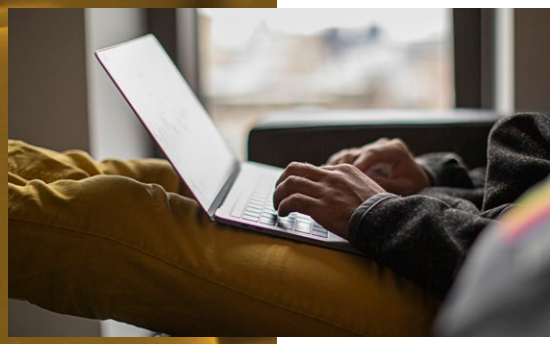
jamf

WHITE PAPER

How to Take Advantage of macOS Big Sur Security Benefits

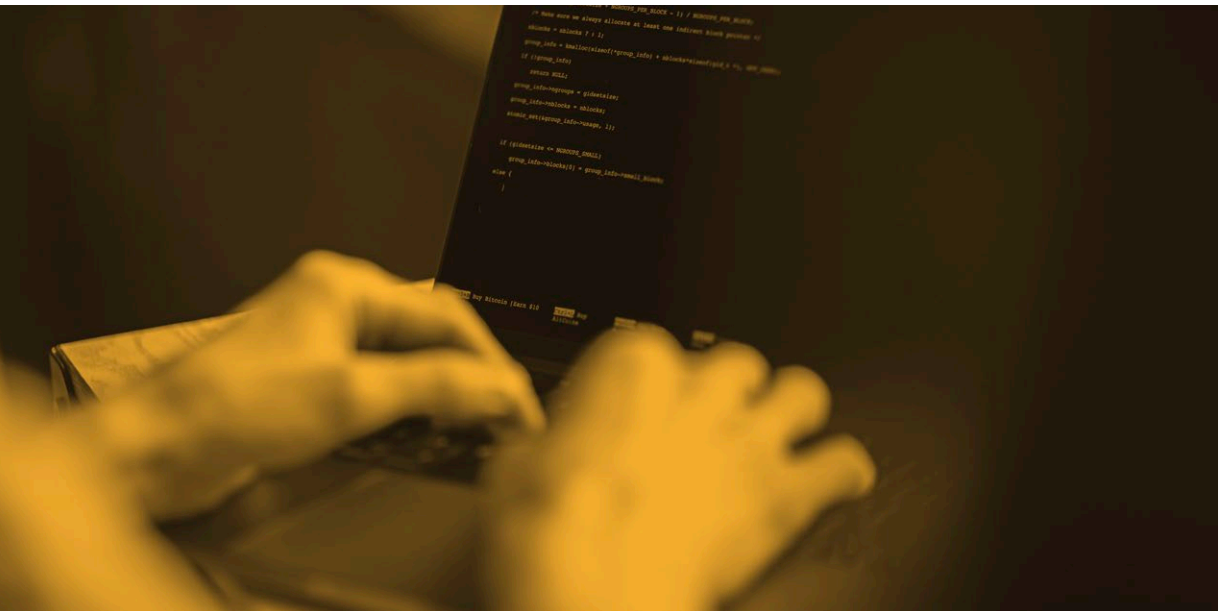


Even the most benign update may include fixes to a series of critical security flaws that an attacker could leverage against the device. Once an OS release is available, it is common for malicious attackers to analyze the updates to identify any patched vulnerabilities and then immediately create attacks against those. Attackers are well aware that not everyone updates their devices immediately; be that due to time, distractions, or the need for organizations to first ensure that the latest update works well with the rest of their software stack.

An OS release is fun, it's exciting, but if you're ill-prepared or your users start upgrading and cause things to break, it can turn into a hectic nightmare, quick. It's this reasoning that drives IT admins and organizations to be constantly fine-tuning their OS update and roll out process often introducing artificial delays while waiting for vendor support. For the last nine years, Jamf offers same-day support for Apple's operating system releases, allowing our customers to upgrade on their schedule, not ours.

When it comes to Mac security, Jamf Protect is designed for macOS from the ground up. It provides anti-virus functionality by preventing known Mac malware, detects malicious and suspicious activity and through application controls that restrict unwanted applications, minimizing your risk profile. As you roll out macOS 11 Big Sur, Jamf Protect continues to prevent Mac-specific attacks without the need to install a kernel extension. Built on **Apple's Endpoint Security Framework**, Jamf Protect provides Apple-first prevention capabilities requiring no manual intervention to upgrade to macOS 11 Big Sur.

With Big Sur came great advancements in hardware including new iterations of iPad, iPhone, and Mac with Apple's new M1 chip, but it also brought much needed security improvements. Each of the new aspects below are great motivating factors to ensure your team and organization is on the latest OS.



Sealing the System

The biggest single change in macOS 11 is its new Sealed System Volume (SSV), which replaces the separate System volume introduced in macOS 10.15. This deepens system protection from the existing read-only volume covered by System Integrity Protection (SIP).

During macOS installation, once its System volume installed, cryptographic hashes are computed for every component on that volume and assembled into a tree (like a Merkle tree), culminating in a single, master hash termed the Seal. Those hashes are saved as metadata and a file system snapshot is made of the volume.

Instead of macOS mounting the System volume read-only as it does in Catalina, only that sealed snapshot is mounted, giving immutable system files further robust layers of protection from tampering and error.

During early startup, macOS Big Sur checks the Seal on the system. If that's broken, the operating system won't boot and has to be reinstalled. Recovery mode offers an option to disable that check, making it possible to customize a System volume and run it unsealed; setting that up is intricate and non-trivial.

Once unsealed, users can't reseal the system, and the only ways of creating a sealed system are using a macOS Big Sur installer or updater, or with the Apple Software Restore command tool asr. Previous methods of copying or cloning the System volume no longer produce a bootable result, and compatible third-party utilities must also use asr to be successful.

macOS Big Sur provides a Sealed System Volume that raises the protection of key system files beyond the reach of all current malware and should withstand the most determined attacker from altering them after the OS has booted. It also guards against inadvertent corruption and guarantees system integrity.

> Apple's new Sealed System Volume is a big step forward in securing the macOS system and has significant consequences for some users. Coupled with improved protection of kernel space by moving user extensions into user space, it makes macOS 11 significantly more resilient.

Certificate Deployment

Trusting Root Certificates on a host is a critical security function. Here are some real-world malware examples of one of the most common attack patterns, predicated on installing a new certificate trust, man-in-the-middle (MiTM) network traffic: Install new cert, redirect traffic via local proxy, decrypt and read traffic before forwarding to intended place.

- **VoiceFive, a Comscore Company Distributes a Man-In-The-Middle Proxy Spyware Compromising Users Security & ALL SSL**
- **OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic**

Prior to Big Sur, any script/installer/application running with root permissions (MDM or locally) could add trusted certificates to the system without additional user interaction. All they had to do was trick a user into installing an application — and prompt for root credentials — and in the background the trusted certificate could be installed.

Starting in Big Sur, any time a script/installer/application attempts to locally install a trusted certificate there will be an additional explicit password prompt to the user before this action is completed. To work around this limitation in the enterprise and to continue to allow for "unattended" installation of legitimate applications, use an MDM to install trusted certificates on your endpoints — as this approach does not require user interaction.

App Security

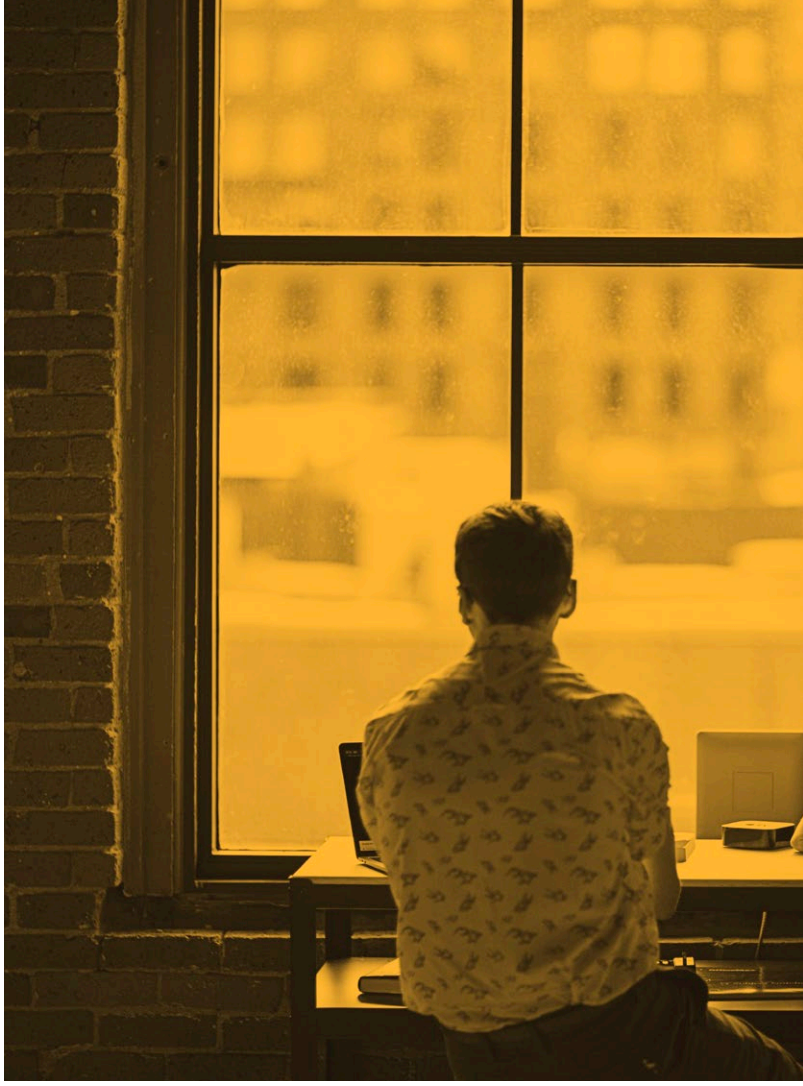
Although there's no overall change in security requirements for apps and other third-party software, notarization is more strictly enforced, with users having to negotiate a sequence of two dialogs before newly-installed apps that aren't notarized can be opened. In Catalina, some users learned that opening a new app in the Finder runs that app from a single dialog even when it isn't notarized. Within macOS Big Sur, this action is made more deliberate, as users must use the Open command a second time before being asked if they really want to run the app despite its lack of notarization.

Unsigned code can still be run on Intel models, but Apple Silicon Macs require all executable code (except scripts) to be signed. Although, that can just be with a locally generated ad hoc signature.

Kextless

KEXT deprecation began with the release of macOS Big Sur, which means now is the time to understand how this affects your environment and find compliant partners to help with the transition.

Kernel extensions, or KEXTs, offer developers the ability to tap into the kernel space and develop within the kernel. From this space, developers can monitor processes, prevent applications from launching and generally monitor all actions on a device. In legacy OSs, many implementations of security monitoring and application's controls leveraged this technology. Coding within the kernel is a 'double-edged sword'. It allows third-party apps and software to have direct access to make substantial changes, but if something goes wrong, it often goes very wrong. Creating extensions into the kernel is no longer supported by Apple because you are often interfering with the operating system itself, potentially in a way that impacts its ability to function properly.



Whether it happens over the course of a few years or within the next few rollouts of macOS, Apple has said they are eliminating KEXT. This means there is a point in the near future when switching to the new user mode frameworks instead of a KEXT will become mandatory. With the release of Apple's newest Mac operating system, macOS Big Sur, it's important to mention that kextless security tools and kextless third-party apps remove a major aspect of stress that revolves around upgrading devices. Since many security providers that rely on a KEXT are still testing their platforms to make sure it will function as desired with the new OS, it causes unnecessary stress on organizations looking to keep their devices compliant with the most up-to-date system and can result in costly downtime.

There is an alternative option to still achieve these security measures without this large amount of risk. One that was built with Apple device security as the top priority. Since applications in user mode never interact with those internal structures and systems, they are safe from these deprecative changes.

Jamf Protect, an endpoint security solution built purposefully for Mac, was designed to use Apple-supported aspects and never required the use of kernel extensions. This also means when Apple announced at WWDC19 the deprecation and eventual elimination of KEXT, while also unveiling the addition of a new System Extensions with the Endpoint Security Framework, Network Extensions and DriverKit, Jamf was ready to embrace this concept, without having to undo any reliance on kernel extensions.

Get e-book

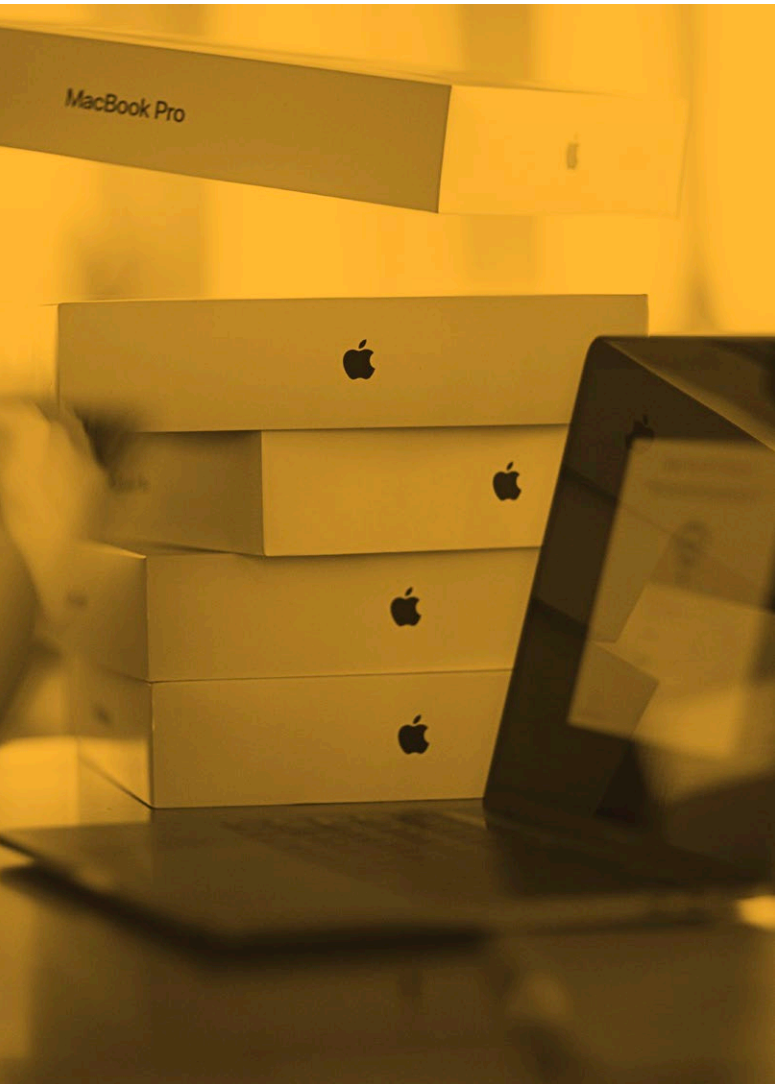
Learn more about going kextless

M1 Chip

Every once in a while, the world of technology makes a giant leap forward. The first personal computers, wide adoption of the internet and the first iPhones were not only fascinating and useful technology in and of themselves, but they also transformed an entire industry, spurring competitors and collaborators to new heights. The Apple M1 chip heralds one of those leaps.

The M1 Chip offers:

- Three times the performance per watt than that of previous Mac chips and two times the CPU speed
- A rather astounding battery life of two-to-three times that of machines without the M1
- Two times the graphics speed than the latest PC laptop chip



- Hardware specialized for specific operations both for end users and the OS
- A requirement that applications either be built specifically for the new architecture or be translated through a special tool in the OS dubbed Rosetta 2
- Restrictions on certain types of older application architectures, such as requiring special deployment steps that cannot be automated to install a KEXT

The requirement that applications be built specifically for the new architecture or be translated through Rosetta 2 and restrictions on certain types of older application architectures could be tricky waters to navigate if your security partner is ill-prepared. Finding one that is built for Apple and focused on Apple will put you ahead of the curve.

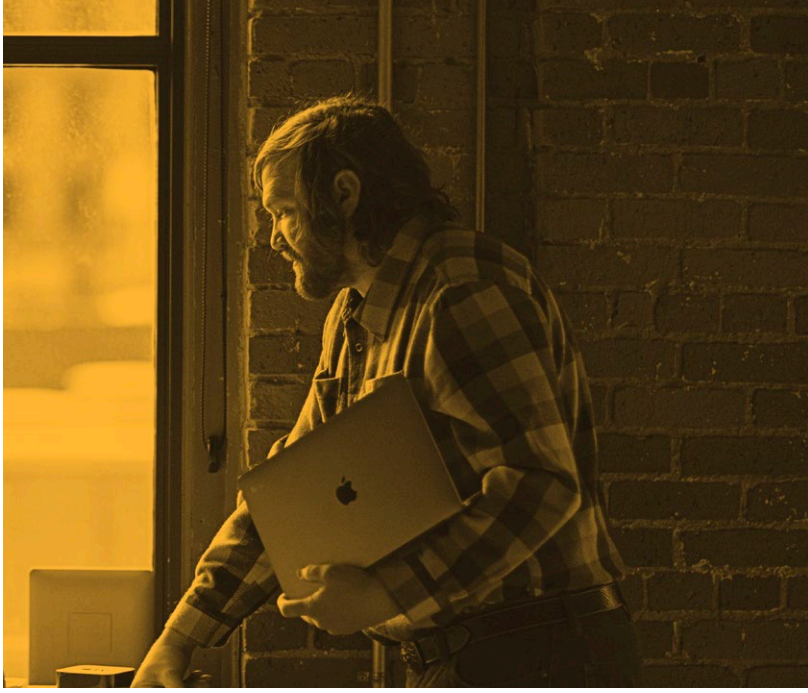
Jamf Protect:

- Already uses a universal binary — can protect both M1 Chip and legacy Mac devices seamlessly
- Kextless — preventing Mac-specific attacks without the need to install a kernel extension
- Using the Apple Endpoint Security Framework means that Jamf Protect adapts easily to the new restrictions in macOS Big Sur and those imposed by M1 device

These features of Jamf Protect allow users to upgrade their team to the latest hardware on their own terms without having to do a mass upgrade and change their entire fleet. It enables companies to comply with new demands while still supporting Intel-based Macs.

Learn about M1

Rosetta 2



While the M1 chip is unquestionably a huge leap forward for Apple, there will be an adjustment period as some software companies scramble to keep up, as mentioned above.

The switch to M1 sets up a common architecture, extending continuity between macOS, iOS and iPadOS applications — seamlessly integrating them across Apple's hardware ecosystem. However, as with any significant hardware transition, applications designed to run on one processor are unable to successfully run on another without:

1. **Breaking compatibility**
2. **Modifying source code**
3. **A translation process that keeps old applications running on the new architecture**

This can create headaches for developers as they attempt to fully support their applications on those devices using M1 chips, and Mac admins as they attempt to integrate Mac computers using the M1 chip into their existing Intel-based fleet. Just how nimbly this will happen depends on how quickly application creators can offer a universal binary that can smoothly accommodate and integrate both Intel-based and M1-based Mac computers.

Until then, applications will have to rely on Rosetta 2 to automatically translate Intel-supported apps to M1 devices with any associated performance impacts.

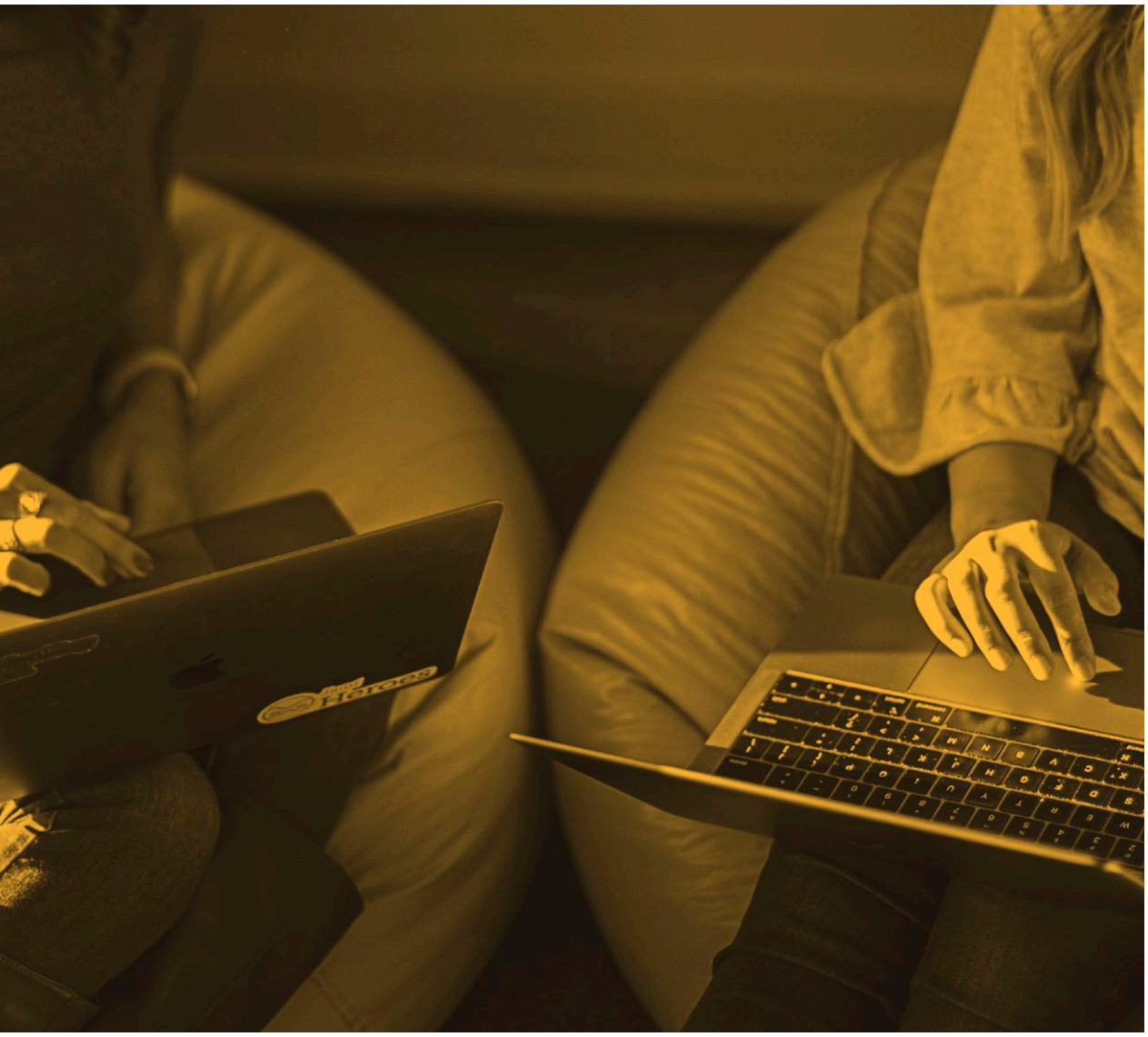
Rosetta 2 is a translation process that allows applications built for Intel-based Macs to run on the Apple silicon-based processor. Rosetta 2, available in macOS 11 Big Sur, boasts technological improvements that includes automatic translation of non-native apps upon installation and no longer interpreting code in real-time making it more efficient at translating older software than the original.

While Rosetta 2 is temporary, it gives developers a bridge as they adapt to the new M1 architecture and create a universal binary with two different compatibilities: one binary for Intel and one binary for M1's ARM architecture.

But don't fret. Jamf is here to help. Of all the Apple Enterprise Management providers in the market today, Jamf is the only one that was around to help organizations through the last Mac processor change. For the first step, if you need Rosetta 2 on your Apple Silicon devices, Jamf Pro will help you get that deployed.

Jamf Pro and Jamf Protect are built with Universal binaries that natively support Macs with either Intel or Apple silicon processors. The universal binary ensures users achieve forward and backward compatibility on any application that supports their current OS version without relying on Rosetta 2 to aide as a translation layer. As a result, Jamf products are current, more efficient and support the newest Macs immediately.

Learn more



Conclusion:

Security is an ever-evolving, fluid state. As more people adopt Mac, in both personal and work settings, more people will try to infect and damage Mac. It's the battle that security teams are tasked with and one that is winnable through preparation and partnership. Apple routinely invests their time, efforts, and upgrades into raising security measures to keep your devices and data secure; however, it sometimes is not enough. Finding a partner that dedicates themselves to your specific device type is becoming a must-have. macOS 11 Big Sur made great strides forward, and Jamf aligns with Apple and continues its work to make Apple devices secure and the best device for every user.

Request Trial

See how Jamf gives you complete Apple security