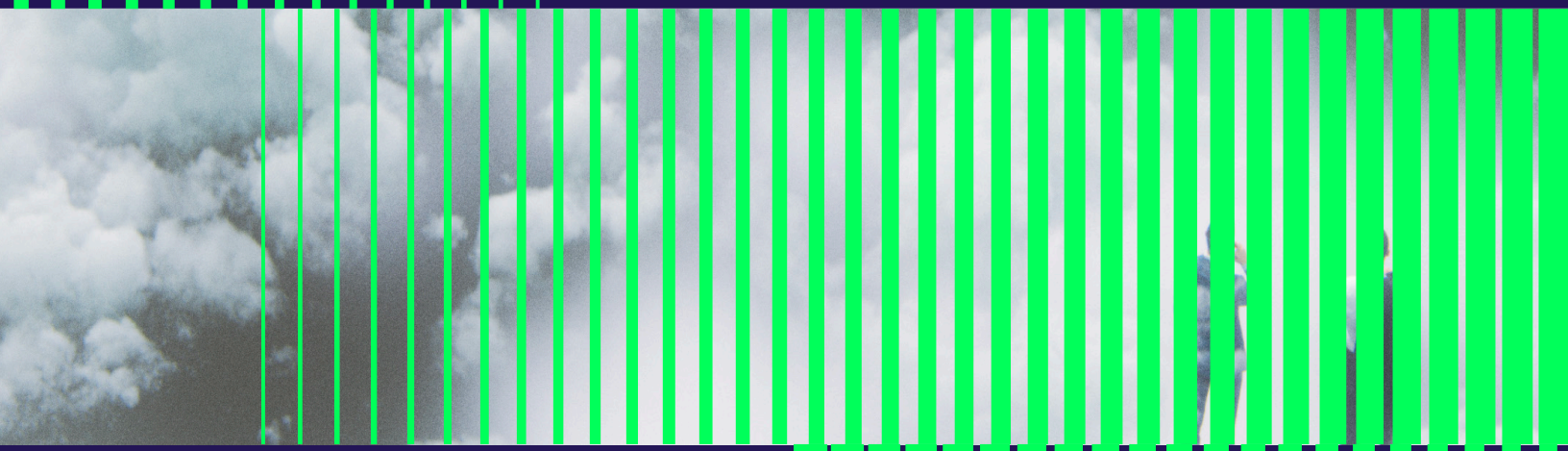
Delinea

關鍵控制

之於現代雲端安全



白皮書

執行摘要

拜雲端所賜，新高程度的速度與規模成為可能，同時也讓人員省下花在內部部署基礎設施的時間與開銷，能夠專心從事關鍵性的專案。有虛擬資源做為您的後盾支援，您再也不必於凌晨 3 點安裝和修補伺服器，維持執行時間和回應問題。

如今，因為移至雲端，所以 IT 作業和安全團隊必須更新其技能和實務，以支應更高效的新工作方式。

雲端模式之中，管理對工作負載、服務和應用程式的特權存取仍為您的責任，不在雲端供應商身上。您也有責任必須確定往返雲端的資料（經由網頁瀏覽器、電子郵件、檔案交換，例如 STP、API、SaaS 產品和串流通訊協定）足夠安全。

可惜的是，對於這類特權存取，許多組織並未充分實作並且落實上述原則。

> 存在的挑戰，不在於雲端本身的安全，而是在於安全的原則和技術，以及對技術的掌控。幾乎所有情形皆為使用者處理掌控不力，並非雲端供應商。”
>
> → Gartner Research[2]

98%

的公司在過去 18 個月內至少有一次雲端資料外洩經驗，相較於前期的 79% 有所升高。

60%

的大型企業指出存取上存在有弱點，成為雲端 資料外洩的主要根本成因。[1]

本文說明 Privileged Access Management (PAM) 如何成為現代雲端安全的關鍵控制利器。我們會談及易受特權帳號攻擊的基礎設施即服務 (IaaS)、平台即服務 (PaaS)、軟體即服務 (SaaS) 和 DevOps，細說最常見的雲端使用案例。

您可了解如何利用 PAM 舒緩全雲端攻擊面的一些最大弱點，以便發揮雲端的潛能，同時保護最敏感的資產。

1. IDC 調查報告：2021 年雲端安全形勢 (https://l.ermetic.com/wp-idc-survey-results-2021)
2. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

活動環節越多 = 風險越高

不難斷言，您若非已在雲端運作，就是有計畫遷移至雲端。

雲端技術已蔚為許多企業以及 IT 職能的核心。存取雲端服務的使用者人次、於雲端進行的活動量，以及雲端服務持有的資料量均日益增加。

這些活動都在增加攻擊面上的弱點數目和類型，許多組織正在經歷這樣的慘痛教訓。

就雲端資源授與保護傘或者常設特權存取容易招致資料外洩，無論是出於外來執行者或內部威脅。零信任方針以「恰好足夠的及時」存取權優先，將所有使用者的特權存取侷限在其所需的系統和功能，再無其他。

本文向您說明如何能夠透過角色型存取控制和權限升高，和監測並稽核人機身分的所有特權活動，以保護所有特權帳號，授與恰好足夠的權限。

以最常見雲端使用案例而言，請看風險提高的領域，並且識別 PAM 控制如何能夠提供協助。

93%

有過企業資料外洩經驗的 IT 安全和身分專家相信，若有更好的安全控制，能夠防止或盡量減輕衝擊。[3]

3. 2021 年保護數位身分安全之趨勢，IT 安全及身分專業人員調查，Dimensional Research，2021 年 6 月

保護雲端環境的 PAM 控制

1. 基礎設施即服務 (IaaS)

透過 IaaS，可迅速新增運算和存儲資源，並且按需自動擴展。此外，儲存資料的大規模「Blob 存放區」（例如 AWS S3）屬全面分散系統，因此哪怕再小的團隊也能儲存 PB 量級的資訊。

McAfee 經過分析數十億個匿名化雲端事件之後，發現 IaaS 組態錯誤的情況四起。組織於任何時點一般至少有 14 個組態錯誤的 IaaS 執行個體在運作，導致每個月平均發生 2,269 次組態錯誤事件。其中可以簡單到於設定過程忘記勾選一個方塊。

65%

的全世界組織使用某種形式的 IaaS。[4]

不受限制存取

欠缺傳入和傳出資料加密

無法開啟多重要素驗證 (MFA)

這些問題中最值得注意的是，所有 AWS S3 貯體中有 5.5% 組態錯誤。大多數組織有至少一個 AWS S3 貯體設定「開啟寫入」許可權，讓所有人都能存取而將資料注入雲端環境，包括能夠修改記錄的惡意程式碼。[4]

4. McAfee https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf

PAM 如何能提供協助

保護資料所在的工作負載。

在您向雲端供應商設定運算資源時，可以採取許多動作以便降低風險。將這些特權認證收藏在 PAM 保存庫，強制實施附有權限升高的最低權限存取控制，並且設定作業階段監測和記錄，以擷取特權活動。

限制對雲端控制台的存取。

您可從控制台或主控台存取雲端環境中的一切，包括伺服器、資料庫、傳訊及其他。這對網路罪犯來說是非常誘人的目標，必須密切管理。藉由將雲端超級使用者帳號妥為收藏，利用 SAML 型 SSO 並且於主控台登入時強制實施 MFA，PAM 能做到更高程度的身分確保。

管理對資源的持續存取。

PAM 解決方案可允許人員和資源使用系統，同時也限制其能採取的行動。利用 PAM，團隊能建立新的運算執行個體，以 SSH 或遠端桌面通訊協定 (RDP) 自動檢索認證，安全地連線到保存庫。在 DevOps 組織中，PAM 能自動高速地建立、封存、檢索和輪換密鑰。

僅於需要時升高權限。

與其授與雲端管理員對雲端資源的廣泛常設存取權，請只提供其日常工作所需的權限。其有需要時，可請求有時限的及時權限升高。

普遍套用 MFA。

經由多重要素驗證 (MFA) 確保身分，能降低伺服器資料外洩的風險。強制登入伺服器時實施 MFA，配合以一致於 Windows、Linux 和 Unix 集中管理 MFA 原則和集中報告，能讓您掌控每個系統各能供誰登入。

2.DevOps CI/CD 環境

開發團隊不再每年發佈幾次應用程式更新，改為推動頻繁微型發行，以更迅速地因應市場需求。他們便是利用雲端達成此一目的。企業有維持競爭力的壓力，可能營造生產力凌駕安全的文化。

52%
的組織使用某種形式的平台即服務(PaaS) 開發應用程式。

94%
的 IaaS/PaaS 用在 Amazon Web Services (AWS)。

78%
使用 AWS 與 Azure 兩者，可見得許多開發人員有多個帳號，需要管理及保護。

27%
使用 PaaS 的組織有資料遭竊的經驗。[5]

DevOps 團隊需要按需存取雲端型應用程式和資料庫，以管理系統及為問題除錯。開發人員經常共用對雲端服務進行程式設計性質存取時所用的 API 私密金鑰和認證，此舉提高外來與內部威脅的風險，無論是惡意還是意外。開發人員可能在所建置的應用程式內硬式編寫密碼，或是儲存在外部的 GitHub 或儲存在本機的工作表，以節省寶貴時間。這些密碼可用來存取位於雲端的資料或其他關鍵企業資源。迅速開發的實務要求針對雲端建置迅速的 PAM 實務和解決方案，並且將身分安全分層鋪陳至開發環境而不影響敏捷性。

PAM 如何能提供協助

管理對管理主控台的存取。

PaaS 資源的控制台或儀表板能閘控用於應用程式開發和部署的容器、微型服務、資料庫及協調工具的使用狀況。PAM 工具能管理、監測及記錄對此中央管理主控台的存取。

保護工具彼此通訊的方式。

整合式 DevOps 工具鏈內的工具需要能夠依照原則和閾值密切合作，以維持開發週期所要求的速度。PAM 解決方案允許開發應用程式之間經由 API 注入進行交互對話，不必人工介入，可避免錯誤和摩擦。

免除硬式編碼或程式碼中有外來認證的需要。

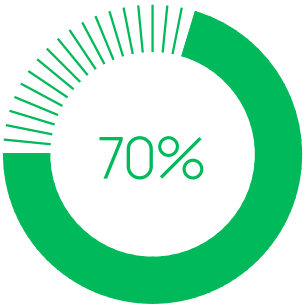
使用 PAM，可自安全保存庫提取認證，在該處可加以隱藏和自動輪換，以舒緩風險。此外，開發人員可為應用程式間的驗證取得暫時權杖（例如 OAuth2），此法較從保存庫提取靜態密碼更為安全。使用狀況亦可追蹤，以監測非預期活動。

5. https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf

3. SaaS 應用程式

1,935

項雲端服務為一般企業所使用，較前一年增加 15%，主因在於 SaaS 成長。



的商業應用程式（例如Office 365、Salesforce.com、專案管理工具等）佔此數據。可惜的是，大多數 IT 團隊認為其組織僅使用 30 項雲端服務。[6]

為何會如此懸殊？

商業團隊往往在 IT 的監督之下直接授權雲端服務。當人員難以記憶多個密碼時，可能會將認證儲存在電腦本機、Google 帳號中，或瀏覽器內。更糟的是，可能對多個工具使用相同密碼，罕見、甚至不曾變更。除了內部使用 SaaS 工具外，他們會與他人協作，可能會提供公開連結給不知名的第三者。

PAM 如何能提供協助

PAM 能為保護 SaaS 認證去除人的要素。不用多個不安全的密碼，PAM 工具允許由中央安全保存庫嚴密控制單一密鑰，於需要時針對特定存取升高一段特定時間。

保存庫能自動將認證注入 SaaS 系統，也能連線至身分管理目錄（例如 OpenLDAP）和雲端目錄（例如 Azure AD 及 Okta），提供角色型存取控制，以為不同層級的使用者管理 SaaS 功能。於是，使用者能繼續使用所需的 SaaS 工具，同時安全和 IT 團隊也具有可見性和控制力，能強制執行一致的安全原則。

單一登入的外掛程式

為達到基本程度的控制，PAM 工具只需將預存的認證注入瀏覽器型 SaaS 工具，使用者即可輕鬆登入，完成工作。

SAML 整合

作為密碼型登入的替代方式，SAML 型聯合單一登入有更佳的安全性，並可降低管理負擔。

6. https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf

Delinea

哪些是適合雲端安全的解決方案？

您已迫不及待，想要妥善地保護雲端資源。隨著業務日漸倚重雲端的基礎設施、應用程式開發和商業流程自動化，安全重點也需要調適。請採取步驟以克服組態錯誤和不一致的控制，以免允許攻擊者趁虛而入，滲透進敏感資料。

請細察雲端系統。

請稽核您的 AWS、Azure、Google 雲端平台，及其他 IaaS/PaaS 組態，以確定依照計畫設定資源。請透過測試和驗證完成確認。

需了解您所使用的 DevOps 工具是否內建有權限安全功能，以及是否符合您的期望。許多 DevOps 工具有新生、不一致或不存在的安全控制。

請徹底審查 SaaS 廠商，了解其具有哪些類型的權限安全控制，包括 MFA 和加密。

請就高效、一致的管理開發 PAM 策略。

即使多項商業和技術功能利用不同類型的雲端資源，您的安全團隊仍然可能綜覽對於全組織的特權存取，並且依照一致的原則管理這些權限。請尋找能夠密切融入不同雲端情境的 PAM 工具。優先選擇自動化和簡單的原則型控制，避免採行人力干預和繁複。

請尋找雲端原生解決方案。

採取內部部署方針，恐怕不易為 PAM 解決方案管理日漸成長的容量，維持頂尖效能。如果內部部署解決方案佔用寶貴的系統資源或是需要數小時甚至數天學習，不僅您的團隊會喪失生產時間，也可能完全迴避使用這些工具。相較之下，雲端型 PAM 解決方案能輕鬆擴展。其能順應特權帳號、應用程式和使用者的成長，不致拖慢其他資源或失去控制。

單純將軟體從內部部署資料中心「隨即轉移」至雲端，與一開始便針對雲端專門建置的解決方案，兩者之間有所差異。針對雲端設計的 PAM 能讓密鑰、雲端型基礎設施和雲端型應用程式之間更加密切地整合，能更迅速地擴展以跟上腳步，甚至配合 DevOps 團隊要求的速度。為協助您充分利用雲端潛能，請選擇雲端原生的 PAM 解決方案。

Delinea

Defining the boundaries of access

Delinea 提供以零信任、最低權限和及時權限升高等原則為基礎的縝密安全防護。若您正在考慮遷移至雲端，或是擔憂現有的雲端資源並未受到妥善的保護，請找雲端專家討論雲端適用的 PAM。

如欲進一步了解 Delinea 的解決方案，請至 **delinea.com**。