cpl.thalesgroup.com

THALES

從傳統IAM轉移到現代化存取管理：指南與最佳實務方法

White Paper

目錄

簡介

企業面對日益嚴峻的挑戰，必須管理雲端應用程式存取、身分驗證、以及確保員工在家安全工作。傳統地端身分驗證與存取管理(IAM)方案例如企業單一登入(Single-Sign On; SSO)、虛擬私有網路(Virtual Private Network; VPN)或Web存取管理(Web Access Management; WAM)的基本概念都是維護網路周邊安全，對於員工能否安全且有效率的存取雲端服務方面可能產生一些限制。因此，對於仰賴地端安全方案以保護雲端服務的企業而言，他們的雲端延展能力將受到局限。

替代方法可以採用以雲端為基礎的身分識別服務(Identity-as-a-Service)架構，例如Thales SafeNet Trusted Access，它讓企業能夠將安全性延伸到網路周邊之外，並保護欠缺現代化標準支援的地端應用程式和公有雲應用程式。

這份白皮書的用意是要提供指南，協助企業從傳統網路基礎設施包括WAM、VPN和傳統SSO轉移到以雲端為基礎的存取管理方案，以受惠於較低的整體擁有成本、更好更聰明的安全性和強化的使用者體驗。

存取管理與身分驗證需求

企業捨棄傳統商業模式，並以快速步調展開數位轉型、擁抱雲端、多重雲與混合雲環境。雲端應用程式的採納率在這幾年急速攀升，各大小企業都轉移到以雲端為基礎的交付模式。

雖然這一開始是基於商業需求促成雲端轉移，例如無所不在的曝光率和客戶參與感，現在則大部分是因為雲端服務供應商例如Microsoft、Google和AWS，而將IT服務轉到雲端。大多數企業已採納SaaS應用程式，以開闢新的工作方式和強化員工協力。

儘管「雲端第一」策略是大多數企業的最高優先目標，但全面性的轉移可能需要經歷數年才能完成。許多企業已將一些應用程式轉移到雲端，並且繼續支援其他地端資料庫。不論一家公司有多創新，成熟的企業無可避免的存在一些仰賴前世代技術的傳統資源。

這些混合部署模式相當普遍。企業可以選擇繼續維護地端基礎設施，因為他們有一些難以捨棄的客製化資料庫和相關應用。另外，他們或許沒有適當的資源可以全力投注雲端轉移。再者，那些地端應用程式或許是他們客戶需要的，基於營收考量而無法犧牲他們。

這些混合部署的存取安全是很關鍵的，尤其是為了確保緊急狀況下的商業連續性。非計畫中的事件例如環境危機、自然災害例如地震、基於國安理由的商務閉鎖、或者人員傳染病等，可能對所有企業造成毀滅性的衝擊。企業的考驗在於能否為所有員工提供可延展且安全的遠端存取能力。

安全是關鍵

企業擁抱現代化技術和雲端運算的同時，最關鍵的就是確保安全性。針對雲端服務發動的釣魚攻擊特別突顯此一重要性，因為很多攻擊已造成大量資料外洩。為此，IT正積極尋求提供集中定義和執行存取控制的方法，以一致的方式管理雲端和地端應用程式的安全性和法規遵循狀態。

傳統上，企業仰賴虛擬私有網路(VPN)、地端單一登入(SSO)和Web存取管理方案(WAM)，例如CA SiteMinder、Oracle Access Manager和IBM Tivoli Access Manager等，以管控企業資源的存取認證和授權。

隨著雲端應用和分散式運算模式的成長，這些傳統方案已無法再滿足現代化IAM的需求。

傳統存取方案的限制

大量轉移到雲端運算和在家工作的結果，暴露了地端周邊安全上的弱點，無法確保安全存取雲端應用程式。這些弱點包括：

- 透過地端方案導引雲端存取流量，造成網路超荷和延緩整體網路流量。
- 仰賴VPN或WAM進行雲端存取的結果形成單一失敗點，而如果VPN當掉也將使得員工無法存取關鍵的雲端應用程式。
- 允許員工以一個單一認證憑證存取整個網路，而如果該憑證遭入侵，那麼從安全觀點而言將造成災難。
- 維護和擴充傳統地端方案以容納數百雲端應用程式所需的成本，遠超過建置一個以雲端為基礎的遠端存取方案。

評估傳統IAM方案能否有效解決雲端存取需求

多因子認證

傳統IAM方案傾向於以硬體或軟體代碼驗證使用者身分，但這是一種在初始登入程序時執行的二進碼決策。在現代化商業環境中，員工可能從任何地方甚至使用自己的裝置存取企業資產，二進碼決策無法匹配風險環境的身分驗證層級。為了能夠提供敏捷且分級的使用者身分驗證方法，IAM方案應提供調適性的方法，以便能夠根據使用者裝置感測器收集的脈絡資料，於風險增加時提升驗證層級。

再者，軟體或免代碼(token-less)認證方法結合簡單的自動化代碼登錄，可確保所有員工享有流暢的登入體驗。為了支援使用者需求，IAM方案應提供一系列免密碼認證方法，以涵蓋不同的需求和安全層級。

	傳統IAM (VPN, WAM, SSO)	IDaaS
無密碼	以代碼為基礎、硬體或軟體	無載具：推送OTP應用程式、簡訊或電子郵件代碼，基於模式
驗證決策方法	在初始登入點執行二進碼(是／否)決策	隨著風險增加而採調適性的升等驗證(step-up)決策

Table 1: Multi-Factor Authentication, Comparison of legacy and IDaaS IAM solutions

企業單一登入

傳統企業單一登入(SSO)方案例如Microsoft AD FS或Ping Federate都建置在地端且通常透過諸如SAML協定支援聯合身分驗證。這些方案允許使用一個在初始登入時提出的單一認證憑證執行單一登入，但如果該單一憑證遭侵入、竊取或遺失，則所有企業應用程式都將陷入風險。

為了提供零摩擦的登入體驗而不犧牲安全性，企業應運用以雲端為基礎的SSO結合脈絡資訊與升等(step-up)認證。這允許使用者以一個單一身分驗證存取他們所有雲端與Web應用程式，而這些存取是以連續方式進行驗證，讓IT團隊可以在高風險狀態維護更強的存取安全。智慧型SSO讓終端使用者可以維護商業生產力，減少多重應用程式重複認證的麻煩。

The table below provides an overview of the Single-Sign On capabilities offered by legacy and IDaaS IAM solutions.

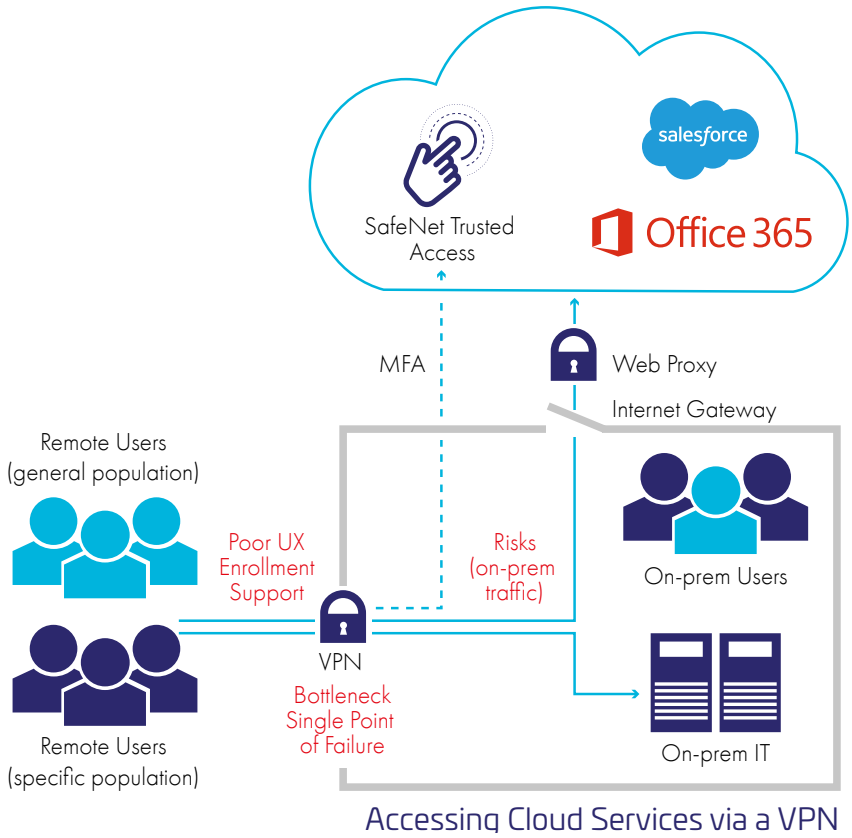
	Legacy (VPN, WAM, SSO)	IDaaS
建置	地端	雲端
聯合驗證	是	是
安全性	廣泛SSO，以相同認證憑證 存取所有應用程式	調適性智慧型SSO，單一身分 識別連續接受升等驗證評估
政策引擎	**Open Access** 一個單一存取政策適用所有 使用者和應用程式	以政策為基礎 根據每一商業需求、應用程式機敏性 和員工功能設定存取政策
認證	點認證 使用者以相同認證方法存取 所有服務	全面認證 對每一次登入實施適當的MFA 或脈絡認證

Table 2: Smart Single-Sign On, comparison of legacy and IDaaS IAM solutions

周邊控制

傳統周邊控制例如WAM、VPN和防火牆都屬於地端方案。它們透過一個地端集線器管控流量。這種設定對於地端流量而言或許有效率，但對於源自或導向雲端的流量則欠缺效率。將流量從雲端送到地端伺服器以檢測安全性和處理存取請求的做法，將形成瓶頸和產生一個單一的存取失敗點。

當員工需要從遠端工作時，現代化的方法是建置一種零信任的存取評估。企業需要確保沒有人是信任的，而且存取請求是在每一應用程式的存取點進行評估。這可以建立依據每一應用程式、每一種政策以及每一次存取而進行評估的分散式存取決策。此種服務將可以對非信任網路升高認證層級，並簡化白名單網路所需的驗證。同樣的，存取管理方案應允許依照應用程式而建立不同的認證規則。



Accessing Cloud Services via a VPN

The table below provides an overview of the perimeter control capabilities for both the legacy and IDaaS IAM solutions.

	Legacy (WAM, VPN, Firewalls)	IDaaS
存取控制	集中式，本地中心	在存取點
零信任	所有應用程式一次登入	對每個應用程式、每個政策和每個登入嘗試進行持續的存取評估
可用性	本地中心產生單點故障	從雲到雲
調試性	一次登入所有應用程序，無需升級	加強對不受信任網路的身份驗證，根據風險降低身份驗證級別
成本	擴展本地基礎架構的成本很高，需要對基礎架構和伺服器進行投資	基於雲的存取管理不需要基礎設施投資。並且包括支持和維護

Table 3: Perimeter Control, comparison of legacy and IDaaS IAM solutions

身分識別服務方案(IDaaS)支援數位轉型和節省成本

身分識別服務(Identity-as-a-service; IDaaS)是以SaaS為基礎的IAM方案，允許企業使用單一登入認證和存取控制，直接對雲端服務提供安全的存取。

IDaaS已成為絕大多數新存取管理部署的優選交付方法，因為它提供多項效益，包括：

- 藉由在存取點保護企業和雲端應用程式以降低入侵風險。
- 減少身分識別管理所涉及的複雜性，讓使用者不論在家或企業外的其他任何地方都能無縫接軌存取所需的應用程式。
- 運用雲端交付方法簡化部署。
- 加速實現價值和成本節省，無需投資伺服器以支援可持續的存取管理功能。
- 高可用性與可靠性，因為IAM服務是在雲端提供，因此免除了單一失敗點。
- 經常且容易的功能升級。

SafeNet Trusted Access如何協助企業建置現代化IAM架構

一個功能完備的IAM平台應涵蓋一系列認證情境，並且為所有企業應用程式提供鐵甲般的存取安全。SafeNet Trusted Access讓企業能以廣泛的認證功能保護企業應用程式，以及在雲端的安全延展，同時藉由智慧型SSO和政策存取控制以確保安全性。

多因子認證

SafeNet Trusted Access藉由以升等(step-up)和風險為基礎的方法提供完整的認證能力，很容易為企業的所有應用程式建置多因子認證。SafeNet Trusted Access的關鍵效益之一是支援廣泛的多因子認證，包括硬體和軟體、簡訊和電子郵件、推播通知和生物認證、以及多項認證方法包括OTP、PKI、調適性與型態認證等。

SafeNet Trusted Access支援多項認證標準，包括RADIUS、OpenID和SAML，全部從雲端交付。再者，SafeNet Trusted Access也以多種方法藉由FIDO支援無密碼認證，包括PUSH OTP、憑證認證、FIDO認證和Windows Hello。

SafeNet Trusted Access

Universal authentication methods

Utilize the MFA schemes already deployed

Extend PKI authentication to the cloud

Offer the appropriate level of assurance

Offer convenience with Passwordless authentication

Figure 1: Thales' SafeNet Trusted Access authentication methods

智慧型單一登入

SafeNet Trusted Access的政策引擎是其核心功能之一，支援以極其彈性的方式設定存取政策。安全政策可設定分級且特別的規則，於連線期間持續對使用者進行再驗證，而非只有在觸發特定事件(例如認證逾時)才執行。如果風險層級改變，SafeNet Trusted Access會迫使使用者重新認證或提升到較強形式的認證。

政策可以針對個別應用程式設定，適用於網路、作業系統和使用者資訊與地點。認證規則可視需要而設成動態和以脈絡資訊為基礎，例如，可設定在特定條件下檢查每一次的存取，例如在較風險條件下要求升高認證層級。

為了提供整合的身分識別驗證能力以執行連續且調適性的存取管理，SafeNet Trusted Access支援下述功能：

- 以脈絡為基礎的條件式存取控制。
- 應用程式及其他風險資訊源之間的整合。
- 在每個連線期間自動評估每一項互動的連續性、風險與信任，這唯有透過整合應用程式才能做到。

周邊控制

SafeNet Trusted Access源自雲端並且運用在雲端，並不需要仰賴地端基礎設施，而且是在雲端控制存取以避免出現瓶頸。再者，由於所有認證和存取管理服務都是在存取點提供，因此為分散式網路環境提供一個無周邊(perimeter-less)的安全性以建置零信任認證方法。

此種無周邊確保安全性不會因為單一失敗點而遭衝擊，而且調適性和風險型認證可適用於每一個別應用程式，不論應用程式駐留在任何地方。

下一步：從傳統IAM方案轉移到SafeNet Trusted Access

以下將提供一步一步的指南，協助將地端和雲端服務從傳統IAM方案轉移到SafeNet Trusted Access。我們知道許多企業無法大量轉移所有應用程式，因此我們建議依照特定群組需求而採分階段部署。

步驟一

釐清所有地端和雲端服務以確認何者需要保護。

步驟二

一旦掌握所有服務能見度，建議執行以下步驟：

- 評估每一服務與應用程式支援的協定，確認應用程式是否支援現代化標準例如SAML或OpenID Connect。許多企業Web應用程式內建SAML能力，但有些或許需要專屬性或非標準整合。
- 釐清經常存取這些應用程式的使用者，例如他們是否屬於特權使用者、主管級使用者或一般使用者。
- 判斷這些應用程式的機敏性，確保每一應用程式都有適切的認證層級。

步驟三

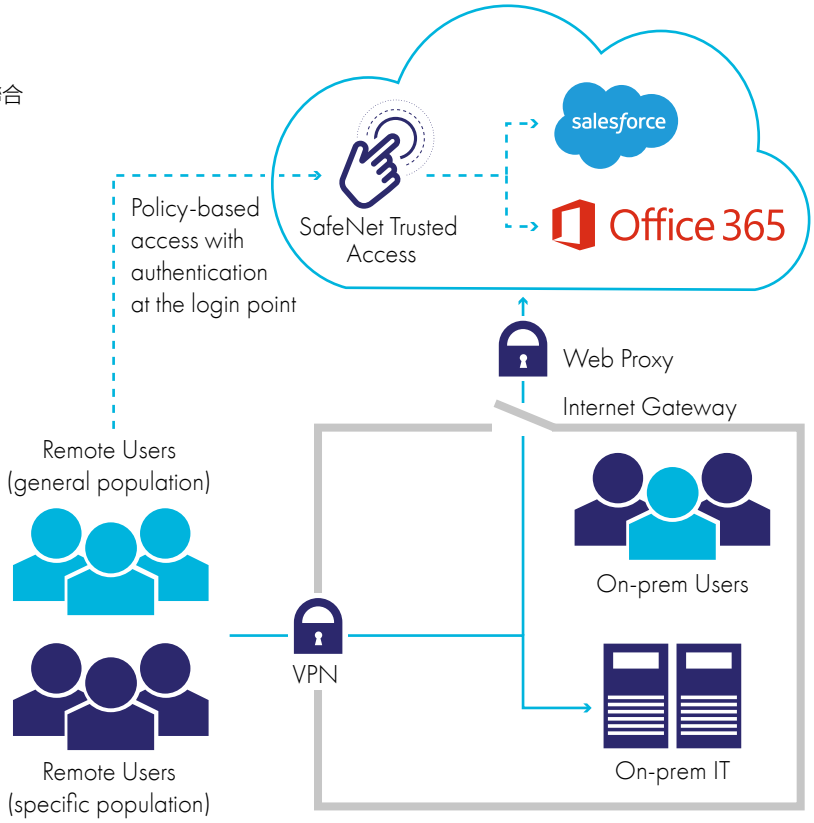
辨識每一項服務用於認證和存取控制的IAM方案，例如WAM、VPN或地端SSO。

步驟四

區分應優先建置的應用程式和使用者群組。建議將透過VPN或WAM存取的雲端應用程式以及那些使用密碼存取的應用程式設為優先。透過SafeNet Trusted Access讓大多數使用者直接存取雲端服務，將可立即減少網路流量並且能在存取點確保那些服務的安全。第二階段的SafeNet Trusted Access建置將包括為需要保護的地端應用程式設為優先，例如那些支援Radius、OIDC或SAML的應用程式。由於SafeNet Trusted Access提供聯合精靈(federation wizards)，因此這些應用程式的支援設定很簡單。第三階段是要處理那些不支援現代化聯合協定的傳統應用程式，例如透過代理或API進行整合。

部署KPI：SafeNet Trusted Access建置後的第一天

- 設定以雲端為基礎的MFA服務。
- 為第一階段優先名單的應用程式建置聯合認證，可使用聯合精靈樣板。
- 依照每一應用程式的風險評估設定存取政策。
- 監控並視需要而調整政策。



Accessing Cloud Services with SafeNet Trusted Access

結論

安全的雲端延展、員工在家工作和降低成本等，現在這些需求遠比以往更重要。事實上，Gartner調查顯示，74%公司計畫在疫情過後永久性的轉移到更多遠端工作模式，以提供行動性和降低成本。

繼續仰賴傳統身分驗證與存取管理工具將不足以支援現代化架構，而且也無法充分受惠於雲端效率。藉由建置一個以雲端為基礎的現代化存取管理平台例如SafeNet Trusted Access，企業將能加速商務發展並降低資料外洩風險，同時確保敏捷性和節省成本。

關於Thales

不論任何企業在個資保護的技術上都透過Thales 保護他們的資料。在資料安全方面，企業面臨著越來越多的決定性時刻。 無論是建置加密策略，移轉到雲端還是滿足合規性要求，在邁向數位化轉型時，您可以依靠Thales來保護您的有價資料。

關鍵時刻，關鍵技術

Thales 台灣辦公室

114 台北市內湖區瑞湖街 88 號 4 樓之 3（亞太經貿廣場C樓）
Tel : +886 2 7745 1888 ｜ Fax : +886 2 2658 3922
E-mail : apacsales.cpl@thalesgroup.com

>cpl.thalesgroup.com<

© Thales - July 2020 • JL v2