McAfee Cloud Identity Manager

簡化及保護雲端應用程式存取

為軟體即服務 (SaaS) 應用程式加入強式驗證、自動帳戶佈建及單一登入。McAfee® Cloud Identity Manager 能藉由強制執行企業需求存取與強式驗證，協助您取得雲端應用程式的控制力，同時提供單一登入、自動佈建及合併稽核記錄的簡潔便利。

主要優點

提升控制力
- 適用於雲端應用程式的單一登入，能強制執行企業安全標準
- 強制執行上下文感知的驗證需求
- 自動、精確的帳戶佈建/解除佈建
- 自動同步身分資料以便管理變更

增加可見性
- 監視所有存取活動
- 佈建變更與服務等級協定 (Service Level Agreement, SLA) 警示

簡化的法規遵循作業
- 強制執行安全標準
- 集中管理稽核記錄與存取報告
- 孤立帳戶報告
- 可匯出的稽核報告資料

打破阻礙雲端應用程式之採用的藩籬

雲端應用程式透過寄存與彈性、可擴充的應用程式，促成新的業務與 IT 模式。然而由於安全考量，大量移轉到雲端遞送之應用程式的趨勢已有減緩的跡象。阻礙企業投入的主要障礙不外乎是喪失控制力、缺乏雲端存取可見性，以及缺乏企業管理與法規遵循的強制執行能力。

這些憂慮主要原因是因爲是企業使用者自行管理雲端應用程式的帳戶，而他們通常會使用和企業身分架構互不相連的弱式密碼。在這些不相連應用程式中的使用者動作不會受到監督或授權，因此會導致敏感資料外洩與法規遵循違規的風險。此外，缺乏標準化的記錄功能也使得管理員無法監視雲端應用程式使用者活動，也無法使活動和內部的稽核存放庫相關聯。

同盟障礙

那麼，組織要如何掌控與傳統安全模式不同的雲端環境存取權與安全性？何不將內部的存取管理系統延伸到雲端應用程式？對於安全宣告標記語言 (Security Assertion Markup Language, SAML) 等驗證與授權標準來說，這是有可能的。不過，針對仲介程式或企業與服務提供者間「同盟」信任而設計的單點解決方案亦遭遇到重大的難題 - 它們擴充的速度不足以涵蓋多個提供者。原因何在？同盟解決方案的範圍狹窄且仍然需要手動佈建帳戶、未包含授權模式，並且缺乏和現有/額外強式驗證技術整合的能力 (亦是存取敏感企業資料的必要條件)。McAfee Cloud Identity Manager 能使帳戶佈建自動化、強制執行強式授權模型，以及和現有企業身分管理系統整合，因此能突破這些障礙。

控制雲端存取的生命週期

您可以部署 McAfee Cloud Identity Manager 來保護企業使用者的 SaaS 提供者存取，以及保護部署在網路雲端中的自訂企業應用程式存取。

即裝即用的連接器

McAfee Cloud Identity Manager 管理主控台使雲端提供者提供之存取原則的檢視、編撰及控制等作業更容易。解決方案套件附有數個隨插即用的連接器，以供您連接常用的身分管理與企業平台 (如 Microsoft SharePoint)。另包含工作階段建立與帳戶佈建連接器，以供您連接常見的 SaaS 與服務提供者平台。同盟驗證與授權通訊協定乃基於 SAML、eXtensible 控制標記語言 (eXtensible Access Control Markup Language, XACML) 等標準，以及能將網際網路身分提供者 (如 Facebook) 和企業身分與授權原則連接的新興開放式驗證 (Open Authorization, OAuth) 與 OpenID 身分標準。

自動佈建
內嵌的佈建引擎提供一組豐富的帳戶佈建與解除佈建功能，因此您不再需要手動建立帳戶。您可以從企業將帳戶佈建流暢地推送到所有獲得企業使用授權的雲端應用程式。也可以從多個授權屬性來源 (支援服務佈建標記語言 [Service Provisioning Markup Language, SPML] 的佈建系統與目錄資料庫) 擷取重要屬性，並在進行更新時使其和多個雲端提供者順利同步。

行動強式驗證
雲端存取的行動性已獲得大幅度地的改善。這意味著雲端應用程式的存取必須跨越時間與地點的限制。若要從行動裝置存取 (並非從企業防火牆後方)，您需要強制執行更嚴苛的安全標準。McAfee Cloud Identity Manager 的單次密碼伺服器能藉由原則，從行動用戶端強制執行第二因素驗證。第二因素驗證可透過單次密碼 (One-Time Password, OTP) 需求來輕易地強制執行。您可以利用簡訊 (快閃記憶體或可儲存形式)、電子郵件、交談程式將 OTP 傳遞到行動電話，或使用隨附的 Pledge OTP 行動用戶端應用程式產生 OTP，完全不需要昂貴的硬體型 Token。

企業用戶端驗證
針對敏感的雲端應用程式，您也許只想允許核准的企業筆記型電腦或確認無惡意軟體的個人電腦用戶端才能存取。同盟單一登入 (或甚至強式驗證技術) 並不足以做爲允許業務關鍵雲端應用程式之存取的保障。爲了解決安全用戶端到雲端連線中最弱的一環，McAfee Cloud Identity Manager 採用第二代 Intel Core i3、i5 或 i7 處理器內建的 Intel Identity Protection Technology (IPT)。

對於使用 Intel IPT 的電腦，雲端服務提供者或企業能驗證使用者是從已知且信任的個人電腦進行登入。除了使用者名稱與密碼之外，在登入時個人電腦還會產生唯一的代碼來驗證使用者是否從註冊帳戶的個人電腦來要求存取。這項技術能獨立於作業系統之外，於內嵌的 Intel Chipset Management Engine 中發揮功效。

整合所有技術：從信任的用戶端到雲端

普遍存在的使用者存取
McAfee Cloud Identity Manager 對一般使用者的意義爲何？它意味著簡單而安全的雲端生產工具存取機制。它代表一般使用者能從任何位置，利用簡單的單一登入與安全的連線存取雲端應用程式。不再需要將寫滿密碼的便條紙貼在鍵盤上，也不再需要請求 IT 重設帳戶密碼。

管理控制、法規遵循、可見性
對於管理員來說，McAfee Cloud Identity Manager 能提供缺乏的控制元素。從單一管理主控台就能實現控制力，您可以針對雲端應用程式撰寫並強制執行複雜的角色型存取、時間、網路及位置授權原則。您可透過和記錄管理平台相關聯的帳戶解除佈建報告及彙總稽核記錄來達成法規遵循的目的。而藉由監視所有雲端應用程式與提供者平台中的使用者活動與開發人員應用程式設計介面 (API)，管理員將能取得可見性。

企業級的安全性與信任
企業能將觸角延伸到內部應用程式與私人雲端之外。McAfee Cloud Identity Manager 能簡化雲端應用程式存取的單一登入與企業安全性整合。McAfee Cloud Identity Manager 能針對需要額外安全性的應用程式，強制執行 Pledge OTP 強式驗證，而不需要昂貴的硬體 Token。它含有讓組織簡單而有效地將企業安全性延伸到雲端所需的任何工具。

類別	說明
Salesforce.com 連接器	• 同盟單一登入 • 使用 OAuth 的 Salesforce.com 資料存取 • 單一產品實例支援的多個連接器 • Salesforce Connect for Microsoft Outlook • 部署於 Force.com 平台上的協力廠商應用程式與自訂應用程式 • 自動帳戶佈建 (解除佈建)、使用者身分屬性同步化、支援分割使用者與分割設定檔
Google 應用程式連接器	• 同盟單一登入 • 使用 OAuth 的 Google 資料存取 • 單一產品實例支援的多個連接器 • 部署於 Google AppEngine 上的協力廠商應用程式與自訂應用程式 • 自動帳戶佈建 (解除佈建)、使用者身分屬性同步化、支援分割使用者與分割設定檔
自訂連接器	• 以同盟單一登入方式登入任何支援 SAML、OpenID 或 OAuth 標準的協力廠商應用程式或自訂應用程式
應用程式整合	• Microsoft SharePoint 2007/2010，.NET 2.0 與更新版本
管理能力	• 集中式的管理主控台 • 支援命令列與指令碼處理 • 生產移轉測試
憑證管理	• CRL 與 OCSP 憑證撤銷檢查
使用者與資料儲存	• 任何符合 LDAP v3 的目錄 • Central Authentication Service (CAS) 3.3/3.4.2 • 監視與稽核專用的資料儲存 (選用) • 任何支援 JDBC 的資料庫
標準	• SAML 2、OpenID、OAuth、XACML、LDAP v3、JMX
支援的硬體	• 內部部署或網路雲端 • Look-Aside 或反向 Proxy 模式 • 軟體、虛擬裝置、Amazon EC2 或支援隔離區域的硬體裝置 (在一部機器中實現雲端身分與存取管理 [IAM]) • 水平移轉以供測試生產支援
系統需求	• 瀏覽器：Internet Explorer 6、Internet Explorer 8、Firefox 3.6 • 伺服器作業系統：32 位元或 64 位元 • Red Hat Enterprise Linux Server 與 Red Hat Enterprise Linux Advanced Platform 5.0 • Microsoft Windows 2003、Microsoft Windows 2008 • 硬體需求：任何配備 2 GB RAM 的 Intel 多核心伺服器

如需詳細資訊或想開始試用 McAfee Cloud Identity Manager，請連絡 McAfee 代表或造訪 www.mcafee.com/tw/solutions/cloud-security/cloud-security.aspx。

邁克菲台北辦公室
台北市 104 南京東路三段
132 號 4 樓 A2 室
886-2-2721-7766
www.mcafee.com/tw

32100ds_cloud-identity-mgr_0711_fnl_ASD