The Advanced Guide to iOS/iPadOS Management

The security landscape

Cybersecurity continues to improve.
According to PwC's recently-released 2023 Global Digital Trust Insights report, cybersecurity has improved in many ways since 2020: over 70% of 3,522 C-Suite leaders from a wide range of industries and global locations initiated improvements in cybersecurity in 2021.

We still have a long way to go.
38% of respondents believed they had completely mitigated risks related to enabling remote and hybrid work, for instance, while 48% believed they had moderately mitigated those risks. 35% reported complete mitigation of issues around swiftly accelerated cloud adoption.

However, **only three percent report that they have fully mitigated emerging cyber risks**. Only five percent reported that they were optimizing in all five aspects of the security workflow of identify, protect, detect, respond and recover.

And the concerns only increase with mobile tech, as malware hidden in what appear to be harmless apps has made headlines. Traditional firewall-based security and management systems simply don't handle mobile devices well, as the nature of mobile devices includes the ability to access work tools from remote locations. And when you add in the recent BYOD surge across organizations, there is a lot to worry about.

So how can InfoSec and IT administrators ensure that all security protocols are in place across all areas of the digital environment, including and especially iOS and iPadOS?

Only

3%

report that they have fully mitigated emerging cyber risks

Proper iOS management is secure iOS management

This 201 guide to iOS and iPadOS management, a follow-up to our iPhone and iPad Management for Beginners e-book, discusses how managing iOS and iPadOS devices is the key to securing your Apple fleet. Proper management isn't the entire picture of the security landscape, but it's the foundation that all organizations must build from.

Read on for more detail on how proper management is security. We'll also cover the key capabilities, workflows and settings needed to securely manage your iOS and iPadOS fleet and cover all the bases.

PKI and push certificates

PKI certificates

A PKI certificate is a text file that contains identification data on users and devices. Basically, it confirms the security of the mobile device and secures information going from one place to another with encryption.

Encryption with certificates not only secures all communication; it also allows for immediate revocation of access from people leaving the company or devices falling out of compliance.

Certifications can be used for Single Sign-On (SSO), enrollment profiles, device management with the Jamf Binary, configuration profiles and more. Admins can deploy them manually through a web portal, through automation with a third party such as Jamf Connect, or through a direct certificate request: an automated process where the device communicates with the server via Jamf Pro.

Read more about this in our Jamf Pro technical documentation.

With Jamf Pro, you can download the built-in certificate authority (CA) certificate; revoke and renew, create a built-in certificate from a certificate signing request (CSR) and create a backup.

Push certificates

A push certificate is an encrypted file generated by Apple that establishes trust between a third-party service like Jamf Pro and Apple Push Notification Service (APNs). A push certificate is created by Apple, but needs a third-party service, like Jamf, and APNs. They use an organization-owned Apple ID rather than a personal Apple ID.

Push certificates allow for the Jamf Pro server and APNs to communicate. APNs control info, specifically info from apps, sent to and from devices. Push notifications are how apps on devices receive communication.

As the file is an encrypted file generated by Apple, you can remotely uninstall an app based on this security information.

How to find certificates

On iOS, certificates are stored in the publisher keychain. You can view a list of certificates by exporting to .csv, .txt., or XML files. Jamf Pro makes this process easier by walking an IT admin through the process to create a push certificate (.pem) and to upload it to Jamf Pro. You'll need a valid Jamf ID and Apple ID, and it's critical that admins keep these certificates up-to-date. If they lapse, APNs will lose connection to mobile device management (MDM) server/endpoints.

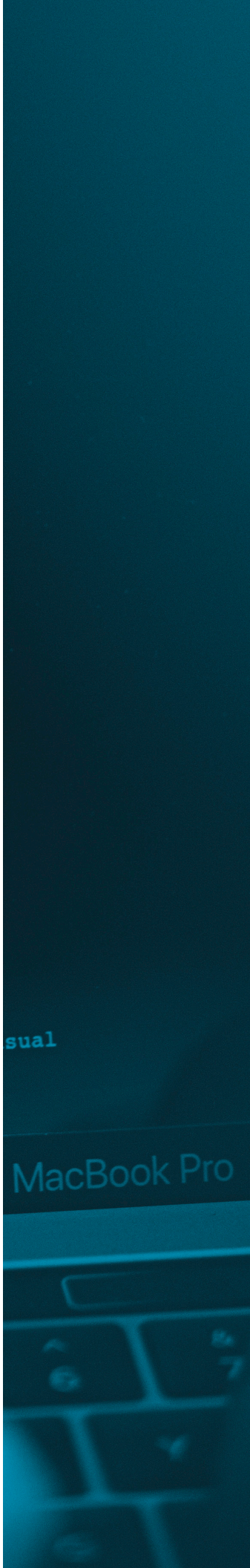
Conditional Access

As mentioned above, most organizations can no longer create a network and protect devices and users via a firewall— especially mobile devices that employees often use from home, on-the-go and on flights.

Conditional Access allows an organization to set parameters for securing an organization's data in multiple locations. It can gate access to organizational data such as email, OneDrive, Word and Excel— and Cloud Apps like Jamf Pro by evaluating the risk at that time.

Requiring a trusted device and a trusted user for access improves management and security, no matter where someone is working.

Organizational iPhones and iPads are managed by Jamf and registered with your identity provider through a cloud connector or manual connector. Jamf and Microsoft's strong partnership ensures that this works seamlessly: Jamf sends iOS and iPadOS device inventory to Intune. Intune evaluates compliance and generates a compliance report. Azure AD enforces access controls.



Device compliance

Device compliance has a lot of moving parts, but none more than mobile devices. First, these devices can be purchased through variety of ways, like directly from Apple, through authorized resellers, or personal devices that are enrolled in a BYO program. Second, the nature of who uses organizational iPads and iPhones for day-to-day work often means that these organizations have an additional level of compliance regulation. Because of this, devices within your organization will require different steps comply with your organization's requirements.

Healthcare organizations, often heavy users of iPhone and iPads in clinical settings, must follow HIPAA. Higher education institutions must adhere to FERPA and K-12 schools have rigorous federally-mandated safety compliance requirements.

A thorough and well-crafted device compliance management program is absolutely essential for cybersecurity, data security, and user security. And an industry leader in mobile device management to help enforce these policies is a must. To learn about creating a comprehensive compliance policy that keeps your devices, users and organizational data secure, please read Compliance Management for Beginners.

Configuration profiles and encryption: working together

Configuration profiles

One important way to secure an admin's control is by implementing configuration profiles. Common use cases for configuration profiles are enforcing passcode requirements, configuring saved Wi-Fi networks and more.

Configuration profiles are XML files with the .mobileconfig extension that provide an easy way to define settings and restrictions for devices and users. They typically use Apple Push Notification service (APNs.)

Configuration profiles can enforce and enhance security in their own right by enforcing security protocols in passcodes, behavior and more.

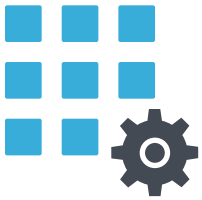
Configuration profiles are built using Apple Configurator 2, Profile Manager or your MDM provider— and can be deployed to devices and users with enrolled in the MDM.

Admins can also configure apps based on granular information and security protocols.

Encryption

Apple uses a technology called Data Protection for encryption. Certain system apps (such as Messages, Mail, Calendar, Contacts, Photos) and Health data values use Data Protection by default. Third-party apps receive this protection automatically.

App management



As apps continue to be the most dominant part of the end user experience, application management is a vital element in managing and securing devices. From sourcing and hosting to updating and deploying, proper app management is critical in securing an Apple fleet while also supporting end-user productivity.

Managed app config

App Config allows organizations with MDM solutions to remotely deliver data to a managed device, which can be used by the app to customize the user experience or app behavior.

Building a single app that can be deployed and customized to meet the needs of all your consumers reduces the longterm cost and maintenance of app development.

Apps that support App Config will continue to function as originally designed for general consumer use cases, while in enterprise deployments they can be extended to support more customized workflows or environments. And with App Config, UI customizations are made possible, providing IT administrators an easy UI to configure an app to meet their needs. Also provides access to user and device information

Apps and Books

Apps and Books is a way to mass distribute or revoke iOS apps or books to end users through Apple Business Manager or Apple School Manager (organizations must use Apple Business Manager or Apple School Manager to use Apps and Books.)

Distributing App Store apps through the managed and easy workflow allows IT admins to assign apps to users in bulk and based on criteria set within your MDM.

iOS apps must meet Apple's app standards to be available through the App Store, which means they are inherently more secure than other third-party apps outside of the App Store.

As part of your security posture, it is key to:

Purchase and license apps and books in bulk from Apple

Distribute them to individuals via Apple ID or directly to devices without an Apple ID

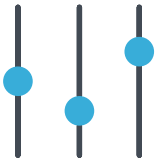
You can link a token (received from Apple) to your MDM solution for assignment and distribution, which allows you to scope and target the correct users.

With device-assigned managed distribution, managed IDs allow for the distribution of content to managed devices without requiring use of Apple IDs. Recommended for user enrolled devices, device-assigned managed distribution restricts apps from appearing within a user's personal App store account, keeping control of the app's updating and management with the organization.

For user-assigned managed distribution, content is distributed to the managed device, but the content license is assigned directly to the user using a Managed or personal Apple ID. This requires registering users with volume purchasing and assigning content licenses to users before you distribute content. This way, you can:

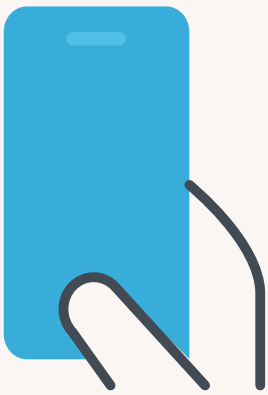
Schedule automatic app updates

Automatically force apps to update



Manually force apps to update

Distribute an app update (individual apps only)

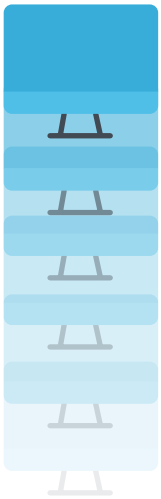


What about BYOD?

Combining profile- or account-driven user enrollment with Jamf mobile device management means that you can secure and manage any employee-owned device. With identity-based access, admins can manage and protect devices based on who is using them.

To learn more about creating a safe and well-managed BYOD program, please read Jamf and Apple: BYOD Programs Done Better.

Mass actions



Another way to perform multiple tedious tasks on many devices simultaneously is mass actions. With Jamf Pro, admins can create mass actions on any Smart Group or static group, device search results or lists of license usage matches. Mass actions can be anything. A few examples: remote commands, editing a side panel or emailing users.

This keeps environments more secure; whether managing five or 5,000 devices, mass actions ensures there is virtually no chance a device will be missed that might cause a security breach.

Jamf security solutions for iOS and iPadOS

While it's clear that diligent management of iPadOS and iOS devices is vital to proper security, it's important to remember that device management is the foundation for security. Using security-specific tools on top of that firm foundation is the last piece in the security puzzle. For a basic overview, please read Mobile Threat Defense for Beginners.

Mobile threat defense and protection

Jamf security solutions for threat defense and endpoint protection go beyond simple antivirus for malware. With Jamf, complete mobile threat defense solution uses advanced machine learning and threat intelligence engine MI:RIAM to identify and prevent novel threats, includes in-network protection, collects real-time insights and enables strong user privacy protections.

You'll also discover the importance of other systems of security, including identity and access management, threat prevention and remediation, content filtering, and Zero Trust Network Access (ZTNA) for keeping users, devices and organizational data secure.

How Jamf can help

Jamf Pro and Jamf School

For a strong and secure foundation, try Jamf Pro — the standard in Apple device management — or Jamf School, (MDM) for schools and districts. You can learn more and request a trial directly from us, or contact your preferred reseller to get started.

Security beyond device management

Read our report on the state of Apple security in the enterprise, which surveyed 1,500 IT and InfoSec professionals. It includes current device usage and approaches, challenges to device security and the future state of endpoint security.

Trusted Access

Trusted Access is Jamf's solution to security beyond management. Trusted Access is a unique workflow that brings together device management, authorized users and endpoint security to help organizations create a work experience that users love and a secure workplace that organizations trust.

Ensuring that only trusted users on enrolled, safe devices can access company data, Trusted Access with Jamf dramatically increases the security of your modern workplace while streamlining work for your users — regardless of where work happens.

Learn more about Jamf's state-of-the-art, Mac-first security offerings to see how we can help you continue to manage and protect your Mac fleet!

At Jamf.com/solutions, discover more about:

- **Identity and access management**
- **Content filtering and safe internet**
- **Device management**
- **Zero Trust Network Access (ZTNA)**
- **Endpoint protection**
- **Security visibility and compliance**
- **Threat prevention and remediation**

> And if you're ready to dive in to managing and security for your Macs with Jamf, **request a free trial today!**

Source:
1. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html