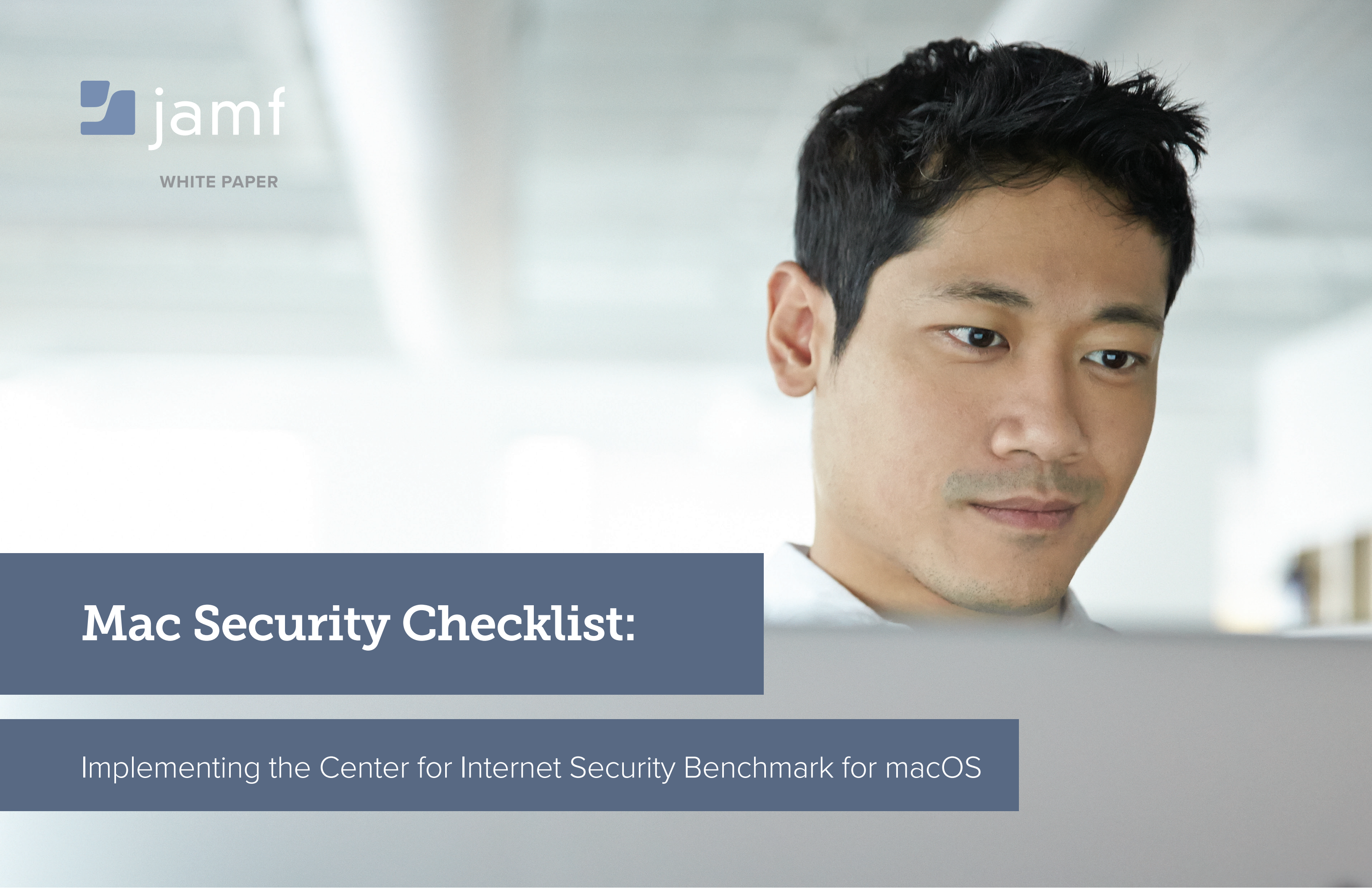
WHITE PAPER



Mac 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 Mac. This white paper from Jamf—the Apple Management Experts—will show you how to implement the independent organizations' recommendations.

To see how Jamf Now can facilitate personalized learning in your environment, visit: **www.jamf.com**

WHAT IS JAMF NOW?

Jamf Now is a cloud-based MDM solution for the iPad, iPhone and Mac devices in your workplace.

WHAT IS JAMF CLOUD?

Jamf Now is entirely cloud-based which means your account lives on the Jamf Cloud to host and scale with the number of devices your organization needs.

WHAT IS A BLUEPRINT?

Blueprints are how device configurations are deployed from your Jamf Now account to specific devices. Updating changes to the Blueprint will send 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

SOFTWARE & SECURITY UPDATES

SYSTEM PREFERENCES

iCLOUD

NETWORK CONFIGURATION

ACCESS & AUTHENTICATION

OTHER CONSIDERATIONS

Installing Software & Security Updates

Jamf Now enables you to keep your OS and Applications up to date from a central location without having to physically have the Mac in hand. You can even report on which machines have been updated and which are still pending, as well as, delay updates to verify that all your team's needed tools function smoothly with the newest operating system.

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 Now:

- Jamf Now allows you to manage OS Updates, including new Security features that come with new operating systems.
    - View what operating system devices are currently running on and decide which devices need to be updated.
    - Delay OS Update is feature that allows you to hold off on updating a device to confirm compatibility with the new operating system.
- Updating apps is a simple as checking a box to "Automatically Update Apps"
    - If you dont want to update automatically, view the apps in a specific Blueprint and select to update the app on every device with that Blueprint deployed.

System Preferences

Jamf Now 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 Mac computers.

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 FileVault 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 Now:

- With 75+ restrictions on Jamf Now and options around FileVault and iCloud, you can customize your devices to be secure through Blueprints and/or Custom Profiles
- FileVault 2 can be enabled and keys escrowed in Jamf Now's device details page
- Password Settings can be set
- Sharing Settings can be set
- Security & Privacy settings can be set
- Restrictions surrounding Java can be set in a Blueprint for deployment

iCloud and Other Cloud Services

Jamf Now 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 Now:

- iCloud can be disabled via Blueprint Restrictions and deployed to specific devices
- If you wish to allow iCloud but want certain aspects like iCloud Keychain or iCloud Email to be disabled this can be done in Blueprints as well

Network Configurations

Jamf Now makes rolling out network configurations easy for you by distributing Wi-Fi, VPN and allowing for website whitelisting/blacklisting. Make employee onboarding simple for your scaling company by ensuring every device has easy access to the basics.

CIS Recommendations:

- Ensure Wi-Fi status is in the menu bar
- Create network specific locations

Features in Jamf Now:

- Network settings can be built into a Blueprint
- Networks can be managed to control which networks can be joined and which cannot. Similar to whitelisting/blacklisting
- The Jamf Now Plus plan offers many more Network Configuration options via Custom Profiles including VPN deployment

System Access, Authentication, and Authorization

Jamf Now helps set file permissions, manage keychain access, and set strong password requirements for users. By creating a Blueprint, you can quickly, easily and remotely enable system access settings to create a more secure Mac.

CIS Recommendations:

- Repair permissions regularly
- Check applications for permissions
- Reduce the Auto-Lock timeout period
- Disable automatic login
- Require a password to wake the computer from sleep
- 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

Features in Jamf Now:

- Keep devices secure by mandating complex and rotating passwords
- Review application permissions
- Password demands and constraints can be set via Blueprints
- Login window and banner can be added via a Custom Profile on the Jamf Now Plus plan

Additional Considerations

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

CIS Recommendations:

- Disable camera
- Logically name your computers
- Inventory your software
- Put a firewall in place
- Disable App Store automatic downloads on other Macs
- Apple ID password resetss

Features in Jamf Now:

- Wi-Fi can be disabled via Blueprints
- Device naming allows you to help with inventory management that matches your organization's breakdown and needs
- Track inventory, licensing, updates and Blueprint details on the Device details page

Conclusion

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

jamf

www.jamf.com

To learn more about how Jamf Now can make an impact on your macOS management, visit **jamfnow.com**.