Identity Management

for Beginners

jamf

EACH WORKER HAS THEIR OWN IDENTITY.

Traditionally, employees would go to an office building, they would have a desktop computer at their desk and the hardware never left that location. Multiply that by the number of employees at any given organization to provide a picture of the devices and access IT had to manage. Today's work environment looks a lot different. The modern worker is mobile, seamlessly transitions from laptop to tablet to phone throughout their day and needs access to their information and data everywhere they go.

The digital footprint of workers has expanded and compounded, both in terms of time spent on devices and the pure volume of data that employees want to access. One of the key tactics companies use to protect that information is to gatekeep who has access to specific files, software and data, and how they access it. This doubles as a simple method of improving the end-user experience by giving them what they need, when they need it, nothing more and nothing less.

It's an aspect of IT that is becoming commonplace, but as the technology world advances and the needs of employees move with them, it's important that companies establish their workflows in ways that are both modern and adaptable. One of which is identity and access management, and it's a top priority.

IN THIS GUIDE, WE'LL DISCUSS THE FOLLOWING:

- Basics of identity management

- Workflows for modern identity and access management

- Why the cloud is critical for modern-day success

- How it all comes together with Jamf

BASICS OF IDENTITY MANAGEMENT

Identity and access management (IAM) is the overarching discipline for verifying a user's identity and their level of access to a particular system. **In order to achieve this, users must be authenticated and authorized.**

Authentication is generally linked to the act of "signing in" and it's the part in which your identification is established and verified. Most commonly, this comes in the form of a username and password.

However, in identity management, authentication doesn't mean you have actual access to anything, it simply refers to the ability a user has to verify themselves. For access to data, software and files, you need authorization. **Authorization** is correlated to what resources, software, data, etc., that you are given access to after authenticating yourself.

Authentication = who you are
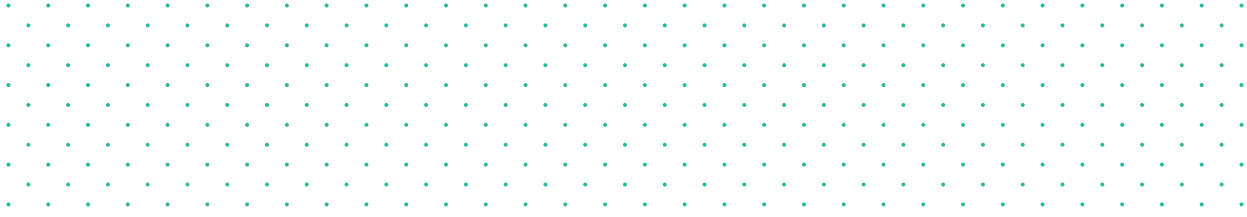**Authorization = what you can do**

BASICS OF IDENTITY MANAGEMENT

In order to bring this concept of authentication and authorization to life, companies created a directory that was, in essence, a catalogue of your employee's technology records. For example: name, device type, job title, department, usernames, passwords, and the software and files they needed to access. This created the foundation for managing identities. This is sometimes referred to as legacy IT.

15 years ago, identity management was somewhat consistent. You had Lightweight Directory Access Protocol (LDAP) for cataloguing your users' identification and details, Kerberos for the user authentication, and putting them together got you Active Directory (AD), which at its core was the extent of identity management. However, over the past decade this process has evolved.

Legacy IT relies on directory services as their "source of truth," but as security and deployment needs evolve, businesses must adopt a new approach to identity as part of their enterprise strategy. With a complete identity stack, businesses unify identity across hardware and software to unlock functionality, advanced workflows and ultimately transform business.

BASICS OF IDENTITY MANAGEMENT

Identity management goes beyond authenticating and authorizing users. It also dictates how users access organizational resources.

For remote and mobile employees, the legacy IT version to access resources is through virtual private networks (VPNs). When using a VPN, access is granted holistically and provides users access to the entire network of resources, which is a significant security risk. If malicious actors were to gain full network access via the VPN, they could move laterally to access any content within that network.

Historically, VPNs are not user- or mobile-friendly. In the modern workforce, users need to be able to have access from anywhere, anytime.
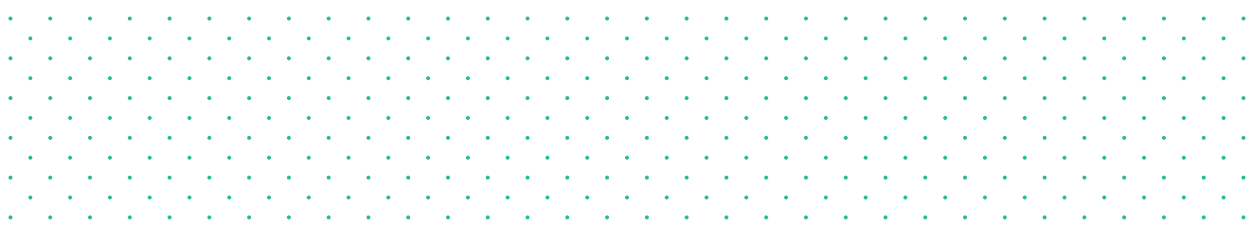
MODERN IDENTITY AND ACCESS MANAGEMENT

A shift from legacy to modern IT isn't just about technology—it's how technology is used to unlock end-user productivity and business transformation.

THE IDENTITY STACK

Directory Services

Acts as a centralized record of employee information, such as name and department. Often leveraged when integrating with management platforms, like Jamf Pro, to deploy customized devices for end users.

Legacy: On-premises Active Directory

Modern: Cloud Directory

Cloud SSO

Building on information from directory services, cloud SSO ensures end users enter secure credentials to access company resources.

Legacy: Users must authenticate every time they access cloud-based apps or resources.

Modern: Users enjoy access to cloud-based apps like Microsoft Outlook and Slack with fewer authentication requests..

Jamf Connect

With directory services and cloud SSO, adding Jamf Connect unifies identity across all company apps and the user's devices, without compromising trust. End users leverage a single cloud identity to easily and quickly gain access to resources they need to be productive.

Modern:

- Streamline provisioning and authentication out of the box for full support of remote employees.

- Automatically sync user identities and device credentials.

- Ensure IT has full identity management capabilities.

- Secure access to business resources and applications with next-gen VPN

Directory Services

Directory Services + Cloud SSO

Directory Services + Cloud SSO + Jamf Connect

MODERN IDENTITY MANAGEMENT

When you look at the modern identity stack, today, it's comprised of three components:

1. **Directory services and cloud-based single sign-on (SSO) from a cloud identity provider (cloud IdP), commonly Azure or Okta**

2. **Jamf for mobile device management**

3. **Jamf Connect to unify your cloud IdP, hardware and software, with secure access to business applications**

The components all work together to improve your end-user experience for mobile workers and raise the overall level of security that surrounds your entire deployment.

What is an identity Provider?
An identity provider (IdP) is a service that stores and manages digital identities. Companies use these services to allow their employees or users to connect with the resources they need. They provide a way to manage access, adding or removing privileges, while security remains tight.

What is single sign-on (SSO)?
Single sign-on (SSO) is an authentication process that enables users to securely authenticate with multiple applications and websites by using a single set of credentials.

MODERN IDENTITY AND ACCESS MANAGEMENT

With workers all in one location, creating a smaller digital footprint by leveraging only the technology available, the basic identity management practices were sufficient. The problem is, technology has changed, more devices are being used daily by your workforce to access a lot more data and software, security risks have increased, and your workforce has gone from static to dynamic.

As with many aspects of technology and IT infrastructure, the game had to change when the workforce mobilized. Identity management was no different. To use AD and LDAP, a user binds their device to an on-premises AD. But as mentioned, the workforce was no longer on-prem consistently, which produced problems:

- Users can only change their passwords on-prem, when AD is reachable. This causes both confusion and costly help desk tickets when a user forgets their password or needs to change it altogether.
- Because AD is built for Windows, leveraging AD as a primary identity provider reduces management capabilities for Mac. This requires the use of third-party add-ons, which adds complexity to user management and higher costs.
- Remote users must be on the local area network (LAN) or use a virtual private network (VPN) to access internal resources. This ruins the user experience and spikes frustrations.

These reasons, plus others, lead to adoption of cloud IdPs a crux of modern identity and access management.

WHY THE CLOUD IS CRITICAL FOR MODERN-DAY SUCCESS

Cloud identity allows IT to centrally and remotely manage users, groups, passwords and access to corporate applications and cloud resources. Cloud IdPs such as Microsoft, Google and Okta offer all employees — remote and onsite — secure access to the resources they need to be productive.

| Legacy Identity	Modern Identity
• Active Directory	• Azure
• Open Directory	• Okta
• LDAP	• Google Suite

Partnering with a cloud identity provider allows organizations to go beyond their office walls and provide a seamless user experience, while keeping their data and devices secure.

WHY THE CLOUD IS CRITICAL FOR MODERN-DAY SUCCESS

Your IdP — Okta, Azure, G Suite, etc., — is going to act as your directory service, (i.e., the "phonebook" for employees). This includes their personal info, what department they are in, their job title, and, most importantly, what apps/resources are scoped to them. When a user logs into the cloud IdP and validates their identity, they then have access to everything that is scoped to them within the cloud directory. **Authentication and authorization in action!**

This cloud IdP will also enable you to leverage the power of SSO to raise your organization's mobile device security levels and improve the user experience in one fell swoop. Rather than having your users authenticate themselves and login to each and every platform, app and service you offer, SSO allows them to do it once, securely, and gain access to everything they need.
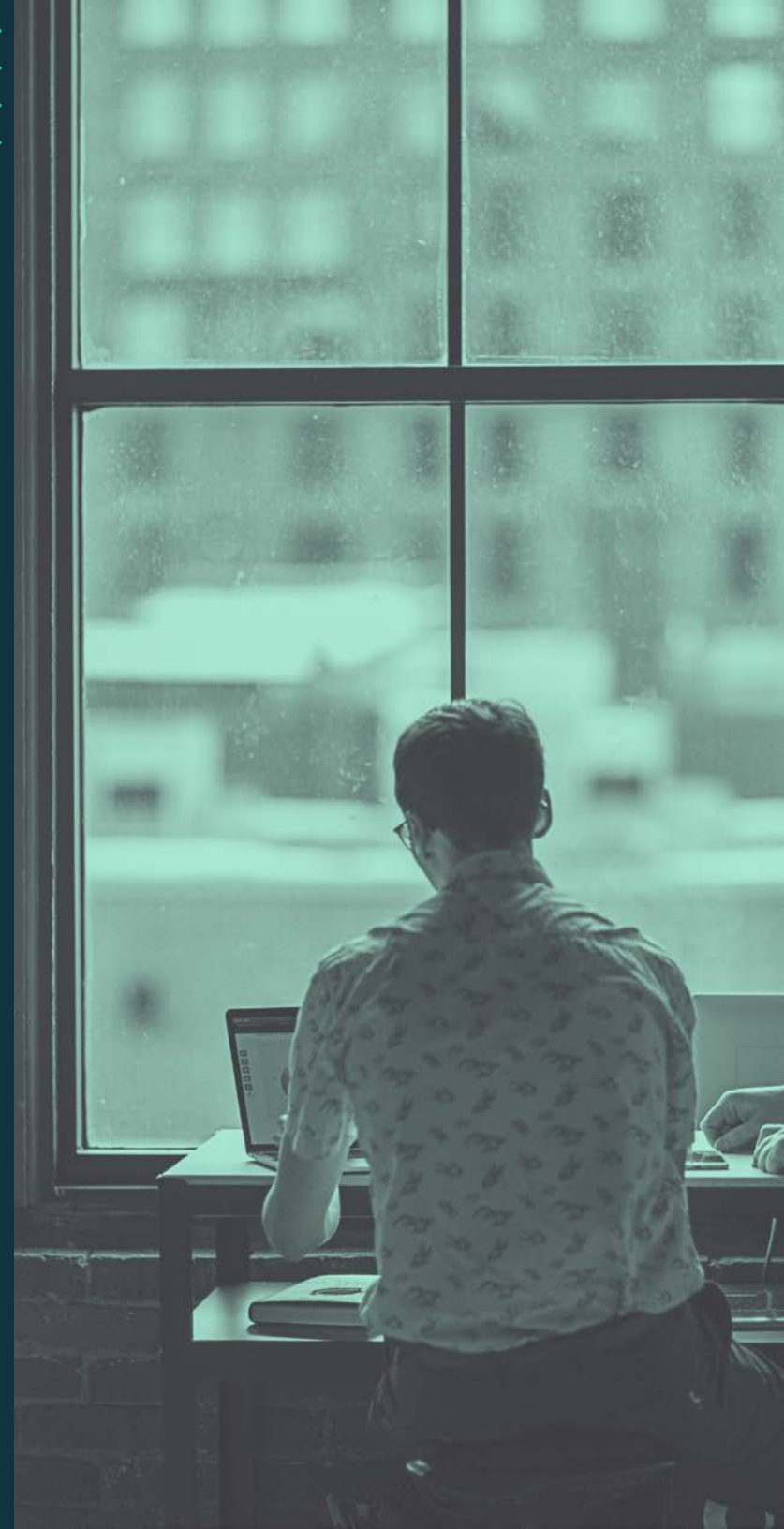
WHY THE CLOUD IS CRITICAL FOR MODERN-DAY SUCCESS

To take this security one step further, companies may look to multi-factor authentication (MFA). By adding MFA into the mix, you add a simple, extra step requiring your end user to confirm their identity beyond a vulnerable username and password, before granting access to the resources they need.

Bringing this to life and unifying your cloud IdP with your devices is where Jamf Connect comes in.

What is multi-factor authentication?

Multi-factor authentication (MFA) is an authentication process that requires the user to provide two or more verification factors to gain access to a resource. This could be a PIN on a user's phone, FaceID, fingerprint verification or a few other options.
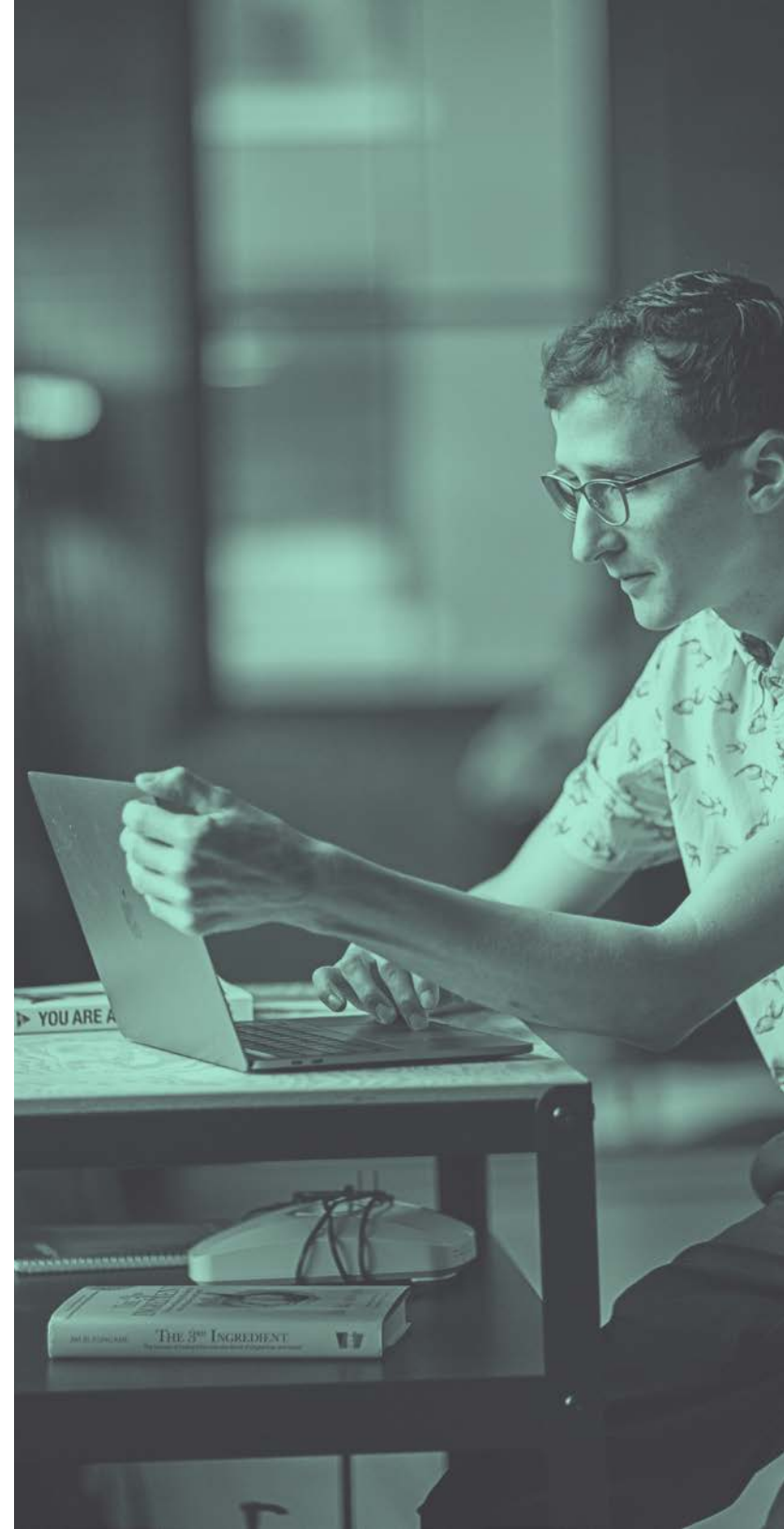
JAMF CONNECT BRINGS IT ALL TOGETHER SEAMLESSLY.

Active Directory was built for Windows, which meant that Apple users didn't have any option besides binding to AD before Jamf Connect changed that.
As organizations shift away from AD and bring on more Mac devices to adhere to the growing demand, organizations must get workflows in place to keep corporate information secure while providing an ideal user experience.

Cloud IdPs integrated with Jamf Connect allow IT to remotely manage user passwords and access to corporate applications. Using an automated MDM enrollment, the process is simple and secure:

1   **A user is invited to enroll in the automated MDM enrollment.**

2   **During the enrollment, Jamf Connect is downloaded and installed from the MDM server.**

3   **Users are taken directly to the Jamf Connect Login window and will enter their cloud identity credentials, as opposed to creating their own username and password.**

JAMF CONNECT BRINGS IT ALL TOGETHER SEAMLESSLY.

The user has the same username and password for everything, creating an incredible experience while also establishing account security.

Benefits include:

Account creation: Create local Mac accounts based on Okta, Microsoft Azure, Google Cloud, identities, resulting in an improved login experience for users and organized fleet of Mac for IT to manage.

Secure enrollment: Leverage modern authentication to monitor what devices are being accessed, from where and by whom, ensuring the right user is on the device before deploying anything sensitive.

Eliminate shared admin accounts: Create multiple IT admin accounts leveraging permissions from the cloud IdP without requiring the use of shared service accounts.

Enforce password policies: Admins can enforce password policies via the IdP to maintain consistency and security across all users.

Password synchronization: Keep the Mac username and password in sync with cloud identity credentials, leveraging a single identity for everything needed to be productive.*

*Password synchronization is not available for Google Cloud at this time
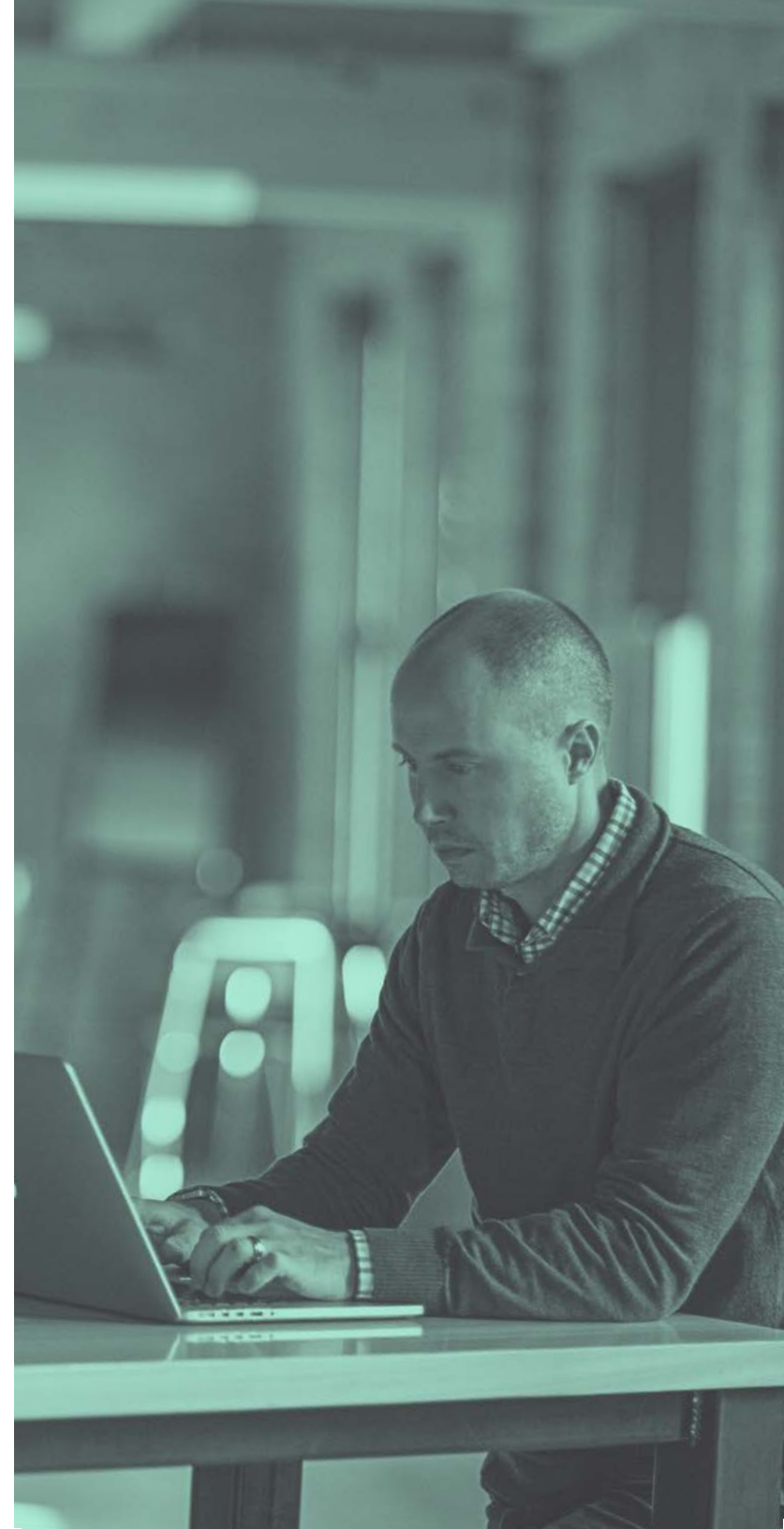
JAMF CONNECT BRINGS IT ALL TOGETHER SEAMLESSLY

Modern identity and access management and a Zero Trust Network Access (ZTNA) solution all-in-one.

When organizations implement ZTNA, their users are authenticated and authorized, and devices are verified each time a user accesses data or resources. Least-privilege enforcement and real-time device posture checks allow access to each application for only specific, authorized users on trusted devices.

ZTNA enables user authentication by way of SSO through your preferred cloud-based IdP. Integration with existing cloud-based IdPs allows for rapid deployment and management of policies. The only way for a connection to be established is for the user to have the appropriate permissions to the specified application.

Learn more about ZTNA with our e-book.
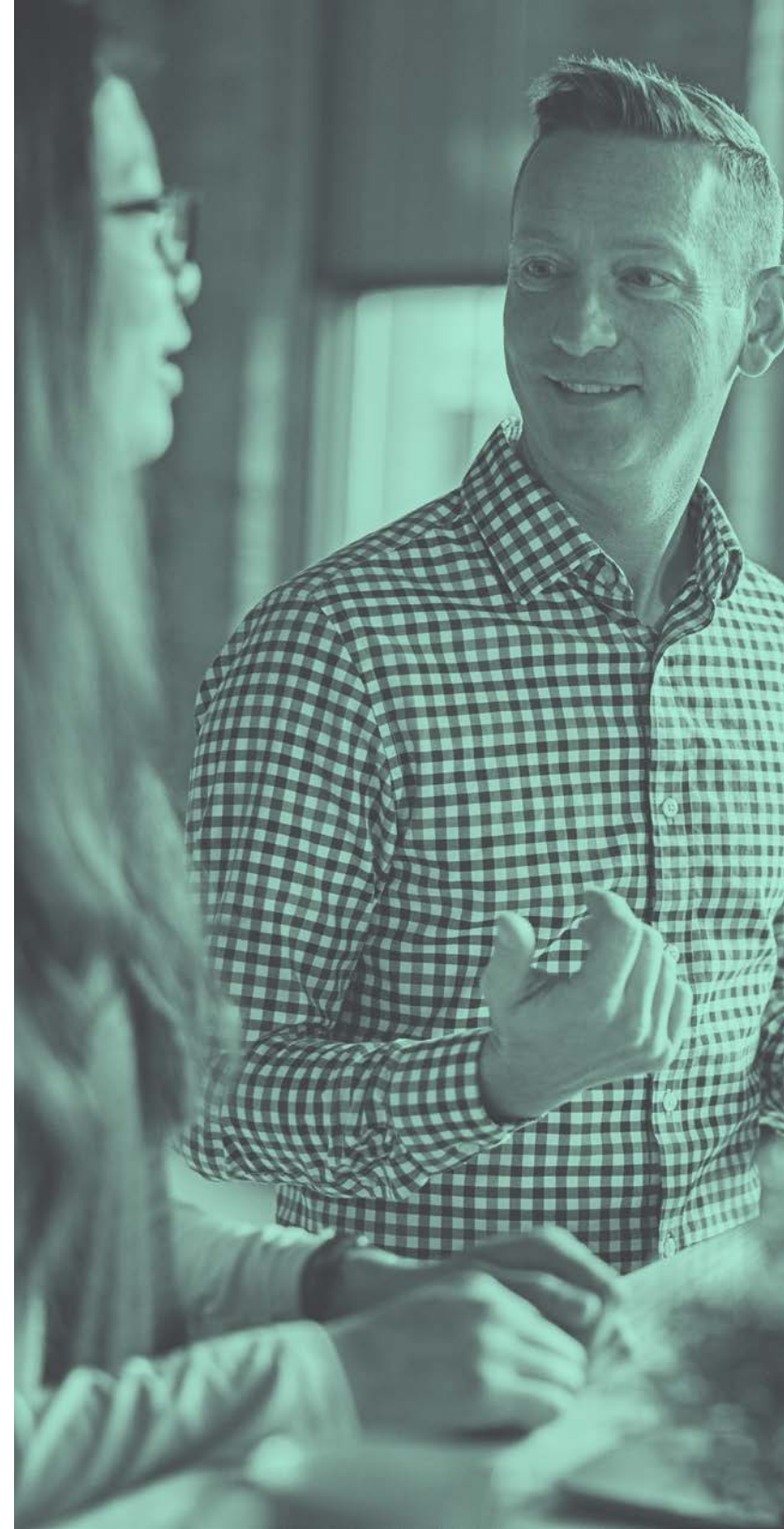
IDENTITY AND ACCESS MANAGEMENT IS HERE.

―――――――――

With more demand for remote workers, a mobile workforce and access to working materials at all times, it's become a necessity. Jamf brings all your infrastructure together in one seamless experience for both users and IT.

Connection®
we solve IT®

Contact your Connection Account Team today for more information.

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/jamf