jamf

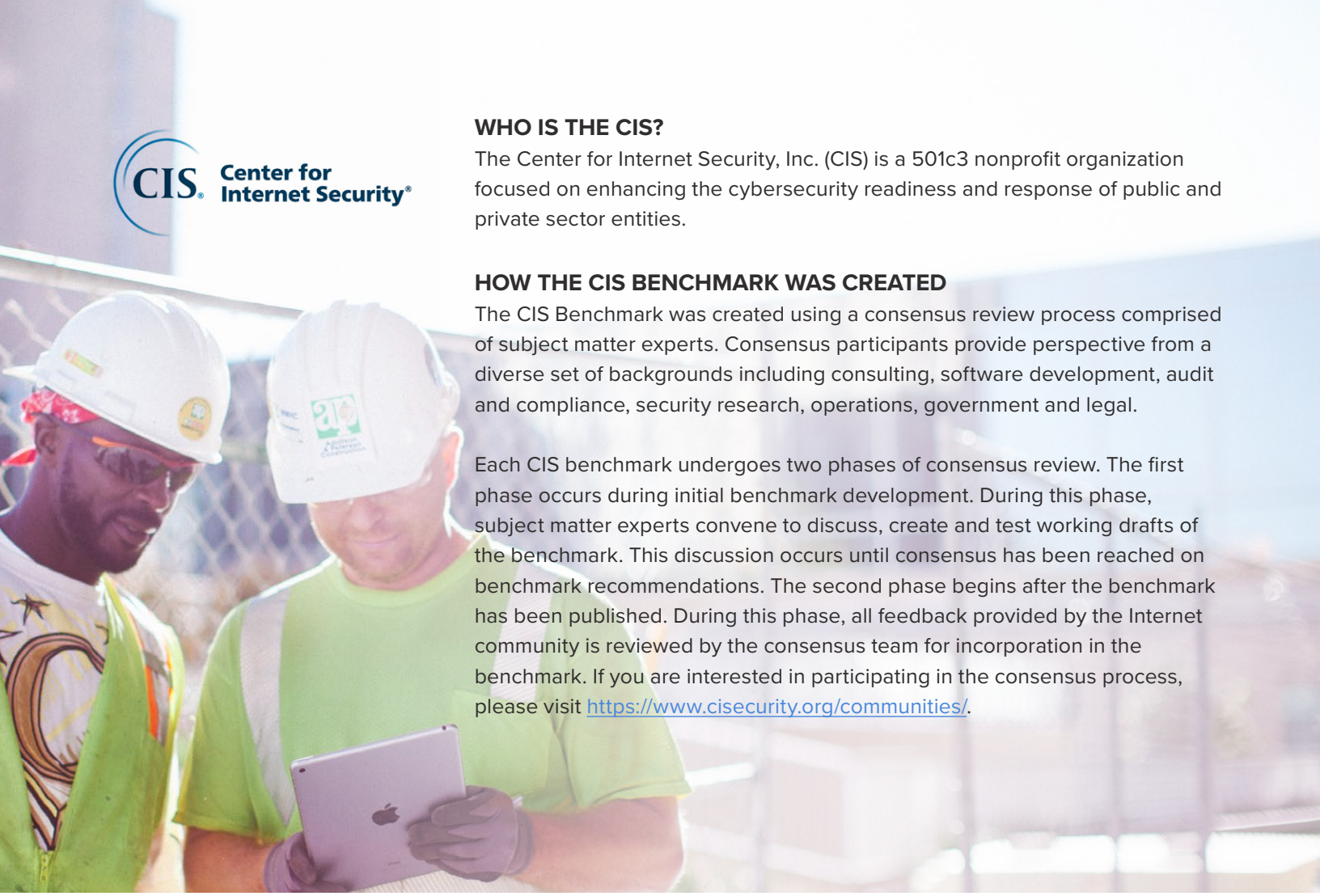
WHITE PAPER

iOS Security Checklist

Implementing the Center for Internet Security Benchmark for iOS

Recommendations for securing iOS.

The Center for Internet Security (CIS) benchmark for iOS is widely regarded as a comprehensive checklist for organizations to follow to secure iPad and iPhone devices. This white paper explains how to implement the independent organization's recommendations.



WHO IS THE CIS?

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities.

HOW THE CIS BENCHMARK WAS CREATED

The CIS Benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://www.cisecurity.org/communities/.

CIS and iOS Management Basics

WHAT IS MDM?

Mobile device management (MDM) is Apple's built-in management framework for iOS, macOS and tvOS. Jamf Pro is the standard solution for Apple MDM.

DEVICE OWNERSHIP

Security requirements are different based on the organization's technology model: personally-owned via a bring your own device (BYOD) initiative or institutionally-owned and distributed to users.

WHAT ARE CONFIGURATION PROFILES?

Configuration profiles define settings on iOS devices and are distributed to devices via MDM.

SECURITY LEVEL

Level 1 (L1) or Level 2 (L2) defines the security requirements and settings that must be applied to a personally or institutionally-owned device. L2 puts the device under greater control and goes beyond basic security requirements.

WHAT IS SUPERVISION?

Supervision provides a deeper level of iOS management once devices are enrolled into management via Apple's deployment programs or Apple Configurator.

WHAT IS APNs?

Apple Push Notification service (APNs) is required for iOS management. Please review the following article to learn more about APNs: https://www.jamf.com/blog/what-is-apple-push-notification-service-apns/requirements.

Securing Institutionally-Owned Devices

A recent survey found that 74 percent of enterprise employees would prefer a company-issued device over a personally-owned device.* Jamf Pro helps organizations securely implement their institutionally-owned iOS device program, and empowers them to streamline distribution and management of institutionally-owned iPad and iPhone devices.

CIS Recommendations

Setup:

- Set a consent message and description for the enrollment profile.
- Ensure the profile can't be removed.

Functionality:

- **L2:** Disable screenshots and screen recording.
- Disable voice dialing while device is locked.
- Disable Siri while device is locked.
- Disable iCloud backup.
- Disable iCloud documents and data.
- Disable iCloud Keychain.
- Disable managed apps to store data in iCloud.
- Enable force encryption backups.
- Disable erase all content and settings.
- **L2:** Disable allow users to accept untrusted TLS certificates.
- Disable allow installing configuration profiles.
- Disable allow adding VPN configurations.
- Disable allow modifying cellular data app settings.
- **L2:** Disable allow pairing with non-Configurator hosts.
- Disable allow documents from managed sources in unmanaged destinations.
- Disable allow documents from unmanaged sources in managed destinations.
- Enable treat AirDrop as unmanaged destination.
- Disable allow Handoff.
- Enable force Apple Watch wrist detection.
- Disable allow setting up a new nearby device.
- Disable show Control Center in Lock screen.
- Disable show Notification Center in Lock screen.

Apps:

- Enable force fraud warning.
- Accept cookies is set to "From websites I visit" or "From current website only".

Domains:
- Configure managed Safari web domains.

Passcodes:
- Disable allow simple value.
- Minimum passcode length is set to “6” or greater.
- Maximum Auto-Lock is set to “2 minutes” or less.
- Maximum grace period for device lock is set to “Immediately”.
- Maximum number of failed attempts is set to “6”.

VPN:
- Ensure VPN is “Configured”.
- Per-app VPN is preferred.

Mail:
- Set up a user’s email account with an Email profile.
- Disable allow user to move message from this account.

Notifications:
- Configure notification settings for all managed apps.

Lock Screen Message:
- Configure “If Lost, Return to...” message.

Features in Jamf Pro

Jamf Pro allows you to set, enable and/or disable all L1 and L2 system preferences above via configuration profiles. A few of these settings require the iOS device be supervised during enrollment. Please review the following for more information on iOS supervision: https://support.apple.com/en-us/HT202837.

Jamf Pro also empowers organizations to set a personalized Lock Screen message to ensure devices are safely returned and not unlocked and tampered with.

*Source: https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/

Securing BYOD and Personally-Owned Devices

Jamf Pro helps organizations securely remove the burden of multiple devices for their employees, and empowers them to utilize one device for both work and home.

CIS Recommendations

Setup:

- Set a consent message and description for the enrollment profile.
- Ensure the profile can be removed.

Functionality:

- Disable voice dialing while device is locked.
- Disable Siri while device is locked.
- Disable managed apps to store data in iCloud.
- Enable force encryption backups.
- L2: Disable users to accept untrusted TLS certificates.
- Disable documents managed from sources in unmanaged destinations.
- Disable documents from unmanaged sources in managed destinations.
- Enable treat AirDrop as unmanaged destination.
- L2: Disable allow Handoff.
- Disable show Control Center in Lock screen.
- Disable show Notification Center in Lock screen.

Apps:

- Enable force fraud warning in Safari.
- Accept cookies is set to “From websites I visit” or “From current website only”.

Domains:

- Configure managed Safari web domains.

Passcodes:

- Disable allow simple value.
- Minimum passcode length is set to “6” or greater.
- Maximum Auto-Lock is set to “2 minutes” or less.
- Maximum grace period for device lock is set to “Immediately”.
- Maximum number of failed attempts is set to “6”.

VPN:

- Ensure VPN is “Configured”.
- Per-app VPN is preferred.

Mail:

- Set up a user’s email account with an Email profile.
- Disable allow user to move message from this account.

Notifications:

- Ensure VPN is “Configured”.
- Per-app VPN is preferred.

Features in Jamf Pro

Jamf Pro’s BYOD solution allows you to create a custom consent message and description for the enrollment profile, as well as a simple process for former employees to remove the BYOD profile if they leave the organization or the program.

If your organization needs to implement all L1 and/or L2 security settings recommended by CIS, please utilize Jamf Pro’s ability to enroll the iOS device as an unsupervised but institutional device. It would also be our recommendation to disable the user-initiated enrollment setting for iOS enrollment of “personally-owned devices”. By creating and distributing configuration profiles within Jamf Pro, all L1 and L2 security settings can be configured, disabled and/or enabled for single or groups of iOS devices.

Additional Considerations

Jamf Pro helps organizations go beyond device management and configuration profiles by ensuring devices are always running the latest software and not leaving the door open to malicious attacks.

CIS Recommendations:

- Ensure the iOS device is not obviously jailbroken.
- Keep software up to date.
- Enable automatic downloads of app updates.
- On end-user devices only, enable Find My iPad and/or Find My iPhone.
- Ensure the latest iOS device architecture is used by high-value targets.

Features in Jamf Pro

Jamf Pro offers zero-day support for iPad and iPhone operating systems, ensuring the newest software is always supported. Additionally, Jamf Pro Self Service allows organizations to build their own custom app catalog with all of the resources, apps and configurations users may need. On-demand access is granted for users, all without them ever submitting a help ticket to IT. If a device is lost or stolen, Jamf Pro can safely lock, wipe and reset the device, ensuring corporate and personal data are never exposed.

Better Device Security Starts Here

Jamf Pro makes it easy to implement and follow the independent organization Center for Internet Security's Apple iOS benchmarks.

Put this guide to practice in your environment by requesting a free trial.

jamf

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