jamf | PRO

幫助企業使用 Apple 取得成功

輕鬆存取、部署與確保
蘋果電腦的資訊安全

基於對蘋果的熱愛，Jamf 成立於 2002 年，僅專注於蘋果設備管理。至今已有超過 26,000 個國際品牌使用 Jamf 管理超過 1300 萬部蘋果設備。在全球數十個不同的國家裡，共擁有超過 1,000 名員工，幫助企業、學校或政府單位在使用蘋果電腦做為工作設備，提供 IT 團隊強大的管理能力，協助企業同仁高效的使用蘋果設備 ，同時保障資訊安全。

此外，企業 IT 團隊也能從 Jamf Nation 受益；Jamf Nation 是全球最大的蘋果 IT 管理社群，超過 85,000 名會員，能互相學習並分享管理觀點、最佳實例，或是建議新功能，幫企業使用者選用最合適的管理策略。

Jamf Pro info

Level 12, Infinitus Plaza 199 Des Voeux Road Central
Sheung Wan, Hong Kong

+852 3008-5865

www.jamf.com/zh

組織企業導入
評估設備的資安思維

我們應該如何管理蘋果的設備？

Apple 從硬體到軟體，所有產品線皆高度整合，包含我們熟知的 macOS、iOS 及 tvOS 設備。確保產品的穩定度與安全性，讓 IT 團隊可以輕鬆的進行部署。員工也會得到與市面上相同的使用者體驗。

Apple 規劃了一項專門計畫簡化整個部署過程，讓用戶獲得完全無需 IT 人員協助的開箱即用體驗，其名稱為 Apple Business Manager（ABM）。

過去，許多公司與組織都在尋求使用單一工具，同時管理所有的 Apple、Microsoft、Google 設備。然而，這會造成公司組織在管理、使用者體驗與安全性上面造成漏洞。使用單一管理工具管理多個平台時，各項安全功能也將無法正常作用，這也讓 Apple 設備優異的安全強項跟著消失。

Apple 系統框架

Apple 框架 ▸ 為了闡明 Apple 所採用的安全措施，我們必須先來瞭解一下 Apple 框架的基礎知識。

Apple 是否需要部署第三方安全軟體？

Apple 設備內建加密與防毒功能，不同於其它作業系統，Apple 設備通常不需要額外的安全層或第三方外部工具。

除了無需第三方介入，就能立即工作。透過 MDM 更能進一步的監控內部資料保密狀況。此外，Apple 將管理框架直接內建在作業系統上，IT 人員只需透過蘋果推播服務（APNs），就能將管理政策推送到設備，達成 MDM 支援的各項管理功能。

避免使用容器化技術添增管理風險

當企業或組織討論資料外洩問題時，經常會提到容器化技術。但這項技術使得 App 架構於該打包技術之上，在作業系統升級時出現程式碼不相容、或是簽章不符合等問題，造成企業管理困擾。Apple 由內而外的整合了軟硬體技術，兼容使用者體驗與資訊安全。只要透過 Jamf Pro 等解決方案就能在原生的方法直接把避免資料外洩，避免因為使用這類技術導致使用者體驗低落、性能下降。

MDM 框架不等同設備管理的完整解藥

Apple 的 MDM 框架十分強大，但對企業與組織來說，許多進階的功能，像是啟用 EFI 密碼等，並沒有包含在 MDM 框架裡面。

Jamf Pro 會在納管電腦裡面安裝 Agent，讓 IT 人員可以設置更進階的策略，配置非 App Store 的軟體（像是 Adobe ），延伸天生的 MDM 能力。

一手掌握所有納管設備情況

了解企業環境內有多少設備、如何被使用、軟體安裝狀態、套用了哪些策略與限制，全面並即時了解設備十分重要。IT 人員可以透過 Jamf Pro 要求所有設備定時回來報到，接著分群分組的定制各項報表。

即便發現設備處於不合規定的狀態，Jamf Pro 的智慧型分組（Smart Group）擁有自我治癒的機制，可強制恢復該設備到合規需求，免去 IT 人員逐一修正的必要性。

Jamf 第零天支援最新版本的 macOS

蘋果每年發表的 macOS 作業系統。Jamf Pro 與 Apple 緊密結合，確保每一代新版本上市，IT 人員都能立即思考升級的可能性，導入最新的安全科技。

macOS 設備具備哪些安全特徵足以我們思考？

FileVault 全硬碟加密功能

使用 256 bits 的加密金鑰進行全盤加密。在搭配具備有 T2 安全晶片上的 macOS 電腦，亦會使用自身的硬體加速引擎，完整保護資料安全。

Apple 數位簽章

Apple 使用數位簽章保護設備在進行軟體更新及安裝時，辨識合法及安全性，遏止潛在的惡意軟體修改 Mac 上受保護的檔案和檔案夾。

GateKeeper 門禁技術

IT 人員可以透過內建的門禁技術（GateKeeper），確保只有受信任的軟體得以在 macOS 上執行。

XProtect

自動偵測並阻止已知惡意軟體的安裝，若惡意軟體突破重圍進入 Mac，在 macOS 裡另外內建了惡意軟體清除工具修正感染狀況。

更多關於 macOS 安全資料請見：
https://www.apple.com/macos/security/

我們該如何制定安全標準管理 Apple 設備？

落實 Apple 設備管理之前，我們需要訂定安全標準加以落實。參考 CIS 是一個很好的開始。CIS 全名為 Center for Internet Security，定期出版的 macOS 安全評量，從八大面向探討，被認作是管理 Apple 設備的完整檢核清單，Jamf Pro 在各面向都有完整的對應方式，滿足資訊安全考量。

軟體更新

Jamf 對應▶延時或強制所有蘋果設備更新最新版作業系統，維持最佳安全性。

日誌與稽查

Jamf 對應▶收集納管設備或擴充上百項資訊並自動匯出報表，掌握資源狀況。

存取與認證

Jamf 對應▶設定密碼規則，定期要求員工更改密碼、不得重複使用密碼等。

偏好設定

Jamf 對應▶開啟磁碟加密、關閉共享及藍牙傳輸，提昇資訊安全、維持員工效率。

網路設定

Jamf 對應▶藉由程式碼部署，禁止設備使用無線網路或成為網路伺服器。

其它考量

Jamf 對應▶維持資產編號及名稱與報表一致，並設定 EFI 密碼確保資產可用性。

iCloud 雲端

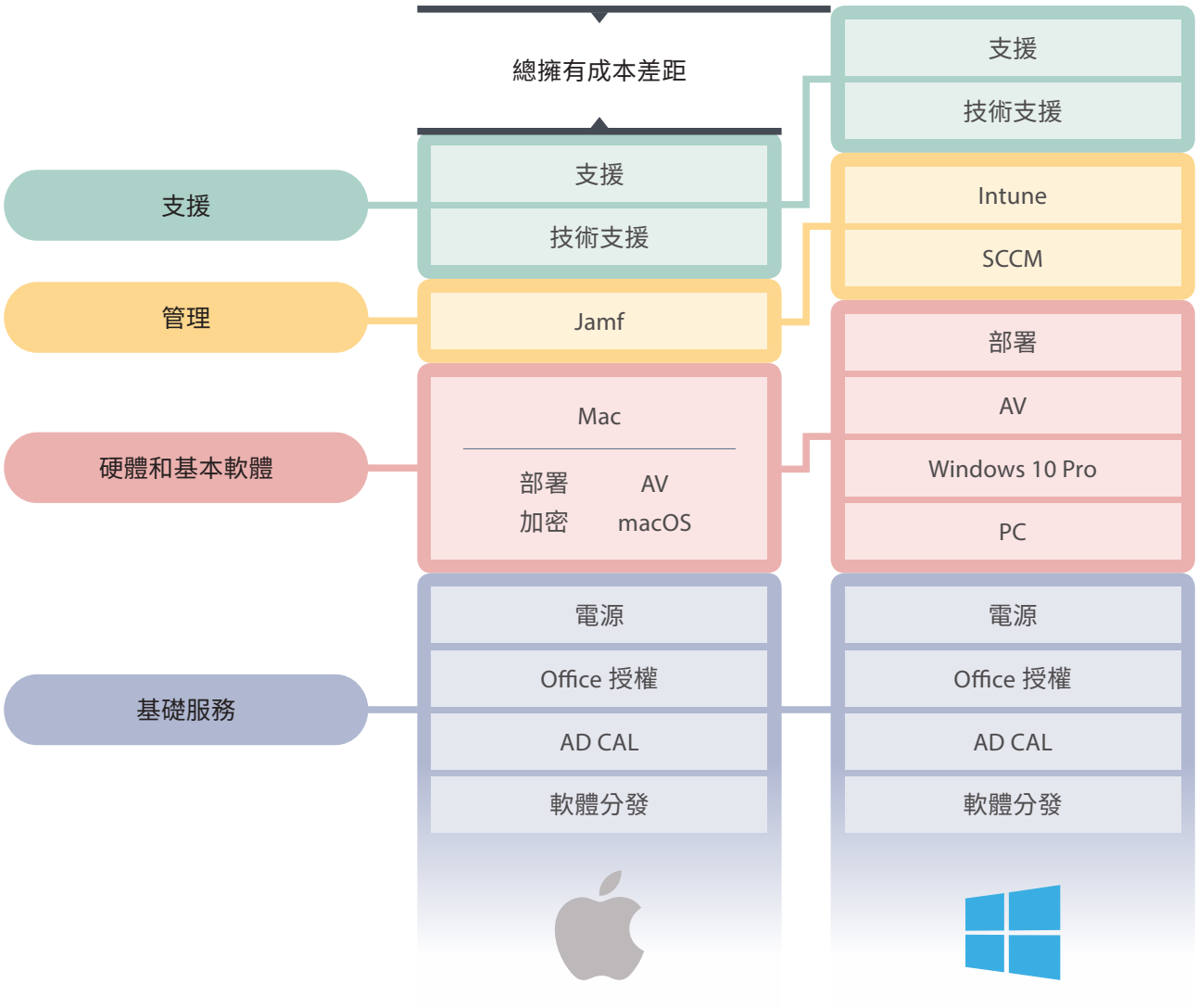
Jamf 對應▶關閉 iCloud 雲端等相關功能，減少資料外流風險。

使用者帳號

Jamf 對應▶整合目錄服務避免員工取得管理權限，但仍能自行安裝軟體。

更多 CIS 的資料請見：
https://www.jamf.com/resources/white-papers/macos-security-checklist/

員工擇其所愛、企業節省成本



當計畫向員工提供 Mac 時，不可避免的需要考慮成本問題。多數的企業在考慮到切換到 Mac 時，心裡總想著：Mac 非常棒，但是購買一台 Mac 的價格是 PC 的兩倍。然而，這樣的迷思可以用 IBM 的真實案例打破，IBM 副總裁 Fletcher Previn 在為公司內部導入 21 多萬台 Mac 後，曾於 2016 年的 Jamf Nation User Conference 提及，現今每導入一台 Mac 的總成本相較於 PC，可減少 273 至 513 美金。

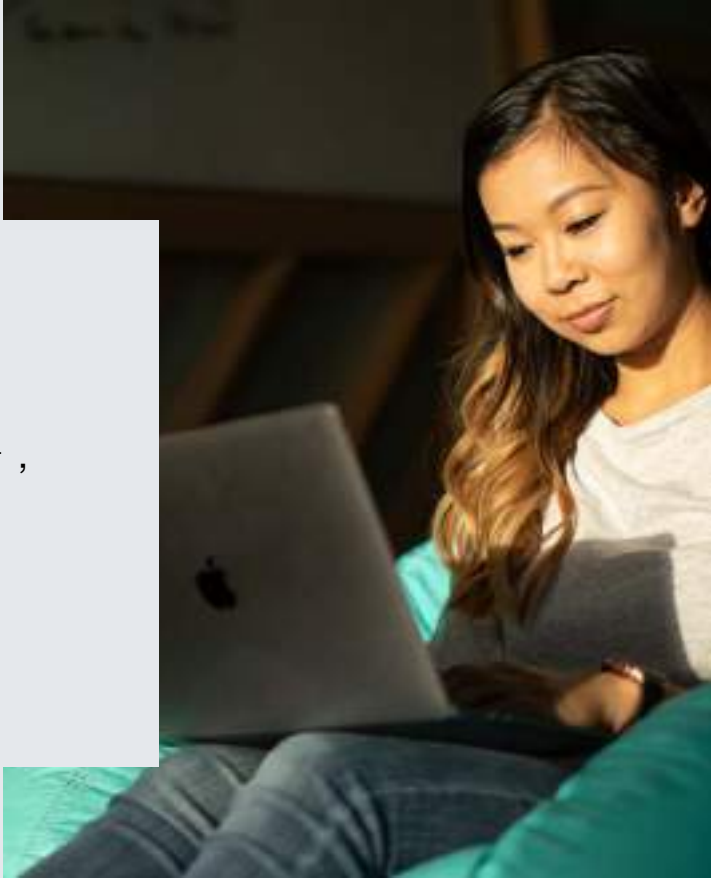
每一台蘋果電腦都已經內建了合法且免費的 macOS 作業系統，不同於 Windows 作業系統有多種版本，例如家用版或是專業版，macOS 僅具備單一版本，因此在功能上沒有差異，所有的 macOS 都能綁入至 Active Directory 服務、全硬碟加密、內建商用等級的防護功能，無需另外採購防毒軟體，避免系統受到侵害。

在管理 Windows 方面，微軟提供 System Center Configuration Manager (SCCM) 以及 Intune 擴充 MDM 功能延伸 SCCM 能力，多數企業都會採購這兩套軟體進行管理。這再一次證明了 macOS 與 Windows 的不同之處，包含 macOS、iOS、tvOS 等都已內建了 MDM 管理框架，Jamf 做為蘋果專門的 MDM 服務提供商，得以利用此框架遠端管理蘋果設備，加上第零天部署的特色，所有蘋果設備推出新版作業系統的當下，Jamf 就能立即提供支援，享有完整的管理功能。

jamf

Jamf Protect
終端安全防護能力

企業採用 Mac 做為工作設備的比例逐步提高，
也引起了駭客對攻擊 macOS 的興趣。



jamf PROTECT

設備安全

- 防毒軟體
- 行為偵測
- 資料控制
- 自動與自定義修復

安全操作

- 自定義分析
- macOS 安全能見度
- 威脅獵捕
- CIS 框架
- 日誌集中管理
- SIEM 整合
- 裝置隔離
- 鎖定裝置
- 檔案修復
- 隔離使用者
- 鎖定使用者

訊息安全

- 監督檔案正直性
- 應用程式控制
- 合規條件監察
- 標準化修復
- 應用程式報告
- 重新部署 macOS

Jamf Protect
Jamf Pro
Jamf Connect

當 macOS 從 Unix 的世界發展出來，其對檔案、應用程序與網路的內部處理方式，使 macOS 成為一個獨一無二的作業系統。面對這樣的環境，針對於 macOS 的攻擊方式，就與攻擊 Windows 或其它作業系統的方式不甚相同。然而，多數的安全防護原廠僅將過往針對 Windows 的系統掃描、防護及修復等功能，移植到 Mac 平台上。

由於現今我們所看見的一體適用資安工具並不是為 Mac 所設計，企業很可能會因此忽視了存在於 Mac 架構上的攻擊。為了要能面對並強化你的企業資安問題，提供專門為 Mac 設計的資訊安全平台至公司目前的資安架構裡顯示更為重要。

Jamf Protect 是一個專為 Mac 量身訂做的終端安全解決方案，持續保障 Mac 設備在公司合規下，聚焦於 macOS 上的惡意程式與威脅，掌握應用程式情報，在最不影響使用者的情況下，偵測並修復針對 Mac 的威脅，維持 Mac 一貫的使用者體驗。若同時整合了 Jamf Pro 或 Jamf Connect，Jamf Protect 就能展現出更強大的自動化、調查研究與修復能力，處理 Mac 設備上大大小小的安全風險。

Jamf 建構於 Apple 為 macOS 設計的安全核心框架，並承諾 Apple 同天支援，當每次作業系統更新時，取得更貼近企業的強大防護力、控管力、能見度以及更完善的威脅修復能力。有別於一體適用的資安解決方案，通常會在 Apple 發表新版作業系統時存在空窗期。Jamf 則是無縫的與最新版 macOS 銜接，隨時保護使用者免於威脅，不受到任何耽誤。

專注於 Mac 的防毒軟體

防毒軟體是大多數組織最基本的安全需求。Apple 內建的 macOS XProtect、Gatekeeper 與 MRT 技術，提供了最基礎的防毒軟體機制。然而，這些科技並未提供相關行動的數據資料，更新也較不定期。 Jamf Protect 提供了深度的防毒軟體功能，延伸了 macOS 底層的安全科技，能夠阻止並隔離 Mac 上的惡意程式，而且遠遠超過以 Windows 做為基礎的防毒軟體所能提供的。

- **防毒:**避免知名 Mac 惡意程式在裝置上執行
- **能見度:**提供組織了解 macOS 內建的 XProtect 與 Gatekeeper 運作狀況
- **洞悉惡意程式:**借重於 Jamf 及其它第三方對 macOS 的惡意程式分析數據，預防常見惡意程式執行
- **隔離:**當惡意程式被識別時，自動從使用者環境移除並且隔離做為分析使用
- **使用者體驗:**Jamf Pro 能確保使用者採取正確措施，尤其在 Jamf Protect 識別到惡意行為時，以防止類似情事再度發生
- **檔案捕捉:**當威脅被識別時，從 Jamf Pro 取回檔案樣本

專注於 Mac 上的偵測與回應

傳統的端點偵測及回應（EDR）工具已存在 Mac 市場一段時間，但大多數並未能針對 Mac 打造，使其擁有比較好的效率去偵測威脅。反而，這些工具更傾向於把 Windows 的模式強加於 Mac 設備上。由於 Jamf Protect 僅聚焦在 Mac，因此 Jamf 能最小化不正確的回報，而且能夠最大化在 Mac 上的偵測效率。隨著與 Jamf Pro 一起使用，Jamf Protect 得以最小化破壞式修復，平均遠超過於其它 EDR 的能力。

- **行為分析:**從一系列在裝置上的行為分析，偵測未知惡意程式或進階威脅
- **涵蓋多項警示範圍:**Jamf Protect 能警示 MiTRE ATT&CK 框架事件，包含初始存取時間、執行階段、持續潛伏、權限提升、防禦逃脫、條件式存取、發現、橫向移動、收集、滲出與衝擊等類別
- **通知:**Mac 以即時的方式透過 Jamf Protect 控制台、電子郵件或是你的 SIEM 等觸發安全警告
- **通知內容:**取得深入完整的資訊，了解為何安全警示被觸發，省去你在分析上的不必要猜測
- **降低偽陽性反應:**在你的環境裡任意調整偵測方式，以最小化誤判事件
- **自定義偵測:**為你的組織自行定義偵測內容，最小化資安風險

安全事件回應

當攻擊被偵測到時，會啟動一連串的機制，包含威脅隔離、移除威脅，或者將使用者或設備移回信任狀態。使駭客在組織內缺乏至其它設備的攻擊點，也就越不能偷取資料、毀損數據或是傷害企業。大多數的自動化資安事件不會通知終端用戶，在某些情況下，會由資安團隊決定下一步動作。

- **隔離:**避免惡意程式執行並隔離，以降低延伸後果並做為分析使用
- **通知使用者:**教育使用者以防止未來類似事件再次發生
- **自動化復原:**自動在資安事件發生時，觸發 Jamf Pro 修正程序，減少設備停機時間
- **檔案取回:**與 Jamf Pro 搭配使用，從被標記惡意行為、需調查的設備上取回檔案

- **資料收集：**當威脅被識別時，由 Jamf Pro 從裝置上取回稽查必須的資料
- **隔離裝置/使用者：**從 Jamf Pro 自動限制裝置在取網路資源，或是經由 Jamf Connect 禁止使用者存取資源
- **鎖定裝置/使用者：**當威脅使設備不再受到信任時，自動使用 Jamf Pro 鎖定該裝置，或是利用 Jamf Connect 鎖定使用者
- **重新部署macOS：**Jamf Pro 透過遠端重新安裝 macOS 作業系統與應用程式，將一個非受信任的設備復原至信任狀態
- **引導使用者：**當可疑事件被偵測到時，經由 Jamf Pro 重新引導使用者至內部訓練教材

控制應用程式以最小化風險

確保使用者不會安裝帶有對公司或內部資料產生危害的應用程式。Jamf Pro 能讓組織提供一系列已信任的應用程式至使用者，而資安單位往往需要涉水更深，有了 Jamf Protect，你將能控制：

- **不受信任應用程式：**避免不希望的應用程式在公司設備上被執行
- **避免已知威脅：**避免執行具備弱點的軟體版本
- **不信任的開發者：**避免未受信任開發者所開發的程式在設備上執行

監控合規行為與威脅捕捉

成熟的資安團隊會從多個安全工具上識別惡意行徑與收集多方資料。換句話說，IT 團隊經常需要共同分擔收集資料的重責，做為合規稽查所用。無論何種情況，有一個持續的流程，能從裝置上取回正確資料至中央是非常必要的。

- **行為能見度：**以最不影響使用者體驗的前提下，在 Mac 上收集檔案、程式與認證資訊
- **裝置日誌：**匯出裝置日誌資料（從 macOS 的日誌紀錄） 做為離線分析
- **資料集中：**將資料統一收集至 SIEM 或其它能做為交互參考或長期保存的系統

資料控制

當使用者及其設備變得越來越行動化，也越來越分散的同時，保護資料越能成為組織成功的中心，聚焦於資料是如何被流動與傳出更是必要。

- **監控USB裝置使用：**抓取USB裝置使用量以確保只有信任設備可被使用
- **控制USB使用：**利用Jamf Pro限縮裝置使用 USB 儲存裝置
- **監控USB活動：**提供USB儲存裝置上檔案異動的能見度
- **監控螢幕截圖活動：**識別任一個未受允許應用程式嘗試進行螢幕截圖等行為

保持資安基準線

只要在意資訊安全，啟動作業系統上的設定以強化設備已是最佳實踐。為不同作業系統所發展出的先進安全框架，也常被不同產業間分享與使用。現在，部署與維護這些設定已成過去式。

- **監控指標：**監控設備符合 Jamf Pro 所部署的安全設定基準線
- **驗證指標變化：**快速識別裝置裡的指標變化
- **重設指標：**在裝置在使用 Jamf Pro 重設基準線
- **檔案正直性驗證：**監看重要檔案變化

更好的用戶體驗

Mac 用戶期待在他們的設備上有一個流暢、穩定及有效率的工作體驗。Jamf Protect 將用戶放在心上 — 保護使用者隱私並最小化衝擊。

- **原生安全框架：**支援蘋果終端安全框架（ESF）減少對終端使用者的影響
- **無需使用 Kernel Extensions（KEXT）：**Jamf 應用程式提供使用者最大的穩定度，而且無需使用系統核心組件，而是在有必要時，使用系統擴充功能（System Extension）
- **同天支援：**Jamf 產品總是能在 macOS 推出新版本時立即釋出支援版本，從未延遲。安全與管理套件不應該成為延後升級作業系統的藉口。
- **即時防禦與偵測：**即時地偵測與防止有害行為。不使用長時間的系統掃描功能影響裝置效能。
- **Mac 量身訂做：**Jamf 只為 Apple 而生。Jamf Protect 能識別在 Mac 設備上的攻擊，而不是對 Mac 無作用的 Windows 威脅。

生態系整合

鮮少組織只在環境內部署一項安全工具。不同的工具互相在技術上或是程序上整合相當重要，才能最大化裝置上的安全與效率。

- **SIEM：**資料與警示可被推回你自己所擁有的 SIEM。
- **自定資料倉：**原始資料及警示可被推回你的 S3 儲存倉。
- **通用第三方支援：**資料與警示可被推送至你的 SOAR 及其它用以 HTTPS 接收 JSON 的系統

Jamf 提供工業級安全解決方式至你的 Mac 設備，具有高防禦能力及偵測率。我們的解決方案簡潔、直觀，與 Apple 原生功能高度相容，並讓設備在被保護時，仍能為客戶帶來高效率工作環境。

前所未見的能見度，領先業界的修復能力。
只為 Mac。

jamf

www.jamf.com

© 2002–2021Jamf, LLC. All rights reserved.

jamf | CONNECT

Transform provisioning and identity management

Reimagine how users authenticate to Mac.

Binding to an Active Directory domain was a great solution to solve authentication issues for 20 years. But in an age of increasingly mobile devices and employees, jobs are performed in a cloud-based environment without connecting to the corporate network. Today, being a member of an Active Directory can be a challenge.

Enter Jamf Connect.

Jamf Connect relieves the binding and gives you the flexiblity to centrally and remotely manage users, groups, passwords, and access to corporate applications and cloud resources. It's the approach to identity and security, evolved.

jamf

See how Jamf solves provisioning and identity challenges.

Jamf Connect allows for simple provisioning of users from a cloud identity service during an Apple provisioning workflow, complete with multi-factor authentication:

Account provisioning

Jamf Connect gives users the ability to access their Mac and their applications with a single identity, providing an improved user experience during setup and day-to-day logins – all without the need for multiple accounts and to bind to Active Directory.

Identity management

Jamf Connect requires a cloud identity, giving IT admins the ability to monitor who is accessing devices, to leverage cloud admin permissions to service machines, and maintain security and compliance standards across all devcies and users.

Password synchronization

Jamf Connect ensures a user's cloud-identity passwords are synchronized down to the local account level on the Mac, even when the password is changed – reducing password fatigue and IT help desk tickets.

Jamf Unlock, Jamf Connect's passwordless workflow, provides users secure access to their Mac via their iPhone. Utilizing Face ID, Touch ID, or PINs, users gain immediate access to their Mac, without needing to type a password.

With key identity provider integrations, Jamf Connect is the best way to manage accounts and authentication.

✓ **Okta** ✓ **Azure** ✓ **Google Cloud Identity** ✓ **IBM Security Verify** ✓ **OneLogin** ✓ **PingFederate**

$48 /device/year

with required onboarding for additional fee

Includes Jamf Standard Support
(Chat, Email and Phone)

Need additional assistance?
Our global support team is standing by.

Jamf Standard Support is included for Jamf Connect + Jamf Pro users and available to NoMAD users for an additional fee.

jamf

www.jamf.com

© 2002-2021 Jamf, LLC. All rights reserved.

To see how Jamf Connect can help you transform your provisioning and identity management workflows, visit **www.jamf.com**.

jamf

JAMF THREAT DEFENSE

保護您的設備、使用者與應用服務，抵禦來自網路世界的威脅

Jamf Threat Defense提供運行在終端設備與連線網路的雲端安全解決方案

功能強大的端點安全

Threat Defense偵測並修復最大範疇的端點威脅，包含端點設備本身漏洞、惡意程式與高風險Apps。全面性的風險評估，不間斷運作地進行威脅辨識、落實安全政策能全時有效執。

網路防禦保護使用者與資料

Threat Defense能洞燭先機地阻擋攻擊。內容保護阻斷來自惡意網站針對商業機密的竊取，包含來自未曾被發現過的第零天釣魚(zero-day phishing)網站。此外，Threat Defense透過高風險網站連線阻斷，事先防止中繼控制(command-and-control)運作與未授權的資料傳送。

可調控的應用程式存取

透過安全與可信任設備的篩選放行，提升商業應用服務存取的整體安全性。Threat Defense透過持續監控大量分析資料與其交互關聯性，避免來自已經遭到滲透或存在高風險之端點設備的應用服務存取。經由零信任網路存取機制或Jamf的管理解決方案Jamf Pro，存取政策能依據需求地在原生系統中被強制執行。

jamf

全方位的威脅偵測與防禦

第零天網路保護

即使是極度複雜的網路攻擊，包含第零天釣魚威脅、中繼控制(command-and-control)通訊與加密劫持(cryptojacking)...等等，Threat Defense能有效地辨識並阻斷。這項服務能與任何應用(App)搭配，如網路瀏覽器、電子郵件、社群軟體與簡訊服務(SMS)。

即時風險評估

Threat Defnese持續地分析從來自作業系統弱點漏洞以及惡意設定檔，協助組織快速地辨識出違反合規的設備與強制進行正確地零信任存取。

詳細的應用程式監看

Threat Defnese提供先進的智慧應用程式檢視用來協助應用程式工作流程審查與安全機制調查。透過詳細的報表呈現可
能導致個人與組織資料曝險的授權允許清單與內嵌的URLs連結，提供每一個應用程式的風險評分報。

動態資料加密

Threat Defnese透過即時資料加密，防止機敏資料透過已遭到滲透的無線網路(Wi-Fi))外洩。

領先的安全特點與能力

全時的端點防禦

Threat Defnese透過端點應用程式(App)來辨識惡意軟體、不安全的設備設置與具有風險的連線，保護行動環境工作人員與設備避免進入風險。

即時的回報與政策控制

聯合的政策引擎允許管理者快速地配置安全政策，安全政策即時調整可透過線上更新強制派發。威脅防禦管理平台提供可視化的詳細報表呈現，亦可透過簡易的整合匯出到第三方報表工具。

條件式的存取政策

防止商業用程式接受超過風險評估數值設定的連線進行存取。透過Threat Defense網路、Jamf整合或帳號識別服務提供方，可提供強制原生執行條件式存取政策。

聯合運作與管理

Threat Defense與管理系統直接整合，讓服務可以快速部署到受管理的設備。如此的整合，伴隨增加可讀性的事件名稱，也可以簡化針對威脅活動的事件監視與威脅獵捕的報告。

Jamf Threat Defense 可與您既有的的IT服務與科技無縫地整合。

深度地與Microsoft、Google、Cisco整合，並可協助延伸既有技術架構的價值。

jamf

www.jamf.com

© 2002-2021 Jamf, LLC. All rights reserved.

需要更多關於Threat Defense如何保護使用者、行動裝置、與組織資料，歡迎蒞臨 jamf.com

jamf

JAMF DATA POLICY

實現遠端工作並幫助員工保持工作效率

強制接受使用，消弭影子IT，防止過度使用資料數據，並教育終端使用者如何跨行動數據、漫遊和 Wi–Fi 網路使用數據。

執行可接受的使用政策

Data Policy的內容過濾允許組織定義哪些網站以及應用程式可以被執行在公司所擁有的行動設備上。Jamf 透過實時監控確保網路行為是合規且可以被接受，並且可以基於類別的策略控制自動執行。

影子IT監管

在受監管行業或處理敏感訊息的組織應遵守各種資訊安全和行業政策。Jamf 可以預防公司機密資料被洩漏，不管是透過瀏覽器或是應用程式都可以阻止訪問未經允許的服務。

實時管理使用情況

僅允許安全且受信任的設備訪問商業程式。威脅防禦持續監管廣泛的遙測和上下文輸入，可用在端點受到威脅或處於高風險狀態時無法使用應用程式。自適應訪問策略可以通過零信任網絡訪問解決方案或 Jamf 的管理解決方案 Jamf Pro 來實施。

jamf

> “在 Campari，我們使用Jamf Data Policy來控制我們的行動數據使用。 配置非常簡單，包括通過無線方式將Jamf Data Policy的應用程式和流量配置文件部署到終端行動設備，終端使用者無需安裝任何程式。 由於節省了數據成本和簡單、集成的行動設備管理，使用此產品將帶來的鉅額的投資回報。”
>
> - Campari

功能特色

即時政策控制

當資料流量使用達到設定限制時啟用流量限制政策。為用戶和管理員客製化警報和通知。

客製化功能

將政策使用在個人、團體或是組織。訂製預先過濾的類別–可以自定義允許、非允許列表。

內容過濾

設定智能規則防止訪問不適當的網站和應用程式。 確保合規的使用 HR、IT 和監管政策。

網路察覺

為不同的網路新增和實施不同的策略。 Data Policy會自動檢測網絡，以允許 Wi–Fi 用戶在沒有數據管理的情況下使用內容過濾。

任何行動設備，任何持有模式

Data Policy支持行動設備和筆記本電腦，讓您可以選擇最適合您的設備。

即時洞察

使用 Jamf 的即時洞察和使用情況分析工具監控數據使用情況。

Jamf Data Policy 與您現有的 IT 服務和技術無縫整合。

深度地與Microsoft、Google、Cisco整合，並可協助延伸既有技術架構的價值。

jamf

www.jamf.com

© 2002-2021 Jamf, LLC. All rights reserved.

需要更多關於Data Policy如何落實您需要的使用政策，歡迎蒞臨 jamf.com

jamf

JAMF PRIVATE ACCESS

提供企業網路資源快速、簡單、安全的零信任網路存取

提供企業團隊無時無刻、任意地點安全地連線所需的應用服務的工作彈性

Private Access透過身份識別與集中化政策，消除大量因使用者無法找尋與取用資料暨應用服務的限制，進而提升工作效率

強韌的安全

Private Access透過雲端基礎與軟體定義邊界(software-defined perimeter-SDP)的架構，與每一個應用程式建立一個安全、隔離的連線。透過最低授權強制管理與即時端點設備狀態檢查，確保每一個應用程式僅能授權特定使用者存取。

提升管理能力

Private Access使用全雲端架構，完全不需要企業內部設備部署來管理或是處理複雜的架構規模需求。Private Access提供更有效率的方式來節省全通道流量帶來的不必要昂貴支出，同時保有資源存取的能見度與控制權(亦即網路策略無需流量引導)

直覺的使用者體驗

Private Access應用了專為快速與安全的遠端工作情境設計的網路協定。透過雲端規模與排除不必要的網路回流，提供使用者毫無延遲感的網路存取絕佳體驗。有效率與優雅地網路傳輸轉換，提供使用者不斷線的行動網路與Wi-Fi網路切換。

jamf

功能特色

雲端軟體定義邊界

Private Access透過雲端基礎與軟體定義邊界(software-defined perimeter-SDP)的架構，與每個應用程式建立一個安全、隔離的連線。透過最低授權強制管理與即時端點設備狀態檢查，確保每個應用程式僅能授權特定使用者存取。

應用程式微通道

Private Access是零信任網路存取解決方案，執行在其上的端點設備與應用程式無需學習其網路基礎架構。

通信連線(Session)的報表呈現

詳細的通信連線報表協助監看使用者行為與其所使用的應用程式。即時的統計分析能為不尋常的行為活動、通訊連線期間與頻寬需求提供洞燭機先的判斷。全面性的能見度讓管理者可以監看不適當的內容傳輸、偵測惡意軟體與判斷資料洩漏的可能性。

新世代的網路協議

大多數的端點設備使用Wi-Fi或是電信行動網路連線，但是使用者與應用程式想要跟實體連線網路有一定的品質。Private Access透過靜默與無縫的連線服務，提供安全快速、廣泛適用性與輕量化的連線，即使使用者處於移動的辦公環境中。

基於身份識別的解決方案

Private Access使用身份識別基礎的策略來提供使用者與應用程式相關授權。透過與現有的目錄服務整合達成策略的快速部署與管理。使用者僅能透過擁有針對相關應用程式的適當權限來建立連線通道。

動態通道分離

Private Access使用智慧通道網路協議，僅將授權使用者設備上針對該應用程式流量傳送到連線對應在雲端軟體定義邊界上的應用服務。這個機制確保應用程式微通道策略被正確地執行，也讓終端使用者有最佳的使用者體驗。

單一封包通訊授權

排除未授權的來源針對應用探詢的可能性。使用者身份識別與裝置認證成功後，單一封包通訊授權才能進行存取連接。

動態通道分離

Private Access使用智慧通道網路協議，僅將授權使用者設備上針對該應用程式流量傳送到連線對應的應用服務。這個機制確保應用程式微通道策略被正確地執行。

Jamf Private Access 可與現行的IT服務與科技完美地整合

與Mircorsoft, Google, Cisco...等公司深度整合，更能協助並延伸您現有的服務與相關科技價值。

jamf

www.jamf.com

© 2002-2021 Jamf, LLC. All rights reserved.

需要更多關於Private Access如何確保員工、終端設備應用服務與企業資料的安全連線，歡迎蒞臨 jamf.com