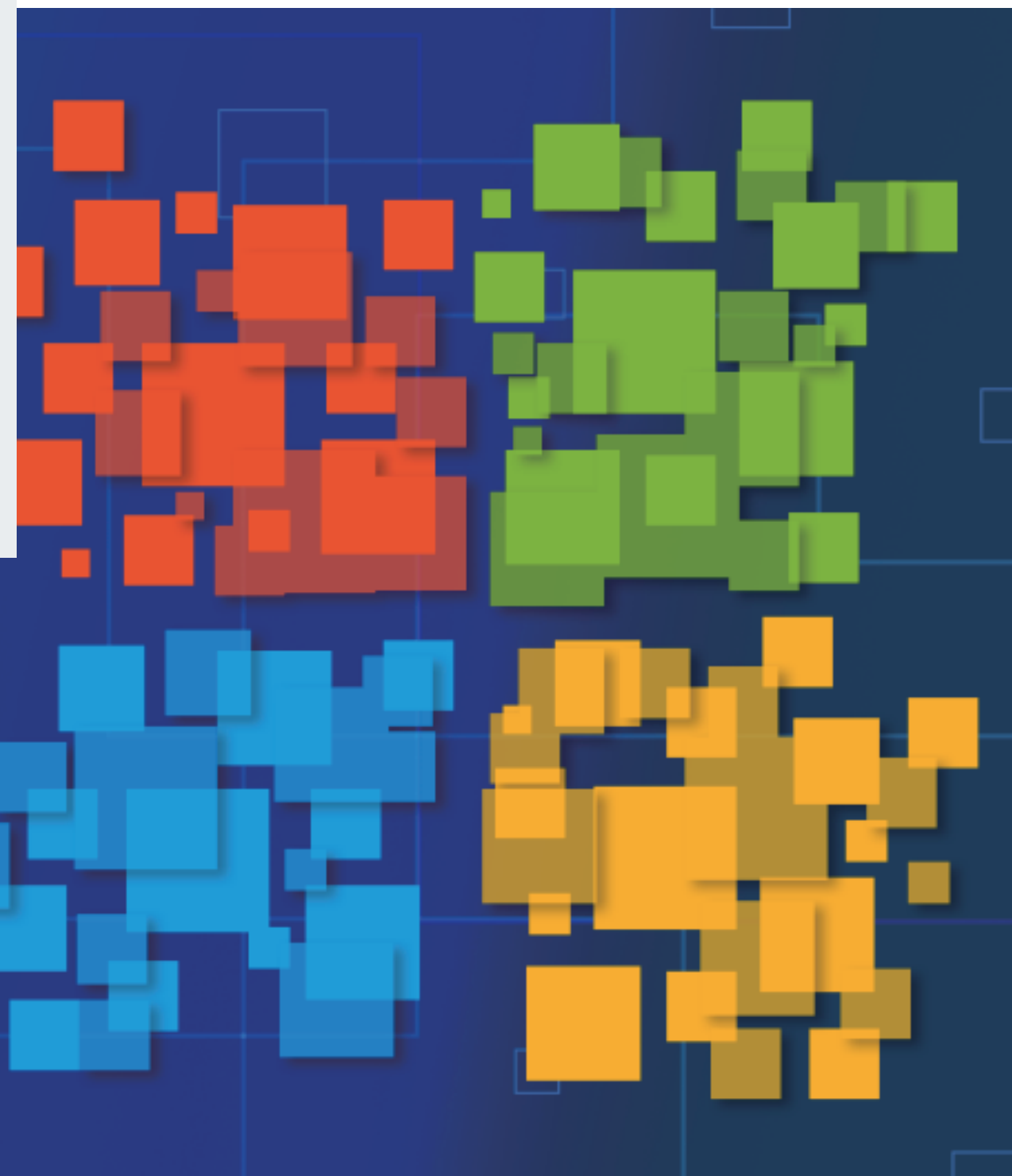




5 個 Microsoft 365 需要備份的原因

為什麼需要第三方
備份解決方案



介紹:

隨著網路的擴展，用戶使用應用程式軟體的方式發生了巨大變化，用戶無需在本機安裝程式，而是通過 Microsoft 365 (以前稱為 Office 365) 和其他 SaaS 雲端應用程式。然而，隨著 Microsoft 365 的廣泛推廣(SaaS 解決方案在雲中託管數據)，人們對其原有的數據保護功能仍感到困惑。

保護數據是您 IT 的首要任務之一，但是，Microsoft 365 應用程式 (例如 Sharepoint、OneDrive 和 Exchange Online) 的備份和還原功能通常是 Microsoft 365 被誤解的一個觀念：Microsoft 本身在其服務內容中提到

“我們建議您定期備份您在 Microsoft 365 上產生的內容和數據，或是使用第三方應用程式儲存數據。”

¹ 8/30/2019, <https://www.microsoft.com/en-us/servicesagreement/>

這份文件解釋了 Microsoft 365 數據的五個重要風險以及如何減輕這些風險：



1 Microsoft 365 數據容易出現人為操作錯誤



2 預防勒索軟體威脅的機制不充足



3 資料保留不完善將面臨不合法規的風險



4 電子蒐證和訴訟保全之功能性不足



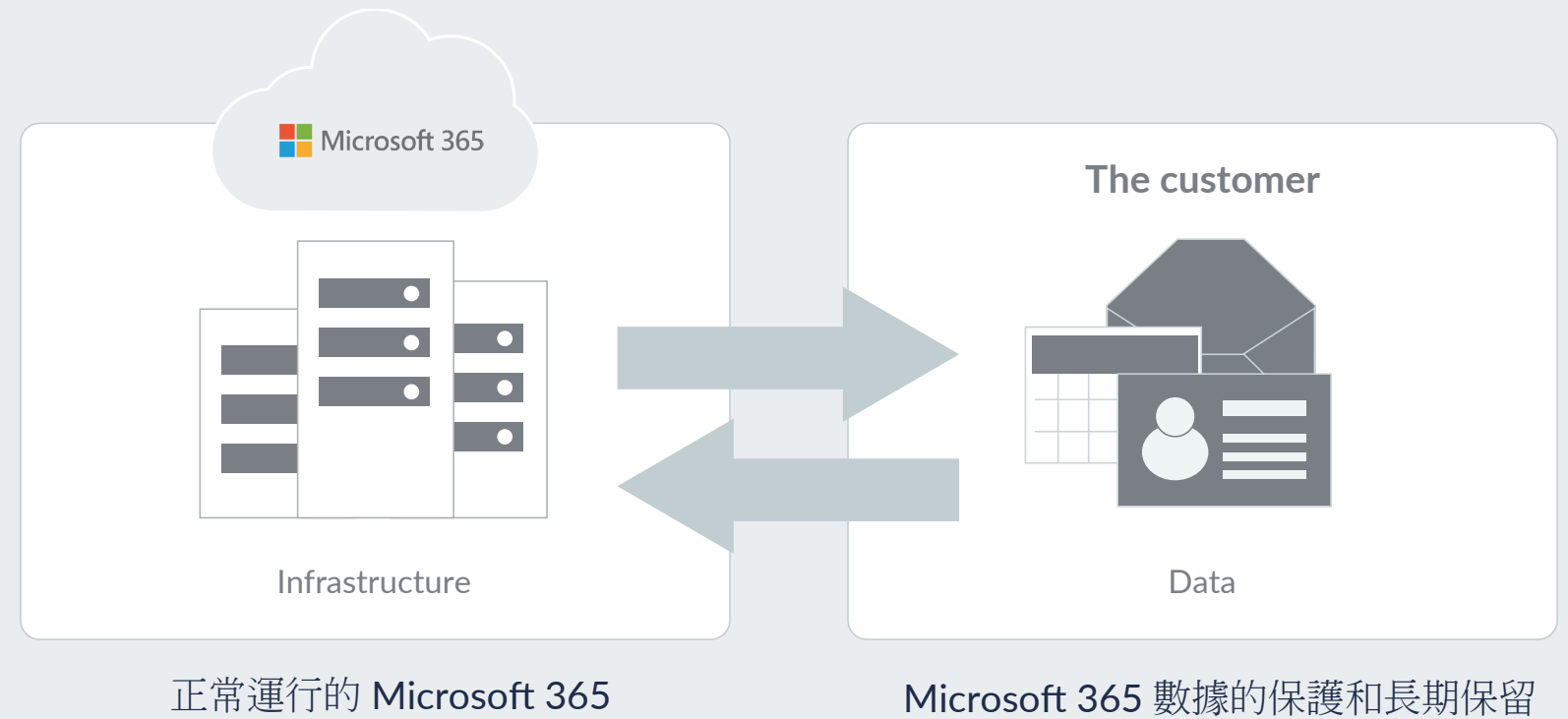
5 內部威脅增加數據風險



Microsoft 365 是一款很好的產品，可以滿足許多業務需求，用於安全、歸檔、數據保護、加密和其他基本業務流程，但它有一些特性和功能不齊全，在使用之前必須先行了解。

有許多第三方解決方案處理這些問題有更好的辦法，應由決策者評估和考量後決定執行方案。

— Osterman Research





1 Microsoft 365 數據容易出現人為操作錯誤

確保數據在發生意外時受到保護

個人或者管理員有時會意外刪除文件、在創作和協同作業時覆蓋原文件，或不正確地同步文件，這可能會導致數據毀損。甚至整個團隊的部分數據也可能被無意中刪除。總之，如果沒有真正的 Microsoft 365 備份處理方案，您寶貴的數據很容易遺失。

通常這種情況下，辦公室人員可能直到幾個月後才意識到他們的關鍵業務數據不見了。例如，一個善意的實習生在整理文件系統，並將大量舊項目數據移動到回收桶。然後將文件永久刪除，他認為正在節省公司的儲存空間和金錢。幾個月後，在實習的 Microsoft 365 帳戶被停用後，另一個部門急需用到被誤刪的數據。不幸的是，這種情況下，數據很可能會永遠丟失。

相反，借助高效的第三方 Microsoft 365 備份方案，您可以實現下列差別：

- 設定固定的時間點備份和無限的數據保留，對比 **Microsoft 365** 有限數據保留功能
- 大批量還原，和細化時間點還原，對比 Microsoft 365 提供的有限恢復選項
- 與 Microsoft 365 的恢復時間相比，更快速的恢復和自助服務選項，滿足了 SLA 的要求

因此，下次您的業務關鍵數據被意外刪除時，專屬的第三方備份和恢復方案在一旁協助你，您將無需再擔心。



原生雲的數據保護和管理為我們
IT 團隊經常遇到的問題提供了解決方案。

— IT Director, San Jose Sharks



2 預防勒索軟體威脅的機制不充足

為網路彈性及保持業務發展做好準備

如果您是企業IT 團隊的管理者，您就會知道勒索病毒是一個可能一直存在的威脅。例如，主管隨意點擊一個看似無害的鏈接，或者訪客插入一個受感染的隨身碟。除了防毒軟體和一些保護性硬體，您還必須為網路還原性做好準備，並建立足夠的IT恢復措施，以確保您的數據可以被可靠且快速地批量恢復。因此，企業員工和企業可以在勒索病毒攻擊之後繼續運營。

如果，只要求企業員工手動復原可能已受到污染的個別文件，並不是完善的處理辦法，且由於員工無法工作，您的企業每秒鐘都在損失金錢。

有效的 SaaS 備份處理方案可以完成 Microsoft 365 無法做到的事情，從而實現以下數據保護：

- **可靠**— 快速檢測首次發生攻擊的時間並確定哪些文件被感染。
- **全面**— 恢復大批量文件夾就像恢復單個文件或電子郵件一樣簡單快捷。
- **安全**— 一項基本的安全規則就是在本地之外保有另一份副本。
- **快速**— 勒索軟體會造成廣泛的損害，要確保企業營運，需要由IT人員快速的恢復到最接近時間點數據

如果發生勒索病毒的攻擊，您使用的第三方備份將準備好處理方式。



在很早期，當我們註冊 Microsoft 365 時，我們就知道我們希望能夠擁有一個第三方備份。

— Director of IT Operations, Workforce Software



3 資料保留不完善將面臨不合法規的風險

通過彈性且無限制的資料保留來滿足合規性的要求

您的組織必須遵守州和聯邦法規和公司數據治理政策。

這就是數據保留發揮重要作用的地方。例如，某些行業（醫療保健）有義務將數據保存七年以上。（美國）

有些檔案需要永久保存，如：具有重要歷史或社會文化保存價值者...等。而金融機構對國內外交易之所有必要紀錄，也至少需要保存五年。（台灣）

可惜的是，Microsoft 365 資料在保留期限和策略方面並不能完全滿足您的需求。

它僅提供 30-93 天的最長保留期，並將審核日誌保留 6 個月。

由於 Microsoft 365 提供侷限的保留方案，將使得企業很難遵守法規的要求。

但是，當您擁有第三方解決方案時，您將：

- 獲得無限的數據保留選項
- 簡化保留設置並消除複雜性
- 在無限的數據保留下，可隨意的審查歷史紀錄

縮小 Microsoft 365 數據保留和合規性的衝突，讓您的企業組織完全滿足法令規章的要求。



像 Microsoft 365 這樣的應用程序通常不會為您提供足夠的備份、合規性或其他關鍵功能

— Director of IT and Cloud Operations,
Frontier Silicon Ltd.



4 電子蒐證和訴訟保全之功能性不足

確保有支援端到端的訴訟保全

為了遵守電子蒐證和訴訟保全的要求並避免代價高昂的罰款，法務部門必須確保整個企業的所有相關案件的數據都受到保護，不會被意外刪除，並且可以快速查閱。

在 Microsoft 365 中，恢復這些數據可能費工又耗時，還需要中斷用戶服務。價格較高的 Microsoft 365 enterprise 提供了一些訴訟保全功能，但它們僅限於 Microsoft 365 數據。這是 Microsoft 365 不足的一個領域，因為受訴訟保全約束的數據，可能留在其他應用程式或是在不被支援的終端設備上。

Microsoft 365 在格式、速度和批量復原方面也有限制。受限的 Microsoft 365 數據保留策略和預設的設置，也可能妨礙您提供關鍵內容的能力，包括離職員工數據或者故意刪除的數據。最後，Microsoft 365 不提供電子蒐證工具的快速整合。所以，您的組織可以做些什麼來滿足電子蒐證和訴訟保全要求？

備份解決方案：

- 提供全面的訴訟保全支援，沒有數據保留限制。
- 整個企業自動完整地收集數據，而不只是 Microsoft 365 數據，並且不打擾員工。
- 支持更快的輸出速度、多種文件格式和大批量保管。
- 輕鬆整合第三方電子蒐證工具。

有了第三方備份的解決方案，您的法務部門將隨時做好準備。



[雲數據保護] 為我們提供完整的數據可見性和 24 X 7 的存取...

— Head of IT, Policy Services



5 內部威脅增加數據風險

預防員工離職時數據遺失

當員工離開您的公司時，關鍵的商業資料會隨他們一起離開嗎？您是否知道寶貴的資料可能已被刪除或篡改？離職員工可能會刪除、隱藏或篡改重要數據的情況並不少見。在許多情況下，這些行為可能在離職幾個月前就開始了，如果沒有適當的備份解決方案，就無法提供保護或進行徹底的資料調查。

不幸的是，在員工離職時，單獨歸檔用戶的郵箱或 OneDrive 並不是一個有效的解決方案，因為那時已經失去知識產權。

您的組織也無法查看事件的歷史記錄或數據遺失的程度。

真正的第三方備份解決方案，您將能夠：

- 通過連續備份和無限制的數據保留，持續不斷地獲取數據（包括已刪除的文件或版本）。
- 在Microsoft 365 之外隔離歷史數據的副本。
- 將數據集還原回管理者或甚至在 Microsoft 365 之外。
- 使用內建搜索和分析功能進行數據調查和取證分析。

當您準備好上述所有功能時，您將擁有面對內部威脅影響時所需的一切，來阻止資料的遺失。



[為Microsoft 365 安排合適的備份]，用戶無需擔心刪除文件，因為只需點擊一下即可復原。

— System Administrator, Wave Computing

Microsoft 365 需要第三方備份解決方案

一個全面、可擴展且經濟高效的 SaaS 平台可保護 Microsoft 365 數據和其他工作負載免受重大威脅，如：意外刪除、文件損壞、內部攻擊、勒索軟體，和不合法規的數據保留、訴訟保全和電子搜證等等而受到影響：

1. 如果用戶覆蓋或遺失數據，它能夠快速恢復。
2. 如果勒索軟體破壞了數據，則可以隨時使用原始、未受感染的版本。
3. 如果產業法規規定了數據保留，那麼您將明白無限保存的重要。
4. 如果訴訟需要，您可以立即取得用戶數據。
5. 如果有惡意的員工隱藏或刪除數據，你已安全地做了備份。

正確的第三方備份解決方案可完成上述所有工作，同時在實體隔離環境（Microsoft 365 環境之外）中提供真正的數據隔離——從風險和合規性的角度來看，這至關重要。

完整補強 Microsoft 365 的數據保護方案：druva.com/microsoft365



銀興科技股份有限公司
電話：02-8792-6128
sales@silvershine.com.tw

客戶若想進一步了解，SaaS架構雲端備份平台、觀看產品Demo、進行POC，銀興科技歡迎您來聯絡！



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

Americas: +1 888-248-4976 Japan: +81-3-6890-8667
Europe: +44 (0) 20-3750-9440 Singapore: +65 3158-4985
India: +91 (0) 20 6726-3300 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](https://druva.com) and follow us [@druvainc](https://twitter.com/druvainc).