Tides of Change: New Workflows to Replace Imaging

Change can be hard. And when you've been imaging computers for most — if not all — of your career, it can be extremely hard.

The whispers of "imaging is dead" accompanied macOS High Sierra as Apple introduced Apple File System (APFS) to the Mac. Now, whispers have turned to shouts as macOS Mojave takes yet another step further in rendering imaging a thing of the past.

What does this mean?

What does this mean for you and what changes, if any, do you need to get in place as you prepare and ultimately upgrade your fleet of Mac computers to the latest operating system?

This white paper examines all things imaging and looks at the reasoning behind the transition, what new provisioning workflows are available to you, and the benefits of adhering to a more modern deployment method.

So, before you lose a wink of sleep over imaging, read on to get the answers (and peace of mind) you need.

Pay our respects to imaging

Imaging is a set of technologies that are used in a variety of deployment scenarios to copy configurations onto a computer, and comes in a variety of forms:

Monolithic imaging
A process that includes erasing an entire hard drive or volume and re-writing it with entirely new data, including the operating system (OS), customizations and applications.

With macOS High Sierra, macOS Mojave and macOS Catalina, Apple no longer recommends or supports monolithic system imaging as an installation method, because the system image might not include model-specific information such as firmware updates. Additionally, Mac computers must be connected to the internet to receive updates. See this article on Apple's support site for more details.

Modular imaging
Similar to monolithic imaging, the entire hard drive is erased. However, a known good operating system is applied first, then components such as configurations and applications are applied on top of it. This method also runs into the similar issue of needing to be connected to the internet for firmware updates.

Thin imaging

While technically not imaging, this method assumes the shipping version of macOS is good and simply applies settings, configurations and applications on top of the shipping OS via a management tool like Jamf Pro. This is often called "user-initiated enrollment," since it requires a user or IT to manually install an enrollment package. This method is great for scenarios where Apple's deployment programs are not available.

While serving its purpose for past IT workflows, it's clear that Apple is pushing IT admins to convert from device imaging to more modern techniques, and with good reason.

Why the days of traditional imaging are numbered

Traditional imaging techniques can be time consuming to build and maintain because software is updated often and new hardware usually ships with different macOS build numbers.

Aside from the time component, security plays a tremendous role in the move away from supporting traditional imaging workflows. The last thing any organization wants is a user to have malicious software installed on their computer. In order to ensure the operating system is genuine and secure, Apple has added additional security to new Mac devices. This security comes in the form of the Apple T2 chip.

The T2 chip controls everything from power management to audio controllers and offers a new level of native security on the Mac with a feature called Secure Boot. Computers with this chip include:

- iMac Pro
- Mac mini models introduced in 2018
- MacBook Air models introduced in 2018
- MacBook Pro models introduced in 2018 or later

Per Apple: During startup, your Mac verifies the integrity of the OS on your startup disk to make sure that it's legitimate. If the OS is unknown or can't be verified as legitimate, your Mac connects to Apple to download the updated integrity information it needs to verify the OS. This information is unique to your Mac, and ensures that your Mac starts up from an OS that is trusted by Apple.

From a security perspective, this is fantastic news for organizations, IT and users. But, the traditional workflows of pushing OSs over the network or block copying monolithic images via cables to Mac devices is rendered incompatible on new Mac hardware with an Apple T2 chip. The writing is on the wall for imaging as Apple looks to expand similar security measures to the rest of the Mac family.

The case for modern provisioning workflows

Shifting to modern deployment methodologies allows organizations to deliver a better experience to users and one that they are already familiar with as Apple consumers.

It's important to understand that the transition from imaging to provisioning workflows is just that, a transition, and not a complete cutover. There are many Mac devices currently being used by employees, staff and students that utilize traditional imaging workflows. These methods will still work on older operating systems, but organizations will need to migrate workflows moving forward.

A modern provisioning technique (and the recommended process for replacing imaging) involves Apple's device enrollment — now part of Apple Business Manager and Apple School Manager. As Apple's modern deployment programs, these services automatically configure systems by loading a mobile device management (MDM) profile onto devices when those devices initially connect to the internet.

This makes devices more secure, and forces all devices to comply with organizational standards, all while empowering IT with zero-touch configuration of endpoints.

With the rapid pace at which third-party software development, patches and updates are published, the pace of provisioning has never been more fluid and matches the needs of organizations as they change and evolve. Hosting and/or moving data to the cloud simplifies deployments further and becomes the source of truth for configuration and security needs — allowing IT to forget about outdated images and old packages.

How you purchase Apple hardware matters

As your organization phases in new Mac devices, Apple recommends purchasing hardware directly from Apple or an **authorized Apple reseller.** These purchasing methods set you up for success and allow your organization to take advantage of automated device enrollment; empowering you to deliver a sealed and personalized Mac in the box directly to users around the world.

The first time the computer is powered on, it will enroll into your MDM solution. From there, your management provider helps with all of the heavy lifting. Shifting the burden from IT employees building images to managing the Mac provisioning workflow over the air is a significant and worthwhile change.

Tips for building new provisioning workflows

Unlike the days when all software was shipped on a physical medium, like a CD, Apple has been distributing all of their software over the internet since OS X 10.7 (Lion). This means large spikes in network traffic whenever there is an update.

Thankfully, Apple addressed this by moving caching services out of macOS Server and making caching directly available within every macOS client using the Sharing System Preference pane. When enabled, the caching service speeds up downloads of Apple software by storing copies on devices on your network.

It also means every device on your network doesn't have to individually download content from Apple every time there is an update. Instead, one copy will be downloaded to a Mac running the caching service and other devices on your network will grab the locally cached version from a Mac with caching services turned on. Allowing content to be cached on a managed Mac is a setting you can turn on or off via Jamf Pro.

New deployment workflows allow IT to standardize certain settings (Wi-Fi), meet security compliance (enforce a passcode) and enable end users (customized app setup). Here are the three primary deployment workflows to consider and adopt:

1. **Provisioning:** The act of preparing a new device for a user. With macOS Mojave, organizations should leverage Apple Business Manager or Apple School Manager to provision new devices whenever possible. Not only do these portals give users a world-class end-user experience, they make life easier for IT. Organizations using Jamf Pro (the standard in Apple device management) can run policies with the Jamf agent and send configuration profiles after enrollment, so the device is set up completely for users while preserving that special Apple experience of opening the box for the first time.

2. **Re-Provisioning:** Re-issuing old hardware to new users often requires erasing the device and starting over — this is where re-provisioning comes into play. You can use Internet Recovery or scripts to trigger the macOS installer to reinstall macOS Mojave and leverage Apple's deployment services (if the device is eligible) to re-enroll. User-based enrollment can be used for non-eligible (purchased outside of Apple or an authorized reseller) devices, allowing a user to visit a webpage and walk through a personalized device enrollment experience. There are even ways to erase the hard drive before reinstalling macOS Mojave. See the "--eraseinstall" option below.

3. OS Upgrades: Installing the latest operating system on a device. When it comes to Apple operating system upgrades, it is increasingly becoming important to leverage the macOS installer. You must be connected to the internet when you upgrade macOS. This is due to the firmware updates Apple installs on the Mac, further strengthening the security of your fleet. Only the macOS installer can download and install these firmware updates, validating Apple as the source of the critical firmware. In fact, installing macOS Mojave on a Mac connected by Target Disk Mode is no longer a supported installation method. Here are the recommended paths to addressing upgrades if you'd like to keep data intact on devices:

A. Macs enrolled via Apple Business Manager or Apple School Manager (formerly part of the Device Enrollment Program) can be upgraded by sending an MDM command to download and install macOS Mojave. No user interaction or admin rights are required for this option.

B. Download the macOS Mojave installer from the Mac App Store. Leverage Jamf Pro tools to package and deploy the new operating system in Jamf Self Service where users can start the upgrade on their own. This is accomplished via two policies: 1) cache the installer on client Macs and 2) a script that will run the startosinstall command once triggered by the user in Jamf Self Service. Caching the install file on users' Macs will reduce your network load.

C. Similar to the Jamf Self Service option, download and cache the installer on users' Macs. Instead of waiting for users to start the upgrade, create a policy to do it automatically. Users will need to reboot their Mac.

D. Alternatively, you can simply encourage your users to download and run the macOS Mojave installer from the Mac App Store. Admin rights are required for this option.

If you'd like to erase all data on the existing Mac, you can utilize these workflows:

A. --eraseinstall option is a command to install macOS and erase the hard drive at the same time. Simply download the macOS Mojave installer from the Mac App Store and upload via your MDM solution. Deploy macOS Mojave via two policies: 1) cache the installer on client Macs and 2) run startosinstall via a script, but this time with the --eraseinstall flag added to the command. Just like above, IT admins can choose to start this install automatically or place it in Jamf Self Service. For more information, read this article.

B. NetInstall lets you deploy macOS images over your network by leveraging NetBoot. This method is still supported but is labor intensive. Plus, you often need specific macOS builds for certain Mac models. NetInstall will not work on Macs with a T2 chip. Jamf or Apple do not recommend the use of Netboot/Netinstall.

By pairing Apple's deployment programs with a device management solution like Jamf Pro, you can easily deploy and configure macOS, iOS and tvOS (coming soon: iPadOS) devices at scale without ever physically touching the devices.

An end user can take a device out of a box, connect it to the network and the device will automatically enroll into and check in with an MDM solution. An MDM solution then automatically performs all of the configurations required, which allows users to get working quickly (e.g. set up mail clients, distribute certificates, install apps, etc.). Beyond MDM for Mac, Jamf Pro installs the unique Jamf agent on macOS, giving IT unparalleled control over devices via scripts, package installations, extension attributes and other technologies.

Get past the imaging mourning period

At a time when organizations are being asked to do more with less, these deployment changes couldn't come at a better time. By centralizing Mac provisioning activities in the cloud and decentralizing the hardware deployment, you can efficiently set up, manage and re-provision Macs without ever physically touching them.

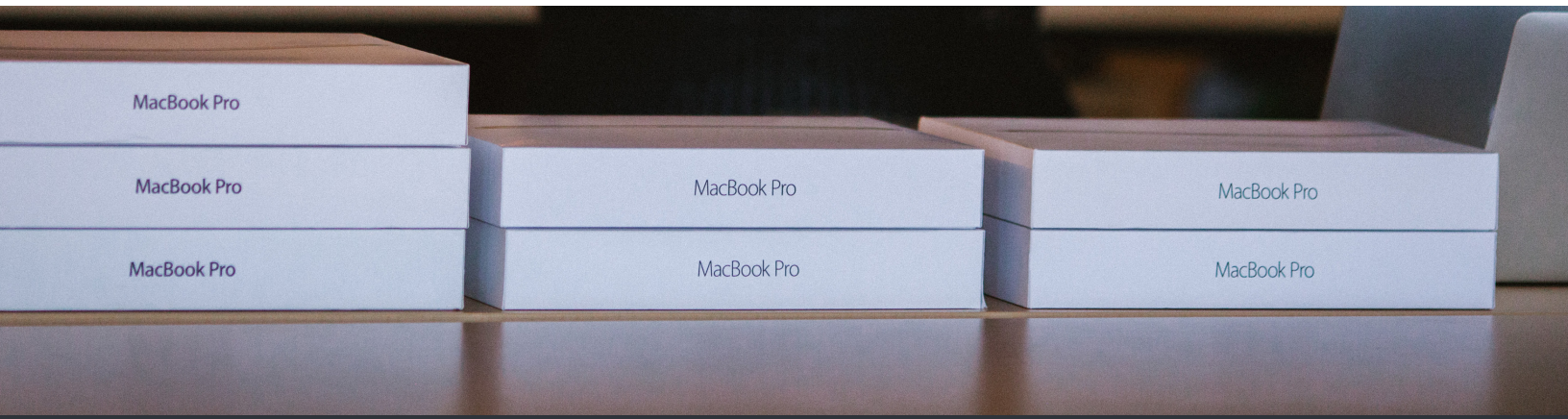
Ready to step into the brave new world of provisioning? With Jamf Pro, you will be.

Contact us today to learn about Jamf Pro's upgrade assistance and day-zero support for new Apple features, and discover why Jamf is the organization trusted by those who trust Apple.

But don't just take our word for it or that of the 96 percent of customers who stick with us year over year. See for yourself by putting our solutions and workflows to the test with a free trial.

Request Trial

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



jamf

www.jamf.com

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