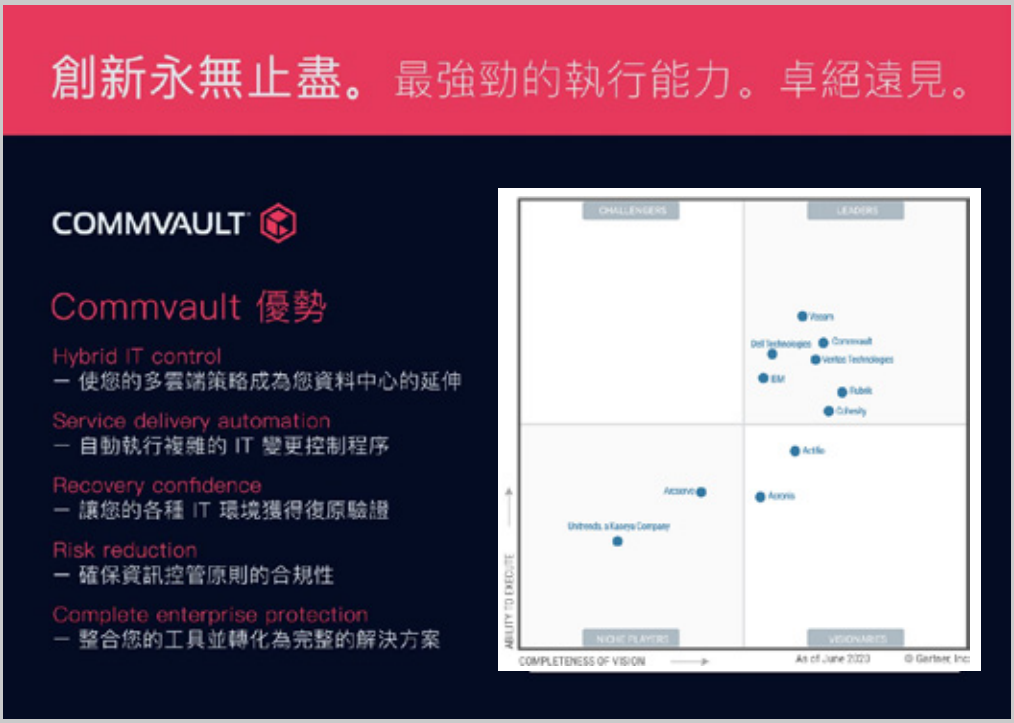
COMMVAULT

關於 Commvault

Commvault 為全球知名資料備份及管理的領導廠商，蟬聯 Gartner 評鑑連續九年領導地位的企業級備份還原軟體，Commvault 有著一體化的前瞻視野，並堅信一定有更好的方式來滿足當前及未來對於資料及資訊的管理需求，這樣堅定的信念一直引導著 Commvault 發展一體化資訊管理（Singular Information Management™）解決方案，Commvault 為複雜存儲網路提供高性能的資料保護，一致的可用性和簡化的資料管理。

Commvault 追求創新，始終如一，期許成為企業最強力資料管理伙伴。



Commvault Complete™ 備份和復原

您現有的備份已不敷使用！不管是缺乏自動化導致回應時間變慢、無法以符合成本效益的方式擴充、縮減、缺少對當今現代雲端環境的支援，或是無法符合 GDPR 等治理法規的要求，過時的解決方案都無法滿足您當前的需求。

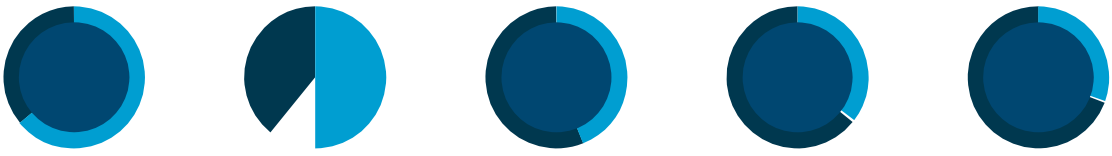
儘管存在這些挑戰，您的資料價值仍在不斷提高，保護您的資料比以往任何時候都更加重要。您需要一個解決方案，讓您的公司能夠創新和發展，同時保持業務不間斷運作，主動實現快速變革，並在法規轉變的情況下應用有效的治理。此外，您需要解決方案來降低管理複雜性，同時以和當前解決方案相同或更低的成本交付。

最終，您需要一個備份和復原解決方案，協助您因應這些挑戰，並提升您在下列領域做出回應的能力：

- **復原整備度**：當業務詢問您面對災難時復原的準備情況，您的回應是什麼？
- **資料控管**：您如何遵守複雜的資料隱私和保護法？
- **瞬息萬變**：您能以多快的速度回應業務和職涯的變化？
- **管理複雜性**：您如何正確管理遠端、實體、雲端和虛擬環境？
- **最佳化成本**：您如何成功最佳化目前和未來的基礎架構利用率？

Commvault Complete™ 備份和復原包括執行備份、復原和歸檔活動、啟用營運報告和執行硬體快照管理所需的一切元件，所有這些功能都包含在一個完整的解決方案中。

使用 COMMVAULT COMPLETE™ 備份和復原，您可以：				
每年的意外停機時間減少	合規暴露和稽核失敗、資料竊取和違規的風險降低	資料基礎架構、軟體和服務的年度支出減少	資料保護或備份工具的數量減少	與資料保護、儲存和資料管理作業相關的每週管理時間減少
62%	**50-61%**	**44%**	**36%**	**31%**
IDC, 量化 Commvault 軟體的商業價值：全球客戶調查分析				



此外，隨著公司的發展和需求的擴展，您可以透過自動化和協調流程 (Commvault Orchestrate™) 簡化災難復原、開發和測試，以及工作負載移轉；您可以擷取資料洞察，以獲得更好的資料控管和業務成果 (Commvault Activate™)，您可以使用軟體件定義的水平擴充架構 (Commvault HyperScale™ 技術)，充分利用內部部署雲端的成本和規模效率。

Commvault Complete™ 備份和復原		Commvault HyperScale™	Commvault Orchestrate™	Commvault Activate™
備份和復原		基礎架構	服務交付	資料控管
功能： • 完整的備份和復原 – 所有檔案、應用程式、虛擬機器 • 檔案/虛擬機器封存 • 加密 • DR – 容錯移轉/容錯回復/轉換 • 硬體快照管理 • 複寫和虛擬機器即時同步 • 備份操作報告 • 企業磁帶管理和追蹤 • 檔案共用	使用者授權： • 端點資料保護 • 信箱保護	內部部署水平擴充備份和復原基礎架構提供「類雲」的規模、成本和靈活性。	在任何環境中佈建、同步和驗證您的資料，以滿足重要的 IT 需求，例如應用程式災難復原測試、開發/測試和工作負載移轉。	擷取資料洞察，以獲得更好的資料控管和業務成果。

可延伸 COMPLETE 以解決客戶擴充/縮減和複雜性挑戰

COMMVAULT COMPLETE™ 備份和復原的主要功能

類　別	功　能	註　解
核心資料基礎架構	將受保護的資料儲存在磁帶和磁碟上，包括整合式重複資料刪除和加密支援，同時支援所有基本備份和復原功能。	許多競爭對手的解決方案推薦使用昂貴的專用應用裝置來解決加密和/或重複資料刪除問題，因為它不是標準功能。
	使用雲端儲存提供者 (例如，Amazon AWS、Microsoft Azure、Oracle Cloud、Google 和許多其他提供者) 儲存受保護的資料。	某些廠商針對在雲端中儲存和管理資料收取費用。有些則僅支援有限的雲端儲存。 Commvault 的原生雲端整合能力，則無需昂貴的第三方解決方案和/或雲端閘道。
	提供備份和復原基礎架構作業的完整視圖。	許多解決方案對營運報告收取高額費用和/或提供比 Commvault 更少的功能。
伺服器、NAS、虛擬和雲端工作負載	Commvault Complete™ 備份和復原支援所有檔案系統、企業應用程式和虛擬平台 (請參閱支援的技術清單)。	許多廠商要求另外付費來保護某些應用程式和/或檔案系統。在許多情況下，這些廠商需要第三方解決方案來提供功能，因為他們沒有這些功能。
INTELLISNAP® 快照管理和複寫	在次要位置建立即時資料的複寫副本。	某些廠商需要另外購買授權或推薦用第三方的解決方案。
	與業界領先的眾多儲存陣列整合，進而從這些快照執行快照和備份作業。	許多解決方案提供與硬體快照引擎的整合，但某些解決方案需要另外收費才能整合快照進行備份。
使用者特定的工作負載	讓您的端點使用者可以保護和復原資料，甚至與他人共用資料。	許多解決方案提供端點資料保護，但檔案共用通常是另外計費或與是另一套單獨產品。
	保護和智慧封存儲存在內部部署和雲端中信箱內的使用者資料，以及其他使用者資料存放庫，例如 OneDrive for Business、SharePoint Online、Google Drive 和 Salesforce.com。	信箱備份和信箱封存通常是獨立產品。少數廠商提供在單一套件中對 Microsoft 0ffice365 和 Google Mail / Drive 的全面保護。這些功能通常需要另外購買。

Commvault Complete™ 備份和復原支援全面的雲端備份

雲端備份和復原功能是資料保護總策略的重要組成部分。
Commvault Complete 備份和復原可在雲端和本機位置提供快速有效的資料保護。

瞭解針對檔案、應用程式、資料庫、虛擬平台以及最廣泛雲端儲存選項（包括 Amazon AWS、Microsoft Azure、Google 雲端平台和 Oracle 雲端基礎架構）的全面備份和復原支援。Commvault 可為單雲端或多雲端、本機工作負載或僅限雲端的工作負載等進行雲端備份和復原。

豐富的雲端備份和復原選項

Commvault Complete 備份和復原可為您提供強大控制力，以管理雲端備份和復原。

- 針對檔案、應用程式、資料庫、虛擬機器的全面備份和復原
- 歸檔檔案和虛擬機器
- 加密動態資料和靜態資料
- 對資料進行壓縮和重復資料刪除操作，以更低成本移動工作負載
- 災難復原
- 硬體快照管理
- 複寫和虛擬機器增量複寫
- 透過 Commvault Command Center 提供備份運作狀況報告
- 檔案共用

面向當今業務需求的雲端備份和復原

藉助 Commvault Complete 備份和復原所提供的雲端資料保護選項，您可以輕鬆應對當今不斷變化的商業環境。

- 全面瞭解各種資料儲存位置：本機資料中心、公用雲端和私人雲端
- 適用於混合 IT 環境的一致的服務層級協定
- 透過始終如一的戰略資料管理規範實現 IT 敏捷性
- 適用於雲端和本機工作負載的策略控制管理。

從雲端備份到資料靈活性：如何建立更強大的雲端

Commvault 是全面的資料管理解決方案，用於在本機和雲端位置中移動、管理和使用資料。
建立功能強大的混合 IT 環境：

- 向雲端中備份和復原
- 在雲端中備份和復原
- 雲端與雲端之間的備份和復原
- 實體到虛擬、虛擬到虛擬、虛擬到實體、實體到雲端、雲端到雲端的支援

全面的雲端備份和復原

Commvault 軟體支援跨公用雲端和私人雲端的 40 多種雲端儲存選項。
請參閱 Commvault 支援的技術的完整清單：雲端儲存選項、Hypervisor、資料庫、應用程式、檔案系統等。

aws Microsoft Azure Google Cloud ORACLE Cloud

項次	原廠料號	產品描述	產品說明
1	CV-BKRC-VM10	CVLT Backup & Recovery for Virtual Machines, Per VM (10-Pack)	虛擬機器備份、恢復以及歸檔
2	CV-DR-VM10	CVLT Disaster Recovery for Virtual Machines, Per VM (10-Pack)	虛擬機器複製 (LiveSync IO、LiveSync Direct、LiveSync)，以及錯誤切換等相關功能
3	CV-DP-VM10	CVLT Complete DP (Data Protection) for Virtual Machines, Per VM (10-Pack)	虛擬機器備份和 DR
4	CV-ED-VM10	CVLT eDiscovery for Virtual Machines, Per VM (10-Pack)	虛擬機器 eDiscovery 功能
5	CV-SD-VM10	CVLT Sensitive Data Governance for Virtual Machines, Per VM (10-Pack)	虛擬機器敏感性資料管制功能
6	CV-FO-VM10	CVLT File Optimization for Virtual Machines, Per VM (10-Pack)	虛擬機器檔存儲統計、分析及優化
7	CV-BKRC-FT	CVLT Backup & Recovery for Non-Virtual and File, Per Front-End Terabyte	資料庫及檔案備份、恢復以及歸檔 (前端容量計價)
8	CV-UBKRC-FT	Commvault Backup & Recovery For Non-Virtual File and Object Data, Per Front-End Terabyte, Perpetual	檔案備份、恢復以及歸檔 (前端容量計價/不做資料庫備份)
9	CV-DR-FT	CVLT Disaster Recovery for Non-Virtual and File, Per Front-End Terabyte	資料庫及檔複製 (CDR、VBR、LiveSync、DB克隆)， 以及錯誤切換等相關功能。 (前端容量計價)
10	CV-DP-FT	CVLT Complete DP (Data Protection) for Non-Virtual and File, Per Front-End Terabyte	具有備份和 DR (前端容量計價)
11	CV-ED-FT	CVLT eDiscovery for Non-Virtual and File, Per Front-End Terabyte	文件 eDiscovery 功能 (前端容量計價)
12	CV-SD-FT	CVLT Sensitive Data Governance for Non-Virtual and File, Per Front-End Terabyte	資料庫及檔案備份敏感性資料管制功能 (前端容量計價)
13	CV-FO-FT	CVLT File Optimization for Non-Virtual and File, Per Front-End Terabyte	檔存儲統計、分析及優化 (前端容量計價)
14	CV-BKRC-C-OI	CVLT Backup & Recover for Non-Virtual & File 500GB Capped Operating Instance), Per OI	以OI (實體機) 為單位，每個 OI 限制 500GB 前端容量
15	CV-BKRC-MB	CVLT Backup & Recovery for Mail and Cloud Applications, Per User	郵件及雲應用備份、恢復以及歸檔
16	CV-ED-MB	CVLT eDiscovery for Mail and Cloud Applications, Per User	郵件及雲應用 eDiscovery 功能
17	CV-SD-MB	CVLT Sensitive Data Governance for Mail and Cloud Applications, Per User	郵件及雲應用敏感性資料管制功能
18	CV-BKRC-EP	CVLT Backup & Recovery for Endpoint Users, Per User	終端資料備份、恢復以及歸檔
19	CV-ED-EP	CVLT eDiscovery for Endpoint Users, Per User	終端資料 eDiscovery 功能
20	CV-SD-EP	CVLT Sensitive Data Governance for Endpoint Users, Per User	終端資料敏感性資料管制功能

WHITEPAPER

COMMVAULT

四種針對勒索軟體攻擊的保護和恢復方法

以醫療機構為例–保護臨床資料以保障醫療品質

針對醫療機構的勒索軟體攻擊事件不斷增多。這已成為網路罪犯的一棵搖錢樹，因此攻擊次數每年都在上升。在攻擊成功後，醫療機構就無法存取重要的電子檔，從而影響對病人的治療。為了恢復存取，醫療機構只能支付贖金並祈禱對方確定會解鎖檔案，或者嘗試臨時進行資料還原，但無法保證能夠可靠的還原最新的資料。為了保護臨床資料以保障醫療服務品質，醫療機構需要採取以下四種最佳保護和恢復方法，以防禦勒索軟體的攻擊。

四種防禦勒索軟體攻擊的最佳方法

實施多層安全性原則，包括防惡意軟體、個人防火牆、硬碟和檔案加密、資料 外洩防護（DLP）等，這一點對於預防日益加劇的網路安全威脅至關重要。但即使採取所有這些終端保護解決方案，仍有一定的機率遭到入侵。根據Gartner終端保護平台魔力象限報告[6]，"44% 部署了 EPP（終端保護平台）解決方案的客戶被成功入侵，顯然這個行業並未實現阻止惡意攻擊這一主要目標。"

為了防範醫療機構遭受勒索軟體的攻擊，建議採取以下最佳措施　：

一. 制定有效的資訊安全計畫

如果您所在的機構不熟悉資訊安全或者只實施了一部分資訊安全措施，請考慮採取表 2 中的步驟以落實有效的安全計畫：

步驟	措施
瞭解關鍵資料的保存位置	瞭解資料位置 · 資料中心。 · 遠端設施。 · 雲平台。 · 各類託管服務提供者。
資料清點及整理	· 瞭解哪些系統負責處理敏感性資料，包括保存、處理和傳輸。 · 瞭解資料流程走向。 · 確定哪些系統會對您的運營產生最大風險。
評估風險	· 包括電子記錄、物理介質以及關鍵系統、服務或設備的可用性。
採用安全控制措施	· 包括電子記錄、物理介質以及關鍵系統、服務或設備的可用性。
評估效果	針對不斷進化的威脅做好準備 · 主動評估基於風險的資訊安全性原則、採用的安全控制措施是否有效，以及安全技術是否得到了合理的實施。 · 針對發現的問題及時採取糾正和補救措施，並進行經驗總結。
教育員工	· 開展員工教育，確保所有人瞭解在收到帶有可疑附件或連結的未知來源郵件時的處理方法。

表2) 有效安全計畫的組成部分

6　Gartner 終端保護平臺魔力象限，2016 年2 月1 日

二、通過最佳技術手段保護資料

隨著威脅數量的增加以及攻擊手段的升級，醫療機構需要清晰的瞭解，為了避免丟失重要資料進而影響醫療工作，需要在網路安全和員工教育方面付出一定的投入。

網路安全是抵禦勒索軟體攻擊的第一道防線。通過實施有效的最佳技術措施，醫療機構可以進一步加強對關鍵資料和IT基礎設施的保護。表3列出了有助於避免勒索軟體攻擊感染的關鍵技術策略。

步驟	措施
探測和預防	部署全方位的安全解決方案 · 防禦基於檔案的安全威脅（傳統防毒軟體）、下載防護、瀏覽器保護、啟發式技術、防火牆和檔案信譽評分系統。 · 保持系統和軟體的修補程式更新。
使用外部CERT（電腦緊急回應小組）團隊	· 通常能比防毒軟體公司更早發現問題。 · 可以立即提出手動過濾等應急處理建議（軟體公司需可能要數小時或數天才會發佈修補程式）。
識別並阻止傳染	制定全面的預防策略 · 包括終端和網路策略與防護相關產品，如防毒軟體、反間諜軟體和防火牆產品。 · 限制未經批准的程式在工作站上運行。 · 限制最終用戶的寫入能力，這樣即使他們下載並運行了勒索軟體程式，也無法加密，除了用戶檔案之外的檔案。 · 電子記錄、物理介質以及關鍵系統、服務或設備的可用性，都應納入到預防策略的範圍之內。
保留系統和配置的“黃金”鏡像	· 資料管理策略的基本單元。 · 通過鏡像複製的方式輕鬆還原受感染的系統。
維護全面的備份策略	· 以最快方式還原存取您的關鍵檔案。 · 更頻繁地進行磁碟層級的快照（每15 分鐘1 次），並長期保存它們。 · 將受影響的系統從網路中同時清除威脅。 · 從一份確認有效的備份中還原任何受影響的檔案。

表3) 最佳技術措施

三・採取有效的備份策略

勒索軟體攻擊是一種逐步進行的駭客攻擊。隨著時間的推移，勒索軟體可以潛伏在後台運行一周或更久，並學習您備份計畫的行為特性。因此，很重要的一點是，作為災難恢復流程的一部分，需要在其他地點保存一份持久的資料備份。

許多依靠快照作為備份的企業將面臨更大的風險。如果來源資料遭到破壞，當快照或其他Instance被複製時，副本資料也會遭到破壞。因此，需要在受保護的場所保存一份來自上一個復原點的資料持久副本。

步驟	措施
採取有效的備份和災難恢復流程	· 直接使用備份副本，而不是保存在同一系統上的多個版本。 · 使用保存外部設備上的資料備份副本，而不是只依賴於保存在來源系統上的快照。

表4) 最佳資料保護措施

使用雲儲存也是一種有效的外部備份方法。由於雲備份資料對於本地作業系統管理員是不可見的，獲得雲使用者的帳號資訊需要更為複雜的過程。雖然在今天大多數人都傾向於把資料備份保存在磁碟而不是磁帶裡，但由於磁碟的線上特性使其更容易暴露在持續性的風險當中，而磁帶在某些場景下仍然可能是更好的一種選擇。

在美國75%受訪的醫院在2015年遭到勒索軟體的襲擊

醫療行業IT新聞
2016年4月7日

四・教育員工保護終端設備安全

最後，教育臨床醫生培養良好的安全習慣對於保護醫療系統和資料安全至關重要。應讓他們瞭解基本的常識。根據網路安全威脅報告[7]的描述，請教育您的員工和用戶掌握表5中的最佳操作規範。

步驟	措施
訓練員工掌握最佳安全操作規範	· 除了來源已知和可信的附件之外，不要打開任何附件。 · 不要運行從互聯網上下載的軟體，除非下載的軟體來源可信或已完成惡意軟體掃描。 · 點擊電子郵件或社交媒體程式中的連結時務必謹慎，即便是來自可信來源和朋友的也不例外。 · 安全使用社交媒體。熱門主題是詐騙的重災區，有些連結會引導至虛假的登錄頁面。 · 鼓勵員工在發現可疑情況時進行舉報。 · 如果Windows用戶在點擊URL或使用搜尋引擎後看到"被感染"的警告時(這有可能是虛假的防病毒報警)，使用者應使用Alt-F4、CTRL+W或工作管理員關閉流覽器，然後告知幫助台。

7 "互聯網安全威脅報告"第21卷，2016年4月21日

採取最佳的終端保護措施	· 在瀏覽器中安裝可以在搜索結果中顯示網站信譽度資訊的外掛程式。 · 只允許使用經企業審核通過的應用程式，並且避免從檔案共用網站上下載軟體。只能從可信的供應商網站上直接下載套裝軟體。 · 在任何提供雙重身份驗證的網站或應用程式上使用雙重身份驗證。 · 讓臨床醫生給每一個電子郵箱帳號、應用程式和登錄帳號設置不同的密碼，尤其是與工作相關的網站和服務。

表5) 員工與終端設備最佳保護措施.

▶ 總結

保護健康資料資訊（PHI）和其他關鍵資訊是醫療機構為病人提供優質醫療服務並且遵守行業規範的前提。防止資訊遭受勒索軟體的攻擊應成為醫療機構避免關鍵資訊和系統丟失的首要任務。通過強調安全、技術、備份和員工方面的最佳操作規範，以保護臨床資料。這樣，您的關鍵資料才能安全，也能在降低勒索軟體風險的同時提高業務連續運行能力。

欲瞭解Commvault 如何說明您智慧的管理醫療資料，請訪問 commvault.com/healthcare.。

COMMVAULT
Be ready
新加坡商慷孚沃德股份有限公司

曹淏翔 Armand Tsao (atsao@commvault.com) 0972 762 327
陳力維 Siegfried Chen (schen@commvault.com) 0988 101 019
售後技術支援專線 :0080 114 7127