jamf

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 Apple Management Experts—will show you how to implement the independent organizations' recommendations.

What Is Jamf Pro?

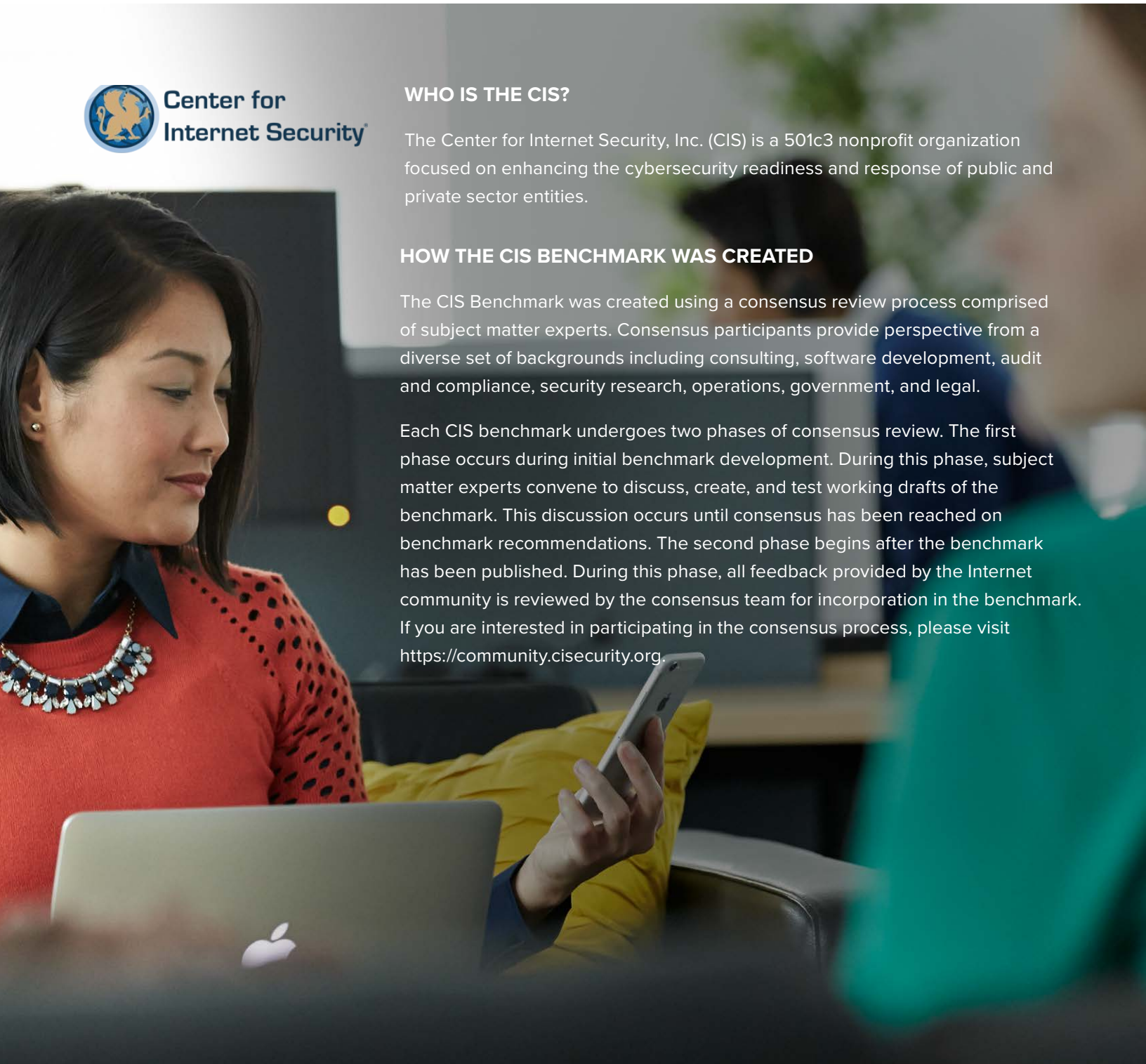
Jamf Pro is a set of administrative tools to help you manage your Apple devices.

What is Jamf Pro Server?

Jamf Pro Server is the management server component to the suite and runs on a Mac, Windows, or Linux server.

What is a Policy?

A Policy is the main tool used to implement changes to a client Mac. Jamf Pro Server sends commands to an agent on the Mac.



Center for Internet Security®

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://community.cisecurity.org.

Categories Of Security For macOS

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 OS and Applications up to date by packaging and deploying updates to your client Macs remotely. You can even report on which machines have been updated and which are still pending.

CIS Recommendations:

- Verify OS and apps are up to date via a Software Update tool
- Enable Auto Update in App Store
- Enable Auto Security Updates

Features in Jamf Pro:

- Patch Management in Jamf Pro allows you to keep macOS up to date
- 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

System Preferences

Jamf Pro helps you configure System Preferences to meet your organization's security needs. Common settings such as passwords and screen saver can easily be turned on remotely and en masse to ensure restricted physical access to Macs. Advanced settings such as disabling SSH or file sharing can also be set to make your Mac secure against remote attacks.

CIS Recommendations:

Bluetooth:
- Disable Bluetooth
- Disable Bluetooth Discoverable Mode

Date & Time:
- Enable set time and date automatically
- Desktop & Screen Saver:
- Set screen saver to 20 minutes or less
- Enable hot corner to start screen saver
- Set Display Sleep to a value larger than
- 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
- Disable sleeping the computer when connected to power

Security & Privacy:
- Enable FileValut 2
- Enable Gatekeeper
- Enable Firewall
- Enable Firewall Stealth Mode
- Review Application Firewall rules (http://support.apple.com/en-us/HT201642)

Other:
- iCloud (see section below)
- Enable Secure Keyboard entry in terminal.app
- Java 6 is not the default Java runtime
- Use Secure Empty Trash

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 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

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 Recommendations:

"Apple's iCloud is just one of many cloud based solutions being used for data synchronization across multiple platforms and it should be controlled consistently with other cloud services in your environment. Work with your employees and configure the access to best enable data protection for you mission."

Features in Jamf Pro:

- iCloud can be disabled via a Configuration Profile and/or Jamf Pro Server Policy
- If iCloud is not allowed, iCloud Drive can be removed from Finder

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:

- Configure asl.conf
- Retain system.log for 90 or more days
- Retain appfirewall.log for 90 or more days
- Retail auth.log for 90 or more days
- Enable security auditing
- Configure Security Auditing Flags
- Enable remote logging for Macs on trusted networks
- Retain install.log for 1yr or more

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 chached by the Jamf Pro Server

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:

- Ensure Wi-Fi status is in the menu bar
- Create network specific locations
- Ensure http server is not running (Apache)
- Ensure ftp 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

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 Recommendations:

- Display login window as name and password only
- Disable show password hints
- Disable guest account
- Disable allow guests to connect to shared folders
- Turn on filename extensions
- Disable the automatic run of safe files in Safari for different purposes

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 DEP or imaging
- Accounts created can either be Standard or Admin, based on needs

System Access, Authentication, and Authorization

Jamf Pro helps set file permissions, manage keychain access, and set strong password polices 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:

- Secure Home Folder (deny read permissions to other home folders)
- Repair permissions regularly
- Check system-wide applications for permissions
- Check System folder for world writable files
- Check Library folder for world writable files
- Reduce the sudo timeout period
- Automatically lock the login keychain for inactivity
- Ensure login keychain is locked when the computer sleeps
- Ensure OCSP & CRL certificate checking
- Do not enable the “root” account
- Disable automatic login
- Require a password to wake the computer from sleep
- Require an admin password to access systemwide preferences
- Disable ability to login to another user’s active and locked session
- Complex passwords (contains numbers, letters, and symbols)
- Set minimum password length
- Configure account lockout threshold
- Create a custom message for the Login Screen
- Create a login window banner
- Disable password hints
- Disable Fast User Switching
- Secure individual keychain items
- Create specialized keychains for different purposes

Features in Jamf Pro:

- Folder permissions can be set via a script in a Jamf Pro Server Policy
- 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

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 Recommendations:

- Consider disabling Wi-Fi and only use ethernet
- Cover iSight cameras
- Logically name your computers
- Inventory your software
- Put a firewall in place
- Automatic actions for optical media
- Disable App Store automatic downloads on other Macs
- Set an EFI password
- Apple ID password resets

Features in Jamf Pro:

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

Conclusion

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