druva

White paper

SaaS 應用數據保護手冊

解決數據備份、恢復和歸檔方面的關鍵差異

Q321-20191

為什麼要備份您的雲數據？

雲架構的應用程式已成為全球企業運營的關鍵，但是，Slack、Microsoft、Google 和 Salesforce等領先的軟體即服務 (SaaS) 供應商，是否使用同樣重要的備份方案來保護其客戶的數據？他們能否在需要時快速輕鬆地復原已刪除的數據，或者直接遺失了？

有一個很大的誤解，認為雲數據是被跨 SaaS 應用程式保護，實際上如果沒有全面的數據保護您將面臨以下風險：

- 使您的組職面臨更多數據遺失、洩露和內部攻擊的風險，尤其是您有的是傳統數據保護方案時
- 需增加管理雲資產和給雲供應商費用的成本
- 延遲雲收益並增加成本
- 遭遇合規問題和審計的罰款

為了克服 SaaS 應用程式數據保護中的這些問題，企業需要一個遵循最佳實踐精神並支持新的雲工作及計劃的單一、全面數據保護策略，實施後，您的企業將能夠將資源集中在更高價值的功能上，交付預期的 SLA、提高數據保護成本的可預測性、降低數據風險並保持行業標準等。

SaaS 應用程式數據保護的不足

保留功能不能讓客戶在需要時，能隨時取得所有版本的數據及任意時間點的資料，實際上，雲服務本就不是基於為數據長期策略保留、搜索、管理和訪問而設計，雲服務供應商提供有限的備份能力服務，但通常會向客戶收取可觀的費用，即使是最少量的數據備份。
問問自己，您是否認為電腦上的回收站是一項“備份方案”？

以下是為什麼任何組職需要擁有第三方雲數據保護解決方案，備份您的 SaaS 應用程式數據至關重要，並提供主要優勢（功能和積極的業務成果）的幾個關鍵原因說明:

數據恢復

Slack、Microsoft、Google 和 Salesforce 等領先的在線服務供應商，提供全球企業運營至關重要的雲架構的解決方案，儘管，這些雲供應商通常會提供一定程度的復原功能但此類備份的用意並非在使客戶可以隨時使用所有數據，這些雲解決方案的設計是為了生產力，而不是數據恢復，並且具有備份功能的雲供應商，可能會向客戶收取可觀的費用。
一般來說，對於大多數在線服務，您單位數據的唯一備份方式是通過回收站進行的，回收站會在一段固定時間後自動清除，在那之後，您的數據將永遠消失。

> *We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services.*[1]
>
> — Microsoft

事實是，一旦您的數據被刪除、更改或損壞（無論是意外還是故意），系統管理員幾乎無法恢復它。

[1] Microsoft Service Agreement, 30 August 2019

文件共享不是數據保護

人們通常認為，因為他們使用雲架構的文件同步和共享解決方案，所以他們的數據自然受到保護，有一個老舊的思想認為“我們已經有了雲文件共享，所以就能把文件儲存在那裡然後直接收工”，簡而言之，這類型的在線服務之間存在顯著且重要的差異，雖然文件共享和數據保護技術具有一些重疊的功能，但它們的方法卻有著根本的不同，以下是你需要知道的:

- 文件共享專為用戶內容的即時協作而構建，但它並非設計用於在出現用戶錯誤、數據損壞或勒索軟體的情況下進行數據恢復。它也沒有解決存檔或合規性以及電子蒐證方面的能力。
- 企業備份軟體與文件同步和共享的不同之處在於，備份軟體會自動為每個用戶的數據製作一份副本，以便快速恢復。端點和雲應用程式數據受到整體保護，如果設備遺失或被盜，遠程擦除和地理跟踪等附加功能可幫助跟踪設備和遠程刪除公司數據。此外，備份用戶的系統和應用程式設置，確保可以快速設置新設備或更換設備，同時保留用戶熟悉的工作環境。

數據丟失的多種原因

雖然主要的在線服務供應商，極不可能因伺服器中斷而完全遺失您的數據，但還是有許多其他非常真實且頻繁發生的數據丟失原因，包括：

意外刪除和用戶錯誤 — 正常情況下，發現數據被員工刪除，可能是同一名員工或其單位後來意識到仍然需要使用已刪除的數據。例如，協作者可能不小心刪除了一個共享項目，或者您可能刪除了一個廢棄的項目，然後發現必須重新啟動它，信息也可能在不知不覺中被用戶和第三方應用程式覆蓋或損壞。

惡意行為——如果人們感覺自己將被解僱或對他們的老闆或同事發脾氣，他們通常會在辭職前刪除數據，駭客也可能是罪魁禍首，他們破除安全系統，使用勒索軟體刪除、破壞或鎖定數據，無論是公司內部或外部，這些不安的因素都可能會存在。

數據損壞——應用程式可以保存不斷更新的超大數據集，當通過批量上傳，將大型數據集導入應用程式，或使用集成的第三方應用程式管理基礎 SaaS 應用程式內部的數據時，覆蓋數據是一個常見問題，以下問題不妨您仔細想想:如果您的項目管理應用程式清除了您所有的行事曆，或用無用的、格式錯誤的消息使您的收件箱超載怎麼辦？如果您的財務報告應用程式被篡改數據或覆蓋了您的稅務記錄電子表格怎麼辦？如果您的營銷分析工具破壞了您的 CMS 數據庫，破壞了您精心編碼的所有網頁設計，該怎麼辦?

雲中的勒索軟體

如今，受勒索軟體威脅不僅司空見慣，而且還有日漸上升的趨勢。大多數企業沒有意識到的是，SaaS 應用程式同樣也會面臨勒索軟體威脅的風險，駭客不斷採用新策略並將這種形式的入侵轉化用來成熟自己的行業。勒索軟體威脅 現在影響到所有單位和企業，同時，威脅不再侷限於物理設備，這也是雲應用程式用戶主要關注的點，企業很快地發現自己對這個令人不安的新威脅感到難以理解，以及不知道如何充分規劃他們對攻擊能採取的對策。

Heimdal Security 報告稱，勒索軟體的平均費用增加到 41,000 美元，佛羅里達州的一個城市花費了 600,000 美元。由於這些犯罪分子繼續活動而幾乎沒有什麼後果，因此這些犯罪活動的頻率和嚴重性繼續增加，勒索軟體的威脅成為公司日常威脅的其中一個部分。根據聯邦調查局的互聯網犯罪報告，有近2,100 起投訴登記案，調查後發現損失超過890 萬美元，而實際數字要比890 萬美元高得多，因為報告的事件是實際事件的四分之一不到。

有什麼利害攸關的關係？

許多單位未能真正理解雲，其實雲只是用戶操作環境的擴展。雲中的數據與其他任何地方一樣容易遺失、被盜或惡意攻擊，企業仍然負責管理公司存放在雲中的數據，若不遵守規定和法規可能會導致巨額罰款，更糟糕的是，聲譽受損。

> *65 percent of enterprise data lives in collaboration and business software-as-a-service (SaaS) applications.*[4]
>
> — McAfee

單位需要考慮數據相關的可用性、合規性和安全性等三個新的面向和注意事項，以充分解決因SaaS 應用程式興起，帶來的數據保護和法規治理的差距：

確保始終在線數據的可用性 — IT 領導者和用戶之間的一個常見誤解是，SaaS 或雲數據不需要受到保護，因為 SaaS 供應商已經根據其服務級別協議 (SLA) 備份您的企業機密信息，但是，許多人不知道他們的 SaaS 供應商提供的 SLA 可能僅涵蓋供應商出現故障（例如服務中斷）時的數據遺失。 SLA 通常不涵蓋由於意外刪除、遷移錯誤、數據損壞或惡意攻擊而丟失的數據。SaaS 供應商可能無法幫助您恢復超過 30 天的已刪除數據，因為作為其標準的一部分，他們的服務會在該期限之後永久清除已刪除的信息。即使SaaS提供商願意與您合作，並且數據仍然存在，他們也可能會額外收取費用，微軟本身建議您使用第三方雲備份解決方案，而即使數據真的被恢復了，很可能在試圖恢復數據時已經失去了無數小時的生產力。

履行法律保留義務—如今，如果企業在法院提出證據開示(documentary discovery) 請求後，結果未能在訴訟期間提出儲存在 SaaS 平台上的數據，則可能面臨非常嚴重的處罰。證據開示要求企業內的法律團隊必須能夠立即訪問可能對其案件辯護至關重要的用戶數據。在許多情況下，這些數據的部分或全部駐留在 Microsoft 365 或 Slack 等雲服務中，並且可能無法全部復原。或者，它可能在整個訴訟過程中不受保護，容易被用戶刪除或不當操作。

[2] Heimdal Security, This Year in Ransomware Payouts (2019 Edition), Bianca Soare, 11 December 2019
[3] U.S. Federal Bureau of Investigation, 2019 Internet Crime Report, 11 February 2019
[4] McAfee, Cloud Adoption and Risk Report, 18 June 2019

法律上證據開示的核心是挖掘數據以識別和區隔與訴訟相關的信息的過程，這需假設信息已正確編入索引，並且搜索功能足夠靈活，此外，在早期案件評估期間，能夠看到即時結果和優化搜索變得至關重要，如果不能及時、輕鬆地訪問當前和歷史數據以進行收集和審查，可能會使單位損失數百萬美元的法律費用，甚至影響訴訟的最終結果。收集留在 SaaS 應用程式中的數據，同時以一種可以在法庭上進行辯護的方式保存和處理數據（沒有數據洩露）對於任何單位及其法律團隊都至關重要。

解決雲中的安全性和合規性問題——任何資訊安全 (InfoSec) 團隊最關心的都是與敏感度和機密數據洩露風險相關的問題。Dimensional Research 進行的一項研究表明，接近 95%的企業在雲中擁有某種形式的敏感數據，不保護這些數據的成本可能是非常驚人的，不僅顯現在監管罰款的形式上，還顯現在對企業聲譽的影響，以及由此導致的嚴重信任損失。

隨著隱私法的不斷變化，監管環境變得更加複雜，歐盟 (EU) 通過的通用數據保護條例 (GDPR) 和隱私保護證明了數據可見性的要求遠遠超出了大多數單位的要求，沙賓法案、健康保險流通和責任法案 (HIPAA) 以及新的數據隱私法規同樣迫使企業徹底改變他們獲取、儲存和保護數據的方式。

第三方 SaaS 應用程式的商業案例

SaaS 應用程式提供了一系列有價值的功能，企業每天都依賴這些功能來提高實現業務目標的效率，但是，這些強大的工具並不是解決上述關鍵問題所需的專用產品，越來越多的企業已採取行動解決最終用戶數據保護、數據復原、合法保留和電子蒐證以及存檔數據的第三方管理。

> *Organizations that assume SaaS applications don't require backup, or that the SaaS vendor's data protection is good enough, may place critical data at risk.*[5]
>
> — Gartner

slack Slack的電子蒐證法律保留

Slack 頻道與特定項目相關的對話和文件，可以成為電子蒐證特別豐富的信息來源，但是，對話是可編輯的，並且出於電子蒐證的目的，必須手動存檔或導出頻道。

- 並非每個 Slack 用戶都可以執行存檔並且存檔頻道不再共享，這可能會降低他們的日常實用性。
- 與大多數 SaaS 生產力應用程式類似，您的計劃成本決定了您可以儲存多少數據，以及誰可以管理它，除非管理員具有自己設定的保留設置（適用於某些計劃），否則一旦所有者或管理員刪除消息，它就會永遠消失。
- 通常企業對跨 IT、法律、人力資源和安全團隊的 Slack 渠道的控制會造成溝通差距，而使 Slack 數據的取證、收集和保存變得複雜。

Microsoft 365 Microsoft 365 數據復原

Microsoft 365 的核心功能雖然強大，但並非構建為滿足公司數據可用性和治理要求的綜合解決方案。

- 在 Microsoft 365 Exchange 中，刪除的項目將移動到“已刪除的項目”文件夾中，直到手動刪除或根據默認情況下為 30 天的保留策略自動將其刪除，一旦從“已刪除的文件夾”中刪除，將在復原文件夾保留最後 14天，期限過後數據將完全消失。

[5] Gartner, Assuming SaaS Applications Don't Require Backup Is Dangerous, Nik Simpson, 8 May 2019

- Microsoft 提供 Exchange Online Archiving 作為其 E3 和 E5 計劃的一部分或作為按用戶收費的單獨附加組件。這是一個僅限電子郵件的存檔選項，必須為每個單獨的郵箱設置，它不包括日曆、聯繫人或任務數據的存檔，雖然可以恢復單個電子郵件，但不提供從特定時間點復原整個郵箱。
- SharePoint Online 和 OneDrive for Business 中已刪除的項目首先進入網站的回收站，然後在93天後自動刪除，從回收站中自動或手動清除項目後，它們將轉到網站集回收站並保留設定的天數（由系統管理員指定），然後再從 SharePoint 中完全清除。

根據 Gartner 的說法，“企業不能認為 SaaS 供應商將提供備份作為服務的一部分或SaaS 供應商必須提供可以用來訪問數據的介面。”

Google應用數據復原

Google 數據保留和恢復因服務而異，因此以下是各種 Google文件中的數據保留政策摘要：

- **Gmail:** 電子郵件在將其移至回收站 30 天後或在點擊“永久刪除”後立即消失。
- **Google Contacts:** 聯繫人在刪除 30 天後永遠消失。
- **Google Calendar:** 項目一但被刪除，其全部詳細信息將無法恢復。
- **Google Drive:** 從垃圾箱文件中刪除文檔後，Google 應用程式管理員最多可以復原 25 天的資料，然而，25天後，它將永遠消失。
- **Google Sites:** 可以從已刪除站點文件夾中恢復已刪除的站點在30 天內，在那之後，該網站將永遠消失。
- **Google Account:** 帳戶只能在“刪除後的短時間內”恢復。

如果 Google 應用管理員刪除了最終用戶的帳戶，則協作者和查看者將無法再訪問該人擁有的檔案和文件，Google 用戶可以手動將選定文件的副本下載到本地 PC，但該過程的可擴展性不是特別好，並且可能難以集中管理。

Salesforce 數據復原

Salesforce 數據復原摘要如下：

- 刪除的 Salesforce 記錄可以在15 天內從回收站中恢復，然後才會被永久刪除。
- 一旦達到回收站儲存限制，Salesforce 會自動刪除最舊的記錄，前提是這些記錄已在回收站中至少兩個小時。
- 自定的刪除不可恢復，因為數據會立即從數據庫中刪除。
- Salesforce 為其企業版和無限版提供管理員導出功能，但導出只能每週運行一次，並且需要系統管理員手動下載和存檔，每週將數據儲存到本地。

如果數據在過去三個月內被刪除，Salesforce 會提供數據恢復服務，此服務的最低費用為 10,000 美元，通常需要 15 個工作日才能恢復數據。但是，元數據不包括在內，因此您可以使用他們提供的 CSV 文件將數據恢復回 Salesforce。額外的備份/恢復功能需要可以提供更多自動化的第三方解決方案，和更簡單的程序。

[6] Gartner, Assuming SaaS Applications Don't Require Backup Is Dangerous, Nik Simpson, 8 May 2019

縮小 SaaS 應用程式數據保護的差距

到目前為止，IT 一直使用人工處理、成本高昂且複雜的流程來訪問和管理數據，而 SaaS 應用程式通過徹底改變部門管理方式，和使用部分關鍵數據軟體的方式，改變了許多舊方式，但是，如果組職想要滿足當今世界的業務需求，就必須改變保護數據和管理雲數據方式。

有時部分方案可用於解決個別問題，但您必須採用一個綜合的、整合的平台來管理數據，而不管設備類型、服務供應商或物理位置如何，該平台應提供單一且集中的數據視圖，可看見已創建和儲存在SaaS 應用程式、端點和伺服器中的數據，這讓組織可以更好地進行分析、評估風險、提高合規性並滿足其他需求。因此，將所有數據源的保護整合在一個介面，是數據保護一個新興標準。

為何要運用Druva

一個功能齊全的雲數據保護方案應該解決所有用戶數據在上述遇到的挑戰，無論它們位於筆記型電腦、移動設備上，或者像 Microsoft 365、Slack 或 Google 應用程式這樣的雲服務上。

Druva 幫助一些全球的大企業或組織保護他們在 Microsoft 365、Google Workspace 和其他 SaaS 環境中的投資，用以避免受到數據遺失和合規性違規的影響，Druva 提供雲架構的數據保護服務，範圍從備份、恢復等到提供網路還原力，客戶還可以利用一系列服務，並且無需管理硬體、軟體或相關的成本和復雜性

以下是您通過 Druva 可獲得的內容：

- 獨特的雲架構和專業知識
- 備份和復原功能，以確保乾淨的副本始終可用
- 數據儲存在具有最高安全級別的實體隔離環境中，保證數據的高可用性和持久性
- 通過統一介面進行管理，使管理員能夠管理數據，而不需通過多個基礎設施
- 透明的商業模式，確保客戶擁有可預測、可控的成本
- 按數據保護的需求，允許客戶擴大和縮小規模以提高業務敏捷性

更多好處

了解並承認您的 SaaS 應用程式沒有得到完整的保護是改善數據的第一步，遵循最佳的單一且全面的數據保護策略將幫助您更好地保護和管理您的雲數據和 SaaS 應用程式。
考慮利用一個功能健全的雲數據保護解決方案，使您能夠：

- 降低 IT 預算
- 重新將 IT 重點放在創新上
- 快速響應業務需求
- 降低安全性事件發生的風險

了解如何實現全面的SaaS 應用數據保護：druva.com/products/saas-backup

druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us@druvainc.