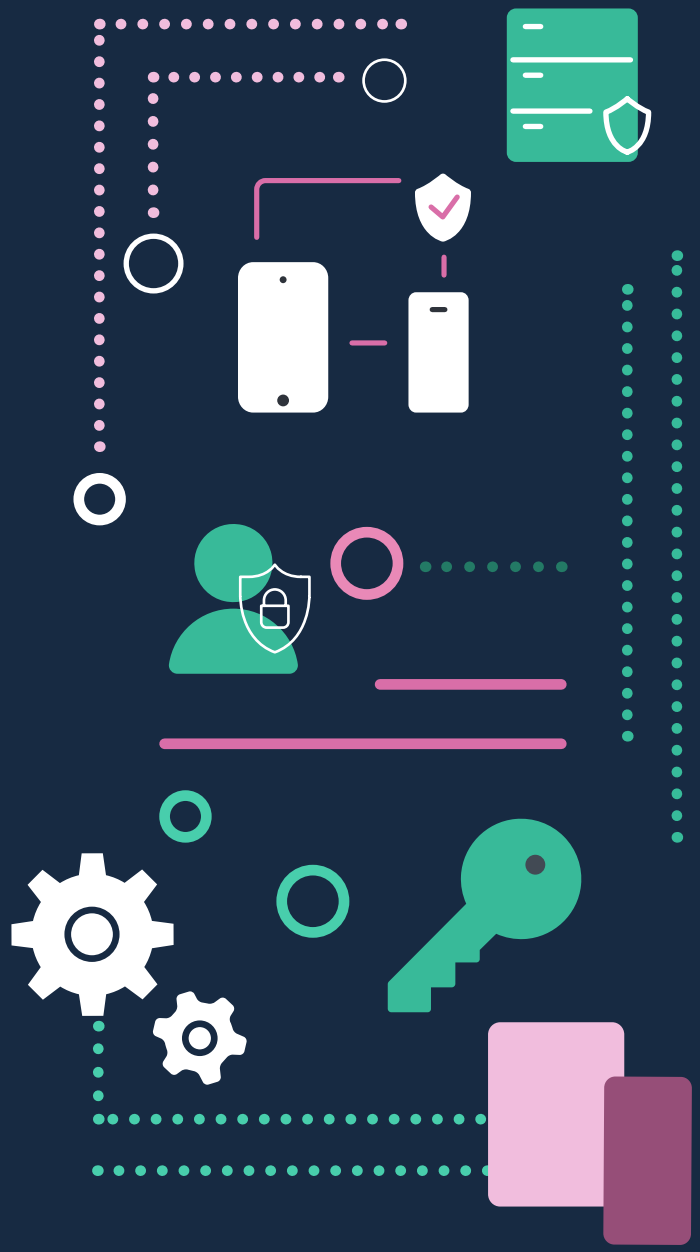


jamf

身分管理和安全性

進階指南

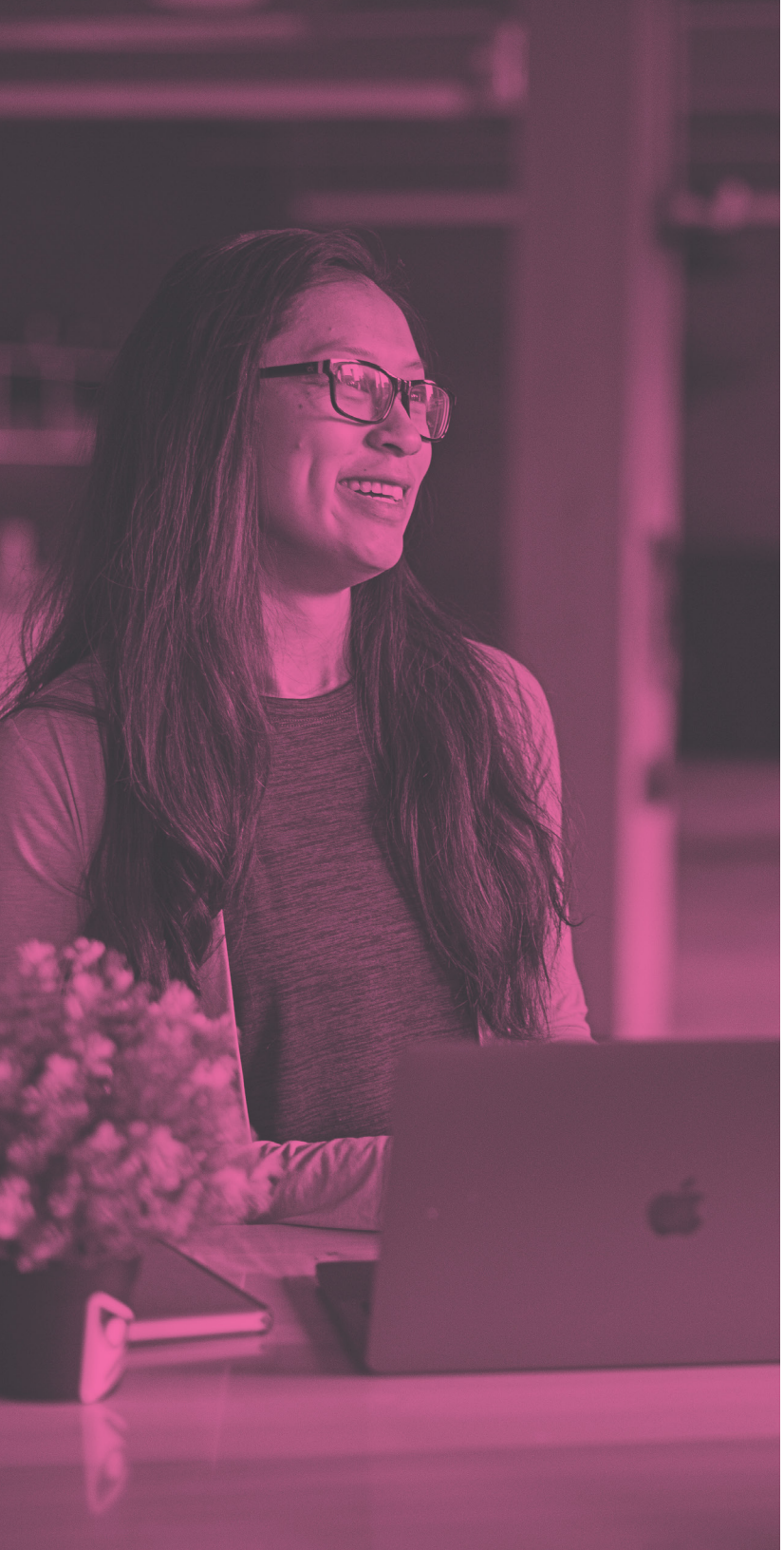
每位員工都有自己的數位身分

在過去的十年中，隨著遠端工作趨勢勁升，企業組織不斷地想方設法以回應這項需求，而身分管理的重要性也就變得顯而易見。從內部部署系統遷移到雲端，使得無數企業組織邁向現代化身分管理更進一步。這個主題我們在《身分管理入門》已有初步探討。然而，身分管理的範疇遠不止於驗證（authentication）與授權（authorization）。企業希望利用使用者的數位身分來實現「零信任」（Zero Trust）安全策略的目標。

零信任安全架構的核心理念，其實您並「不信任」連接使用者與任何服務之間的構成的橋樑其中一個最不應該相信的部分就是網路本身。為了讓您更了解其中各個環節，我們將涵蓋一些您在規劃身分與安全策略時可能需要考慮的技術和細節。如果您尚未閱讀我們關於零信任的介紹：《 Putting Trust in Zero Trust》，建議您先從那裡開始本電子書將深入探討先前提到的概念，並將那些基礎概念提升到更進階的層次。

在這份指南中，我們將探討以下內容：

- **現代化驗證的運作方式**
- **確保網路流量安全的技術**
- **如何新增條件式存取工作流程**
- **Jamf 如何將這一切整合在一起**



現代化身分驗證快速上手

在我們的《身分管理入門》電子書 中，我們已介紹過驗證（Authentication）與授權（Authorization）的差異，現在讓我們探討如何透過現代化服務實現單一登入（SSO）。

雖然驗證使用者的方法有很多，但目前最常見的是 SAML（Security Assertion Markup Language）和結合 OIDC（OpenID Connect）的 OAuth。這兩種系統的目標類似，都是將使用者驗證至某個可信來源，通常稱為 IdP（身分提供者），並生成可與其他服務共享的授權碼來證明您的身分。如果您曾在 Active Directory 中使用過 Kerberos，就會發現它們有許多相似之處。

現代化身分驗證快速上手

管理者需注意的關鍵要點：

- SAML 驗證會生成 Assertion，這些 Assertion 是經過簽署的 XML 區塊，用於確認您的身份，並讓其他服務信任您的驗證結果。
- SAML 要求任何服務在與 SAML 驗證提供者通訊時使用個別的憑證，因此在使用原生應用（Native Apps）時會更加複雜。
- OIDC 與 OAuth 搭配使用，可生成簽名的 JWT（JSON Web Token），這些 JWT 使用 JSON 而非 XML，但功能上與 SAML 的 Assertion 類似。
- OIDC 還有一項額外的優勢，即 ID Token 始終是一個 JWT。這個 ID Token 是一份便攜的使用者記錄，並經過簽署以驗證其有效性。

在使用 SAML 或 OIDC/OAuth 驗證服務時，服務本身永遠不會接觸到使用者的密碼，因為密碼僅由 IdP 處理。取而代之的是，該服務會獲得由 IdP 簽署的 SAML Assertion（斷言）或 OAuth Token （代號），以此建立信任。雖然兩者之間有實作上的細節差異，但 SAML 和 OIDC/OAuth 都提供了非常安全、現代化且可擴充的方式來驗證使用者與服務之間的關係。

現代化身分驗證：快速入門

以下是一個 SAML Assertion 的範例：

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                     AssertionConsumerServiceURL="https://[servername].jamfcloud.com/saml/SSO"
                     Destination="https://login.microsoftonline.com/[tenant]/saml2"
                     ForceAuthn="false"
                     ID="a4a9efd7a384732928bf1bdbg2afab3"
                     IsPassive="false"
                     IssueInstant="2021-04-02T16:30:58.826Z"
                     ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                     Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://[servername].jamfcloud.com/saml/metadata</saml2:Issuer>
</saml2p:AuthnRequest>
```

用於參考差異，以下則是一個 OAuth Token 的範例：

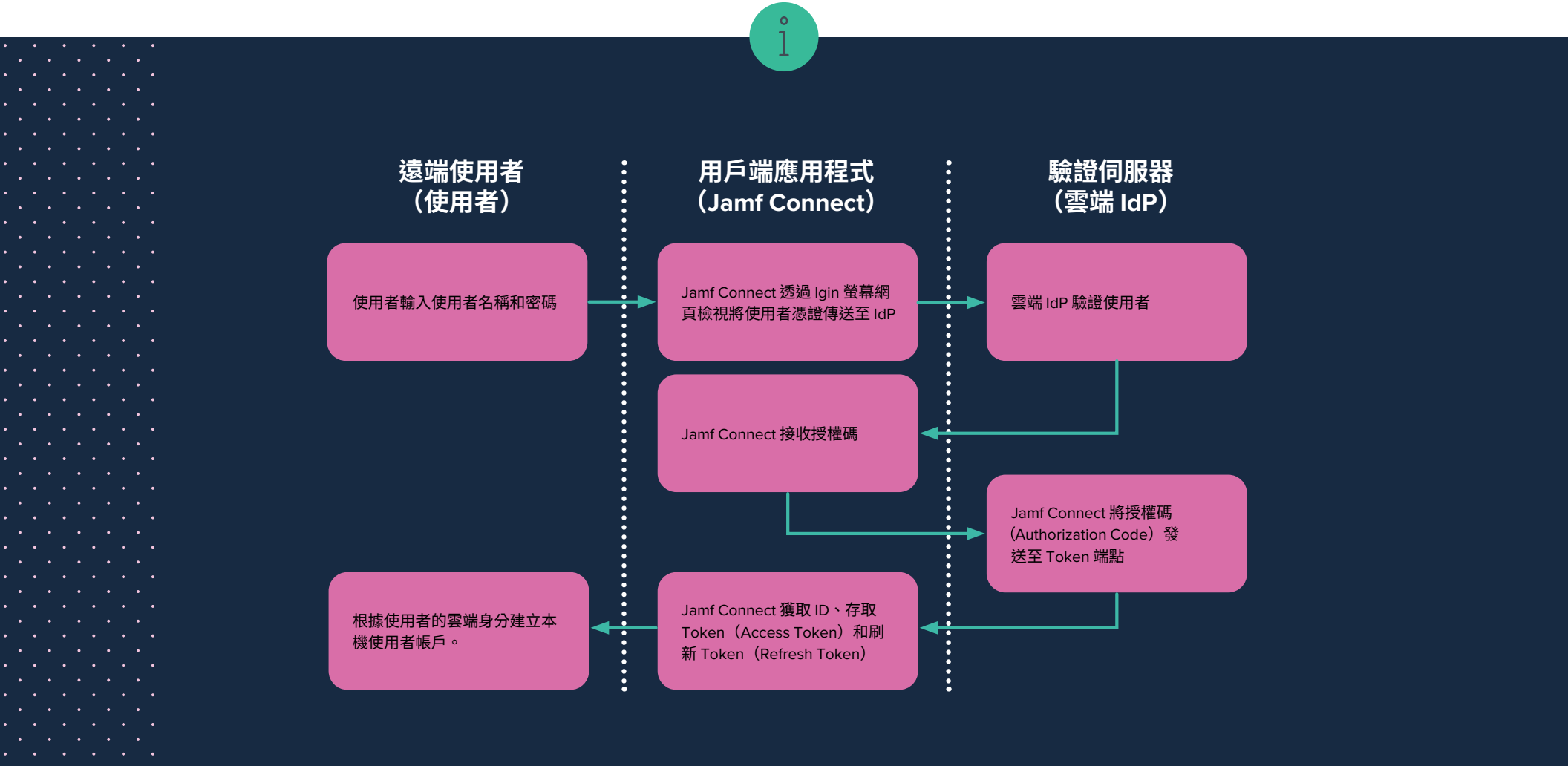
```
"app_displayname": "My Sample OIDC App Name",
  "appid": "2520beb2-535e-4e42-bf70-1d4cd5429551",
  "appidacr": "0",
  "family_name": "Lastname",
  "given_name": "Firstname",
  "idtyp": "user",
  "ipaddr": "52.205.5.180",
  "name": "Firstname Lastname",
  "oid": "0fa4b783-1c00-4765-b40d-c2b72de03079",
  "onprem_sid": "S-1-5-21-1861720204-2608728089-2580082577-1523",
  "platf": "5",
  "puid": "100320004CDFC4DB",
  "rh": "0.AQ4A2rA -GiB-Uuv8iVxxpwOALK-ICVeU0JOv3AdTNVClVEOAQ8.",
```

注意： 這僅是部分範例，並非完整的 Token 樣本。

JAMF 中的 SAML 和 OIDC/OAUTH

Jamf 的不同產品使 用不同的驗證方式： Jamf Pro 支援 SAML。 Jamf Connect 與 Jamf Protect 使用 OIDC/OAuth 對 Jamf Connect 而言，SAML 並不適用，因為需要憑證，以及將憑證和私密金鑰推送至使用者裝置，而您不知道是否可以信任這些裝置。總體來說，Jamf 提供了一種簡化的方式，能輕鬆支援來自雲端身分提供者（IdP）的多重驗證（MFA），而無需對每個服務進行使用者的細緻管理。

以下是一個範例，說明 Jamf Connect 如何使用 OIDC 的授權碼授權（Authorization Code Grant） 流程：Jamf Connect 透過 OIDC 驗證使用者的雲端帳號與密碼，並交換一個授權碼，然後將此授權碼發送至 IdP 的 Token 端點。



現代化身分驗證身分識別提供者同盟（IDP FEDERATION）

談到現代化身分驗證，就不能不談到 IdP 同盟。例如，您可能使用 Azure AD 搭配 Microsoft Office 365，但實際上身分驗證是同盟化到 Okta，因為它是您的主要身分提供者（IdP），擁有使用者密碼的「真實來源」。雖然同盟驗證可能很複雜，涉及多層重定向，但其基本概念是：一個 IdP 可以將身分驗證交由另一個 IdP 處理。

在大多數情況下，能夠透過 SAML 或 OIDC 與 IdP 整合的服務不需要知道或關心您是否與其他提供者同盟。這些細節通常在初始連接時被抽象化處理。

多重要素驗證 (MULTI-FACTOR AUTHENTICATION)

既然都提到了認證方法，接下來應該來談多重要素驗證 (MFA) 和無密碼認證。

登入憑證被盜是組織目前面臨的最大安全問題之一。根據世界經濟論壇 (World Economic Forum) 的資料，80% 的資料外洩事件都是因為密碼被盜或密碼強度不夠的問題，但用於撤銷受損憑證的支出卻不到 10%。為了解決這個問題，許多企業組織利用其身分提供者（IdP）來實施 MFA 和無密碼安全性。

IDP 可以支援多種 MFA 解決方案，其次是無密碼解決方案。傳統的 MFA 類型是以一次性密碼 (One Time Passwords, OTP) 為基礎，除了密碼之外，還需要使用者輸入一組不斷改變的數字。該數字可以由一個帶有 LCD 螢幕的小型鑰匙扣上生成或由 裝置上的應用程式生成。

為了簡化使用者體驗，許多 IdP 現在提供行動裝置應用程式，使用者輸入密碼後，會收到推送通知，並通過生物 辨識， 如 Face ID 或 Touch ID 進行身份驗證，以確保回應 推送通知的是正確的人。

另一種越來越熱門的 MFA 是 FIDO (Fast Identity Online)，它是一種注重隱私與安全的驗證方法，內建於大多數的現代網路瀏覽器中，也可以採取外部安全金鑰的形式。FIDO 和其他形式的 MFA 也可用於無密碼驗證，不需要實際輸入密碼。整個過程中都使用 MFA 即可。

Jamf 的產品支援多種 MFA 選項由於大多數 IdP 認證都是在網頁檢視中處理，因此 MFA 的所有具體配置和設定都由 IdP 本身處理。

舉例來說，Jamf Connect 可以使用 Okta Authentication API 來為使用者配置主要的 Jamf Connect 任務，例如：

- 雲端身分驗證到本機 帳戶
- 密碼同步
- 登入使用者至 Okta

請閱讀 Okta 的開發人員文件， 以瞭解更多關於此 API 的資訊。

邁向無需 VPN 的連線方式

在零信任技術之前，為了保護使用者裝置與服務之間的通訊，通常會使用 VPN（虛擬私人網絡）。雖然 VPN 對 IT 部門仍然是非常有用的工具，但也存在一些缺點：

- 大多數 VPN 需要用戶端軟體才能執行
- 可能不支援雲端身份驗證
- 通常需要專用硬體，且可能無法保護雲端服務
- 使用者在行動裝置上的體驗通常很差
- 行動裝置上的使用者體驗不佳

由於大多數使用者家中的頻寬都越來越快，要支援能夠處理使用者可能產生的流量的 VPN，可能很快就會變得非常昂貴。

零信任網路存取 (ZTNA)

零信任網路存取（ZTNA）是一種更現代的安全連線理念。ZTNA 不需要 VPN，也通常不需要客戶端軟體。反之，使用者透過網頁瀏覽器連線至 ZTNA 服務，該服務可能需要現代化驗證，然後透過代理或其他方式保護使用者的連線。

雖然 ZTNA 解決方案最初是用於保護無法使用現代化驗證的地端服務，但現在也可以用來保護雲端服務。ZTNA 解決方案可以是雲端架構，也可以部署在您的資料中心內以便掌控更多權限。隨著 ZTNA 解決方案變得越來越完善，您可以保護的不只是網頁流量，甚至完全取代 VPN。

了解 Jamf 的零信任網路存取（ZTNA）

Jamf Connect 的 ZTNA 解決方案 結合了以身分為核心的安全模型、風險感知的政策管理，以及針對應用程式的微型隧道（microtunnels），專為現代化計算環境設計。

條件式存取

穩健的零信任架構通常會包含條件存取或裝置信任的元素。在這些情況下，裝置的狀態會成為判斷是否信任該連線（以及信任程度）的因素之一。受管理的裝置能夠幫助企業組織理解裝置風險，並決定哪些受信任的使用者、裝置和應用程式，能夠存取資料與資源。

條件式存取通常由 IdP（身分提供者）與本機代理或裝置管理解決方案合作完成，檢查裝置的作業系統版本、安全政策或其他屬性來確定裝置的狀態。IdP 可根據這些資訊允許連線，或者在某些情況下要求額外的驗證（例如多重要素驗證）以完全驗證使用者身份。

條件存取，顧名思義，是根據使用者嘗試使用的應用程式來設定條件。舉例來說，存取低安全性的服務（如 IT 工單系統）可能不需要 MFA。但存取原始碼儲存庫則可能需要使用者通過 MFA，並使用公司擁有且管理的設備。

有許多廠商協助管理身分與存取服務，包括 Centrify、Duo Security、Microsoft、Ping Identity、Okta 和 Salesforce。這些工具可與現有的驗證架構（例如雲端身分提供者）協作，並使用 OIDC 和 SAML 等協議將身分延伸至雲端服務。

讓我們以 Jamf 和 Microsoft 合作實現之條件式存取為例。Jamf Pro 可透過 Enterprise Mobility + Security（EMS）條件式存取，在裝置上強制執行政策，以便存取 Microsoft Office 365。Jamf 管理的 Mac 電腦可根據 Microsoft 端點管理員（Microsoft Endpoint Manager ）的裝置合規政策來存取 Microsoft 應用程式。一旦 Mac 的資料進入雲端，Endpoint Manager 和 EMS 就能與 Jamf 完全整合，在裝置上提供管理功能。如果未管理的 Mac 嘗試存取電子郵件或其他雲端服務，IT 團隊可以啟用使用者自助註 冊 流程，確保未受保護的設備在獲得存取權限之前被納入管理。

JAMF 的條件式存取不僅支援 MICROSOFT，還支援 GOOGLE 和 AWS 等主要業界領導者。

當 Microsoft 驗證使用者憑證、Jamf 驗證裝置憑證時，會進行風險分析（包括使用者風險、裝置風險和應用程式風險），以即時決定是否授予存取雲端資源的權限。

現在，企業組織可透過已驗證的合規性，延伸多重要素驗證的方式

1. 使用者名稱和密碼
2. Code 與 Token
3. 裝置合規

這讓企業組織可以根據使用者、裝置和使用情境的具體情況，來提供合適的存取權限，以滿足現代多裝置、多位置工作的彈性需求。

端點防護

無論是現場還是遠端工作狀態，凡是透過身分識別管理實施的安全措施，都會在員工任職期間影響終端使用者與 IT 部門。SaaS 應用程式以及將員工連線至企業資源，提供了降低端點、使用者和企業資料風險的機會。

端點防護即是降低終端使用者的裝置或端點遭受惡意攻擊的風險。當資料分散在各種 SaaS 應用程式時，確保經授權的使用者將裝置和資料用於合法用途也就更加重要。為了達成這個目標，許多層面都必須共同協作 - 身份管理是其中之一，但也包括防毒 (AV)、安全配置管理、端點偵測與 回應等。

企業組織不能等到惡意軟體、廣告軟體或其他問題出現才採取行動。安全工具若對裝置造成的影響大於其保護作用，會妨礙終端使用者的生產力。組織的防毒機制應能有效識別並修復針對 Mac 的攻擊，而不是浪費資源在 Mac 上偵測本是針對 Windows 的威脅。談到安全性，需要考慮的事情有很多，但好消息是 Jamf 可以協助解決 以上所有問題。

除了 Jamf Connect 的身分管理功能和 Jamf Pro 的內建安全工具外，Jamf Protect 旨在無縫融入您組織的安全架構，以防止惡意軟體、防範針對 Apple 的威脅，以及監控端點的 合規性。

對於使用多樣化安全工具的複雜環境，Jamf 和 Microsoft 的整合提供了解決方案。IT 管理員和安全團隊能透過熟悉的單一控制面板，查看整個 Mac 裝置的安全活動。Jamf Protect 是專屬 Mac 的端點防護平台，只需最少的配置即可將所有特定的 Mac 安全性數據和警報資料推送到 Azure Sentinel 中。所有惡意或可疑的 Mac 活動以及惡意軟體通知都可以輕鬆地與預訂好的工作流程整合，您的資安團隊幾乎不需要付出任何精力和時間。Jamf Protect 的攻擊檢測和日誌記錄資料讓 Azure Sentinel 能識別並修復針對 Mac 裝置的廣泛攻擊，從而提升組織的整體安全性。

重新透過身份管理
調整您的安全態勢

很明顯地，傳統的「圍牆式安全」（perimeter-based security model）已不再是企業保護數據的主流做法透過利用許多提供身份管理的合作夥伴，企業組織可以同時實現現代化的安全性，甚至是零信任。人們的工作方式與過往不同，資料的存儲與流向也有所改變，企業組織需要現代化的解決方案來應對這些轉變。他們需要考慮裝置型安全、使用者型安全、多重要素驗證等問題。他們需要保障端點的安全。

Jamf 提供了一種將這一切結合起來的方法。更完善的安全性就從這裡開始。

立即開始免費試用吧！

或是聯絡您偏好的 Apple 經銷商。