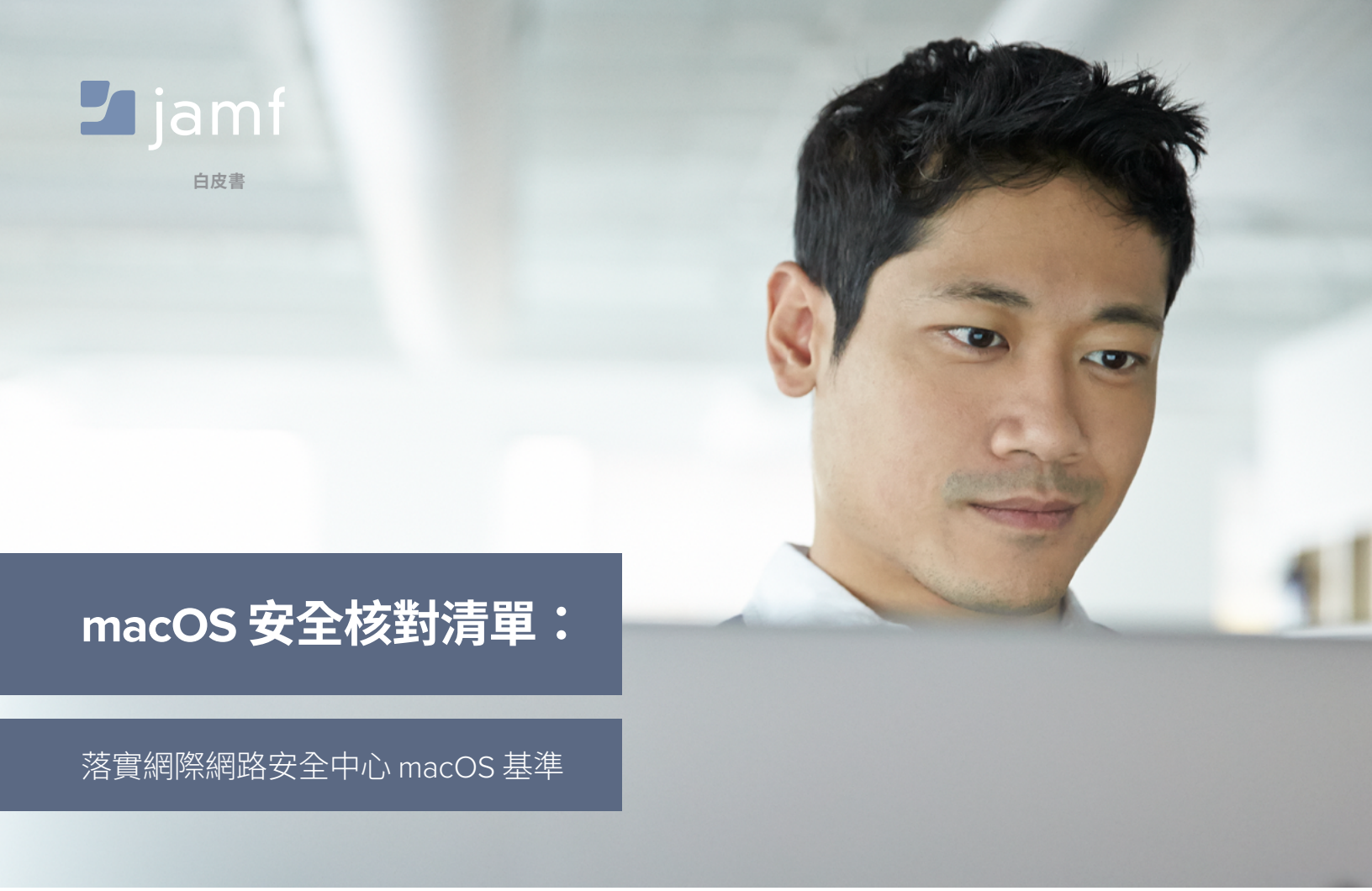
jamf

白皮書



macOS 安全核對清單：

落實網際網路安全中心 macOS 基準

保護 macOS 的建議

網際網路安全中心 （CIS） macOS 基準被廣泛認為是企業組織保護其 Mac 的綜合清單。Jamf 的這份白皮書（也是 Apple 企業管理標準）將向您說明如何落實獨立組織的相關建議。

jamf PRO

什麼是 JAMF PRO？

Jamf Pro 是一套管理工具，可協助您管理 Apple 裝置。

jamf PROTECT

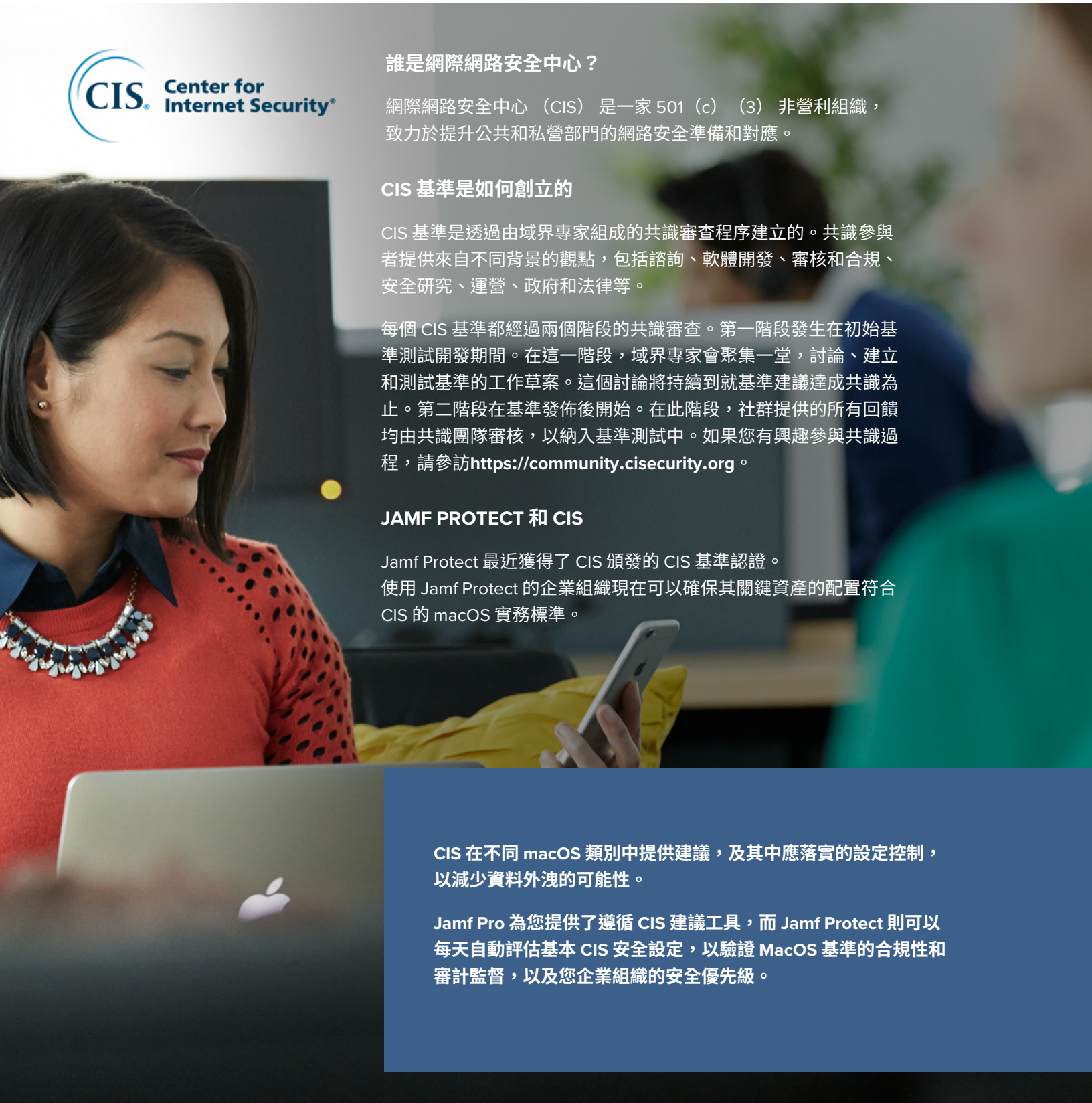
什麼是 JAMF PROTECT？

Jamf Protect 是專為 Apple 和企業組織的 Mac 所設計的端點安全解決方案。

jamf CONNECT

什麼是 JAMF CONNECT？

Jamf Connect 可在任何 Apple 裝置上提供單一雲端身份，以便立即存取您所需的資源。



CIS Center for Internet Security®

誰是網際網路安全中心？

網際網路安全中心 （CIS） 是一家 501（c） （3） 非營利組織，致力於提升公共和私營部門的網路安全準備和對應。

CIS 基準是如何創立的

CIS 基準是透過由域界專家組成的共識審查程序建立的。共識參與者提供來自不同背景的觀點，包括諮詢、軟體開發、審核和合規、安全研究、運營、政府和法律等。

每個 CIS 基準都經過兩個階段的共識審查。第一階段發生在初始基準測試開發期間。在這一階段，域界專家會聚集一堂，討論、建立和測試基準的工作草案。這個討論將持續到就基準建議達成共識為止。第二階段在基準發佈後開始。在此階段，社群提供的所有回饋均由共識團隊審核，以納入基準測試中。如果您有興趣參與共識過程，請參訪**https://community.cisecurity.org**。

JAMF PROTECT 和 CIS

Jamf Protect 最近獲得了 CIS 頒發的 CIS 基準認證。
使用 Jamf Protect 的企業組織現在可以確保其關鍵資產的配置符合 CIS 的 macOS 實務標準。

CIS 在不同 macOS 類別中提供建議，及其中應落實的設定控制，以減少資料外洩的可能性。

Jamf Pro 為您提供了遵循 CIS 建議工具，而 Jamf Protect 則可以每天自動評估基本 CIS 安全設定，以驗證 MacOS 基準的合規性和審計監督，以及您企業組織的安全優先級。

macOS 安全性的類別


更新和修補程式


系統偏好設定


iCLOUD


記錄和審核


網路配置


使用者帳戶


存取和身份驗證


其他注意事項

安裝更新、修補程式和安全軟體

Jamf Pro 可以遠端打包更新包並將其部署到用戶端 Mac，確保 macOS 和應用程式維持在最新狀態。你甚至可以建立一份報告，即時監控 macOS 的升級狀態，確保你的 Mac 機隊運作的都是最新、最安全的作業系統。

CIS 基準測試建議：

- 驗證 Apple 提供的所有軟體均為最新版本
- 啟用自動更新
- 啟用應用程式更新安裝
- 啟用系統資料檔案和安全性更新安裝
- 啟用 macOS 更新安裝

Jamf Pro 的功能：

- 修補程式管理可協助您讓 macOS 和熱門應用程式維持在最新的版本。
- 自訂軟體更新伺服器可讓您將 Mac 核准的更新列入白名單。
- 採用透過 App Store 啟用自動更新的政策
- 採用檢查用戶端 Mac 上的更新的政策

Jamf Connect 的功能：

- 需要雲端使用者名稱和密碼
- 隱藏訪客帳戶
- 不為本機帳戶提供密碼提示

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以驗證更新、修補程式和資安軟體的合規性

系統偏好設定

Jamf Pro 可協助您配置系統偏好設定，以滿足您企業組織的安全需求。 可在您的 Mac 機群中設定通用和進階設定，以增強您的安全性，抵禦實體和遠端攻擊。

CIS基準建議：

藍牙：

- 停用藍牙
- 停用藍牙可搜尋模式

日期及時間：

- 啟用自動設定時間和日期
- 確保時間設定在適當的範圍內

桌面與螢幕保護程式：

- 將螢幕保護程式的使用者閒置時間或非使用狀態設定為 20 分鐘或更短
- 保護螢幕保護程式熱點
- 讓使用者熟悉螢幕鎖定工具或熱點來啟動螢幕保護程式

共享：

- 在「共享」中停用 Apple 遠端工序指令
- 停用網路共享
- 停用螢幕畫面分享
- 停用共用印表機
- 停用遠端登入 （SSH）
- 停用 DVD 或 CD 共享
- 停用藍牙共享
- 停用文件共享
- 停用遠端管理 （ARD）

能源節約器：

- 停用網路訪問喚醒

安全性與隱私權

- 啟用檔案保險箱（FileVault）
- 確保所有使用者儲存 APFS 卷宗都已加密
- 確保所有使用者儲存 CoreStorage 卷都已加密
- 啟用門禁技術（GateKeeper）
- 啟用防火牆
- 啟用防火牆隱藏模式
- 查看應用程式防火牆規則
- 啟用定位服務
- 監控定位服務權限
- 停用向Apple 發送診斷和行為數據資料

其他：

- iCloud（見下文）
- 時光機（Time Machine）自動備份
- 時光機（Time Machine）卷宗已加密
- 如果已啟用則將配對遙控紅外線接收器
- 在 terminal.app 中啟用安全鍵盤輸入
- Java 6 非預設的運行時
- 根據需求安全地刪除檔案
- 確保 EFI 版本有效並定期 檢查

Jamf Pro 中的功能：

- 上述所有系統偏好設定都可以 通過 Jamf Pro 伺服器政策和／或設定描述檔進行設定
- 可以啟用檔案保險箱 2（FileVault 2），並將金鑰託管在 Jamf Pro 伺服器的清單中
- 可以 設定螢幕保護程式和密碼設定
- 可以設定共享設定
- 可以設定安全和隱私設定
- 可以部署停用 Java

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以驗證系統偏好的合規性

iCloud 和其他雲端服務

Jamf Pro 讓 IT 管理員可以封鎖或啟用雲端服務，從而協助落實企業組織的 iCloud 策略。

CIS 基準建議

「Apple 的 iCloud 是一個以消費者需求為導向的服務，允許使用者儲存資料以及尋找、控制和備份與其 Apple ID（Apple 帳戶）關聯的裝置。在企業裝置上使用 iCloud 時，應符合所管理之裝置的可接受使用策略（AUP），以及使用者處理之資料的機密性要求。如果允許使用 iCloud，複製到 Apple 伺服器的資料很可能會在個人和企業裝置上複製。”

iCloud：

- iCloud 配置
- iCloud 鑰匙圈
- iCloud 雲端硬碟
- iCloud 雲端硬碟文件同步
- iCloud 雲端硬碟桌面同步

Jamf Pro 中的功能：

- 可以透過設定描述檔停用 iCloud
- 如果不允許使用 iCloud，則可以從 Finder中刪除iCloud 硬碟。

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以 驗證 iCloud 和其他雲端服務的合規性

記錄和審核

Jamf Pro 可以幫助 IT 管理員追蹤 macOS 產生的紀錄檔並將其集中在一個位置。
管理員還可以對這些記錄檔執行進階報告，以查找任何潛在的安全問題。

CIS 建議：

- 啟用安全審核
- 配置安全審核標誌
- 確保安全審核保存
- 控制對審核記錄的存取
- 保留 install.log 365 天或更長時間
- 確保防火牆已配置為記錄

Jamf Pro 中的功能：

- 可透過腳本修改設定描述檔
- 記錄檔可以發送到 Jamf Pro 伺服器並根據需要存儲
- Jamf Pro 伺服器可以緩存其他記錄檔

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以 驗證記錄和審核的合規性

網路配置

Jamf Pro 透過分發 Wi-Fi、VPN 甚至 DNS 設定，讓 IT 管理員可以輕鬆部署網路配置。Jamf Pro 還能確保不會使用 macOS的一些舊伺服器元件，這樣使用者就不會不小心打開他們不知道的連接埠。

CIS 建議：

- 停用 Bonjour 廣告服務
- 啟用「在功能列表中顯示 Wi-Fi 狀態」
- 建立專用網路位置
- 確保 HTTP 伺服器非為運作中
- 確保 nfs 伺服器非為運作中

Jamf Pro 的功能：

- 網路設定可以內建在設定描述檔 中
- 可以透過 Jamf Pro 伺服器政策停用 Apache、FTP 和 NFS

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以驗證網路配置的合規性

使用者帳戶和環境

Jamf Pro 協助企業組織管理 Mac 上的本機帳戶 - 允許建立管理員或標準使用者。用戶端電腦上的 Jamf 二進位檔案會建立一個隱藏的管理帳戶，該帳戶具有執行命令和建立新使用者的權限。能夠建立政策來進一步保護登入畫面並停用訪客帳戶。

CIS 基準測試建議：

- 登入視窗顯示名稱和密碼
- 停用「顯示密碼提示」
- 停用訪客帳戶登錄
- 停用「允許訪客連接到共享 資料夾」。
- 刪除訪客主資料夾
- 開啟檔案副檔名
- 停用 Safari 中自動執行安全文件的功能
- Safari 停用全域使用的外掛程式
- 對非 集中管理的系統使用家長監護功能

Jamf Pro 中的功能：

- 可以透過設定描述檔設定登入視窗
- 可以透過 Jamf Pro 伺服器政策停用訪客帳戶
- 可以透過「設定 助理」和 Apple 商務管理註冊建立使用者帳戶
- 根據需求可以選擇建立標準 帳戶或管理員帳戶

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以 驗證使用者帳戶和環境的合規性

系統訪問、身份驗證和授權

Jamf Pro 協助設定檔案權限、強密碼原則並管理使用者的鑰匙圈存取。通過創立設定描述檔或 Jamf Pro 伺服器政策，您可以遠端啟用系統存取設定，讓 Mac更安全。

CIS 建議：

檔案系統權限和存取控制：

- 確保主資料夾的安全
- 檢查系統範圍的應用程式是否有適當的 許可權
- 檢查系統資料夾中是否有全域可寫檔
- 檢查資源庫資料夾中是否有全域可寫檔案

密碼管理：

- 配置帳戶鎖定閾值
- 設定最小密碼長度
- 複雜密碼必須包含字母
- 複雜密碼必須包含數字
- 複雜密碼必須包含特殊字元
- 複雜密碼必須為大寫和小寫字母
- 密碼期限
- 密碼歷史記錄
- 縮短 sudo 預設超時時間
- 為每個使用者/tty 組合使用單獨的時間戳記
- 登入鑰匙圈在不使用時自動鎖定
- 確保 電腦在睡眠狀態時鎖定登入鑰匙圈
- 啟用 OCSP 和 CRL 憑證檢查
- 不要啟用「root」帳戶
- 停用自動登入
- 需要密碼才能將電腦從睡眠狀態或螢幕保護程式中喚醒
- 確保系統設定為休眠狀態
- 需要管理員密碼才能存取 系統範圍的首選項
- 停用「登入其他使用者正在執行中 及鎖定的活動」的功能
- 建立登入視窗橫幅
- 不要輸入與密碼相關的提示
- 停用快速切換使用者
- 確保個人鑰匙圈和項目的安全
- 為不同 目的建立專用的鑰匙圈
- 系統完整保護狀態

Jamf Pro 中的功能：

- 修復權限指令可透過 Self Service 啟動或自動執行
- 可以建立報表來掃描系統和資源庫中的檔案是否有錯誤的權限
- 通過設定描述檔啟用密碼原則
- 可以透過 Jamf Pro 伺服器政策新增登入視窗和橫幅
- 可以透過 Jamf Pro 伺服器政策中的腳本設定資料夾權限

Jamf Connect 的功能：

- 可為登入畫面建立自訂訊息，根據雲端身份政策的要求強制執行複雜密碼

Jamf Protect 的功能：

- 評估所有此處強調的設定，以 驗證系統存取、身份驗證和授權的合規性

其他注意事項

Jamf Pro 透過設定 EFI 密碼、在安全環境中停用 Wi-Fi 等，協助 IT 管理員自訂其他安全設定。您還可以使用 Jamf Pro 伺服器重新命名您的 Mac，這樣清點庫存就更加容易了。此外，Jamf Pro 讓您能夠清點企業組織擁有的軟體資產並追蹤許可證。

CIS 基準測試建議：

- macOS 上的無線技術
- iSight 視訊鏡頭隱私和保密 問題
- 電腦名稱注意事項
- 軟體清單注意事項
- 防火牆注意事項
- 自動操作光學媒體
- App Store 自動下載在其他 Mac 上購買的應用程式
- 可擴充韌體介面 （EFI） 密碼
- 使用 AppleID 重置檔案保險箱（FileVault）和本機帳戶密碼
- 7不再需要修復權限
- App Store 密碼設置設定
- macOS 上的 Siri
- macOS 的 Apple Watch 功能
- 系統資訊備份到遠端電腦
- 統一記錄
- AirDrop 安全注意事項

Jamf Pro 中的功能：

- 可以通過設定描述檔停用Wi-Fi
- 電腦命名可以在 Jamf Pro 伺服器中自動進行
- Jamf Pro 伺服器 中的軟體清單和許可證追蹤
- 可以透過政策設定 EFI 密碼

Jamf Protect 中的功能：

- 評估所有此處強調的設定，以驗證合規性來考慮其他注意事項

總結

Jamf 讓落實與遵循網際網路安全中心的 macOS 基準測試變得相當容易。

jamf

www.jamf.com/zh-tw/

免費試用 Jamf ，用最好的方式來落實這些安全基準。**立即開始。**