WHITE PAPER

macOS Security Checklist:

Implementing the Center for Internet Security Benchmark for macOS

Recommendations for securing macOS

The Center for Internet Security (CIS) Benchmark for macOS is widely regarded as a comprehensive checklist for organizations to follow to secure their Macs. This white paper from Jamf — the Standard for Apple Enterprise Management — will show you how to implement the independent organization's recommendations.

jamf | PRO

WHAT IS JAMF PRO?

Jamf Pro is a set of administrative tools to help you manage your Apple devices.

jamf | PROTECT

WHAT IS JAMF PROTECT?

Jamf Protect is an endpoint security solution designed specifically for Apple and organizations' Macs.

jamf | CONNECT

WHAT IS JAMF CONNECT?

Jamf Connect provides a single cloud identity on any Apple device to gain immediate access to the resources you need.

CIS. Center for Internet Security®

WHO IS THE CENTER FOR INTERNET SECURITY?

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) 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 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://community.cisecurity.org**.

JAMF PROTECT AND CIS

Jamf Protect was recently issued CIS Benchmark certification by CIS. Organizations that leverage Jamf Protect can now ensure that the configurations of their critical assets align with the CIS Benchmark consensus-based practice standards for macOS.

CIS provides recommendations within different macOS categories where setting controls should be implemented to lessen the possibility of data exfiltration.

While Jamf Pro gives you the ability and tools to follow CIS recommendations, Jamf Protect automates the assessment of the essential CIS security settings on a daily bases to validate compliance and auditing oversight across the Benchmark for macOS and your organization's security priorities.

Categories of macOS Security

UPDATES & PATCHES

SYSTEM PREFERENCES

iCLOUD

LOGGING & AUDITING

NETWORK CONFIGURATION

USER ACCOUNTS

ACCESS & AUTHENTICATION

OTHER CONSIDERATIONS

Installing Updates, Patches, and Security Software

Jamf Pro enables you to keep your macOS and applications up to date by packaging and deploying updates to your client Macs remotely. You can even build a report to monitor the status of macOS upgrades in real time to ensure your Mac fleet is running the latest, most secure OS available.

CIS Benchmark Recommendations:

- Verify all Apple-provided software is current
- Enable Auto Update
- Enable app update installs
- Enable system data files and security update installs
- Enable macOS update installs

Features in Jamf Pro:

- Patch Management helps you keep your macOS and popular app titles current with the latest versions available.
- A custom Software Update Server lets you whitelist approved updates to your Macs
- Run a policy to enable Auto-Update via App Store
- Run a policy to check for updates on a client Mac

Features in Jamf Connect:

- Requires a cloud username and password
- Guest accounts are hidden
- No password hints for local accounts

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for updates, patches and security software

System Preferences

Jamf Pro helps you configure System Preferences to meet your organization's security needs. Common and advanced settings can be set across your Mac fleet to harden your security against both physical and remote attacks.

CIS Benchmark Recommendations:

Bluetooth:

- Disable Bluetooth
- Disable Bluetooth Discoverable Mode

Date & Time:

- Enable set time and date automatically
- Ensure time set is within appropriate limits

Desktop & Screen Saver:

- Set an inactivity interval of 20 minutes or less for the screen saver
- Secure screen saver corners
- Familiarize users with screen lock tools or corner to Start Screen Saver

Sharing:

- Disable Remote Apple Events in Sharing
- Disable Internet Sharing
- Disable Screen Sharing
- Disable Printer Sharing
- Disable Remote Login (SSH)
- Disable DVD or CD Sharing
- Disable Bluetooth Sharing
- Disable File Sharing
- Disable Remote Management (ARD)

Energy Saver:

- Disable wake for network access

Security & Privacy:

- Enable FileVault
- Ensure all user storage APFS volumes are encrypted
- Ensure all user storage CoreStorage volumes are encrypted
- Enable Gatekeeper
- Enable Firewall
- Enable Firewall Stealth Mode
- Review Application Firewall Rules
- Enable Location Services
- Monitor Location Services Access
- Disable sending diagnostic and usage data to Apple

Other:

- iCloud (see section below)
- Time Machine Auto-Backup
- Time Machine Volumes Are Encrypted
- Pair the remote control infrared receiver if enabled
- Enable Secure Keyboard Entry in terminal.app
- Java 6 is not the default Java runtime
- Securely delete files as needed
- Ensure EFI version is valid and being regularly checked

Features in Jamf Pro:

- All of the above System Preferences can be set via a Jamf Pro Server policy and/or configuration profile
- FileVault 2 can be enabled and keys escrowed in your Jamf Pro Server's inventory
- Screen Saver and Password Settings can be set
- Sharing Settings can be set
- Security & Privacy settings can be set
- Policy to disable Java can be deployed

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for system preferences

iCloud and Other Cloud Services

Jamf Pro helps implement your organization's iCloud strategy by giving IT admins the ability to either block or enable the cloud-based service.

CIS Benchmark Recommendations

"Apple's iCloud is a consumer oriented service that allows a user to store data as well as find, control and backup devices that are associated with their Apple ID (Apple account.) The use of iCloud on Enterprise devices should align with the acceptable use policy for devices that are managed as well as confidentiality requirements for data handled by the user. If iCloud is allowed the data that is copied to Apple servers will likely be duplicated on both personal as well as Enterprise devices. "

iCloud:

- iCloud configuration
- iCloud keychain
- iCloud Drive
- iCloud Drive Document sync
- iCloud Drive Desktop sync

Features in Jamf Pro:

- iCloud can be disabled using a configuration profile
- If iCloud is not allowed, iCloud Drive can be removed from Finder

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for iCloud and other cloud services

Logging and Auditing

Jamf Pro can help IT admins keep track of the logs that macOS generates and centralizes them in one place. Admins can also run advanced reports on those logs to look for any potential security issues.

CIS Recommendations:

- Enable security auditing
- Configure Security Auditing Flags
- Ensure security auditing retention
- Control access to audit records
- Retain install.log for 365 or more days
- Ensure Firewall is configured to log

Features in Jamf Pro:

- Configuration profiles can be modified via a script
- Log files can be sent to the Jamf Pro Server and stored as long as needed
- Additional logs can be cached by the Jamf Pro Server

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for logging and auditing

Network Configurations

Jamf Pro makes rolling out network configurations easy for IT admins by distributing Wi-Fi, VPN, and even DNS settings. Jamf Pro also ensures some of the legacy server components of macOS are disabled so users are not accidentally opening up ports they don't know about.

CIS Recommendations:

- Disable Bonjour advertising service
- Enable "Show Wi-Fi status in menu bar"
- Create network specific locations
- Ensure http server is not running
- Ensure nfs server is not running

Features in Jamf Pro:

- Network settings can be built into a configuration profile
- Apache, FTP, and NFS can all be disabled via Jamf Pro Server Policy

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for network configurations

User Accounts and Environment

Jamf Pro helps an organization manage local accounts on a Mac — allowing the creation of admin or standard users. The Jamf binary that lives on client machines creates a hidden management account that has admin rights to execute commands and create new users. Policies can be created to further secure the login screen and disable the guest account.

CIS Benchmark Recommendations:

- Display login window as name and password
- Disable "Show password hints"
- Disable guest account login
- Disable "Allow guests to connect to shared folders"
- Remove Guest home folder
- Turn on filename extensions
- Disable the automatic run of safe files in Safari
- Safari disable Internet Plugins for global use
- Use parental controls for systems that are not centrally managed

Features in Jamf Pro:

- Login window can be configured via Configuration Profile
- Guest account can be disabled via Jamf Pro Server Policy
- User accounts can be created via Setup Assistant and Apple Business Manager enrollment
- Accounts created can either be Standard or Admin, based on needs

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for user accounts and environment

System Access, Authentication and Authorization

Jamf Pro helps set file permissions, strong password policies and manage keychain access for users. By creating a configuration profile or Jamf Pro Server policy, you can remotely enable system access settings to create a more secure Mac.

CIS Recommendations:

File System Permissions and Access Controls:

- Secure Home Folders
- Check System Wide Applications for appropriate permissions
- Check System folder for world writable files
- Check Library folder for world writable files

Password Management:

- Configure account lockout threshold
- Set a minimum password length
- Complex passwords must contain an Alphabetic Character
- Complex passwords must contain a Numeric Character
- Complex passwords must contain a Special Character
- Complex passwords must uppercase and lowercase letters
- Password Age
- Password History
- Reduce the sudo timeout period
- Use a separate timestamp for each user/tty combo
- Automatically lock the login keychain for inactivity
- Ensure login keychain is locked when the computer sleeps
- Enable OCSP and CRL certificate checking
- Do not enable the “root” account
- Disable automatic login
- Require a password to wake the computer from sleep or screen saver
- Ensure system is set to hibernate
- Require an administrator password to access system-wide preferences
- Disable ability to login to another user’s active and locked session
- Create a Login window banner
- Do not enter a password-related hint
- Disable Fast User Switching
- Secure individual keychains and items
- Create specialized keychains for different purposes
- System Integrity Protection status

Features in Jamf Pro:

- Repair permissions command can be triggered via Self Service or run automatically
- Reports can be created to scan for files in System and Library for bad permissions
- Password policies enabled via Configuration Profile
- Login window and banner can be added via Jamf Pro Server Policy
- Folder permissions can be set via a script in a Jamf Pro Server policy

Features in Jamf Connect:

- A custom message can be created for login screen enforcing complex passwords as cloud identity policies dictate

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for system access, authentication and authorization

Additional Considerations

Jamf Pro helps IT admins customize additional security settings by setting an EFI password, disabling Wi-Fi in hyper-secure environments, and more. You can also use the Jamf Pro Server to rename your Macs, so inventory is easier. Additionally, Jamf Pro allows you to inventory the software assets your organization has and keep track of licenses.

CIS Benchmark Recommendations:

- Wireless technology on macOS
- iSight Camera Privacy and Confidentiality Concerns
- Computer Name Considerations
- Software Inventory Considerations
- Firewall Consideration
- Automatic Actions for Optical Media
- App Store Automatically download apps purchased on other Macs Considerations
- Extensible Firmware Interface (EFI) password
- FileVault and Local Account Password Reset using AppleID
- Repairing permissions is no longer needed
- App Store Password Settings
- Siri on macOS
- Apple Watch features with macOS
- System information backup to remote computers
- Unified logging
- AirDrop security considerations

Features in Jamf Pro:

- Wi-Fi can be disabled via configuration profile
- Computer naming can be automated in the Jamf Pro Server
- Software inventory and license tracking in the Jamf Pro Server
- EFI passwords can be set via a policy

Features in Jamf Protect:

- Assesses all settings highlighted here to validate compliance for additional considerations

Conclusion

Jamf makes it easy to implement and follow the Center for Internet Security's Benchmark for macOS.

jamf

www.jamf.com

Put these security best practices to the test with a free trial of Jamf. **Get Started.**