Security Considerations for Apple in the Enterprise

This white paper addresses common security discussions and explains what organizations need to know about the macOS and iOS platforms, so that internal teams are well educated about security best practices before bringing Apple devices into their environment.

Topics covered include:

- Apple's approach to device management
- What security features are unique to Apple
- What to consider when adding new Apple devices
- What Apple integrations are available to leverage what you already have

How the Apple ecosystem is structured

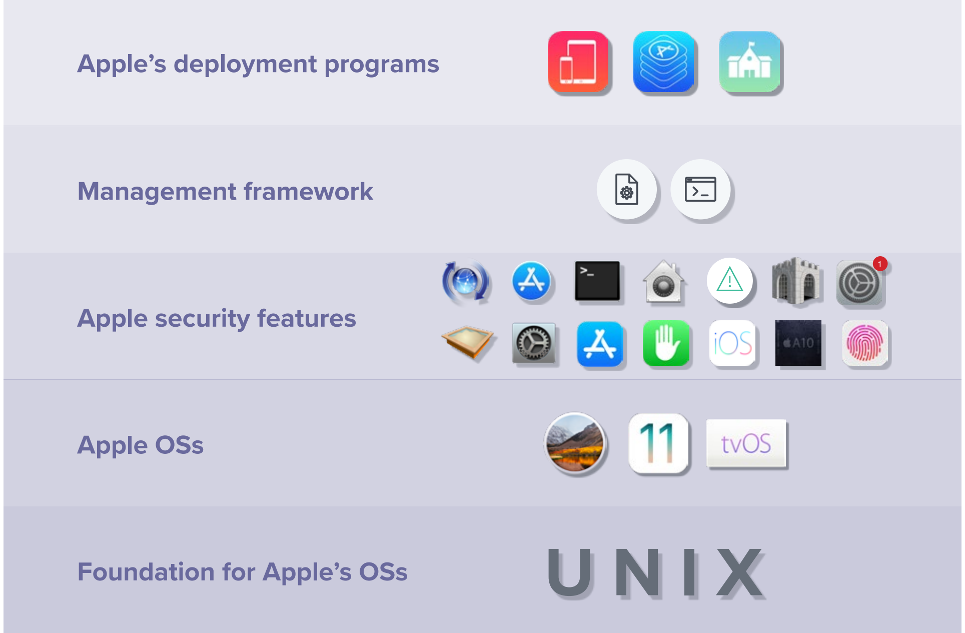
How should we approach Apple device management?
Apple designed the iOS and macOS platforms with an integrated approach to hardware, software and services that provide security by design and make it simple for IT teams to configure, deploy and manage. Just as employees expect a consistent experience when using iPhone, iPad and Mac at work, IT should expect a similar experience when managing both platforms for employees.

Apple has specific enterprise programs to help streamline deployment and security to create an out-of-box experience for users. Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP), combined with mobile device management (MDM), result in consistent and protected management of Mac, iPad, iPhone and Apple TV devices.

Many organizations look to one tool to address the needs of all of their Apple, Microsoft and Google devices. This leaves organizations with gaps in management, user experience and security. When a single management tool is used to manage multiple platforms, security features are not properly utilized and the benefit of Apple's integrated approach is lost.

The Apple Framework

To articulate Apple's approach to security, one must first understand the basics of the Apple framework.



Apple's deployment programs

Management framework

Apple security features

Apple OSs

Foundation for Apple's OSs

How Apple management differs from Microsoft

How does Apple differ from traditional Microsoft endpoint management?
The key to Apple's ease of use is its built-in management framework known as mobile device management (MDM). MDM allows IT to build configuration profiles that manage various settings inside of an OS. These profiles are delivered over the air via Apple Push Notification Service (APNs). APNs keeps a constant connection to Apple devices so IT doesn't have to. MDM enables management capabilities that traditional Windows admins may only believe they can get through binding or Group Policy Object (GPO).

Does APNs influence our security posture?
APNs is a secure and highly efficient service for propagating information to iOS and watchOS, tvOS and macOS devices. APNs is a critical layer for Apple deployment programs and other security features, such as Remote Lock and Remote Wipe. In fact, Apple's programs such as DEP, VPP or MDM will not work without APNs in place, because these programs cannot be leveraged through a proxy connection. They must be accessed through a direct channel with Apple, i.e., APNs.

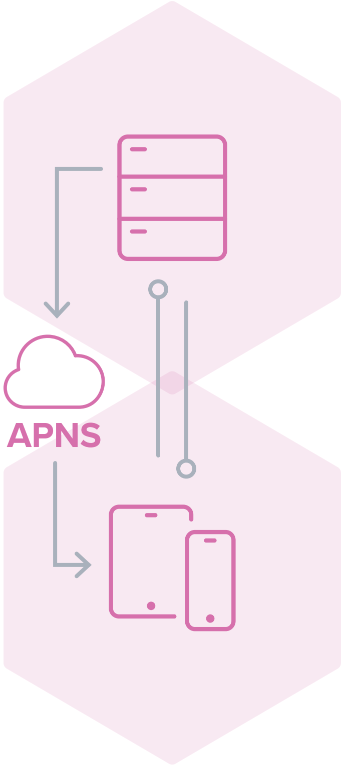
Additional benefits of APNs include:

- Enhanced security posture for managing corporate-owned Apple assets. APNs allows you to remotely lock/wipe a lost/stolen/compromised device over the air.
- MDM is dependent on APNs for sending critical commands such as software installations or inventory updates.
- While MDM configuration profile payloads can be delivered to macOS "offline," this method requires significantly more overhead than managing over the air.
- APNs trigger each device to automatically check-in with the MDM server.

The unique technology that appears to be a security challenge delivers many benefits.
Many Google and Microsoft services are beginning to require the same level of trust and direct connection as APNs. Cisco's VOIP solutions for iOS rely on APNs for push messages and Callkit. APNs is critical to security and user experience. Services like App Store, iCloud Authentication and Internet Recovery won't fully function (or not all) without APNs. If you open your ports to Apple's specifications, everything will fall into place.

For more information, see Apple's website: https://help.apple.com/deployment/macos/#/ior9d28751c0.

Apple Push Notification Server Architecture



Does Apple require third-party security software?
Unlike Windows or Android, an additional layer of security or bolt-on third-party tools is less commonly used for Apple devices.

Traditional Windows-focused security companies tend to lag behind Apple's development cycles, potentially slowing the adoption of new operating systems and security features. In fact, treating Apple as you would another platform often prohibits employees from being their most productive and disrupts the user-friendly experience Apple is known for. Plus, adopting a Windows software version on an Apple device is a recipe for poor code execution, memory hogs and kernel extension (KEXT)-based panics — all equating to endless IT and security headaches.

Apple's built-in encryption and anti-virus enable many organizations to operate without third parties, but some still look for solutions for managing corporate data leakage. However, corporate data leakage can be monitored through MDM, with additional protections on the network side leveraging tools such as Cisco Security Connector.

In February 2018, Cisco, Apple, Aon and Allianz introduced a first-of-its-kind cyber risk management solution for businesses, comprised of cyber resilience evaluation services from Aon, the most secure technology from Cisco and Apple, and options for enhanced cyber insurance coverage from Allianz. For more on this partnership, read the full announcement on [Apple's website](#).

66%

of organizations say Mac is easier to secure than PC.

90%

of organizations say iOS is easier to secure than other platforms.

What is the experience like when managing Apple devices?
Traditionally, the IT mindset has been "we don't have the same quality of tools to manage Apple like we do our Windows devices." This perception, compounded by the misconception that Apple is more challenging to manage than other platforms, has left many organizations shying away from offering and supporting Apple.

Surveys have shown that Apple is in fact easier to manage than other platforms. A [Dimensional Research survey](#) cited that 66 percent of respondents say Mac is easier to secure than PC, while 90 percent say iOS is easier to secure than other platforms. Similar findings were reported when asked if Apple devices were easier to deploy, configure and support.

Industry giant IBM is just one of the many organizations that have decided to offer an employee-choice program with the Apple platform. In fact, the now CIO of IBM, Fletcher Previn, has proven that [IBM makes and saves money with every Mac](#) chosen over a PC.

This demonstrates that the enterprise craves a consistent deployment and user experience. Apple brings this consistency and security right out of the box.

What security features are unique to the Apple ecosystem

What security features are built into macOS?
The foundation of macOS is formed by integrated and secure software.

Built-in macOS system security features include:

- **FileVault** is a layer of encryption built into macOS to protect user data if a device is lost or stolen.
- **Software updates** come directly from and are digitally signed by Apple so organizations and IT know they can be trusted.
- **System Integrity Protection (SIP)** protects core operating system files that could otherwise be targets for exploits from user and application access.
- **Gatekeeper** lets IT define where users can download their applications from. It works to prevent unsigned apps (or malware) from running and therefore works together with XProtect to swiftly halt the spread of malware.
- **XProtect** is an automated anti-malware utility, kept up to date by Apple. This prevents malicious software and/or often outdated, vulnerable plug-ins like Java and Flash from running on a Mac.
- **Malware Removal Tool**. Apple can remove malware that does manage to get on the system.
- **App Store** apps available in the App Store are always vetted by Apple and only Apple-approved resources are available. Apple has the ability to remove app availability and revoke developer certificates instantly.
- **App Sandboxing** ensures that apps do not share (or steal) data from the system or one another.
- **Privacy controls** are available for users and IT to define – a transparent process, which lets users know when location services are used, which apps have access to contacts or calendars, and what information is being shared with Apple and/or app developers.

For a complete list of Mac security features, please visit: https://www.apple.com/macos/security/.

Why should we leverage FileVault for disk encryption?
FileVault is built-in disk encryption for macOS, meaning IT does not have to add any additional software in order to encrypt a drive. This can be enabled manually or IT can remotely enable it across all Mac computers. Encryption keys can be centrally managed so IT can access necessary data after an employee leaves the organization or if they simply forgot their password and need assistance logging in. Encryption keys can also be rotated easily for increased security.

What security features are built into iOS?
Many of the same core security capabilities of Mac are available for iPad and iPhone, providing a consistent and secure experience across the Apple ecosystem:

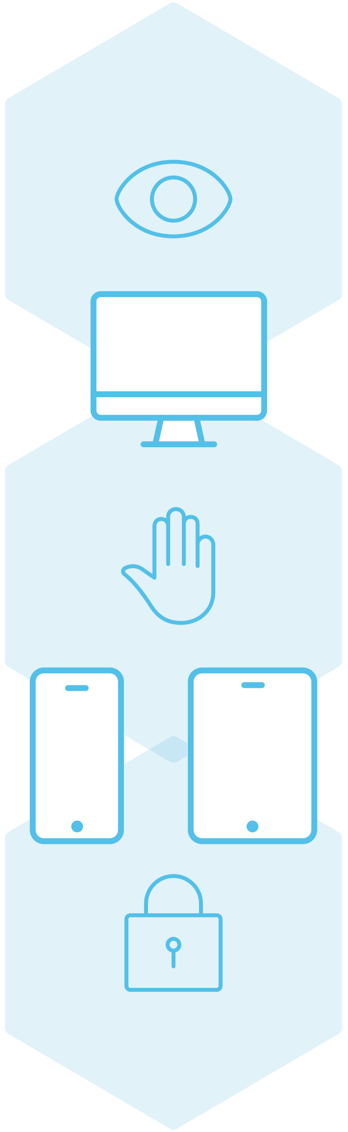
- System security includes technologies such as Secure Boot, Software Authorization, Secure Enclave and more to ensure the OS has not been compromised. IT also has the power to erase the entire iOS operating system and start over.
- Touch ID / Face ID leverages fingerprint sensing and facial recognition to streamline the login process and ensure only authorized users can access the device.
- Encryption and data protection ensure personal and corporate data can’t be compromised even if other aspects of the device have been wiped due to theft or loss.
- Supervision is an additional set of features that can be leveraged by IT to gain added management capabilities in more controlled environments.

For a complete list of iOS security features, please visit: https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

What to consider when adding new Apple devices

How do we demonstrate security of our Apple devices?
The basis of Apple device management is the ability to create configuration profiles. By building configuration profiles with a mobile device management solution like Jamf Pro, IT can enforce passcodes, restrict settings, define network protocols, configure VPN settings and mail accounts, and much more. IT can then deploy any of these settings to their managed devices.

Why don’t we need to use app containers?
Apple-focused management tools, like Jamf Pro, are used to deploy approved apps to devices and keep unapproved apps from getting on devices. iOS already supports the ability to manage corporate apps using native app management with solutions like Jamf Pro. This method of management separates corporate data from personal data and manages data flow without using container apps that tend to slow down performance or break with each release of the OS.



What security controls exist for Mac outside the MDM framework?
For macOS, solutions like Jamf Pro go beyond basic device management with the Jamf Agent. The Jamf Agent is a binary that gets installed after a Mac is enrolled into management. This allows IT to create a hidden admin account that grants remote root access to all Mac computers under management.

With Jamf Agent installed, IT can run more advanced policies and scripts, install software that is outside of the App Store like Adobe, and much more. It expands customization and extends management capabilities beyond what MDM is capable of.

How can we validate, enforce and report the compliance of Apple devices in our environment?
For highly regulated industries, audits can be constant and tedious, so being able to prove that devices are indeed under management and secure is important to demonstrating compliance.

Collecting inventory is key to achieving regulatory and enterprise security requirements. Knowing how many devices are in the organization's environment, who has what device, the status of software updates, what profiles and settings have been assigned to each device, current encryption status, and what restrictions and configurations are applied are key to any healthy and secure environment.

Solutions like Jamf Pro allow IT to run reports on virtually endless amounts of inventory categories to help organizations make better business decisions and demonstrate compliance. If a device falls out of compliance, deploying configuration profiles to the appropriate device forces it back in to compliance.

If more than one device is out of compliance, or a check of the entire environment must be run, leverage Jamf Pro to create dynamic Smart Groups of devices. Smart Groups are based on advanced inventory criteria defined by IT and can trigger automated management actions based on the inventory report.

How do we handle the patching of third-party macOS software?
Software can become out of date quickly, and when that happens, the device, data and network can become vulnerable to internal and external threats. These vulnerabilities can be addressed quickly and efficiently leveraging patch management.

Your MDM's patch management functionality should allow IT to receive patch alerts when updated third-party software versions become available, create software packages with the appropriate patch (updated software version), distribute the patch to the appropriate devices, then receive a patch report via inventory management to make sure the patch was installed correctly.

By knowing immediately what apps and software are out of date, then quickly taking action to ensure the most current and secure version is installed, organizations are taking a proactive approach to security workflows.

Why shouldn't we bind our Apple devices to Active Directory?
When it comes to deployment, Mac differs from a traditional 1-to-1 deployment. With tools like Jamf Pro, Enterprise Connect and NoMAD, binding is a thing of the past. Not only does binding impact DEP workflows if an organization does not have their Domain Controllers exposed externally, but organizations leveraging binding also lose out on the ability to drop-ship new devices to remote users. While binding is an option, organizations using a solution like Jamf Pro can manage local accounts to apply the same password complexity and expiration requirements without worrying about connections or getting out of sync with AD. This means less password prompts for your end users and less calls to the IT help desk.

How do cloud services work with Apple devices?
The shift to the cloud is growing. With cloud-hosting, access to the database is limited rather than sitting on a server in your network. For decades, organizations built "walls" around their company and leveraged network perimeters as the first line of defense. As workspaces become increasingly mobile and data no longer simply lives behind the firewall, organizations must move to a more modern, identity-based model of security.

Microsoft is moving enterprise data to the cloud with Azure Active Directory. To ensure that only trusted users on trusted devices using trusted apps are accessing this corporate data in the cloud, Microsoft and Jamf offer an exclusive integration to achieve proxy-free conditional access.

Read more here: https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/.

The mobile workplace transition and growing reliance on the cloud is more than a passing fad.

85%

of organizations keep sensitive information in the cloud.

80%

of employees use non-approved SaaS apps for work.

41%

percent of employees say mobile business apps change how they work.

How do we enforce industry security standards?
As most InfoSec teams know, enforcement depends on what the security standards are and which compliance standards must be met. SOC 2 is different from HIPAA and PCI is different than CIS. Knowing what to adhere to is an important first step.

Jamf Pro provides a flexible framework to help you comply with many common regulatory standards. IT can simply define the applicable standards, build the corresponding profiles and policies, and apply. These could include restricting consumer features such as iCloud Drive, enforcing Gatekeeper to ensure only secure apps are being downloaded, enforcing FileVault to encrypt Mac, or restricting apps by searching for a restricted app (or even macOS) across all your managed Apple devices and once located, delete the app. IT simply needs to define what the settings are and use that information to build out configuration profiles and policies, and apply them to devices.

Check out this white paper to learn how to adhere to the Center for Internet Security (CIS) guidelines: https://www.jamf.com/resources/white-papers/macos-security-checklist/.

Why should we use Apple deployment programs?

Apple's deployment programs for the enterprise, DEP and VPP, are free and exclusive to Apple. Not only do these programs allow for a higher level of device security, they give IT the ability to automate and personalize device setup at scale.

- DEP is Apple's method for getting institutionally owned Apple devices into a secure and managed state. DEP allows for zero- touch deployment, meaning the traditional process of imaging or the need for manual IT configuration and setup is removed. Users are able to enroll themselves quickly and seamlessly into the environment, minimizing onboarding time and securing the endpoint within just a few clicks. Devices ordered directly from Apple or an Apple Authorized Reseller are eligible for DEP and are automatically enrolled into management during the initial setup.
- For macOS, iOS and tvOS devices, DEP enables additional management controls, granting a deeper level of management.
- When combined with mobile device management, or MDM (Apple's built-in management framework), the end state is delivered via a dynamic method to users based on their needs as opposed to baking a one-size-fits-all image.
- VPP lets IT license apps from the App Store and distribute the software to either individuals or devices. If distributed directly to the device, no Apple IDs are required. Apple IDs identify a user and allow them to access Apple services such iCloud, iTunes and App Store.
- IT can manage purchased VPP apps and reclaim them for redistribution if an employee leaves the company or no longer requires a particular app.

> **"Not every Apple device management solution supports Apple's programs and services. Check with your vendor to ensure they support these programs, as well as the incremental changes."**

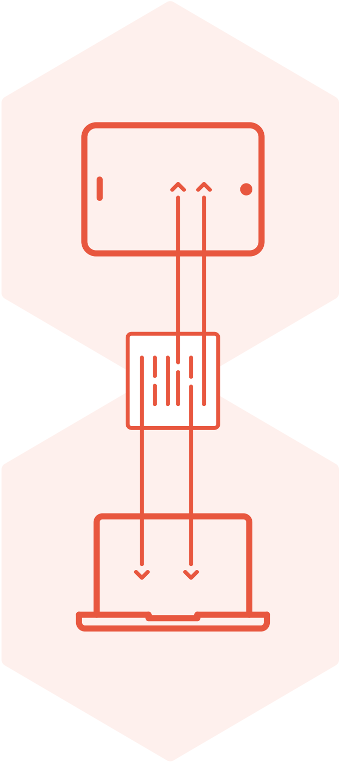
What Apple integrations are available to leverage what you already have

How does Apple (and Jamf) integrate with our existing IT technology stack?
Organizations, IT and employees don't live in a bubble. Apple has demonstrated their commitment to the enterprise by partnering with technology companies such as Cisco to deliver modern and secure business services.

Many companies require services outside of the Apple ecosystem. With secure and compatible integrations, organizations can leverage all aspects of their environment and welcome an array of services to drive the business forward.

Examples include:

- Jamf's Application Programming Interface (API) which provides the flexibility to build integrations with existing IT tools.
- Microsoft EMS integration with Jamf to offer an exclusive proxy-free integration for conditional access on the Mac.
- Cisco ISE to create and enforce security and access policies for devices connected to a company's network.
- Cisco Fast Lane to save on network bandwidth by prioritizing apps and automatically configuring quality of service.
- ServiceNow to automate IT and business processes for operations management.



As modern organizations move to enterprise tools like Cisco, adding Jamf for Mac management offers a fully integrated solution without skimping on any supported platform.

Plus, in its recently released Security Data Report, identity management company, Okta Inc., released several findings focused on the growing popularity of cybersecurity applications in the enterprise. Security tools like Jamf all ranked in the top 15 fastest-growing apps for the first time this year.

Apple + Jamf for unmatched device management and security
The most secure platform requires the most robust management solution to ensure all possible security features are enforced and installed. No other mobile device management company integrates with Apple and its services better than Jamf, and no provider is more suited to ensure Apple success.

That's why security-minded organizations, such as 10 of the top 10 U.S. banks and nine of the top 10 technology companies, trust Jamf to manage their Apple environment.

With day-zero support for all Apple operating systems and features, Jamf is the product trusted by businesses looking to embrace and empower its employees with Apple.

Jamf provides the necessary tools to secure 100 or 100,000 Apple devices, while giving organizations the freedom to focus on the strategic tasks that save time, improve user experience and enable the business to succeed.

Ninety-six percent of Jamf customers renew their contracts year after year.
To learn more about how Jamf Pro can make an impact on your Apple device management, visit jamf.com/products/Jamf-Pro.

jamf

www.jamf.com

To learn more about how Jamf Pro can make an impact on your Mac and iOS management, visit **jamf.com/products/Jamf-Pro**.