Why Better Mac Security Starts with Cloud Identity

Evolving workforce creates new opportunities.

For years, employees drove to an office, opened their computer, logged onto a corporate network with their username and password and got on with their workday.

But working standard hours in a fixed office location is becoming more and more rare. In fact, a report by Gallup found that 43 percent of American employees work remotely.[1] This growing mobile workforce requires the same, secure access to resources as their onsite counterparts — without connecting to the corporate network. And both onsite and remote employees need secure ways to access the expanding number of applications and resources that are hosted in the cloud. To accommodate, enterprise technology and IT practices must adapt.

The first step in providing employees with the modern tools their new work lives call for comes in the form of an employee-choice program. This gives the individual the ability to choose a PC or Mac computer for work purposes. As more employees choose Mac, IT needs a streamlined solution to protect the device and the user no matter where they are located.

In this white paper, we explain new and better ways of leveraging cloud identity to secure the Mac, the user and data on the Mac, and the organization the Mac user works for.

Authentication on a Mac today

While Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) have been good technologies for authentication on the Mac over the years, they are quickly becoming antiquated in today's modern environments.

Users are forced to take the old-school approach of being on an organization's local area network (LAN) or use a virtual private network (VPN) to connect to internal resources, which provides a sub-optimal user experience. If you're using the Active Directory plugin, users can only change their passwords when AD is reachable — which often causes both confusion and costly help desk tickets.

This dated and patched process presents two major challenges:

1. Wasted IT resources

When employees work remotely, they are not automatically on a company network. This creates password issues. Gartner reports up to 40 percent of an IT desk's volume are password resets.[2] Many of these resets are from remote workers looking for a lost password.

Every help ticket costs money. According to Gartner, the average help desk call was $17.88.[2] And if organizations outsource IT, they're likely billed a large lump sum for every ticket submitted — even if it's for a simple password reset.

Tickets and dollars quickly add up. Companies could be wasting thousands of dollars on password resets alone.

2. Increasing security threats

It's very hard to implement multi-factor authentication or even think about increasing your security through methods like device trust while using AD, LDAP and Kerberos as your primary means of user authentication.

iPass conducted a report showing the biggest threat to company data security is the mobile workforce. In fact, 57 percent of global CIOs and IT decision makers suspect that their mobile workers have been compromised or caused a mobile security issue in the past year.[3]

On-premises tools aren't adequate

Microsoft Active Directory has been the gold standard for on-premises identity and account management. Active Directory ensures company data and applications are protected from anyone outside of the directory that is not an employee.

A majority of companies used Active Directory to solve authentication issues in the past, yet it doesn't meet current challenges.

Why?

As the enterprise world shifts away from Windows to Apple, IT pros question the best practices for integrating Mac with Active Directory.

In fact, currently there are multiple issues with supporting safe and user-friendly ways for remote workers to authenticate through Active Directory:

1. If authenticating against Active Directory, employees have to be on the domain. This doesn't work for remote workers.

2. Organizations have historically leveraged Active Directory as a primary identity provider, yet many employers are shifting to offering Mac devices. This reduces control for remote Apple users — and user management capabilities are limited. This requires the use of third-party add-ons, which adds complexity to user management and higher costs.

3. IT admins can't deploy commands and scripts in the form of policy documents that apply their settings to the computers and users within their control.

Binding to an Active Directory domain was a great solution to solve authentication issues for 20 years. But in an age of increasingly mobile devices, passwords and clocks get out of sync, Domain Name System (DNS) records aren't always available externally, and Active Directory is no longer as viable.

Legacy IT systems and processes are not the way to go. Employees in this day in age want to work anywhere with a sense of security and ease of use.

So how do you eliminate the need to bind a Mac to Active Directory, but maintain account security? Cloud identity!

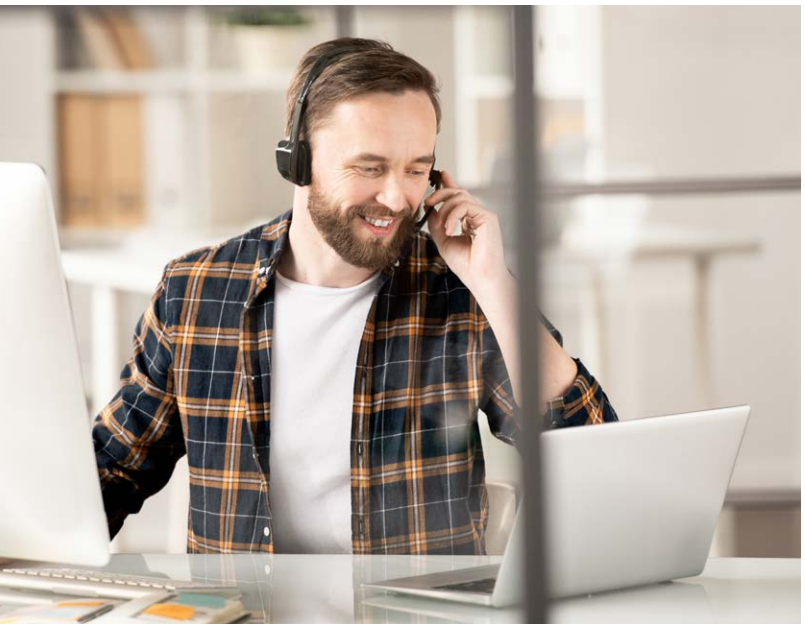
> **With 81 percent of enterprises operating multi-cloud landscapes and 26 percent spending over $6 million annually on public cloud infrastructure, staying on top of identity and security has never been more difficult.[4]**

Cloud identity primer

Without the right tools, security is threatened for remote devices. The approach to identity and security has to evolve. Cloud identity providers — such as Microsoft, Google, Okta, IBM and OneLogin — and Security Assertion Markup Language (SAML) and Open Authorization (OAuth) are offering a path to making this evolution a reality.

What is cloud identity?

Cloud identity allows IT to centrally and remotely manage users, groups, passwords and access to corporate applications and cloud resources.



As such, Microsoft is encouraging organizations to move away from on-premises Active Directory and leverage cloud-based Microsoft Azure Active Directory.

Microsoft Azure is cloud services that allow businesses to build, manage and deploy applications on a massive, global network using specific tools and frameworks. In fact, 95 percent of Fortune 500 companies use it.[4]

But Microsoft Azure is not the only cloud identity provider; there are many options when it comes to cloud identity providers. So, which one(s) should organizations turn to?

Jamf Connect for cloud identity integration

With Jamf Connect, it doesn't matter which cloud identity provider you select. Jamf Connect allows for simple provisioning of users from a cloud identity service during an Apple provisioning workflow, complete with multi-factor authentication.

It offers the flexibility to leverage local users controlled by the same policies and controls you depend on from a directory service or identity provider.

With Jamf Connect, a user can unbox their Mac, turn it on and access every system-approved application after signing on with a single set of cloud identity credentials.

Here are the benefits:

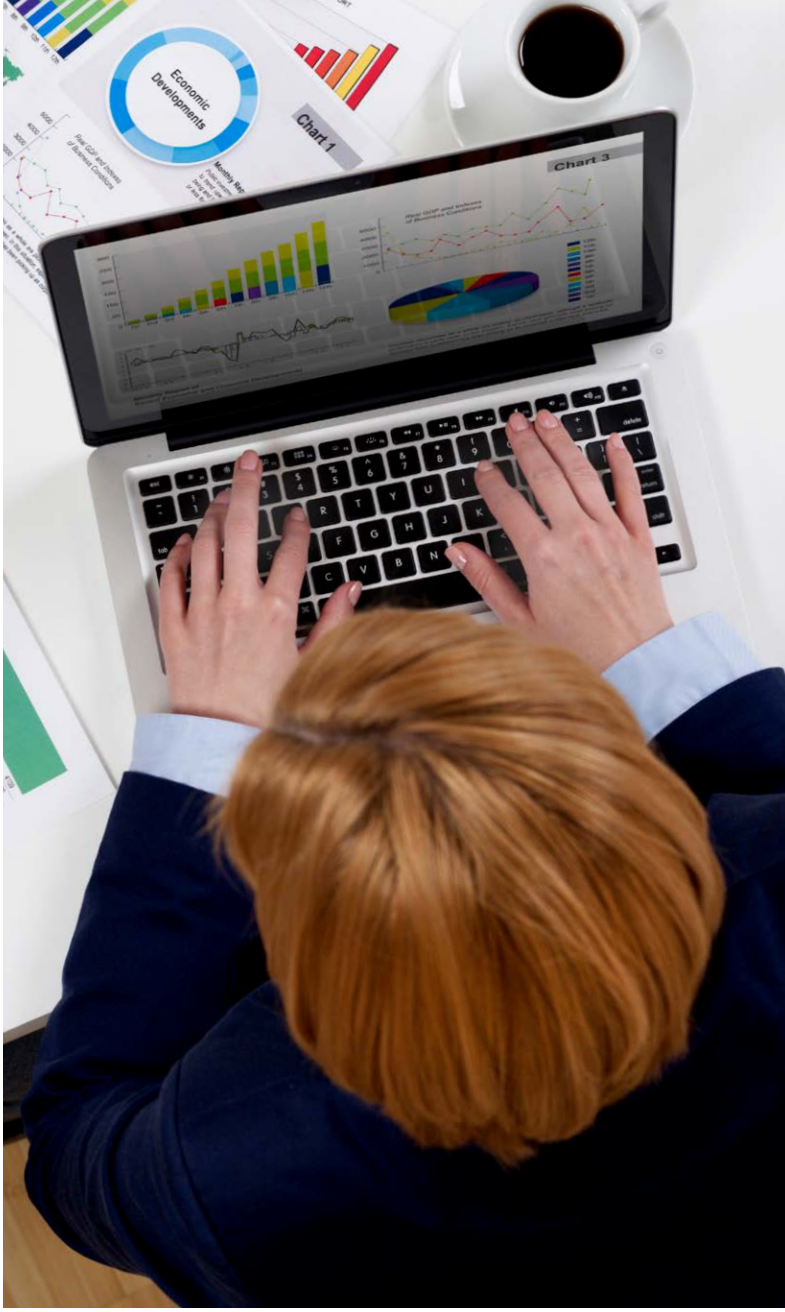
1. **Secure the enrollment process:** Leverage modern authentication to ensure the right user is on the device before deploying anything sensitive to that device.

2. **Just in time account creation:** Create local accounts based on Okta, Azure, Google Cloud, IBM Cloud and OneLogin identities.

3. **Cloud multifactor:** Use supported Okta, Azure, Google Cloud, IBM Cloud or OneLogin multifactor methods at the login window.

Have on-premises?

NoMAD is your answer. Unleash your Macs with the power of NoMAD, a seamless way to sync accounts in environments that leverage Active Directory.



Mobile device management (MDM) and conditional access

As organizations shift away from on-premises Active Directory and see an increase in Mac devices in the workplace, it's paramount that organizations keep corporate information secure, while providing the best-in-class user experience Apple is known for.

Cloud identity providers integrated with Jamf Connect allow IT admins to remotely manage users' passwords and access to corporate applications — ensuring confidence that information is secure in today's mobile world.

Using an automated MDM enrollment system, the process is simple.:

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

2. During this enrollment process, the Jamf Connect package is downloaded and installed from the MDM server.

3. Users are taken directly to the Jamf Connect login window as opposed to having to create their own username and password.

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

In fact, when done right with a dedicated Apple MDM, it's the out-of-box, automated setup experience regardless if an employee is in the office or on the other side of the world.

Let us help you

If you're ready to make your environment more secure and cut down on the number of password-related IT support tickets, connect with us today and we will help you take the next step in Apple device security.

Let Jamf solve your authentication conundrum.

Contact us today to get started or take Jamf Connect for a free trial and put our cloud identity integrations to the test first.

Contact Now **Request Trial**

Or contact your preferred authorized reseller of Apple devices to take Jamf Connect for a test drive.

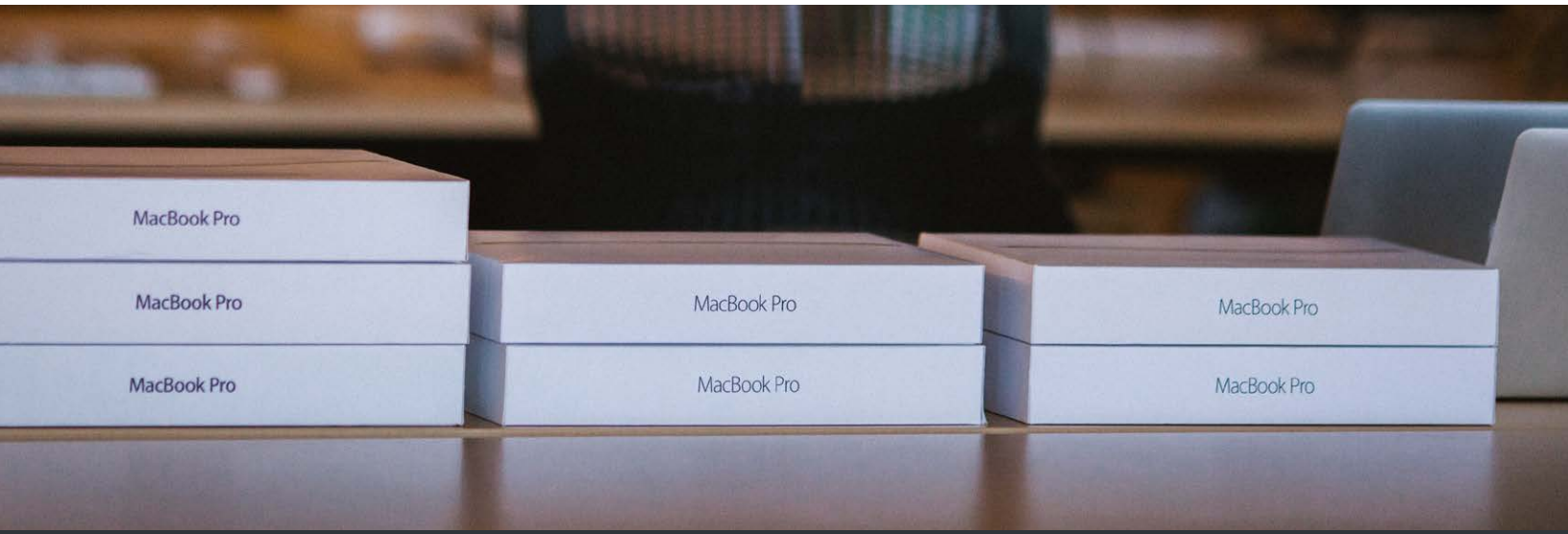
SOURCES:

1: http://news.gallup.com/reports/199961/7.aspx#aspnetForm

2: Gartner Document #G00258742

3: https://www.ipass.com/mobile-security-report/

4: https://www.rightscale.com/lp/state-of-the-cloud



jamf

www.jamf.com

To see how Jamf Connect can help you transition to more modern workflows, visit **www.jamf.com.**