AN OVERVIEW FOR MAC, IPAD, IPHONE AND APPLE TV

Apple Device Security

FOR BEGINNERS

A well-planned cyberattack or an accidental download of malware can mean the difference between a productive day and all work grinding to a halt. As hackers get more sophisticated, organizations concerned about their bottom line and security of their customer, employee or student data must stay on top of security.

Apple security concerns, like all IT security concerns, are real.

While Apple has invested a great deal in its security features and has rapidly become the leader in device and data privacy and security, no operating system is immune to security challenges.

This means that administrators must not only respond quickly to security issues, but also proactively guard against them.

This guide is for administrators and managers who want to get serious about their organizational security of their Apple devices, and offers basic information for newcomers or a simple refresher for Apple management veterans.

Introduction to Apple Security

The basic building blocks

Several factors work together to ensure the security of your organization's hardware and data, and you can break them down into six main areas:

Apple native security

Security systems already built-in to macOS, iOS and tvOS

Page 4

Securing devices

Keeping your physical devices secure and protecting those using them

Page 6

Data encryption

The basics of encrypting data at rest and data in transit

Page 8

Compliance monitoring

Monitoring devices to pinpoint needed updates

Page 11

Application security and patching

Keeping up-to-date software

Page 12

Secure deployments

Deploying with the highest level of security available

Page 14

Building Block One: Apple Native Security

How to make the most of them with device management

Security features already built in to macOS (operating system for Mac), iOS (operating system for iPad and iPhone) and tvOS (operating system for Apple TV) are extensive and come with several benefits:

- Apple operating systems are based on a UNIX foundation, a very well-researched and developed foundation with excellent stability
- Strong OS security framework
- Device security in the form of locking and device finders
- Ability to implement and configure security controls through configuration options via mobile device management (MDM)

An MDM solution can take these existing security configurations and deploy (and enforce) them to a large group of devices. So, you can set up not only one Mac securely, but thousands.

You also have more expansive security controls with an MDM tool that can lock and wipe devices that are lost or removed from the facility.

Security feature details

Native security features for macOS, iOS and tvOS

macOS Security Features

- Software Updates
- System Integrity Protection (SIP)
- Gatekeeper
- App Store
- FileVault Encryption
- XProtect
- App Sandboxing
- Privacy Settings

iOS Security Features

- Software Updates
- Secure System
- App Store
- Touch ID
- Hardware Encryption
- App Sandboxing
- Privacy
- Supervision
- Remote device finder for lost devices

- Direct software updates from Apple
- Vetted and secure App Store apps
- Supervision (with use of MDM)
- App restrictions
- Airplay settings and passwords
- Banner/screen default

Building Block Two: Securing Devices

Tracking, securing and protecting devices and users

One of the simplest ways to damage an organization's security framework or to compromise end-user's safety is through access to a single device. Whether your organization serves students, teachers, healthcare workers, remote staff, retail floor employees or frequent travelers — at any given moment your devices could be in twenty different places.

Lost or stolen devices

A lost or stolen iPad, iPhone or Mac isn't just a financial loss: it's a huge security risk. The damage can be incalculable: a thief manages to find private student data from a lost laptop or accesses the entire organization's database from that laptop. A former employee who still has her work laptop making private information public or offering it to competitors. Even a malware introduction from a remote source.

Devices get lost and stolen. Accidents and moments of inattention happen, and planning with the assumption that the question is only when someone will lose track of a device is vital.

In addition, many devices — especially those serving students and patients, or devices shared by multiple users — require safeguards against misuse, accidental discovery of another's data, or viewing of inappropriate content.

Securing or restricting devices manually:

Mac

- Require passwords on all devices
- Enable Find My Mac through System Preferences > iCloud
- Depend on individual user to be able to sign into iCloud and remember password
- Track all Mac serial numbers
- Report to Apple online if a device has been lost or stolen
- Enable parental controls on the device to block websites (Only affects Safari browser)

iPad and iPhone

- Require passwords on all devices
- Enable Find My Phone through System Preferences > iCloud
- Depend on individual user to be able to sign into iCloud and remember password
- Report to Apple online if a device has been lost or stolen
- Enable parental controls on an individual device, creating different accounts for each device

Apple TV

- Require passwords on all Apple TVs
- Use restrictions:
  - From the main menu, go to Settings > General > Restrictions
  - Select Restrictions to turn it on
  - When asked, make a four-digit passcode
  - Enter the four digits again to confirm, then select OK
  - Ensure that you remember the passcode
  - Repeat for all Apple TVs

Securing Devices

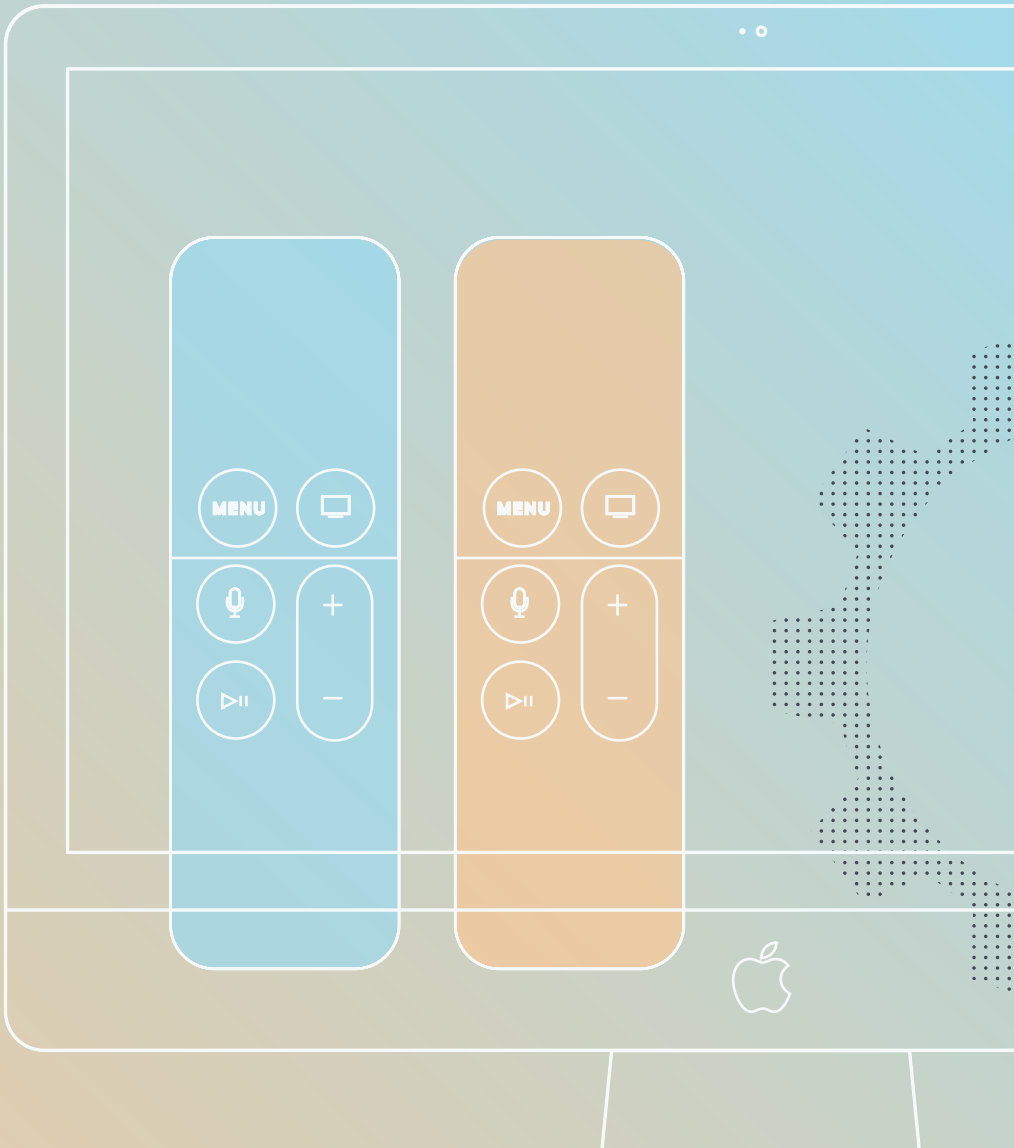
Restricting Airplay for Apple TV:

- From the main menu, go to Settings > Select AirPlay
- Turn AirPlay on or off
- Choose from:
  - Everyone
  - Anyone on the Same Network
- Repeat for all Apple TVs

Securing or restricting devices with an MDM such as Jamf:

Mac, iPad, iPhone and Apple TV

- Set all restrictions and security features from first use or setup with configuration profiles or policies
- Lock any lost or misused device centrally
- Wipe any lost or misused device centrally
- Enable multiple users to securely share devices, leveraging their own sign-ons with their own settings, or by wiping the device between uses, such as with patients



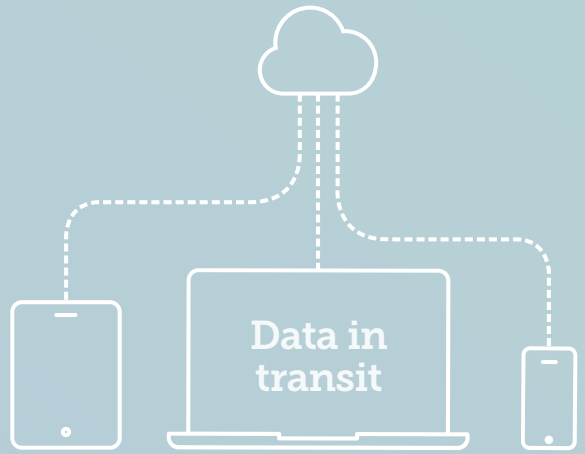
Building Block Three: Encrypting Data

The basics of data at rest and data in transit, and how to keep both types secure.

Whether your organization is a school protecting student information, a health care facility guarding patient health histories, or a business intent on protecting your intellectual property, encryption is no longer an option for your organization: it's critical. Business best practice is to encrypt all data on devices.

There are two types of data:

Data on devices or in databases.



information moving wirelessly from one location to another.

Encrypting Data

Data at Rest:
Disc or device encryption.

- macOS already has built-in disk encryption: FileVault. You don't have to add any additional software in order to encrypt a drive on a Mac.
- FileVault is FIPS 140-2 certified. That means Apple's encryption system meets the highest standards for federal government encryption.
- You can enable FileVault manually or remotely: user can choose the option themselves on one device, or IT can enable FileVault (using Jamf) across hundreds or even thousands of devices in one session.
- Jamf ensures that encryption keys are centrally stored in case you need to uncover data, someone leaves or someone forgets their password.

To manually enable FileVault:

1. Navigate to System Preferences > Security and Privacy > FileVault
2. Select the toggle switch to turn on the option from there
3. Repeat for all devices

To enable FileVault across your organization's devices, leverage an MDM solution to automate, deploy and enforce encryption. You can deploy a configuration profile or policy that will enable FileVault, and IT can retrieve encryption keys in case staff need to de-encrypt the device down the road.

1. Create a configuration profile through a simple selection of options within Jamf
2. Deploy to as many devices as you'd like
3. There is no step three

With Jamf, you can also configure for recovery key redirection — even if the user turns on FileVault themselves. IT will then have the key saved within their management solution.

What about an iPad or iPhone?

Encrypting iOS devices is even easier. iOS devices have built-in encryption as soon as a passcode is set. You can do this individually, or you can do it from Jamf, as well as setting up parameters for the passcode such as length and complexity.

Encrypting Data

Data in Transit:
A VPN (Virtual Private Network) can protect data as it moves wirelessly from one device to another service.

People traveling or working remotely should use a VPN to connect to your organization's network. This best practice creates a secure connection back to your trusted organization network, which ensures that the data you're sending will be encrypted end-to-end.

Both macOS and iOS have built-in VPN clients to allow you to connect to a number of well- known VPN service providers.

What you'll need for data in transit

- A secure network connection
- A VPN server

To connect to a VPN manually:

After you have set up a VPN provider:

1. Go to Preferences > Network
2. Type in the VPN server address on the device
3. Select it from your network options
4. Repeat for each device

To connect multiple devices to a VPN:

After you have set up a VPN provider:

1. Create a configuration profile in an MDM such as Jamf for iOS and/or Mac
2. Deploy configurations to however many devices you'd like
3. You guessed it — there is no step three

How can I be sure that my encryption is seamless?

One important way of ensuring security and consistent encryption is to host your MDM in the cloud. With a reputable product such as Jamf Cloud, you can rest easy knowing that your server is secure and your data safe, and that any updates or patches are immediately available.

Building Block Four: Compliance Monitoring

Ensure that protocols and controls are in place on all devices

A security system is only as good as its weakest point. For the best coverage, administrators must monitor the organization's devices to ensure that every device is updated, has received the most recent patches, and has the correct encryption options enabled.

Monitoring compliance manually:

To ensure that all of your organization's devices are protected, you would need to constantly audit devices.

1. Physically track down each device
2. Go into each option individually to ensure that
   - Software updates are all current
   - Encryption is enabled
   - No one has introduced malware or a virus
3. As updates are only as good as the last update you performed, repeat
4. And repeat
5. This will require constant vigilance and a great deal of buy-in and cooperation from end users

Monitoring compliance with Jamf:

To ensure that all of your organization's devices are protected through Jamf's inventory feature:

1. View up-to-date, real-time information on all devices simultaneously
2. Deploy updates and security configurations for any device that is not secured properly
3. Say it with us: there is no step three

The ability to see device statuses helps administrators know which updates to send where, and which security features to configure. Dynamic smart groups based on department, permissions, devices, or any other categorization method mean that administrators can be as targeted or all-encompassing in updates as they choose.

Building Block Five: Application Security and Patching

Keeping up-to-date on patches and ensuring the safety of applications

Application Security: It's vital to know that your applications don't contain malware or other hostile code. If you can't trust your application sources, you'll compromise security.

Apple has made apps as safe as possible to download and use with the following features:

- They've adopted a **sandbox model**: each app lives in its own space and can't interact with other applications. To allow apps to read or write to others' shared data requires approval from the user or administrator.
- Apps in the **App Store** have been vetted to alleviate security risk. This is the only way to get apps on an iOS device, which controls security. Confining Mac users to the App Store for their apps is a way that administrators can control security device-wide.
- **Gatekeeper for macOS** is a feature that either users can select or, with an MDM like Jamf, administrators can configure for all devices. Users or administrators may select from three Gatekeeper options, allowing apps downloaded from:
  - Mac App Store
  - Mac App Store and identified developers
  - Anywhere

Best practice is to allow the Mac App Store and identified developers, especially if you create your own applications or repackage apps. Sign them yourself so they'll be trusted by Gatekeeper.

While Mac allows for an 'anywhere' option, know that only making sure you know where the app is coming from and that it is signed by developer you trust will ensure that it hasn't been modified in transit.

Setting up Gatekeeper options manually:

1. Navigate to: Preferences > Security & Privacy > General
2. Select from the three options available
3. Repeat for every device in your organization

Setting up Gatekeeper options with Jamf:

In keeping with the pattern, set up and deploy a configuration profile to all devices.

That's it.

Application Security and Patching

Patching:

All software, created by humans who make mistakes, will have bugs. There is just no way of avoiding this. Humans are, well, human.

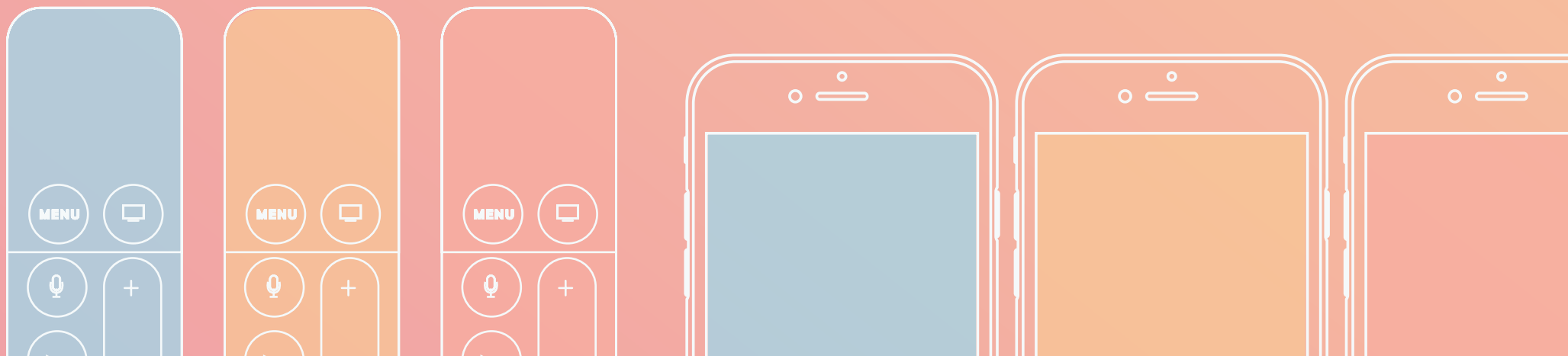
That is why it's imperative for organizations to implement a strategy for incorporating bug fixes as quickly as possible — especially as bugs can be security vulnerabilities.

Options for managing patches manually:

- Educate users to self-update as soon as they receive update notifications on their devices.
- Collect all devices when an app releases a new patch and manually download.
- Catch devices up that are missing patches during your manual compliance monitoring.

Options for managing patches with Jamf:

- Jamf receives automatic updates and automatic patch notifications, along with tools for deploying patches to all of your organization's devices, so you are never surprised by a patch you missed.
- You can make it easy for users to update with Jamf's Self Service app catalog, which can notify users that they need to update before continuing to use the app.
- Or, you can disallow individuals from implementing updates, and send out patches as policies to all devices, or targeted with dynamic Smart Groups.



Building Block Six: Secure Deployments

Conduct secure device and software deployments with Jamf and Apple Device Enrollment

The first step to ensuring secure deployments to all of your devices is to enroll in Apple's free Device Enrollment program.

With Device Enrollment, you can inform Apple of all devices your organization owns, and tell Apple that you want all of these devices managed by your organization's MDM. Then, when a device enrolled in this program first starts, it will automatically enroll itself in your organization's MDM – allowing for tighter security controls and swifter security updates, as well as applying all configuration profiles. This not only saves time, but also ensures security and eliminates guesswork.

jamf

With Jamf, you get:

Zero-touch enrollment

Scalable deployment

Secure configurations

For Mac, iPad, iPhone and Apple TV

Device and data security is no laughing matter.

Organizations have the choice to get ahead of possible attacks or thefts by implementing the strongest possible security protection through Apple — and Jamf can make this easier, faster and far more secure than manual security protocols.

jamf

Don't find yourself surprised and scrambling. Take proactive steps to secure your devices and data to ensure the safety and security of your organization — and the individuals who make it.

Get the best security options for your organization by taking a Jamf product for a free trial run or start by contacting a Jamf representative.

Try Product | Contact Us

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