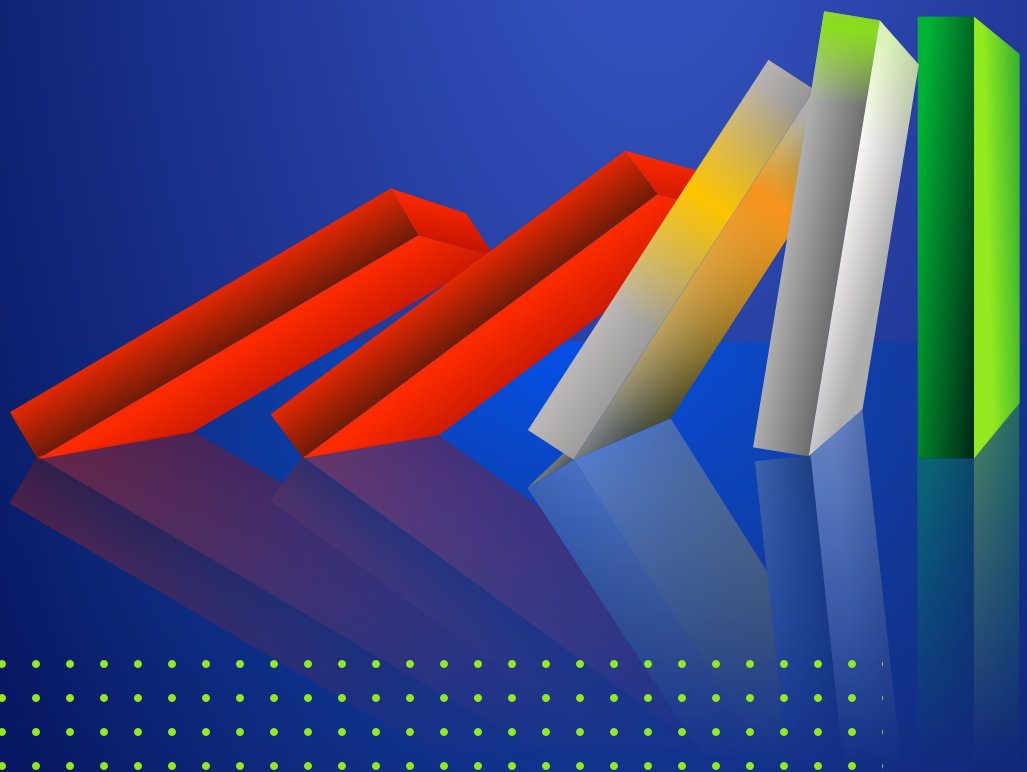
勒索軟體：

6 需要快速恢復的種功能

Dave Russell
Veeam Software
企業策略部門副總裁

Jeff Reichard
Veeam Software
企業策略部門資深主管

Chris Hoff
Veeam Software 資料保護
與勒索軟體部門行銷經理



目錄

企業面對的網路攻擊防不勝防 2

打造有利於彈性復原的架構 3

Veeam 勒索軟體最佳建議作法與精選功能. 4

安全備份是您的最後一道防線 4

1. 防止修改、成效備受信賴 5
2. 備份驗證 7
3. 3-2-1-1-0 法則 7
4. 即時大規模復原 8
5. 安全的資料復原作業. 9
6. 災難復原自動化腳本. 10

總結 11

適用於勒索軟體修正實務的 Veeam 產品 11

Veeam Software 簡介 11

作者簡介 12

企業面對的網路攻擊防不勝防

過去十年來、勒索軟體不斷增長和演變無疑是極具破壞力的一大趨勢。 勒索軟體數量暴增、勢不可擋、顯然已從經濟犯罪變成對全球安全影響甚鉅的犯罪型態。 北約、美國聯邦政府和軍方、甚至連 G7 都在近期認同勒索軟體威脅的嚴重性、呼籲政府和業界有必要廣泛合作、有效因應。

政府和業界聯手打擊勒索軟體需要時間。 與此同時、現今各種規模的組織除了需要保護自身安全、還必須保護客戶和子公司。幸好、使用現成工具和安全架構採取具體步驟就能獲得成效。

面對當今複雜精巧且適應力強大的勒索軟體和其他網路威脅、需採取靈活的多層次防禦予以應對。 不過、許多組織仍沿用只能處理單一攻擊媒介的獨立式安全性產品、這類產品很容易被攻擊方成功迴避。 員工缺乏安全性專業知識也使各種技術問題雪上加霜。 近期的估計報告指出、全球有超過 300 萬個網路安全職缺找不到合適人才。 人員短缺問題不僅關乎技術層面的技能、還包括了解如何運用政策來塑立一致性、並提供可衡量組織整體成效的方法[i]。無論是人員、程序或技術方面的落差、都讓老練的的網路罪犯比以往更容易攻擊您的資料。

網路攻擊或許防不勝防、但組織必須採取必要步驟做好萬全準備、才能在遭受攻擊時有效保護資料。

2016 至 2021 年勒索軟體日益猖獗

全球付出的成本：3.25 億至 200 億美元

頻率：每 2 分鐘到每 11 秒一次

創新：比特幣、勒索軟體即服務、雙重/三重勒索

打造有利於彈性復原的架構

有效的安全計畫的開端在於完備的結構、才能清楚了解哪些資料需要保護以及企業所需負擔的成本、以便在該資產遺失時決定保護措施的實施方式。 許多組織藉由以相同方式、相同層級的重要性來嘗試保護所有資產的辦法展開其安全性歷程、不過隨著組織拓展以及採用最佳建議作法、使得風險得以分類、並以更妥善的方式來定義及衡量各種回應。 隨著架構實作、安全性團隊也逐漸成熟、並且瞭解其所面臨的威脅以及其攻擊者所採用的手法、使團隊得以抵禦攻擊並在攻擊得手時迅速進行復原作業。 這種調理分明的方法也能清楚展現網路安全的投資成果、有助於證明相關投資的合理性。 此外、反覆推進的流程模式可允許分階段實作、有利於從之前的實作週期中學習、精益求精。

如果沒有結構化的網路安全風險管理方法、很容易將所有心力集中在防火牆和防毒軟體這類偵測型防禦工具上、而忽略了有效回應攻擊事件並從中復原所需的流程和工具。 換句話說、堅實的防禦就是最好的進攻、包括擁有備份和保護資料與工作負載的完善策略。 成功的備份是面對網路攻擊的最後一道防線、而且可能成為避免長時間停機、資料遺失和支付高額贖金的決定性因素。 對此、我們彙整了以下最佳作法指南、為您提供保護資料安全的實用建議。

Veeam 勒索軟體最佳建議作法與精選功能

自 2019 年以來，Veeam® 現代化資料保護平台的各個版本始終提供強大的網路復原力和安全的勒索軟體保護功能，幫助組織從任何網路攻擊事件中快速而穩定地復原。 我們採取軟體優先的方法，除了可讓您保有彈性以維持復原力、更禁止修改內部部署和雲端儲存空間中的資料，同時不受限於特定廠商的專屬硬體。 這些最佳建議作法可讓您擁有適當的保護措施，以持續為您的重要基礎架構服務提供可靠的備份與復原機制，並確保您能在需要時馬上取用資料。

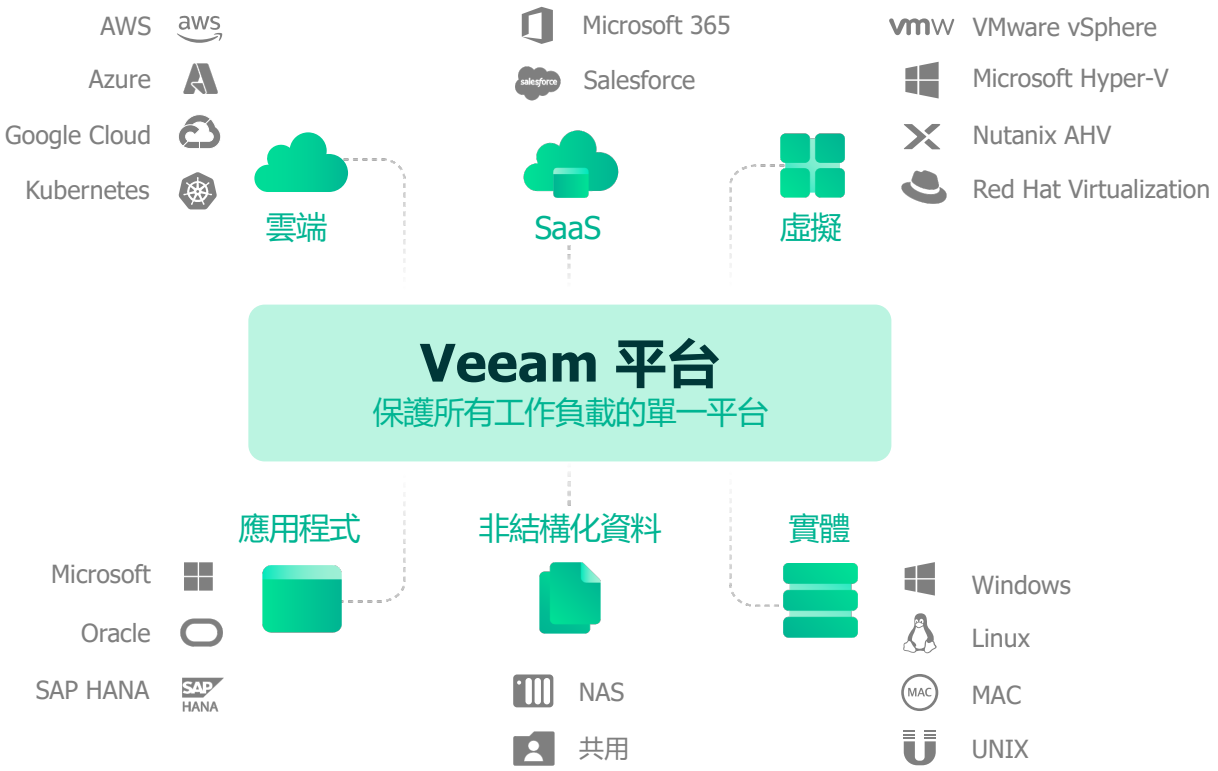
安全備份是您的最後一道防線

部署的可用性解決方案應該要能保護所有任務關鍵工作負載、無論型態為實體、虛擬或容器、均應獲得妥善保護。無論工作負載的部署型態為內部部署、雲端 (以 IaaS 形式部署) 或 SaaS、關鍵任務的資料現在會保存在許多位置、而且必須要能移動到不同帳戶、才能因應未來的需求。 保護平台應具備擴展或縮減規模的能力、具體規模則視實際需求和受保護的工作負載而定。備份解決方案應該要能透過多種方法擷取資料、包括備份、複寫、連續資料保護 (CDP) 和儲存陣列整合。

Veeam 提供可橫向擴充的軟體定義儲存 (SDS) 架構。 一方面，Veeam 可輕鬆擴充以擷取更多資料，以因應備份磁碟區或效能需求的變化。 另一方面，Scale-out Backup Repository™ (SoBR) 採取軟體定義型結構，為備份資料匯集不同類型的儲存裝置。 透過 Veeam 的儲存策略，資料可存放於最適合的裝置、包括內部部署的直接連結儲存裝置 (DAS)，重複資料刪除設備、網路附加儲存 (NAS)，物件儲存和雲端；系統會自動長期管理或透過服務供應商加以管理。

Veeam 平台可提供此等全部功能，使解決方案能隨著您的業務及其需求不斷發展而擴展。 Veeam 採取模組化且可彈性擴展的方法，不僅不需採用單點式解決方案、不強制仰賴特定硬體，也不必擔心解決方案會過時。

Veeam 的軟體定義勒索軟體修正功能適用於目前和未來的任何基礎架構。不需採用特定廠商專有的基礎架構，使企業能部署於自行選擇的硬體或雲端。 基礎架構彈性不僅能讓組織決定其備份解決方案運作的硬體，而且無論組織的重要資料位於何處，都能有效防範備份資料免遭勒索軟體侵襲。



1. 防止修改、成效備受信賴

網路犯罪份子現在經常試圖加密或刪除組織的備份、這已然成為所有勒索軟體攻擊的常態。 在勒索軟體攻防中獲勝可說至關重要、因為如果沒有備份的話、受害者就必須付出可觀的代價才能復原資料。

具復原能力的備份就是有心人士無法損毀的備份 — 即使對方取得了管理憑證、也無法對資料上下其手。

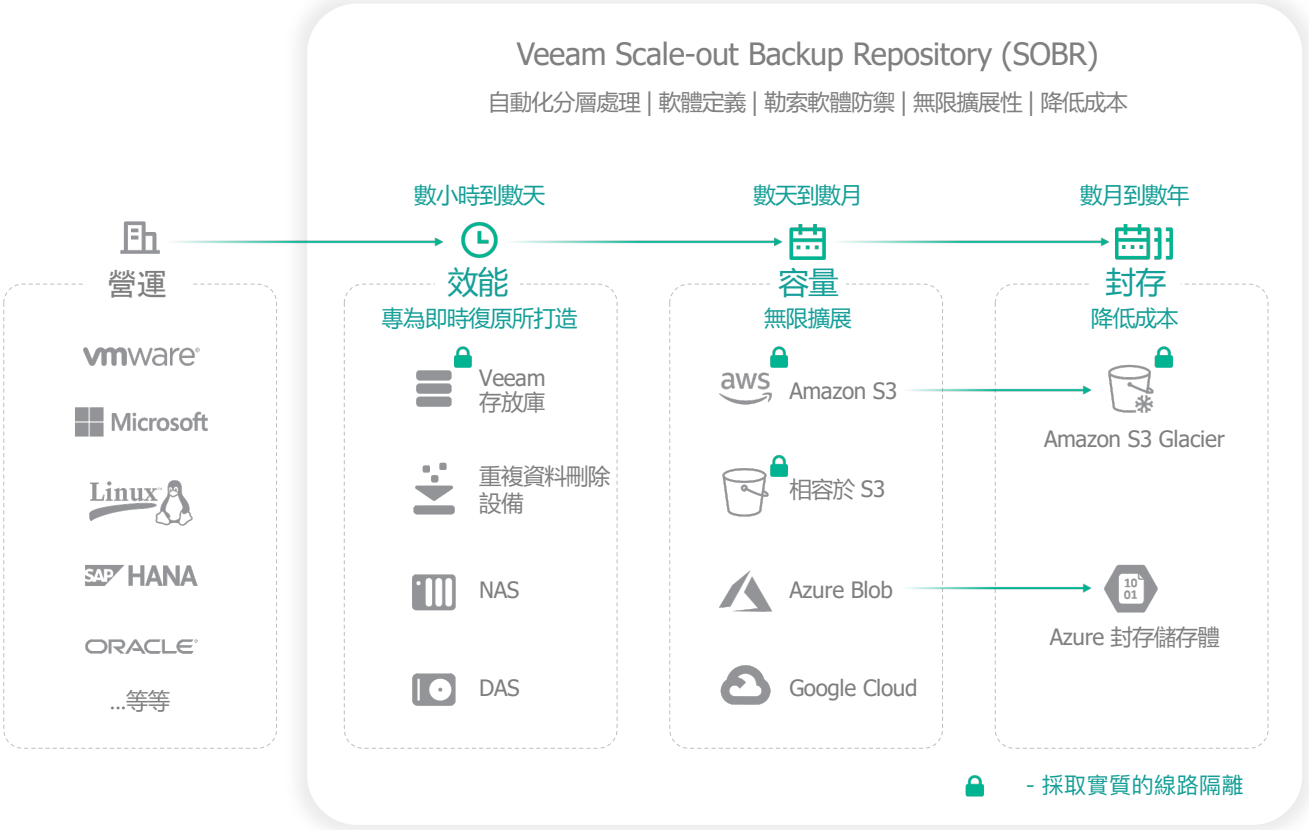
從最簡單的層面來說、先備份到卸除式磁碟或磁帶、隨後再將備份裝置與磁帶庫分開存放、即可實現強大的復原力。 以實質的線路隔離保存備份正是第一步。

Veeam 提供萬無一失的政策導向型資料管理方法、廣泛適用於各種具復原能力的儲存選項。 強化整體復原力、採用通過認證[ii]的 Veeam 儲存解決方案[iii]、並透過我們多元的合作夥伴生態系統、均可確保備份禁止修改的特性 (在規定時間內無法刪除或變更資料)。 **這些選項包括 Veeam 強化的儲存庫、這能為您的內部部署備份提供強大的不可修改選項。**如果您偏好將資料保留在雲端、Veeam 可以透過 AWS Amazon S3 和其他經核准的 S3 相容物件儲存供應商所提供的物件鎖定功能、確實貫徹備份禁止修改的特性。

將備份寫入具有復原能力的儲存空間、將會是確保從勒索軟體攻擊中復原最關鍵的防禦措施。所謂具復原能力的備份儲存空間、是指在以下任意的媒體組合上保存一或多份備份資料副本：

- 磁帶備份 (與磁帶庫分開存放或標示為 WORM)
- S3 或 S3 相容物件儲存空間中不可修改的備份
- 實質的線路隔離 (即卸除式磁碟、旋轉式磁碟機)
- 具內部防護 (服務導向功能) 的 Veeam Cloud Connect 備份
- 強化的儲存庫中不可修改的備份

Veeam 平台的核心產品提供齊全的勒索軟體修正功能、可供客戶輕鬆部署、並且能與任何基礎架構、內部部署或雲端環境靈活搭配使用。



政策導向型備份資料生命週期管理

有些 Veeam 客戶嘗試採取兩種或三種禁止修改備份的實務方法、實踐禁止修改的原則。這些方法可能包括利用 Veeam 強化的儲存庫執行內部部署、初級備份、再於自動管理的 Veeam 容量層中利用禁止修改功能和 S3 物件鎖定功能、完備雲端或內部部署的物件儲存需求、並/或將備份自動寫入 WORM (一次寫入、多次讀取) 實體磁帶媒體；值得注意的是、Veeam 原生支援實體磁帶、不需另外整合第三方技術。

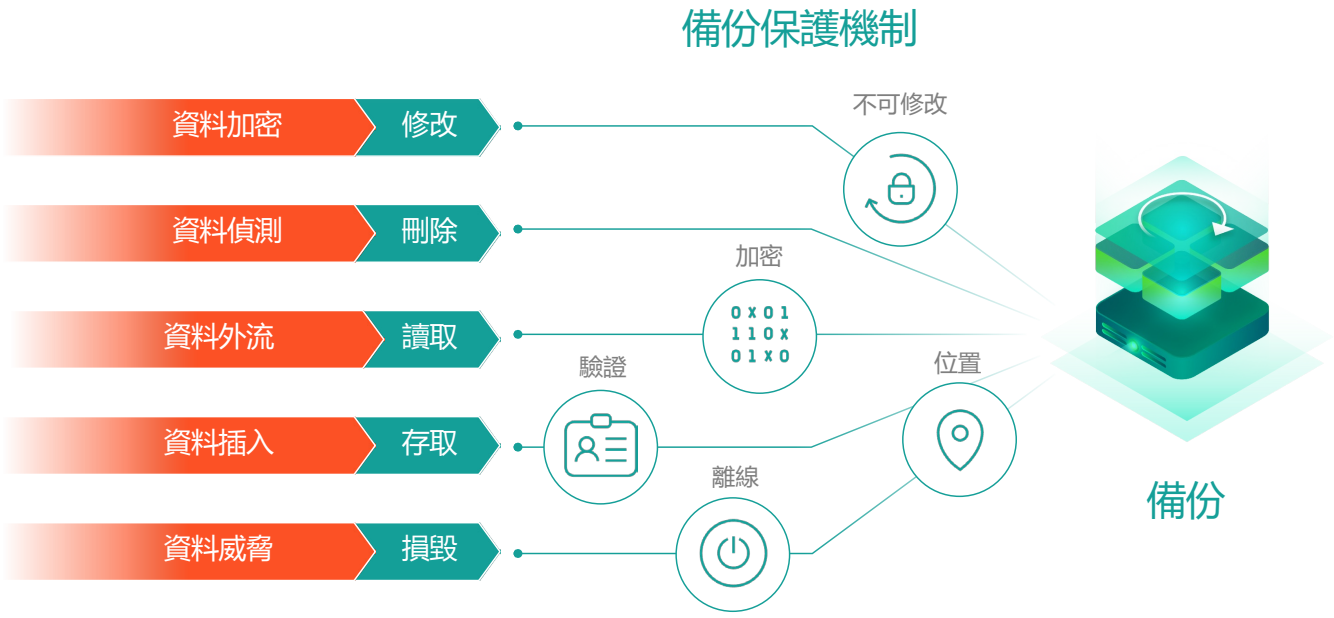
雖然禁止修改的特性 (無論是透過一種、兩種或三種禁止修改的方法來實作) 對於修正網路威脅幫助不小、不過這只是全方位勒索軟體防禦的開端。

系統仍需採取端對端加密、以防範資料外流。如今、增長速度最快的網路威脅之一就是資料洩漏和資料外流、受害者往往必須支付贖金、才能避免機密資料在暗網中流傳。

為防範資料插入造成的損害、系統必須具備適當的驗證機制和「數位保健」措施、設定最嚴格的存取權限。此外還需保護資料不受更動、確認原本有效的記錄和項目並未遭有心人士惡意變更成無效。

其他數位保健最佳作法包括：

- 所有登入來源的密碼不重複。這能確保某組密碼或某台電腦遭到入侵時、駭客無法使用其所竊取的密碼存取其他帳戶。
- 密碼管理員。稱職的密碼管理員可協助您管理所有登入資訊、讓您更輕鬆地建立及使用高強度的非重複密碼。
- 多重要素驗證 (MFA)。您可以設定多重要素驗證、規定每次登入時需繼續完成第二項驗證、為帳戶提供額外的安全保障。
- 從所有伺服器上移除未使用的裝置、應用程式和非必要的程式和公用程式。
- 修補程式管理 — 確認所有使用中的軟體、硬體和韌體均執行最新的軟體等級、全面防堵各種已知漏洞。



2. 備份驗證

健全的全方位網路防禦策略的起點永遠是有效備份。可靠且經過驗證和測試的備份、無疑是成功復原資料的第一步。忙碌的 IT 團隊需要一套自動化機制、使系統能在備份時自動驗證備份資料是否完整 萬一發生任何問題、團隊可以在營運資料依然可供使用的情況下再備份一次、以免在營運資料無法使用、資料外洩或不足以信賴以及不夠完整時、資料可用性的問題才浮上檯面。

Veeam SureBackup® 開創了自動化備份驗證的先河、堪稱我們的勒索軟體復原力最佳建議作法中的關鍵功能。 SureBackup 能在與網路隔離的環境中自動啟動伺服器和應用程式、並執行各環節的健全狀態檢查、包括檢查許多內建的應用程式驗證機制、例如執行特定的 Active Directory 或 SQL 命令、以驗證應用程式是否完整。 這種自動化測試功能可根據您的需求彈性擴展和自訂、並安排於您認為最適當的時間執行、測試結束後還會隨即將狀態報告傳送至您的信箱。

3. 3-2-1-1-0 法則

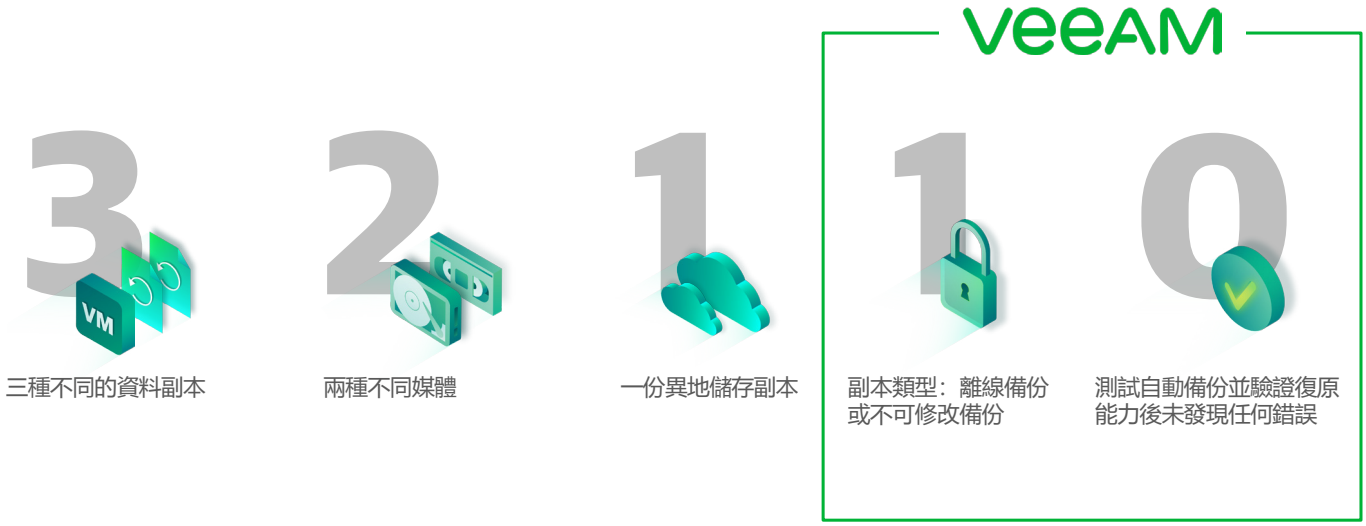
Veeam 建議遵循 3-2-1-1-0 備份法則、這是我們改良業界普遍採行的 3-2-1 法則所得到的成果。

多年來、Veeam 不斷倡導在一般資料管理策略中落實 3-2-1 法則。 3-2-1 法則建議應為重要資料保留至少三份副本、並存放於至少兩種不同類型的媒體、其中至少要有一份副本採取異地儲存的方式留存。 3-2-1 法則不規定或要求使用任何特定硬體、其適用範圍廣泛、足以解決幾乎所有故障情況。

隨著勒索軟體威脅加劇、Veeam 已強調至少應有「一份」資料副本可供復原 (即採取實質的線路隔離保存或內容無法修改)。對於增強抵禦勒索軟體的復原能力而言、這項建議可說勢在必行。

3-2-1-1-0 法則的現代化應用不僅彰顯了要求備妥各種可復原副本的必要性、也是企業可付諸實行的重要概念、如此即可更充分地做好抵禦網路威脅和修復損害的事前準備。

離線資料副本需妥善保存、以因應內部人士所構成的威脅、包括資料損毀。內部人士威脅日漸受到重視、有些分析公司表示、未來三年的網路威脅大宗可能來自企業本身的員工。



4. 即時大規模復原

在勒索軟體興起之前、組織一年內通常只還原 3% 至 5% 的備份資料。 不過在勒索軟體攻擊事件中、惡意軟體可能會加密或污染所有營運資料、而您則需要迅速地將所有資料全數復原。快速存取資料至關重要、比起為了所有重要作業而還原、維持運作不中斷是更重要的目標。

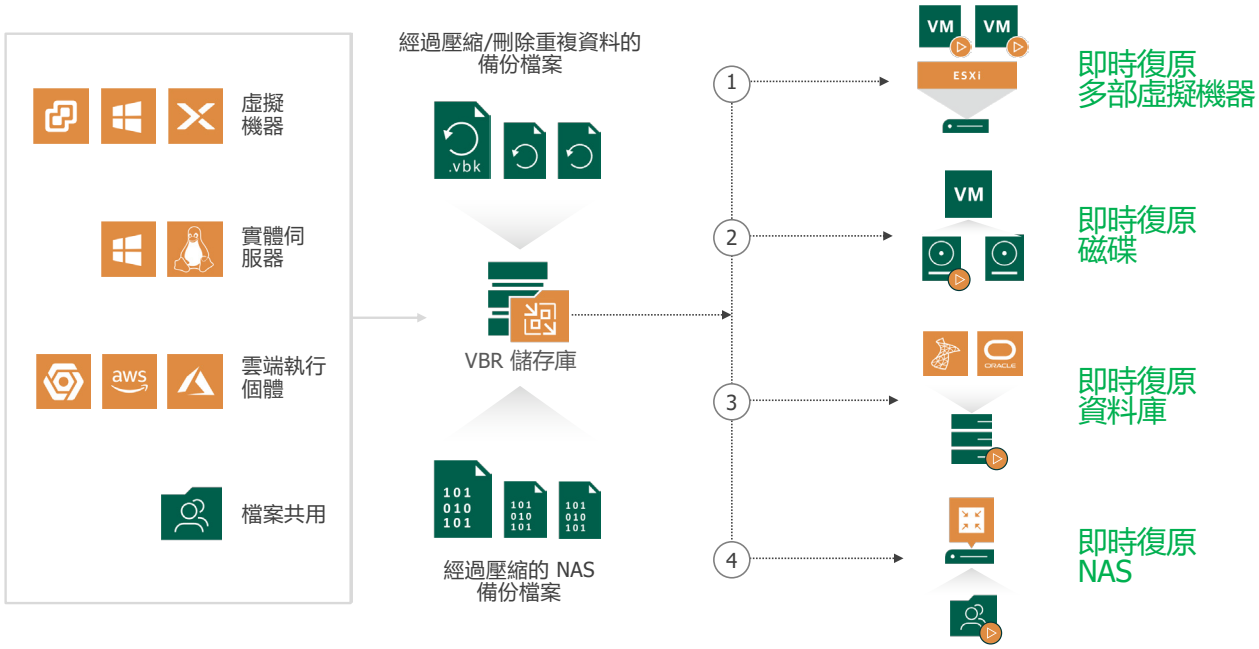
Veeam 於 2010 年即已開創即時復原資料的先河、此後不斷精進及擴展這項功能。時至今日、Veeam 已完成最佳化、可同時快速還原多部機器、甚至滿足最大規模的企業復原需求。

Veeam 提供即時復原資料的優勢：

- 不需使用昂貴的專有設備或固態硬碟
- 不侷限於僅復原最新的備份資料
- 只要按兩下滑鼠、即可將實體和虛擬檔案與工作負載復原到虛擬化環境 (例如 VMware vSphere、Microsoft Hyper-V 和 Nutanix AHV)、甚至能在虛擬機器管理平台之間自動移轉
- 只要按兩下滑鼠、即可將實體和虛擬檔案與伺服器復原到雲端環境 (例如 AWS、Azure 和 Google Cloud Platform)
- 可即時復原重要的企業應用程式 (例如 Oracle 和 SQL Server 資料庫)、以供立即使用
- 可將完整網路附加儲存 (NAS) 與檔案共用回復到感染前的良好狀態、以利業務快速恢復正常運作

資料即時復原功能可利用可攜式資料格式提供跨平台資料存取機制、確保隨時隨地都能依需求快速復原。 舉凡 AHV、Hyper-V 或 vSphere、實體 Windows 或 Linux 乃至 Azure、AWS 或 GCP、Veeam 平台能全面滿足您的需求。

Veeam 即時復原



5. 安全的資料復原作業

勒索軟體的佇留時間 (攻擊者發動攻擊之前潛伏在受害者網路上的時間) 可能長達數月、 因此您需要採取自動化機制、以免將惡意軟體復原到已清理乾淨的環境或新環境中。

SureBackup 工作 (上述第 2 點) 的其中一項功能是讓工作維持運作狀態、以便從備份還原點對系統執行額外的驗證和鑑識作業、 而這可能包括執行手動檢查、以調查特定檔案的方式確認勒索軟體威脅是否仍然存在。

在前述即時復原功能的基礎上、Veeam 與領先業界的反惡意軟體解決方案整合、透過提供自動化復原程序來檢查及清理受感染的備份資料、確保復原到營運環境的備份資料不再遭受任何網路威脅所侵擾、杜絕二次感染。

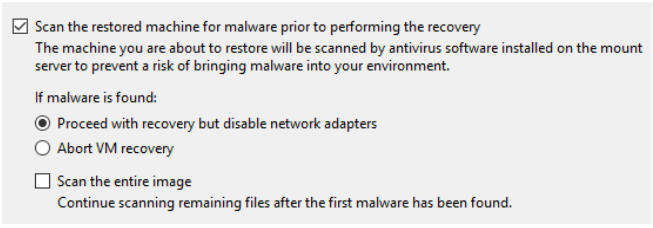
Veeam 安全還原功能可在使用者選擇的復原程序中、提供全面整合的防毒掃描步驟、由使用者自由選用。 此功能可確保您要使用或需要復原到營運環境中的任何副本資料均處於良好狀態、且未挾帶任何惡意軟體、解決與管理惡意軟體相關的問題。**安全還原功能是我們領先業界的另一項創舉、目前正在申請專利、可針對隱藏在備份資料中的惡意軟體所發動的攻擊進行修復。** 這項功能可為使用者確保威脅已妥善排除、不復存在於環境中、讓您更加安心。

安全還原功能可透過 PowerShell 完整設定、換句話說、如果您透過第三方整合功能或入口網站自動執行復原程序、也可以利用此功能來確保威脅不再重新進入您的營運環境。

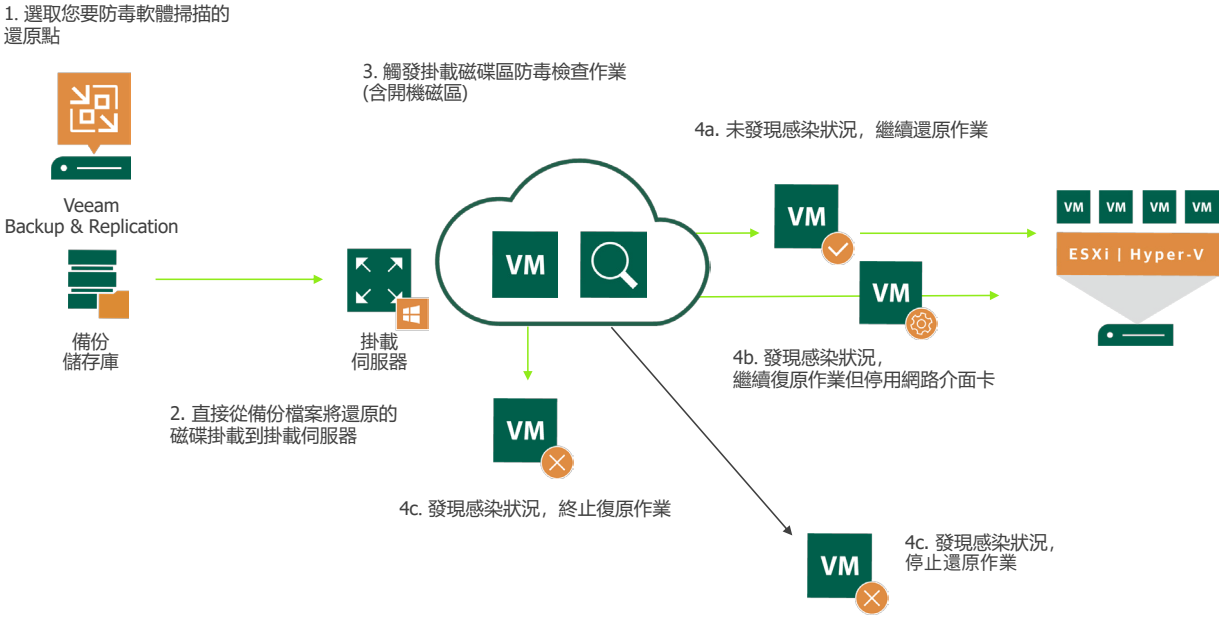
此強大功能的用途包括：

- 偵測潛藏於備份資料中「休眠」的勒索軟體、並在資料復原到營運環境之前叫用防毒修復功能、將資料徹底消毒
- 先行針對來自遠端和分公司 (ROBO) 等 IT 控管較薄弱之處的備份加以驗證、再還原到主要資料之中
- 以額外的防毒解決方案掃描備份資料、進一步偵測罕見或零時差的惡意軟體

與所有 Veeam 平台功能一樣、只需按幾下滑鼠即可快速又輕鬆地設定安全還原功能：



Veeam DataLabs：安全還原



6. 災難復原自動化腳本

網路攻擊堪稱災難、這點無庸置疑。在緊急情況下、您的團隊需仰賴自動化機制重複操作、以獲致穩定的處理成效。 您的工具集必須要能定期測試及稽核災難復原速度、包括在執行還原作業後、自動測試伺服器和應用程式的存取狀態和可用性。此外、測試過程和結果都會自行記錄下來、以滿足管理作業和外部安全稽核的需求。

Veeam Disaster Recover Orchestrator (VDRO) 領先業界、可針對複雜工作流程實現全面自動化、並隨時妥善記錄、包括使用動態文件在不影響正常營運作業的情況下進行大規模復原測試。 使用者也可以利用非 Veeam 資訊來更新事件回應/復原文件、例如聯絡人清單和其他任務關鍵回應資訊。

可靠復原

- 穩定可靠、可擴展的編排機制
- 以應用程式為中心

自動化測試

- 不中斷正常運作
- 排程和隨需執行
- 整備度檢查

動態文件

- 稽核記錄
- 合規報告
- 內建變更追蹤功能
- 主動修正

大部分組織都有許多類型的業務持續性 (BC) 計畫和災難復原 (DR) 計畫、 以下列舉幾個例子：

- 應用程式層級故障
- 網站層級故障
- 基礎架構元件故障
- 關鍵任務應用程式
- 開發/測試應用程式

如同各種自動化備份驗證 (例如 Veeam 的 SureBackup) 對日常備份操作極其重要、針對網路的整體復原能力定期測試復原計畫、其重要性也不容忽視。 擬定復原計畫後、接下來最重要的工作就是測試。 您需要知道您所研擬的計畫是否有效。 組織普遍未全面測試災難復原計畫、或甚至根本從未測試。 大多數組織每年最多只會局部測試災難復原計畫一或兩次。

在如今應用程式日新月異的情勢下、持續測試可說格外重要。為配合各種變動和設定調整、每當應用程式有所變更、組織都必須連帶更新復原計畫、例如增加伺服器以擴充容量、或移除舊伺服器。 測試時、務必特別注意非預期的突發狀況。 這是讓災難復原計畫更臻完善的唯一方法。 測試的真正目的在於確定您的計畫是否有效。

網路復原力和勒索軟體修正都必須納入整體災難復原計畫之中。 想要針對網路安全性事件做好萬全準備、制訂事件回應計畫是最清楚明確的方法之一。 建立明確定義的事件回應計畫後、您就能釐清安全性事件的偵測、通訊、控制和修正流程、以利員工了解發生網路安全事件時的因應之道。

此外、此計畫必須要能自動測試、動態更新重要的文件、並能和其他必要的工具和工作流程整合、以確保重要業務能恢復正常運作。

一鍵式網站復原和災難復原測試

Veeam Disaster Recovery Orchestrator

總結

公司的資料是最寶貴的資產；然而、勒索軟體對各種規模、產業和地理位置的組織而言、無疑都是日益嚴重的威脅、使重要資料暴露於風險之中。 公司必須持續改善安全性計畫、以確保資料受到妥善而安全的保護、且各組織皆可使用健全的功能從事件中快速安全地復原。 制定全方位的安全性計畫需要整合人力、流程和技術、所採取的方法必須專注於如何持續改善、同時盡可能提供最理想的防禦。 無論公司選擇哪種方法、其架構均需定義可衡量的結果、讓 IT 團隊能夠防禦攻擊、並在遭受攻擊後快速復原。

想要妥善回應勒索軟體這類威脅、組織勢必要實施面面俱到的修正策略。 Veeam 的勒索軟體修正功能齊全、提供市面上最完整的功能組合和最專業的知識、可確保危機期間還能正常使用資料。 我們的作法是採取軟體優先原則、讓您能在內部部署和雲端享有靈活的彈性、進而持續保有兼具復原力和禁止修改特性的儲存空間、而不受限於特定廠商的專有硬體。 只要您遵循最佳建議作法並部署 Veeam 的現代化資料保護平台、Veeam 就能協助組織實現數位復原力、無論您的資料保存在任何位置、均可使用全自動化流程還原資料及執行災難復原自動化腳本、並在過程中徹底杜絕勒索軟體、從將遭受勒索軟體攻擊後的停機時間縮到最短。

無論您的資料保存在內部部署或雲端、擁有一套完整的勒索軟體修正功能都是關鍵。若能將這些最佳建議作法納入您的安全計畫、既可簡化對網路攻擊的回應、又能避免資料遺失或支付高額贖金。

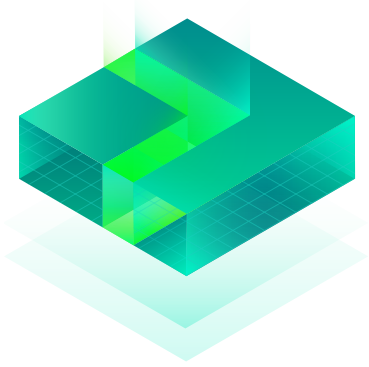
Veeam Software 簡介

Veeam® 是備份、復原和資料管理解決方案的領導廠商、提供現代化資料保護。 我們針對雲端、虛擬、SaaS、Kubernetes 和實體環境提供一體適用的單一平台。 藉由業界最簡單易用、彈性靈活、穩定可靠且功能強大的平台、客戶的應用程式和資料都能受到周全保護、且隨時可供使用、使客戶高枕無憂。 我們在全球各地保護超過 400,000 個客戶、其中 82% 名列《財星》的 500 大企業、更有 60% 躋身全球 2000 大企業。 Veeam 的全球生態系統包含超過 35,000 個技術合作夥伴、經銷商、服務供應商和聯盟合作夥伴、並在超過 30 個國家/地區設有分公司。 若要深入了解、請造訪 www.veeam.com/tc-tw、或追蹤 Veeam 的 LinkedIn 帳號 @veeamsoftware 與 Twitter 帳號 @veeam。

適用於勒索軟體修正實務的 Veeam 產品

適用於勒索軟體修正實務的 Veeam 產品

- Veeam Backup & Replication
- Veeam ONE
- Veeam Disaster Recovery Orchestrator
- Veeam Backup *for AWS*、Veeam Backup *for Azure* 和 Veeam Backup *for Google Cloud Platform*
- Veeam Backup *for Microsoft Office 365*
- Kasten K10 by Veeam



如需 Veeam 勒索軟體抵禦功能的詳細資訊、請造訪以下專門說明網站：https://www.veeam.com/ransomware-protection.html。

如需勒索軟體最佳作法的詳細技術白皮書、並了解 Veeam 網路安全功能的深入探討內容、請造訪：https://www.veeam.com/wp-protection-yourself-from-ransomware.html?wpty。

作者簡介

Dave Russell 已在儲存產業深耕 32 年、目前擔任 Veeam 企業策略部門的副總裁、負責推動策略性產品和上市計畫、同時引領公司在產業中的參與計畫、並宣傳 Veeam 的現代化資料保護願景。 加入 Veeam 之前、他在 Gartner 擔任了 13 年的副總裁兼特聘分析師、也在 IBM 服務了 15 年、從事大型主機和開放式系統備份/復原的產品開發工作。

Jeff Reichard 是 Veeam 企業策略部門的資深主管、專職處理風險、合規和合作夥伴關係相關事務。 Jeff 在資料保護/可用性、業務持續性和法規遵循解決方案方面擁有 25 年的經驗。 他之前的職務包括設計 SAN 和資料備份解決方案、以及為公部門和企業客戶提供系統工程與工程領導力服務。 加入 Veeam 之前、Jeff 剛卸下 Commvault 聯邦民營系統工程團隊負責人一職。 Jeff 在 Veeam 與合作夥伴、客戶和產業分析師合作、宣傳 Veeam 對雲端資料管理和數位轉型的願景。

Chris 的職業生涯與網路安全領域息息相關、進入這個產業至今已超過 15 年、具有豐富多元的技術經驗。 他目前在 Veeam 負責推動安全性和資料保護行銷業務。 加入公司團隊之前、Chris 曾擔任各種工程、銷售和產品管理職務。 在職業生涯中、他透過設計符合業界架構、計畫和合規要求的解決方案、協助眾多組織管理網路風險。

[i] https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-1/

[ii] 為回應金融業的監管規範、禁止修改儲存內容的相關技術認證應運而生。 許多政府規範旨在確保受監管組織於規定時間內保留未更改的財務記錄副本 (以美國為例、請參閱 SEC 規則 17a-4(f)、FINRA 規則 4511 和 CFTC 規則 1.31 (c)-(d))。 值得慶幸的是、同一套確保財務誠信的控管認證也可以保證備份資料不受刪除和更改。

[iii] 如需 Veeam 強化的 Linux 儲存庫最新的合規認證資訊、請參閱 https://www.veeam.com/blog/hardened-repository-passes-compliance.html。