIDC Authorization Code Grant to authenticate the user's cloud username and password in exchange for an authorization code, which Jamf Connect sends to your IdP token endpoint.



User enters their username and password

Jamf Connect passes user credentials to IdP via login screen web view

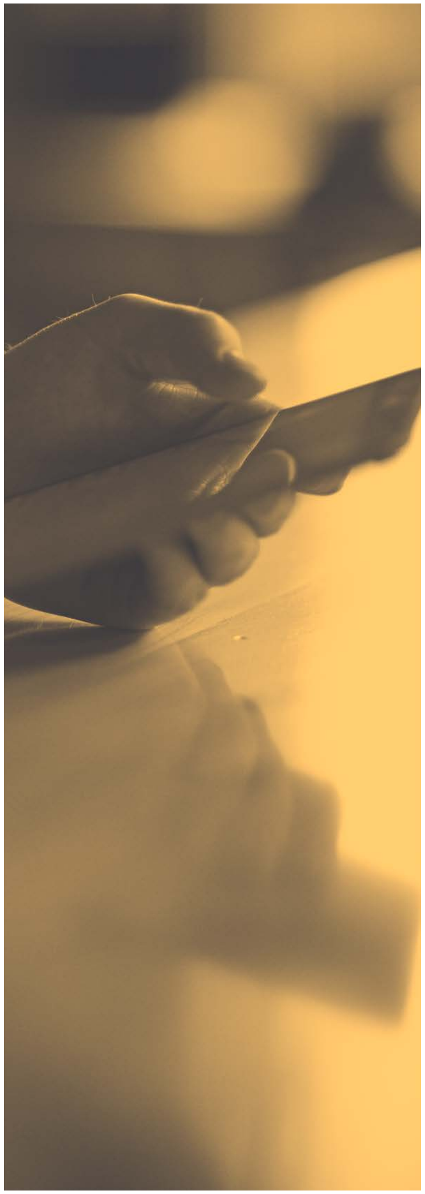
Cloud IdP authenticates the user

Jamf Connect receives an authorization code

Jamf Connect sends authorization code to token endpoint

Jamf Connect obtains an ID, access token and refresh token

A local user account is created based on the user's cloud identity



Modern Authentication and IdP Federation

You can’t talk about modern authentication without getting into the topic of IdP Federation. This is where you may use Azure AD with Microsoft Office 365, but identity is really federated with Okta because that’s your IdP that has the “truth” for what a user’s password is. While federation can get very complicated and involve multiple layers of redirection, the basic concept is that an IdP can pass off authentication to another IdP.

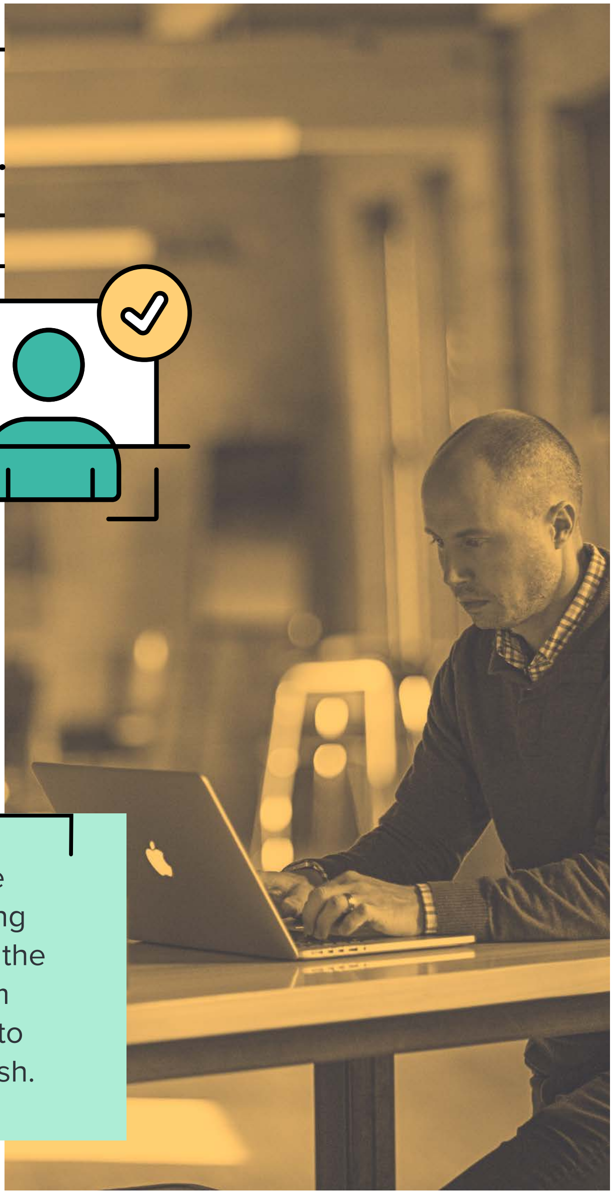
For the most part, services that can integrate with an IdP via SAML or OIDC shouldn’t need to know, or care, if you’re federated with another provider. Most of those details are abstracted from the initial connection.

Multi-factor Authentication

Since we've talked about authentication methods, we should talk more about multi-factor authentication (MFA) and passwordless authentication as well.

Stolen login credentials stand as one of the top security problems facing organizations today. In fact, 80% of all data breaches involve stolen or weak passwords, yet less than 10% is spent on eliminating compromised credentials according to **World Economic Forum.** To combat this, many organizations are leveraging their identity provider to introduce MFA and passwordless security.

IdPs can support a wide variety of MFA, and to a lesser degree passwordless, solutions. Traditional MFA types were based around One Time Passwords (OTP) which required the user to enter in a constantly changing number in addition to their password. The number was generated either on a small key fob with an LCD screen or an application on one of their devices.



> To make things easier on users many IdPs now have their own app for mobile devices where after entering a password the user receives a push notification on the device, and have to respond, usually with some form of biometric authentication like Face ID or Touch ID to ensure that the right person is responding to the push.

MULTI-FACTOR AUTHENTICATION

Another MFA type that's gaining a lot of traction is FIDO (Fast Identity Online), which is a privacy and security-focused method of authentication that is built into most modern web browsers and can also take the form of an external security key. FIDO, and other forms of MFA, can also be used for passwordless authentication where the user doesn't have to actually type in a password. Instead, MFA is used for the entire process.

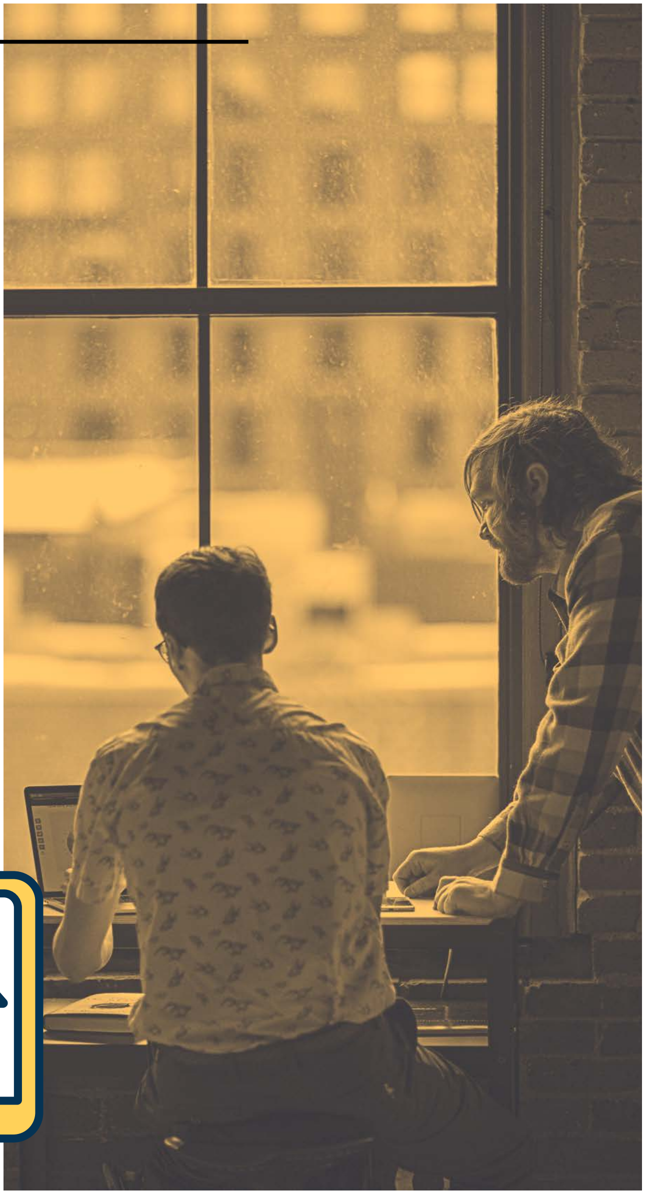
Jamf products support a wide variety of MFA options. Since most IdP authentication is handled within a web view, all of the configuration and setup of the MFA specifics are handled by the IdP itself.

For example, Jamf Connect can use the Okta Authentication API to configure primary Jamf Connect tasks for users, such as:

- Cloud authentication to a local account
- Password synchronization
- Signing in users to Okta

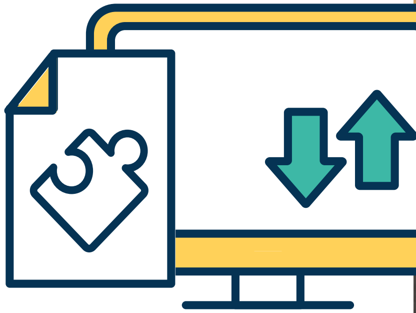
Read Okta's developer documentation to learn more about this API.

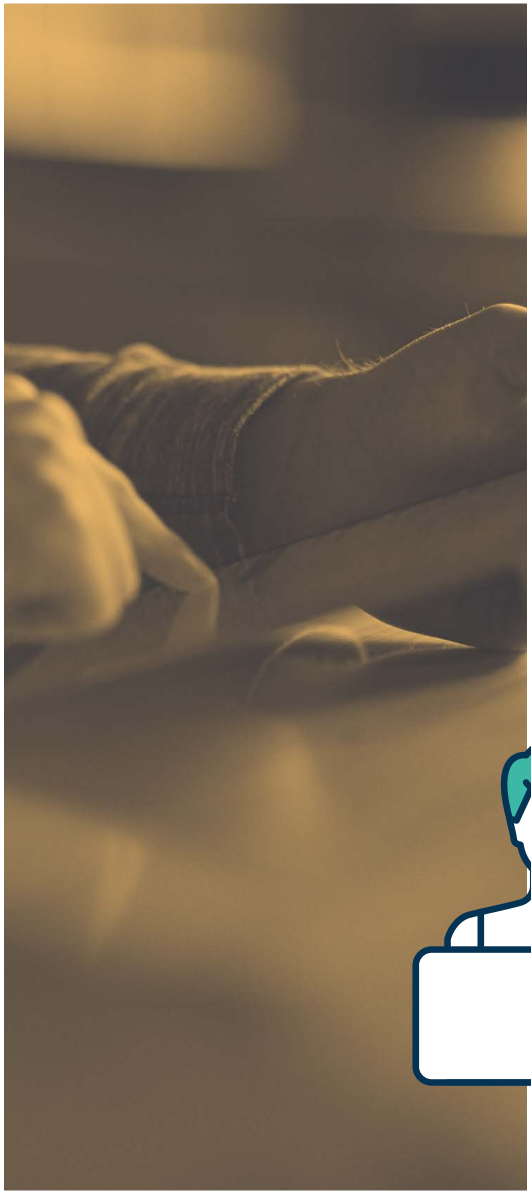
Moving beyond VPNs



Prior to zero trust, if you wanted to protect traffic between your user's devices and the services that you were providing, you were most likely using a VPN (Virtual Private Network) to secure all communications with your users. While VPNs are still a very useful tool for IT departments to leverage, they do come with some downsides. Most VPNs require client software to run, may not support cloud authentication, typically require dedicated hardware in your network and maybe most importantly given current trends, don't easily protect services in the cloud.

With most users having increasingly fast bandwidth at their homes, being able to support a VPN that can handle the traffic your users may produce can get very expensive quickly.





Zero-Trust Network Access

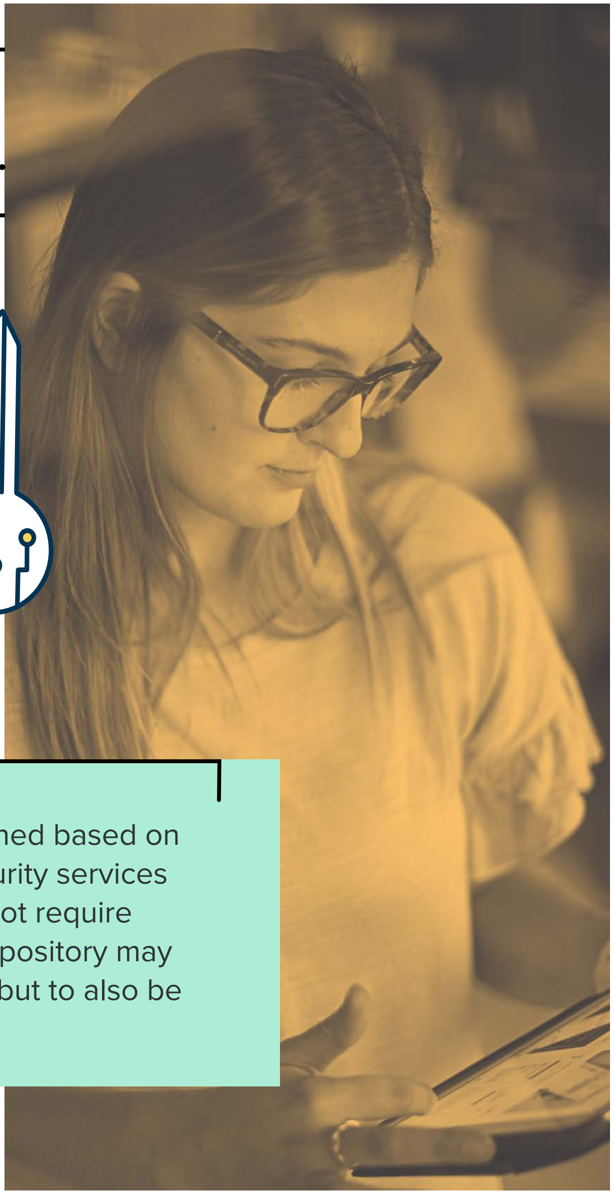
A newer philosophy of connecting clients to services in a secure fashion is ZTNA (Zero-Trust Network Access). With ZTNA there is no VPN required, or in most cases, not even client software. Instead, users connect through a web browser to a ZTNA service which can require modern authentication which then proxies or otherwise secures the user's connection.

While ZTNA solutions were originally designed to protect legacy on-prem services where adding modern authentication would have been otherwise prohibitive, many will now also protect cloud-based services as well if desired. You can find ZTNA solutions that are themselves cloud-based or designed to live within your own data center if you want more control. As ZTNA solutions get more robust you can secure more than just web traffic, which may allow you to really move off of a VPN for securing access to your network.

Conditional Access

A robust zero-trust architecture will often include elements of conditional access or device trust. In these situations, the state of the device itself becomes part of the decision as to how much, if at all, to trust the connection. Managed devices help organizations better understand device risk and decide which trusted users, on trusted devices, using trusted applications can gain access to data and resources.

Conditional access is typically a combination of your IdP working with a local agent or your device management solution to determine what version of the OS the device is running, what security policies may be in place, or a number of other attributes that help determine the posture of the device. The IdP can then allow the connection, or in some cases, require more authentication like additional MFA, before fully authenticating the user.



> Conditional access, as the name implies, is conditioned based on what app a user is attempting to use. For lower-security services such as accessing an IT ticketing system, you may not require any MFA at all, however, access to a source code repository may require the user to not only pass an MFA challenge but to also be on a corporate-owned and managed device.

Conditional Access

There are a number of vendors who help manage identity and access to services, including Centrify, Duo Security, Microsoft, Ping Identity, Okta and Salesforce. Many of these tools work with existing authentication infrastructure, such as your cloud identity provider, and extend those identities to cloud services using the protocols discussed above — OIDC and SAML.

Let's use an example of how Jamf works with Microsoft to achieve conditional access. **Jamf Pro** can enforce policies on devices in order to access Microsoft Office 365 by leveraging Enterprise Mobility + Security (EMS) conditional access. Jamf-managed Mac computers now get access to Microsoft applications, provided they meet the Microsoft Endpoint Manager device compliance policies to do so. Once the Mac's data is in the cloud, Endpoint Manager and EMS can fully integrate with Jamf for management capabilities on the device. If an unmanaged Mac requests access to email or other cloud services, IT can enable a user-initiated enrollment process from **Jamf Pro** and ensure that non-secure or unmanaged devices are enrolled under management before being granted access.

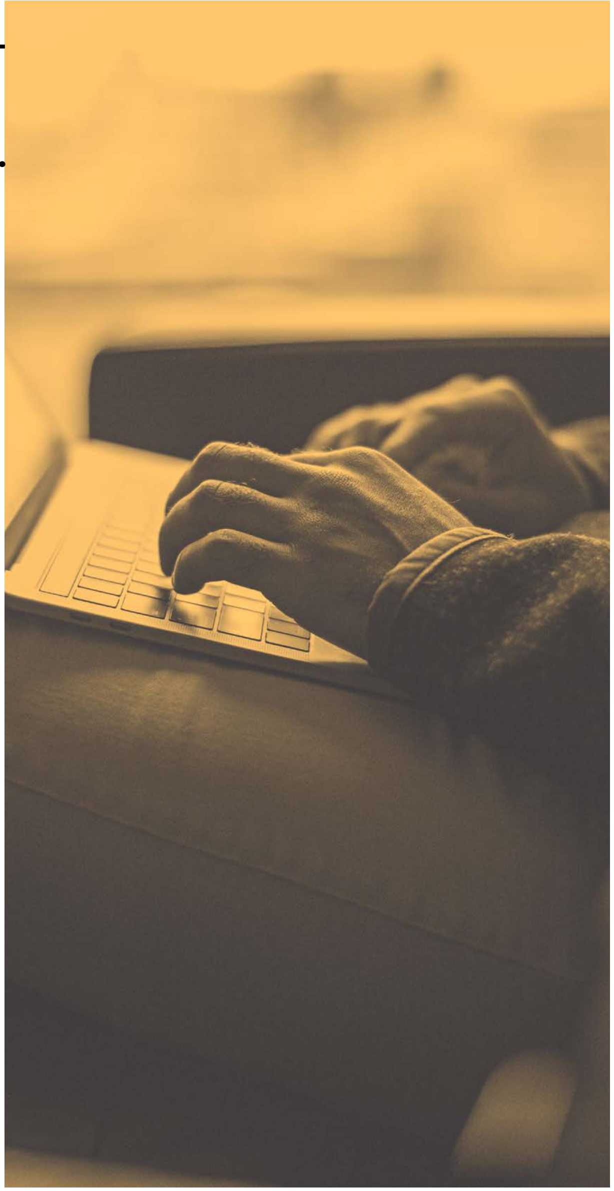
Conditional Access

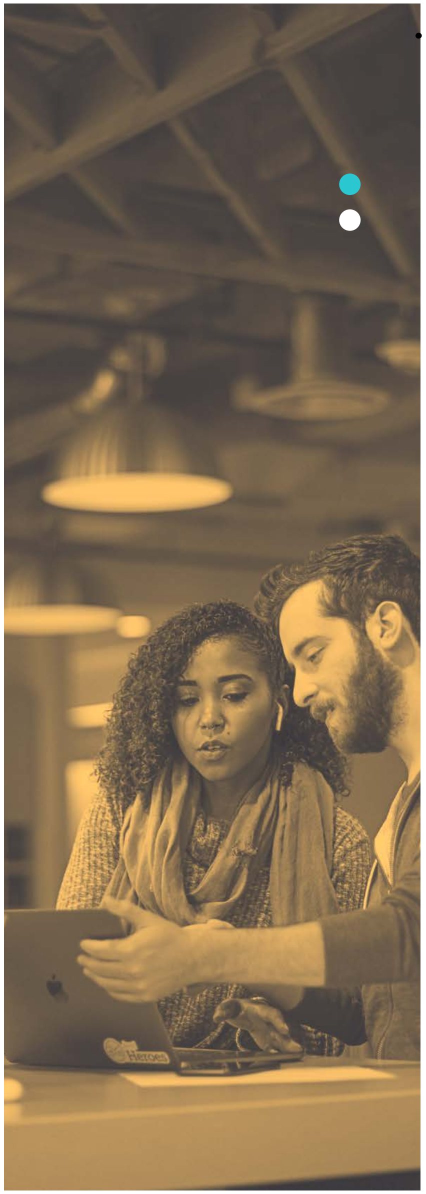
When user credentials are verified by Microsoft and device credentials by Jamf, an analysis of the user risk, the device risk (is it compliant or not with an organization's policy) and the application risk (what app is being used) is run to determine whether to grant access or block access from cloud resources, all in real time.

Now organizations get an extension of multi-factor authentication through verified compliance:

1. Username and password
2. Code and token
3. Device compliance

This allows organizations to contextually and dynamically provide the right access based on a user, device and the context of that use-case, effectively delivering the adaptive and flexible perimeter demanded by today's multi-device, multi-location worker.





Endpoint Security

Security measures implemented through identity management affect both end users and IT throughout the employee lifecycle, regardless of an on-site or remote-work status. SaaS applications and connecting employees to enterprise resources provide opportunities to mitigate risks to your endpoints, your users and corporate data.

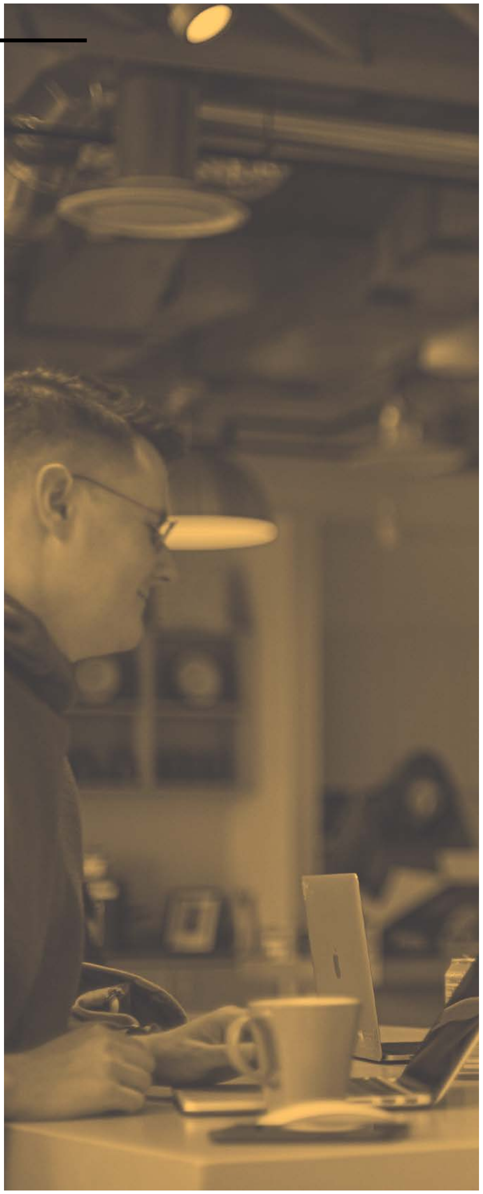
Endpoint security is the practice of mitigating risks to devices or endpoints of end users from being exploited by malicious actors. Ensuring devices and data are used for legitimate purposes by authorized users is of increasing importance, especially as data is distributed in various SaaS applications. To accomplish this goal, there are many moving parts that must work together — identity management being one of those but also antivirus (AV), security configuration management, endpoint detection and response.

Endpoint Security

Organizations can't wait until malware, adware or other unwanted software issues arise, and security tools that impact the device more than they protect it will only prohibit end-user productivity. They need to be thinking about implementing antivirus that effectively identifies and remediates Mac-specific attacks without spending resources looking for threats to Windows on a Mac. There is a lot to think about when it comes to security, but the good news is Jamf can help with all of the above.

In addition to identity management capabilities with Jamf Connect and built-in security tools with Jamf Pro, **Jamf Protect** is designed to seamlessly fit into your organization's security landscape to prevent macOS malware, protect from Mac-specific threats and monitor endpoints for compliance.

For those organizations that have more complex environments with a variety of security tools, let's again look at combining the capabilities of Microsoft and Jamf. IT admins and security teams can have complete visibility into security activities across their Mac fleet from within their familiar single pane of glass. Jamf Protect natively pushes all Mac-specific security data and alerts directly into Azure Sentinel with minimal configuration. All malicious or suspicious Mac activity, as well as malware notifications, integrate easily with preexisting workflows, which means little effort and time demanded of security and IT staff. With Jamf Protect's attack detection and log information, Azure Sentinel can extend its capabilities to identify and remediate broad attacks against all of the Mac devices, while maintaining better security for the organization as a whole.



Realign your security posture with identity

It's become clear that it's time to rethink the traditional, perimeter-based security model. By leveraging many of the same partners helping to provide identity, organizations can achieve modern security and even zero trust at the same time. People have moved, data has moved, and organizations need modern solutions to address those changes. They need to think about device-based security, user-based security, multi-factor authentication and beyond. They need to secure their endpoints.

Jamf offers a way to tie it all together. Better security starts here.

Get Started

Or contact your preferred reseller of Apple hardware to get started.