Apple Device Security

FOR BEGINNERS

A well-planned cyberattack or an accidental malware download 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 the security of their users' data, like customers, employees or students, must stay on top of security.

Apple security concerns, like all IT security concerns, are quite real and pose a critical threat to organizational resources and stakeholder safety.

Apple makes incredibly secure operating systems; there's no doubt that its focus on the security and privacy protections baked into its hardware and software has played a significant role in its rise in popularity and mass adoption within enterprises, education institutions and other industry organizations. And as Apple continues to be the platform of choice for personal and professional hardware, it has become a more attractive target for attackers. This means that administrators must respond quickly to security incidents as they arise and not wait until an issue occurs. Instead, MacAdmins and security teams (and the stakeholders they support) are better served proactively guarding against them before threats can evolve into something far worse by leveraging solutions tailored or purpose-built for Apple to protect against Apple-centric threats effectively.

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

Introduction to Apple Security

Several factors work together to ensure the security of your organization’s hardware and data:

1 **Apple native security:** Security systems already built in to macOS, iOS, iPadOS and tvOS

2 **Enrolled devices:** Enrolling and deploying devices with secure, centralized management and visibility

3 **Securing devices:** Protecting your physical devices and safeguarding your users from threats

4 **Data encryption:** Securing data at rest and in transit, on device and in network at all times

5 **Compliance monitoring:** Monitoring devices to determine health status and enforce baselines

6 **Application security and patching:** Staying up to date with operating system, app and software patches

1

BUILDING BLOCK ONE:

Apple Native Security

Apple devices are the most-secure out-of-the-box hardware options on the market, and purpose-built management and security solutions extend the power of Apple.

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

- **Apple operating systems are based on UNIX underpinnings which creates a rich computing foundation from a mature, well-researched platform with deep development roots for rock-solid stability.**
- **Strong OS security framework:**
  - Notarization
  - Gatekeeper
  - XProtect
  - Malware Removal Tool (MRT)
  - Transparency, Consent and Control (TCC)
  - Rapid Security Responses
  - Lockdown mode
- **Physical device security in the form of locking and lost device tracking with the Find My service**
- **Ability to implement and configure security controls through configuration options via mobile device management (MDM)**
  - Secure enrollment modes are built in to Apple devices, such as Automated Device Enrollment and User-initiated enrollment for company- and/or personally-owned devices to meet all ownership model needs (like BYOD, CYOD and COPE) without risky enrollment URLs or suspicious email invitations
  - Seamless integration with Apple Business Manager or Apple School Manager to aid in centrally managing all institutional hardware, including enabling Supervision of devices over-the-air and secure hand-off to your MDM solution for device management functions, like managed app deployment, secure device provisioning and zero-touch onboarding workflows

A purpose-built MDM solution can take these existing security configurations, align them to your unique organizational needs, including industry benchmarks, and deploy (as well as enforce) them to your entire Apple fleet, regardless of size. So, you can securely and efficiently set up one Mac just as easily as you would thousands. You also gain more expansive security controls with an MDM tool that makes performing administrative tasks easy on any devices you select. For example, you can make short work of repetitive tasks by remotely locking and wiping devices that are lost or should be removed from your facility's inventory, to name a few. Learn more with our Apple Device Management for beginner's e-book.

Security feature details

Native security features for macOS, iOS, iPadOS and tvOS

macOS	iOS and iPadOS	tvOS
Software Updates	Software Updates	Software Updates
System Integrity Protection (SIP)	Secure System	App Store
Gatekeeper	App Store	Airplay settings and passwords
App Store	Biometric Identification	App restrictions
FileVault Encryption	Hardware Encryption	Screen saver
Supervision	Supervision	Supervision
XProtect and Malware Removal Tool (MRT)	App Sandboxing	
Find My	Find My	
Privacy Settings	Privacy Settings	
Notarization and file quarantine	Secure Enclave and Biometric Identification	
Endpoint Security API	Notarization	
App Sandboxing		
Secure Enclave and Biometric Identification		

2

BUILDING BLOCK TWO:

Securely Enrolled Devices and Deployments

As with all building blocks, the key to success is a solid foundation. This informs each subsequent building block that follows and sets the overarching tone for the management and security as it pertains to the hardware and application lifecycles.

The first step to correctly provisioning devices and securely deploying them across your entire fleet in a standardized, efficient manner is to use Automated Device Enrollment, which is included as part of the free services offered by Apple through Apple Business Manager and Apple School Manager.

With Automated Device Enrollment, you can inform Apple of all devices your organization owns, as well as other ownership models discussed below, and assign them to be managed by your organization's MDM. Then, when an enrolled device in this program powers on, it will:

- Automatic enrollment to your MDM instance
- Enable Supervision, which is integral for allowing tighter security controls
- Allow administrators to apply configuration profiles and harden settings
- Ensure critical security settings and payloads are deployed before the user can begin using a device
- Streamline management and deployment of OS updates and security patches
- Cut down on the quantity of device provisioning workflows by centralizing app procurement, configuration and deployment, which also ensures security of apps from vetted, trusted sources
- Reduce device setup by empowering users to maintain their devices without needing support from IT
- Permit remote management regardless of which supported device is used, from where and over any network connection

Device ownership models

Automating the management and security of your device fleet is a critical feature, especially as device counts grow and as the workforce becomes decentralized. The rise in the adoption and reliance on the Apple platform and mobile devices in the workspace has become as diverse as the industries and users that rely on these devices to remain productive.

Some organizations have embraced Apple products by implementing employee choice programs that assign company-owned devices running macOS and iOS and iPadOS, while other organizations have embraced Apple at work by allowing employees to use personally owned devices to access business resources. By empowering them to work more comfortably using the hardware and software they are most familiar with, organizations offset the expense of providing equipment for each stakeholder—especially when users already have a functional device they know and love.

This shifts the question from “How do we provide user’s devices?”
to “How do we ensure company resources remain secured?”

This is where your organization's MDM and flexible device ownership models meet to form the solution of multiple device ownership models, such as:

Bring Your Own Device (BYOD)

Arguably the most common model, allowing users to use their personally owned devices to access business resources. By requiring that users manually enroll their devices in the organization's MDM before gaining access to work resources, the dual-fold benefit is that users can rest assured that they will obtain the tools necessary to access the data and services required for them to perform their job functions; organizations rest easier knowing that enrolled devices are provided the necessary security software and settings to keep business data secured while in use, at rest and in transit.

Choose Your Own Device (CYOD)

This a variation on BYOD above, except that often, the organization or institution owns the devices used in this model and are to be used in carrying out job-related functions or in the pursuit of learning (in the case of education.) By instituting a program of employee choice, stakeholders can choose which Apple device meets their needs best. Each device is enrolled, assigned to a stakeholder and managed by the organization's MDM. The apps, configuration profiles, device settings and security software are provisioned according to a baseline of the organization's security posture and taking into account the assignee's job requirements.

Company-Owned Personally Enabled (COPE)

The COPE model is a growing trend among larger organizations, especially those that have gone fully remote or with hybrid work environments. Here, organizations purchase and own the equipment, while enrolling and managing it fully within the organization's MDM. Like CYOD, the tools necessary for stakeholders to perform their job tasks are installed and managed according to the device and the company's security posture. But similar to BYOD, the organization allows and even encourages users to utilize the devices for personal use alongside professional usage. This ensures that company data stays secure within managed apps and configuration profiles. While this can open up the issue of personal, private data being accessible to companies via COPE devices, it's important to consider the privacy of the data and provide the right amount of management and privacy to these devices through means of Acceptable Use Policies (AUPs) and data managment.

Flexible enrollment methods

To simplify the management of multiple device ownership models within the same MDM environment, Apple has developed two different enrollment methods used in conjunction with one another to manage and enforce organizational security without compromising user privacy and vice-versa.

Automated Device Enrollment

This is the most common method that most organizations with company-owned equipment prefer to choose. This method certifies that each step in the enrollment chain is verified: from procurement from Apple (or an authorized third party) through pre-staging in the MDM to the enrollment phase that starts when the device is powered on — each step follows in an automated procedure from Apple to MDM to administrator for on-going management. Because this chain is verified, Supervision is enabled on devices enrolled through Automated Device Enrollment, which acts as a trusted foundation that allows IT to obtain full control over the device throughout its lifecycle. Supervision is the root of trust, required when performing certain management tasks on managed devices.

User-initiated device enrollment

This enrollment method is newer and more common when the enrolled devices are personally owned as part of a BYOD model. With Automated Device Enrollment, the enrollment relies on the user or owner of the device to manually enroll their device within the Settings app and authenticate using their company credentials. After completing the user enrollment process, the organization's MDM is two-way secure communication between the user's device and organization's management solution.

Once enrolled, personally owned devices are manageable through the MDM, with administrators permitted to install managed apps, deploy configuration profiles and modify certain settings using a set of configurations allowing organizations to set device-specific requirements as well as associate management actions or requirements with the user, not the entire device. Apple designs the limitation to allow organizations to take the steps necessary to secure how their data is accessed, interacts with apps, is stored on device and transmitted over networks without impacting the personal apps, data and private information on the device. Organizations can customize the visibility of managed devices by associating a personal Apple ID with personal data and a Managed Apple ID with company data.

3

BUILDING BLOCK THREE:

Securing Devices

Keeping devices, data and users safe from threats

“Hackers only need to get it right once; we need to get it right every time.”

— Chris Triolo, HP

If we look back at some of the largest, most complex and even deadliest data breaches in recent history, we’ll find a common thread. Attacks such as Stuxnet disabled Iran’s nuclear enrichment program by infecting a contractor’s laptop performing updates to the SCADA equipment. LinkedIn was targeted by a developer that exploited its API to effectively scrape PII from 700 million users before selling the data dump online. Aadhaar—home to the largest ID database, including PII and financial data, for more than 1.1 billion Indian citizens—was stolen and sold by threat actors after gaining entry through an unprotected website linked to the database. In these and similar cases, attacks were made possible by targeting and compromising just one device.

One of the most common ways to bypass an organization’s security framework and gain access to sensitive data while also putting end-user safety at risk is by compromising a single device. Regardless of which industry your organization represents or whether it provides data and/or resources to knowledge workers, students, teachers, healthcare providers, remote staff, retail staff or frequent travelers — at any given moment, your devices could be anywhere in the world and connecting via any number of untrusted networks — exponentially increasing the exposure to risk of threats for both the device and the company’s network.

Lost or stolen devices

A lost or stolen iPhone, iPad or Mac isn't just a financial loss: it also represents a massive security risk where the potential for fallout may be incalculable. Consider the following examples as underscoring the criticality of mitigating risk for lost and stolen devices:

REAL-WORLD SCENARIOS

A remote employee is prepping legal documents for an ongoing liability case being argued in court and is working from a nearby coffee shop. They leave the company-owned Mac laptop unattended briefly while refilling their coffee at the precise moment a thief swoops in and steals the laptop. With the device unlocked, the attacker has unfettered access to sensitive and possibly confidential company information that could negatively impact current legal proceedings and the company's reputation.

In a second example, a student using their personally owned iPhone to access school-related resources via the educational portal misplaces their device while changing classes. Another user finds the phone and proceeds to access the student's account details, gaining access to sensitive PII, like their address, phone number or student ID. An unauthorized user can utilize PII information like this for identity theft or to commit crimes while impersonating the victim. The device may even be further compromised with malware and returned to the victim, placing their safety and well-being at risk from remote tracking and stalking by threat actors.

Simply put: Devices get lost and stolen. Accidents and moments of inattention happen. Yet, planning — with the assumption that it is only a matter of when, not if, someone will lose track of a device — is a vital key toward ensuring that the proper mitigation strategies are in place to minimize risk before devices become lost or stolen.

Additional consideration points for user and data security are that many devices — especially those serving students and patients or shared device environments serving multiple users — require safeguards against misuse, the accidental discovery of another's data or the access and viewing of risky and inappropriate content.

Depending on your organization's unique needs, hardening settings for security while configuring devices so that they're aligned with organizational and compliance requirements could be a considerable undertaking that is time and labor-intensive, especially as device counts grow.

When securing or restricting devices manually, you need to:

Mac

- Require passwords on all devices
- Enable Find My Mac through System Preferences>iCloud
- Depend on individual users to be able to sign into iCloud or remember their password (prerequisite to enabling FindMy)
- Report to Apple if a device was lost or stolen while enabling the ability to initiate wipe/erase
- Track all inventory by Mac serial numbers or asset tags
- Enable parental controls on the device to block inappropriate content and malicious websites (using Safari browser)
- Keep Macs up to date with all system and app updates to minimize vulnerabilities
- Configure and harden device settings to minimize misconfigurations that could leave data unsecured
- Deploy supported applications and keep them updated
- Install and configure endpoint security to monitor devices, identify and remediate threats

Phone and iPad

- Require passwords on all devices
- Enable Find My Mac through System Preferences>iCloud
- Depend on individual users to be able to sign into iCloud or remember their password
- Track all inventory by device serial numbers or asset tags
- Report to Apple if a device was lost or stolen while enabling the ability to initiate wipe/erase
- Enable parental controls on an individual device, creating different accounts for each device
- Keep iOS-based devices up to date with all system and app updates to minimize vulnerabilities
- Configure and harden device settings to minimize misconfigurations that could leave data unsecured
- Deploy managed applications and keep them updated
- Install endpoint security to monitor devices, identify and remediate threats

Apple TV

- Require passwords on all Apple TVs
- Configure 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
  - Remember the passcode
  - Repeat for all Apple TVs

To restrict 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

On a best-of-breed MDM solution, like Jamf Pro, the same management tasks performed above to secure or restrict devices goes like this:

Mac, iPhone, iPad and Apple TV

- Set all restrictions and security features from the first use or enable them automatically with Supervision and trusted configuration profiles and policies
- Lock or wipe any lost or misused device remotely, regardless of its physical location — and regardless of whether the device has an iCloud account signed in or not (no Apple ID required)
- Enable multiple users to securely share devices by wiping a device between uses and allowing users to use their credentials and settings that are connected to the user — not the device
- Configure managed Apple IDs to be assigned to the device for business tasks while allowing the user to access personal apps, data and settings stored in iCloud with their consumer Apple ID
- Maintain inventory of all devices, including the ability to group them by any category — not just serial number or asset tag — to glean any data necessary, such as user assignments, OS version or apps installed to name a few
- Perform management tasks that issue commands to a single device or in bulk, such as deploying security updates, upgrading to a new OS version or administratively clearing forgotten passcodes on locked devices
- Implement parental controls and block access to risky or inappropriate apps, applying granular restrictions based on certain criteria or to all devices at once
- Deploy managed applications necessary for users to remain productive at home, in the office, at school or anywhere else. Pre-approve apps to be hosted within the Self Service app, empowering users to access the software they need exactly when they need it
- Integrate endpoint security solutions with your MDM to ensure that devices are constantly monitored and protected against security threats while sharing rich telemetry data with the MDM to enable policy-based management for automating incident response
- Manage each facet of device management tasks centrally to ensure devices, users and data remain secure against cyber threats while upholding user privacy

Not only does this experience streamline work for IT administrators and staff, but it also supports the end users. It provides the experience people love and have come to expect from Apple without sacrificing organizational, industry compliance and security requirements or user privacy in favor of tighter security controls.

4

BUILDING BLOCK FOUR:

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 healthcare 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 a critical requirement for any business wishing to keep sensitive, confidential and mission-critical data, or really data of any classification type safeguarded, the best practice is to encrypt all data on devices.

Below is a summary of the three states of data at any given time on a device:

Data at rest: stored locally (usually) on a device that is currently not being accessed or used.

Data in motion: transferred data — both being received or transmitted — over a communications channel, like a wired or wireless network.

Data in use: neither kept in permanent storage nor transmitted over networks, this refers to data currently being worked on by applications or other processes.

Each has inherent risks unique to its state, meaning that, generally speaking, a solution for one state may not fully compensate (or work at all) for another. While this adds complexity to your security strategy, fret not, because effective solutions all center around the fundamental function of encryption.

REAL-WORLD SCENARIOS

A new hire in the HR department at your organization receives their new Mac and quickly completes the setup process to begin working. One of their job functions requires creating an emergency contact tree **using spreadsheet software**, including each employee's name, job title, company email address, personal address, personal contact number and specifying whether they are a primary or alternate contact. This information is to be **backed up locally** to the computer, including the personal contact information for members of the management and C-suite teams, and a duplicate copy must be made available to authorized stakeholders to **access from a cloud repository securely.**

In the scenario above, the portions in bold indicate a specific example of each data state. First, "using spreadsheet software" is an example of data in use, indicating that data must remain secure while it's being worked with within the app. This requires the software's integrity to be checked and verified to ensure that a threat actor or malicious code has not compromised its internal security. Second, "backed up locally" is an example of data at rest, indicating the criticality of enabling encryption to prevent data from being accessed and read by unauthorized individuals. Third, "securely access from a cloud repository" is an example of data in motion, as in data sent and received across a network connection. The network connections used for communication must be encrypted end-to-end, ensuring that only the two connections at either end can successfully decrypt the message and protect this data from unauthorized receipt or eavesdropping attacks.

And while this third data state may sound a lot like legacy VPN services, the component that separates it from legacy VPN is the wording "authorized stakeholders," since Zero Trust Network Access (ZTNA) provides encryption for data in motion, ZTNA also integrates with your identity provider (IdP) ensuring only users and devices that have both authenticated successfully and are provisioned the necessary access permissions are granted access to the requested resources behind additional layers of protection, upholding the principle of least privilege. Also, unlike legacy VPN services which often grant access to the entire network once authenticated, ZTNA's implementation of securing connections utilizes micro-tunnels to establish a unique tunnel for each protected app or service. This provides greater security by enforcing the principle of least privilege while employing health checks to ensure that devices meet minimum requirements — in conjunction with user authentication requirements — each time a request is made and before granting access.

How to encrypt the three states of data

Data at rest

Volume or full device encryption

Encrypting the data stored on a mobile device or within a volume on your computer is a best practice for several reasons. Consisting of proactive and reactive measures, the easy-to-configure process of enabling encryption provides the maximum safety and security for data at rest in permanent storage. Utilizing algorithms that would take attackers hundreds, or more likely thousands of years of working around the clock using the most powerful computers to defeat given the relatively minimal effort required to setup encryption, it's a "no brainer" when it comes to including this security control as part of a defense-in-depth strategy — like The Alamo, or the proverbial "last stand" between a threat actor and confidential data.

Take for example some common security incidents that are effectively mitigated by enabling full device or volume encryption:

Loss or theft of a device

Misplaced devices, like iPhones, iPads or MacBook laptops, are especially common for mobile devices. The greater the mobility, the greater the risk of loss or theft. That said, once a device is out of your hands, threat actors have free rein to attempt to obtain the data stored on the device.

Sure, a complex passcode or strong password should protect your device. However, depending on the device, there could still be alternate means for attackers to access some or all of the data contained within the device — except when it's encrypted. The simple act of enabling encryption scrambles the data to the degree that it is unreadable unless the decryption key unscrambles it. It doesn't matter if the device is booted to the login screen or the SSD is somehow accessed and connected to another device as an external drive. Encrypted data remains encrypted until the decryption or recovery key is used to decrypt it — any other scenario renders the data unreadable and, therefore, useless.

Physical access

Similar to the lost or stolen devices section above, obtaining physical access to a device doesn't mean it must first be misplaced. Think of a shared device in a workspace, perhaps the dedicated computer assigned to you at your desk or any computing device that a threat actor may attempt to use when no one is looking. When your session is over and you log out, shut down or even lock your device while stepping away or not in use, the data contained in the volume or device is and remains encrypted. A decryption or recovery key is required to decrypt the data to gain readable access to the secured data.

Regulatory compliance

Depending on the industry your organization belongs to, you may be subject to laws — known as regulations — that govern minimum requirements for safeguarding data and how it is processed while also mandating limitations over which job roles are allowed to work with protected data types. Specific industries are regulated more aggressively than others; these are highly regulated industries, like the finance sector and healthcare, while others may only focus on certain aspects of data security, like education regulations that aim to protect the welfare of students and the PII associated with them.

As mentioned before, regulations are based on laws and violating them could have dire consequences for the organization or institution if they did not properly adhere to the rules of the governing bodies. Often, encrypting data is a tentpole security control required during different data states, like at rest or in motion to minimize the risk of regulated information falling into the wrong hands through data leakage, exfiltration or even exposure to unauthorized users.

Data encryption and Apple devices

- macOS already has built in volume encryption in FileVault. You don't have to add any additional software to encrypt a folder, disk or volume on a Mac.
- Newer Macs, like those powered by Apple Silicon, rely on the secure enclave. A dedicated hardware component that handles the creation and storage of encryption keys while also performing algorithmic calculations.
- Intel-based Macs rely on a similar dedicated hardware component named the T2 security chip to perform similar functionality to the secure enclave.
- FileVault is FIPS 140-2 certified. That means Apple's encryption system is certified by and meets the highest standards for federal government encryption.
- You can enable FileVault manually or remotely: personal users can choose the option on one device, or IT can automate and enforce enablement (using Jamf Pro) across hundreds or even thousands of devices with one policy.
- Grant users access to encrypt/decrypt volumes simply by authenticating to macOS or entering their passcode on iOS and iPadOS devices. Users of supported devices can leverage Apple's TouchID or FaceID technologies to add a layer of security to data protection through biometrics using either their fingerprint or facial recognition patterns.

To manually enable FileVault on macOS:

- Navigate to System Settings > Privacy & Security > FileVault
- Select the button "Turn On..." to enable volume encryption
- Repeat for all devices

To enable FileVault across your organization's devices, leverage your MDM solution to automate, deploy and enforce encryption. You can deploy a configuration profile or policy that will enable FileVault. IT can retrieve recovery keys if staff need to decrypt the volume down the road.

- Create a configuration profile through a simple selection of options within Jamf Pro
- Deploy granularly to as many devices as you'd like or to all macOS-based devices
- **There is no step three**

With Jamf Pro, you can also configure recovery key redirection — even if the user turns on FileVault themselves. IT will then have the key saved within its management solution for easy retrieval by device record.

What about an iPad or iPhone?

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

Data in transit

Encrypting network connections from end-to-end

Conventional best practices dictated the use of a VPN to protect data as it moves from one device to another service. This method heralds back decades, being developed at a time when VPNs were used to bridge two disparate networks securely over an untrusted network, like the Internet.

And while this security control still remains in active use by many personal and enterprise users, changes in the computing landscape over the last few years, stemming from the adoption of Apple at work, the explosive growth of mobile devices for personal and business use and organizations migrating to fully remote and hybrid work environments has revealed the limits of VPN technology to effectively protect devices, users and data across the modern threat landscape.

These changes have all combined to revolutionize the way we work — and play — on computers and mobile devices. So, why are you still relying on legacy processes for your security strategy to keep data in motion safe?

The answer short answer is Zero Trust Network Access, or ZTNA for short. The long answer is that this solution was developed from the very real-world need to keep various types of devices, local and distributed users and teams. Also, data accessed over untrusted networks and relying on cloud-based services to extend infrastructure while eroding the organization's network perimeter. All this while securing them against existing and novel security threats employed by threat actors, with a notable increase in threats targeting macOS and mobile devices in general.

Simply put: Securing network connections is no longer just for employees traveling or a few special use cases to remain productive remotely.

It also extends beyond merely encrypting communications between two points, requiring granular security protections, to safeguard stakeholders and prevent access to company resources while minimizing the introduction of threats. Some of the ways ZTNA accomplishes this is by:

- Integrating with cloud-based IdPs to extend centrally-managed user accounts to include permissions that follow the user around.
- Frequent device checks ensure that endpoints meet minimum requirements, such as being up to date with patches, ensure that security integrity remains intact by checking for jailbroken or rooted devices and that endpoint security is both installed and configured properly.
- If endpoints fail a health check or have been deemed compromised, ZTNA integration with a best-of-breed MDM solution, like Jamf Pro, enables policy-based management by securely sharing telemetry data to suspend access and execute remediation workflows to perform the necessary tasks to bring the endpoint into compliance, verifying that any detected issue(s) are resolved.
- Forgoing implicit trust, like legacy VPNs, instead operating by the mantra of “never trust — always verify” each time access to any requested company resource is made. It is only after verification has occurred successfully that access to the requested resource is granted.

What you’ll need for data in transit

A secure network connection to a VPN server

To connect to a VPN manually:

iOS and iPadOS	macOS
▸ Go to System Settings> VPN	▸ Go to System Settings> Network>VPN & Filters
▸ Select “Add VPN Configuration”	▸ Select “Add VPN Configuration”
▸ Type in the VPN server address on the device	▸ Type in the VPN server address on the device
▸ Select it from your network options	▸ Select it from your network options
▸ Repeat for each device	▸ Repeat for each device

To connect multiple devices to a VPN:

After you have set up a VPN provider

- Create a configuration profile in an MDM such as Jamf for iOS and/or macOS
- Deploy configurations to however many devices you’d like
- 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.

Benefits of ZTNA over legacy VPN:

- Security is enhanced by shifting from implicit trust to the explicit Zero Trust model that requires verifying users and devices before granting access to requested resources.
- Split-tunneling secures business traffic while personal traffic is routed directly to the Internet — not back to a central network, reducing overhead and saving bandwidth, which equals greater performance and improved privacy protection for end users.
- Always-on protection means that resources are protected — even if the service is disabled — upon requesting access, it will automatically enable to ensure traffic remains protected every time.
- A minimal footprint and cloud hosting means no expensive support contracts, complex configurations or hardware to manage.
- It also supports macOS, iOS, iPadOS, Android and Windows, which lowers the TCO and alleviates the administrative burden on IT teams supporting multiple hardware and software types.

In this section, we've discussed the basics of data encryption, the types of solutions native to Apple devices and even explained the steps to enable this security control on macOS, iOS and iPadOS. We've also discussed how modern ZTNA technology goes beyond legacy VPN protection by continuing to secure remote network connections while including additional layers of security to verify users and devices before granting access requests and ensuring that data remains secure at rest (former) and in motion (latter). But what about when data is being used, or processed by apps?

Unlock the other two data states; data in use does not have a specific security control to mitigate this risk. Instead the solution lies in conjunction with ongoing management and security workflows.

When apps access and process data, the data passes from the memory (RAM) to the app for processing, then gets swapped back to memory before being saved permanently on the device's storage. Apps developed by known, trusted developers all contain security mechanisms to ensure the app's internal security remains intact. Among the many reasons for this, one such reason is to ensure that data processed within an app is not shared with or leaked with other apps, services or processes running on the device. This is designed to uphold the integrity of the data while the app's integrity is maintained.

However, apps that have become compromised through an exploit to a vulnerability had unauthorized modifications to their internal security or are rogue apps, marketed as performing one task really performing other clandestine tasks all place data security at risk while in use.

So, what's the best solution, you ask? The answers below include a combination of best practices, a defense-in-depth strategy, and processes and workflows leveraging Jamf Pro to keep data in use as secure as possible:

- A continual patch management policy that procures applications from legitimate sources, like the Apple App Store, developer website, or from a trusted management vendor — like App Installers with Jamf.
- Deploying managed apps through your preferred MDM solution and implementing policy-based management to keep apps up to date.
- Verifying secure device settings by installing configuration profiles to minimize the possibility of threats from misconfigurations.
- Harden device settings to restrict risky behaviors that could introduce threats, like jailbreaking iOS or iPadOS, or side-loading applications from unauthorized or insecure sources.
- Implementing an ongoing user training program to keep stakeholders informed of common threats and how certain actions, like Shadow IT, introduce risk.
- Develop an Acceptable Use Policy (AUP) that all stakeholders sign to make them aware of behavior expectations and consequences of violating company policy.

5

BUILDING BLOCK FIVE:

Compliance Monitoring

Know the status of protocols and controls 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 verify that every device is updated, has received the most recent patches and has the correct configuration options set.

"Awareness of ignorance is the beginning of wisdom."

— **Socrates**

By continuously gathering rich telemetry data, the details of each device that provides insight into the security controls, settings and health status, IT can better protect devices, users and data while making sure that endpoints that are out-of-scope are quickly remediated and brought back into compliance before threats can lead to far worse outcomes, like data breaches.

As with most of the building blocks in this e-book, there are multiple paths to monitor endpoint compliance: manual and automated methods. Depending on your organization's requirements, compliance monitoring's efficacy can be impacted by contributing factors, such as knowledge base, device and security management solutions used and budgetary considerations, to name a few of the most critical.

Monitoring and managing inventory and compliance manually means:

- Ensuring that all of your organization's devices are protected by constantly auditing devices
- Physically tracking down each device for inventory management needs
- Individually updating software applications on each device to ensure they are up to date
- Verify that security settings, like encryption, are configured consistently on every device
- Monitoring and confirming that no one has introduced risks, such as malware or suspicious apps
- Performing OS and critical security updates as soon as they're available to patch known vulnerabilities and fix bugs in software
- Deploying adequate personnel to triage detected issues, quarantine compromised devices and perform remediation tasks to bring affected endpoints back into compliance

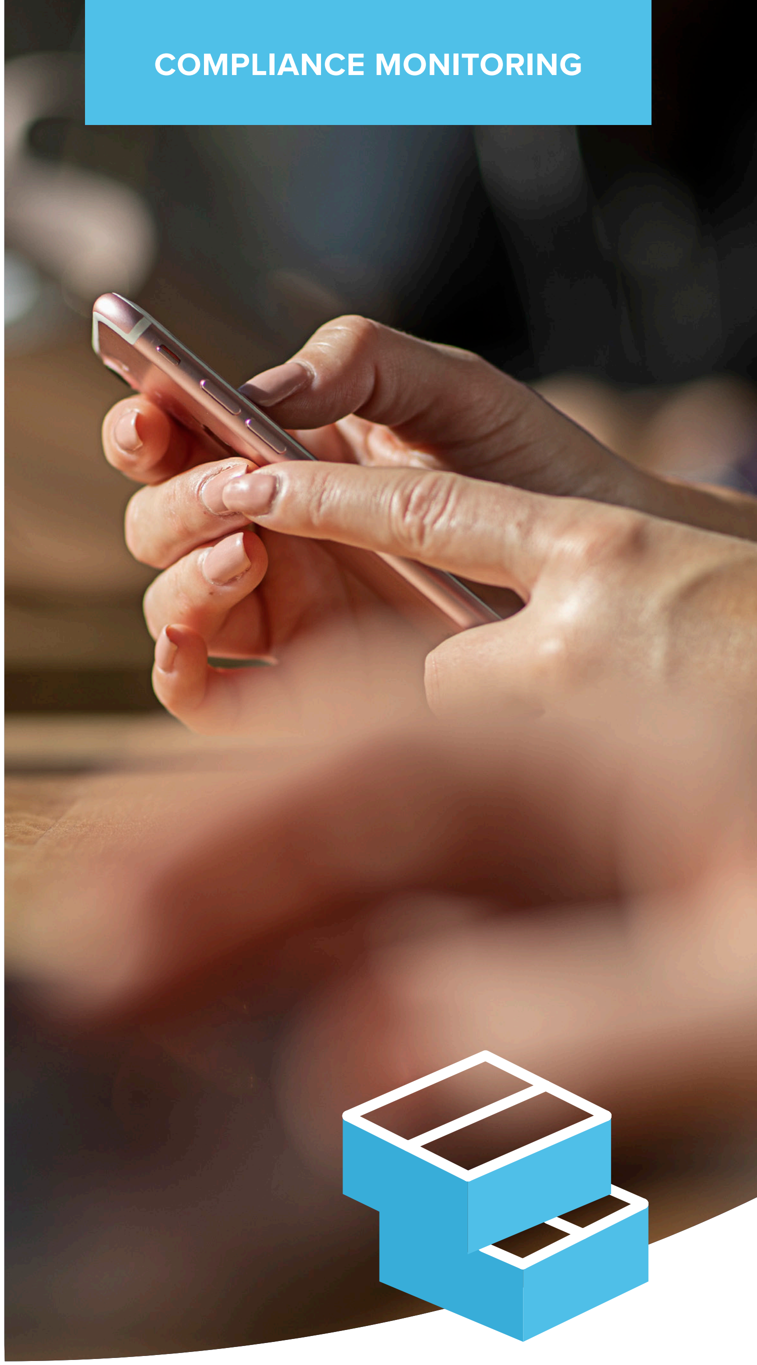
This method requires constant vigilance and large windows of time for administrative overhead related to completing management tasks. A great deal of buy in and cooperation across stakeholders and management teams is needed to be successful. It is also important to note that this method is largely reactive in nature, meaning that time-sensitive issues, like incident response times, will likely be lengthened, occurring after issues are detected — yet seldom beforehand.

As a last consideration, the number and types of devices supported an increase in size, the time for IT and Security to respond to issues manually will also increase exponentially. This gives threat actors more time to expand threats in their attack chain against organizations, simultaneously increasing the risk of a data breach.

Monitoring inventory with Jamf means:

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

The ability to see device inventory statuses helps administrators keep their finger on the pulse of every Apple device in their fleet. By knowing the current status of a device, administrators can efficiently manage devices and security by knowing which updates to send where, and which security features to configure respectively. Creating Smart Groups, based on dynamic criteria means that administrators can be as targeted or all-encompassing in updates as they choose. Whether based on granular permissions, specific device types, or virtually any other categorization method, Jamf Pro provides powerful tools to make short work of compliance-related tasks while maintaining the flexibility to zero in (or send tasks to all devices in your fleet) through customizable criteria. Learn more with our Inventory Management for Beginners e-book.



Managing compliance with Jamf means:

- Audit endpoints based on Center for Internet Security (CIS) benchmarks
- Stream all your compliance data to the cloud for centralized management
- Access macOS unified logs and comprehensive endpoint telemetry to identify threats quickly and efficiently
- Enforce compliance using policies to automate remediation tasks and keep endpoints in-scope
- Monitor for Common Vulnerabilities and Exposures (CVE) to understand the vulnerabilities that exist in your environment
- Prevent security threats using comprehensive analytics mapped to the MITRE &TTACK framework
- Securely share telemetry data between management (Jamf Pro) and security (Jamf Protect) solutions via API to develop advanced workflows to automatically minimize incident response times and resolve identified issues without delay

It's not enough to secure your devices; many regulations mandate that organizations be able to prove that devices continue to be secure and meet compliance requirements. This means organizations must provide documentation to corroborate compliance levels during various points in their timeline. After all, if you can't provide evidence the device was compliant at a given time, then for all intents and purposes — it wasn't compliant.

However, Jamf's data and reporting provides organizations with the necessary tools to obtain telemetry data from every endpoint and organize this data using critical categorizations, like patch levels, vulnerabilities detected and timestamps that identify actions performed during the device's lifecycle. Plus, integration allows the secure sharing of telemetry data with first- and third-party tools to further extend data through centralized dashboards to include data visualizations and export to other formats for sharing compliance reports with regulatory investigators.

6

BUILDING BLOCK SIX:

Application Security and Management

Patch reporting, policies and App Installers to maintain apps updated while enforcing security easily.

Application Security

Knowing that identified vulnerabilities are patched is vital to the device's security posture. But do you know where your applications come from? And are you confident that they don't contain malware or other malicious code? The answer to those questions is critical to your organization because if you can't trust your application sources, you risk compromising the security of your devices, as well as end-user privacy and exposing sensitive data.

Apple makes preserving security and privacy a top priority. When it comes to app security, they make apps as safe as possible to download and use.

Features of application security and management:

1 **Apps run in a sandbox:** Each app runs in its unique space and can't interact with other applications. Before allowing apps to read/write to/from others' shared data, explicit approval is required from an authenticated user.

2 **Centralized and secure app procurement:** Apps in Apple's App Store are vetted to alleviate security risks. Part of this is achieved by notarization while the other part provides a secure, cloud-based repository managed by Apple to host apps that have passed rigorous security assessments. It also provides a means for developers to place the latest version of their hosted apps directly in the hands of users, eliminating the possibility of introducing risk from downloading illegitimate software from risky sources.

3 **Notarization signs off on security integrity:** Notarizing apps gives users more confidence that software signed by a developer's unique ID — and downloaded to your Mac — has been checked by Apple for malicious components and code-signing issues. When an app is notarized, you can trust it hasn't been tampered with or compromised.

4 **Gatekeeper blocks suspicious apps from running:** Before any macOS application is permitted to run the first time (and following each subsequent update), notarization tickets assigned are checked against Gatekeeper to determine if the ticket is valid or revoked. Suppose the former, the app is allowed to run without issue. In that case, if the latter, the app is restricted from running, informing the user that it may have been modified by an unauthorized party, impacting the integrity of its internal security.

5 **Restrictions on app usage:** On iOS-based devices, the only secure way to get apps is via the App Store. That said, jailbreaking iOS and iPadOS devices introduces the ability to access third-party app stores that are often used to distribute apps that have been "cracked", or had their internal security removed, such as paid apps that are made available for free but often have been injected with malicious code by threat actors to steal data or spy on users. With an MDM, like Jamf Pro, administrators can set up alerts to notify them when jailbroken devices are identified, allowing them to perform remediation workflows to correct the security issue.

On macOS, users (or administrators with an MDM) may select from two Gatekeeper options:

- Mac App Store
- Mac App Store and identified developers

Confining macOS users to the Mac App Store for their apps allows adminstrators to control app security device-wide while minimizing the risk of introducing threats — malicious or otherwise — from suspicious, risky and/or compromised apps. However, if requiring third-party apps that are only available from the developer's website, the second option permits obtaining apps from both the App Store and identified developers that are vetted by Apple and create software packages signed with their respective developer ID for greater security.

Best practices

For macOS, configure allowing the Mac App Store and identified developers selection, especially if you create your own applications or repackage apps for deployment. Also, apply for a developer ID from Apple and sign internally-developed applications by the organization so Gatekeeper will trust them. Lastly, by using Jamf Pro as your MDM solution, the Self Service app catalog can be deployed to all devices, whereby IT pre-approves apps, settings, configurations and much more to end users, allowing them to access and install the tools and services they need, when they need them, without requiring a help desk ticket, modification of permissions or an Apple ID.

Setting up Gatekeeper options manually:

- Navigate to: System Settings > Privacy & Security > Security
- Select from the two options available
- Repeat for every device in your organization

Setting up Gatekeeper options with Jamf Pro:

- Set up and deploy a configuration profile with your Gatekeeper settings to all your devices.
- **That's it!**

Application and security patches and updates

OS updates, version control with MDM commands, rapid security response and more

Organizations must implement a patch management strategy to test for and incorporate bug fixes as quickly as possible to keep their hardware, data and users protected. Testing is an often overlooked necessity when deploying patches, especially when bugs present themselves in the form of security vulnerabilities that need to be addressed as quickly as possible. By performing both as soon as possible, IT reduces the impact of security threats spreading while introducing greater issues — stemming from patches that fix one thing but inadvertently break other, more critical functions — to a minimum.

Throughout this e-book, the trend of how long administrative tasks performed by IT will take to complete is directly correlated to the number of devices managed. When managing patches, this rule continues to be the case except for one variable: the number of patches required to deploy could range from few to many, exponentially increasing the administrative tasks by an unknown quantity per device.

Let's review some of the options available to administrators managing patches manually and via MDM:

Options for managing patches manually:

- Educate users to perform updates themselves as soon as they receive update notifications on their devices.
- Collect all devices when a new patch is released a new patch and manually deploy.
- Remediate devices missing patches as part of your ongoing compliance monitoring processes.

Options for managing patches via MDM (i.e. Jamf Pro):

- Updates and patch notifications are automatically received by Jamf, along with tools for deploying patches to all of your organization's devices, so you can update on your timetable — not someone else's.
- Jamf's Self Service app catalog makes it easy to empower users to update anytime a new patch is available by notifying users that they need to update before continuing to use an affected app.
- Eliminate the reliance on end users while alleviating the burden on IT by automating patch distribution. Send out patches as policies to all devices, or target them with dynamic Smart Groups to ensure that devices are up to date.

To learn more about the app lifecycle and automating and deploying apps, check out our white paper.

Leveling up your security

If you haven't guessed by now, security is not a "one-size-fits-all" solution. There are layers to a comprehensive strategy that will holistically protect your devices, users and data while also providing granular protections that weave together to form a digital safety net. This is referred to as defense-in-depth, meaning that if one layer does not catch a threat, the next one above or below it is there to contain it.

You're likely already familiar with the layered security approach and may not even know it. Let's use something you're very familiar with as an example: your home.

With the blend of legacy and new security protections available for home safety, you've no doubt got some (or maybe all) protecting your loved ones and yourself at home:

- Deadbolt locks on your doors
- Home alarm system
- Video camera surveillance
- Security guards that patrol the grounds
- Smoke and carbon monoxide detectors
- Fire extinguisher
- Homeowner's or renter's insurance

Each of the solutions above can theoretically work as a standalone solution to provide home security. But on its own, it only provides one piece of the overall security necessary, right? However, when you combine them, the multiple pieces fit together like a puzzle to illustrate the full picture and comprehensively target the full range of issues. Cybersecurity and the management and security of your Apple device fleet are based on similar principles, forming the crux of empowering and informing users to have and follow good security practices to minimize risk and mitigate threats.

One such layer of endpoint security is being alerted to risks to devices. For example, some users may be able to detect a phishing attack and therefore not click on a malicious link yet; some users may be a little too trusting and carry out the instructions of the malicious link, thereby potentially introducing risk to the device, user and data. How would this affected user even know they clicked on a malicious link or performed an action that has compromised their device or credentials?

There's an app for that! Jamf Trust protects against user-initiated risks, like the above phishing attack example, by notifying users in the form of Apple Push Notifications when Jamf detects a threat on their device — like if that malicious link that was clicked on previously delivered malicious code in the form of malware currently recording keystrokes on the device.

The solution has determined a threat exists and has informed the user (and the administrator, as well). Helping the user to be mindful of the danger and to look out for those like it in the future while IT can respond to the incident and remediate it quickly, utilizing a combination of Jamf Pro and Jamf Protect to quarantine the device from the network, clean out the infection, patch any vulnerabilities present and restore the device to its baseline. Lastly, use the lessons learned to inform future security awareness training for stakeholders.

Device and data security is no laughing matter.

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

When it comes to cybersecurity, no one likes surprises and certainly doesn't want to find themselves scrambling in response to an attack if they can help it. Get the best security options for your organization by taking Jamf product solutions for a free trial run, or start by contacting a Jamf representative today to discuss what a customized, comprehensive Apple management and security solution looks like for your organization's unique needs.

You've tried the rest...now go with the best!

Try Jamf

Or contact your preferred reseller of Apple devices for a free trial.

jamf