
改變未來現在式

綜合型錄

# Acronis
# Cyber Protection

## 資安防護與資料保護的領導者

# Acronis
# 資安防護與資料保護的領導者

# 目錄

Acronis 資安防護與資料保護的領導者 ..... 03

選擇 Acronis 的四大理由

1. 20 年專精於備份技術: 無毒備份很實在，災難復原及異地備援很放心 ..... 05
2. 化繁為簡，單一管理介面: 一個介面完成資料保護、資安防護及端點管理 ..... 07
3. 感受多層次防護強大力量: 打造專屬防護計劃，事件各面向都讓你好安心 ..... 08
4. 台灣在地資料中心: 遵循台灣法規要求，提供在地化的速度和可靠度 ..... 09

拉長資安戰線的多層次防護三部曲

1. 無懼入侵事前預防 ..... 10
2. 無憂勒索事中防護 ..... 11
3. 無毒備份事後回復 ..... 12

成功案例分享

F1 威廉斯車隊利用 Acronis Cyber Protect Cloud 增加新的保護層 ..... 15

BlueBerry 選擇 Acronis Cyber Protect Cloud 保護 Microsoft 365 ..... 16

使用案例實務

政府單位引進 Acronis Cyber Protect Cloud 強化資安、法規遵循一次達成 ..... 17

Acronis 助傳統產業提升防護力 Cyber Protect Cloud 雲端服務快又穩定 ..... 18

學校借助 Acronis 在預算內同時完成資安防護、資料備份 ..... 19

# Acronis
# 資安防護與資料保護的領導者

Acronis 藉由其備份、災難復原、雲端儲存、反勒索軟體以及高安全性的檔案同步與共用解決方案，提供簡單、高效和安全的網路保護（cyber protection）。

在 Acronis，我們保護每個組織的資料、應用程式、系統和生產力 — 保護它們免受網路攻擊、硬體故障、自然災害和人為錯誤的影響。Acronis 協助服務供應商保護他們自己及其客戶的基礎架構，並維持高獲利率；同時， Acronis 也幫助企業 IT 團隊和家庭辦公使用者，能以高可靠性和低成本保護其企業關鍵基礎架構。

## 全球布局的科技公司

## 廣獲資安界的肯定

MICROSOFT VIRUS INITIATIVE ( MVI ) 成員

Cloud Security Alliance 成員

MRG-Effitas 參與者和測試獲勝者

VIRUSTOTAL 成員

ICSA Labs 認證

Anti-Malware Test Lab 參與者和測試獲勝者

Anti-Malware Testing Standard Organization 成員

AV-Comparatives 認可的商業安全性產品

AV-Test 參與者和測試獲勝者

Anti-Phishing Working Group 成員

VB100 認證

NioGuard Security Lab 參與者和測試獲勝者

## 全球在地化的多雲環境支援及異地備援服務

Acronis 託管、Google Cloud 和 Microsoft Azure


Acronis Cloud 資料中心 ● Google Cloud Platform ● Microsoft Azure ●

**52 座 資料中心**

在地化的台灣資料中心於 2021 年 11 月落成，能因應本地產業和政府機關對法規的要求，並提升對資料傳輸速度和安全的保障。

# 選擇 Acronis 的四大理由

## ❶ 20 年專精於備份技術：無毒備份很實在，異地備援及災難復原很放心

**自 2003 年創立至今，Acronis 持續提供創新的新世代資料保護技術，現在更延伸其資料保護能力為完整的網路保護。**

### 以 AI 技術整合網路安全與資料保護

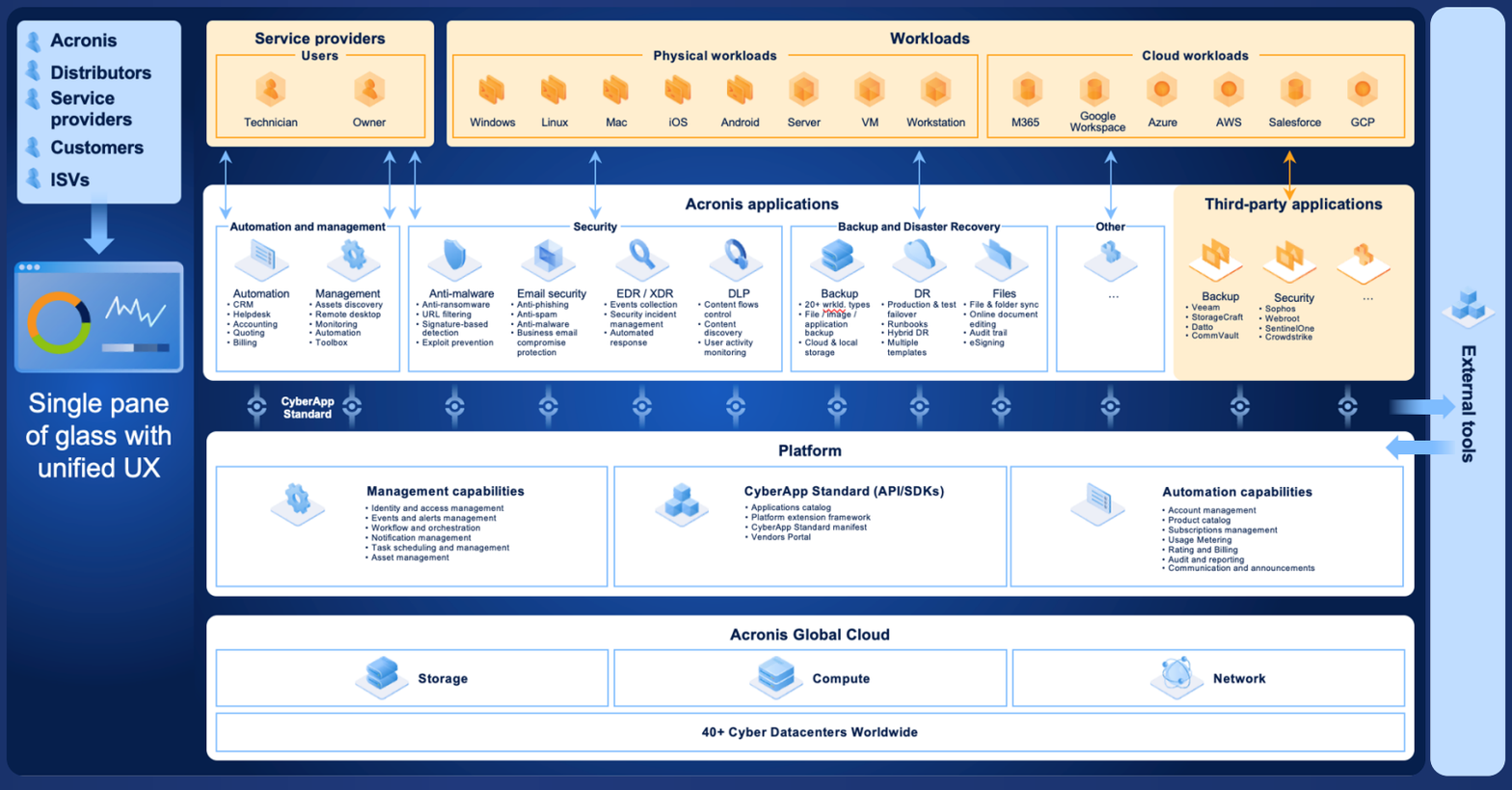
Acronis 能對備份檔案定期執行惡意程式掃描，找出潛在的弱點和惡意軟體感染，進而確保管理人員還原的是無惡意軟體的備份。Acronis 除提供雲端備份與防惡意軟體、防毒軟體等網路防護功能結合的獨特方案，支援實體和虛擬工作負載災難復原的 Acronis Cyber Protect Cloud Platform，還能以雲端為基礎，輕鬆、可擴充、高效率地復原所有常見工作負載 (包括 Windows 和 Linux 實體伺服器及 VM、主要 Hypervisor 與 Microsoft 應用程式)，將停機時間縮到最短。

事實上，Acronis 完整涵蓋美國國家標準暨技術研究院 ( NIST ) 資通安全框架所提出的五大功能構面：識別 ( identify )、保護 ( protect )、偵測 ( detect )、回應 ( response )、復原 ( recover )，能以多層次的防護能力，協助企業將有限的資源應用在當前防護最弱，最需要加強的構面，達到最高效益。

# Acronis Cyber Protect Cloud Platform 是資安防護與資料保護的最佳組合


Acronis 積極進行資料保護跟資安防護技術的超融合，單一介面就能部署備份、災難復原、資安和 IT 管理功能，提供高效又簡單的多層次防護

# Acronis Cyber Protect Cloud 的技術市場架構



## ❷ 化繁為簡，單一管理介面：一個介面完成資料保護、資安防護及端點管理

**啟用與管理 Acronis Cyber Protect Cloud 所有功能，就是 如此簡單**




Acronis 提供單一的整合介面，讓 IT 人員只需點擊一下就能部署備份、災難復原、安全和 IT 管理功能。事實上，此一單一管控介面可讓管理人員在每個用戶端或群組層級上，有效地啟用、停用及設定服務和原則，其範圍包含所有資安防護層面：備份、防毒及惡意軟體防護、災難復原、URL 篩選、弱點評估、修補程式管理。

此外，IT 人員可以安全連接至遠端裝置（即使位於私人網路上的防火牆後方），無需變更防火牆設定或建立其他 VPN 通道，如同該裝置就在 IT 人員身旁一樣，快速從遠端支援或修正任何端點的操作問題。

## ❸ 感受多層次防護強大力量：打造專屬防護計劃，事件各面向都讓你好安心

Acronis Cyber Protect Cloud 以人工智慧技術融合資安防護與備份解決方案，是少數能符合 NIST 資安五大構面建議的跨領域解決方案。以識別、保護、偵測、回應、復原五大面向為基礎，Acronis 為企業或組織提供了資安問題與事件的事前預防、事中防護、事後回復等多層次防護能力。

Acronis Cyber Protect Cloud

### 資安防護 3 部曲

事前預防　事前預防　事前預防

世界唯一
**AI 智能**
多層次防禦架構

安全

無懼入侵
**事前預防**

上網安全管控　弱點掃描
郵件安全管控　安心更新
周邊裝置管控

防護

無憂勒索
**事中防護**

惡意程式防護
零時差勒索軟體防護
防護系統自我保護

復原

無害備份
**事後回復**

快速資料備份　異地備援服務
遠端資料抹除　無病毒安全復原
鑑識資料留存

## ❹ 台灣在地資料中心：遵循台灣法規要求，提供在地化的速度和可靠度

提供資料安全儲存備份及異地備援的 Acronis 全球資料中心，目前已有 52 座，且每年持續增加中。此外，位於美國、瑞士、以色列及新加坡的全球資安情資中心 Acronis Cyber Protection Operation Centers ( CPOC )，則全年無休、持續監控網路安全態勢，並針對惡意軟體、勒索軟體、漏洞、自然災害和可能影響資料防護的其他全球事件提供即時警示，資深的安全專家還能協助提供快速補救的復原措施及額外的安全服務協助。

2021 年 11 月在台設立的 Acronis 全球資料中心，採高可用性與備援架構並即時加密，能徹底杜絕未經授權的實體存取行為，讓客戶安心放心。

### Acronis 台灣全球資料中心

以在地化優勢高格保資料安全

ISO / IEC 20000-1:2018 ， ISO / IEC 27001:2013

**高可用性與備援架構**

以 need plus one ( N+1 ) 原則，提供更優異的備援能力，根除單點故障癱瘓系統的機率

**即時加密**

Acronis 在資料傳輸和閒置時，採取 AES - 256 加密機制保護，符合台灣法律規範

**安全專業人員服務**

優異的 Acronis 團隊解決任何安全性問題，保障客戶資料絕對安全

**深耕在地市場**

簡化和支援企業雲 / 遵循台灣法規要求

- 委託雲端服務，確保資料復原不丟失
- 實施實地稽核或保留稽核權利
- 端點偵測及應變機制導入
- 資通安全弱點通報機制導入
- 建立統一管理制度，強化高風險資產

**多層防護架構**

無懼威脅攻擊 / 安心備份備援

- 輩分防毒弱點掃描
- 零時差勒索攻擊
- 安全備份與復原
- 遠端資安可視化管控
- 檔案安心同步分享

**快速連線品質**

提供快速穩定連線 / 強化可靠度與溫度

- 連線速度快且安全穩定
- 本地法規認證與技術支援
- 即時服務資安備份
- 雲備援萬無一失

# 拉長資安戰線的多層次防護三部曲

Acronis 發揮合而為一的力量，從領先的資料保護方案，延伸到一流的資安防護技術，進而拉長資安戰線，堅守最後一道防線！不論是備份、災難復原、安全、管理和自動化功能，Acronis Cyber Protect Cloud 以最安全、易用、可靠的資安解決方案，提供企業及服務供應商多層次的資安問題事前、事中及事後防護功能。


## 1. 無懼入侵 事前預防

### 弱點掃描

透過每日持續更新的 Acronis 弱點與修補程式管理資料庫，偵測工作站、伺服器，包含 Windows、Linux 及 MacOS 系統、Microsoft Office 和相關元件的軟體弱點，提供修補程式可用性資料，以減少潛在威脅並防止攻擊。現今，已擴大支援掃描 285 種以上最常被攻擊的協力廠商軟體，如 Adobe、Oracle Java、瀏覽器、遠端會議軟體及 VPN（Teams、Zoom、Webex、TeamViewer）等。

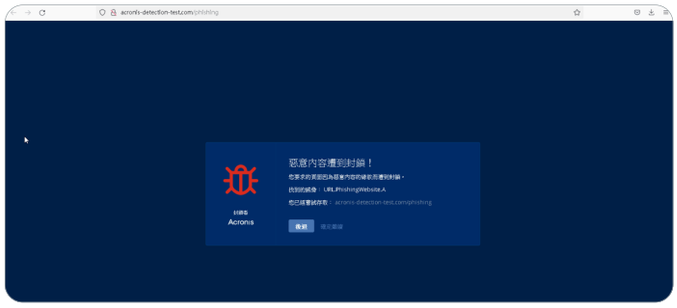

### 更新管理 ( 安心更新 )

★ 獨家

有問題的系統修補程式會導致系統不安全，為縮短安全性漏洞被利用的時差，Acronis 可自動預先建立所選主機的備份，若遇到更新導致系統或服務問題，可以進行時光回溯，以便快速回復服務。

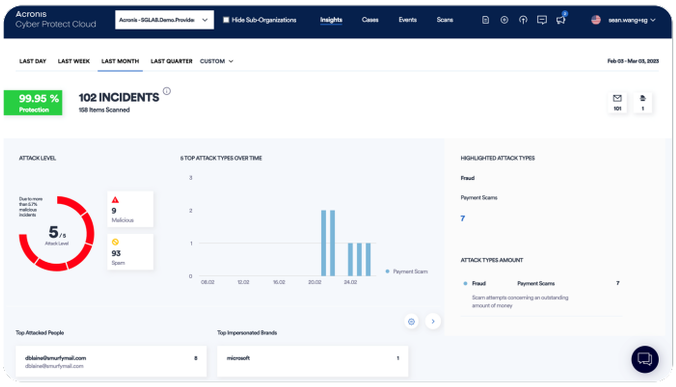
## 上網安全管控

Acronis 具備自有的特徵碼資料庫，提供 AI 智慧型偵測、HTTP / HTTPS 攔截器、網址黑白名單、惡意網址的有效負載分析功能，可根據網址清單中包含的訊息允許或拒絕存取特定網站，從而控制使用者對網站的存取，阻絕惡意 / 駭客攻擊的網站，達到安全性並獲得更好的合規性及提高生產力。



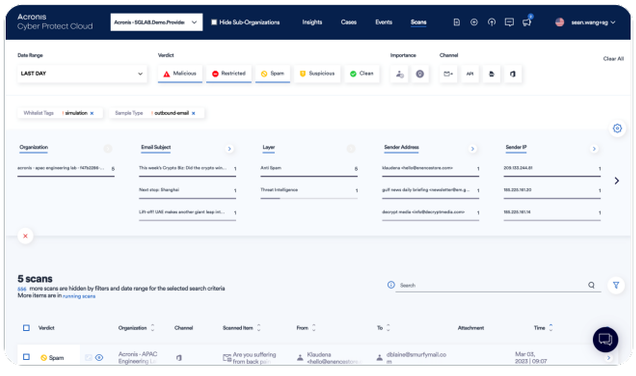

## 郵件安全管控

藉由 Advanced Email Security 模組，在電子郵件威脅接觸到終端使用者之前就搶先封鎖，包括垃圾郵件、網路釣魚攻擊、商務電子郵件入侵 ( BEC )、進階持續性威脅 ( APT ) 與零時差攻擊都不放過。




## 週邊裝置管控

Acronis 能控制裝置與周邊裝置之間的資料流與使用者存取 ( 拒絕、允許、唯讀 )，包括端點 ( Windows PC、工作站、伺服器 )、連接埠、周邊和重新導向的裝置、剪貼簿、虛擬的工作階段，並加密卸載式媒體與螢幕截圖擷取控制功能，以消除資料外洩的風險。




# 2. 無憂勒索 事中防護

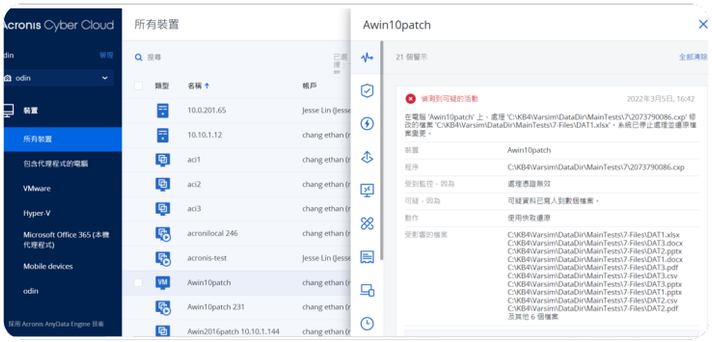
## 防護惡意軟體

整合了最佳備份和復原的反惡意軟體功能，能與客戶目前的防毒軟體相輔相成。藉由防止入侵、URL 篩選、對備份資料進行反惡意軟體掃描以及增強型病毒碼簽章資料庫，提升偵測率與速度，攔截更多威脅。


## 零時差勒索軟體防護

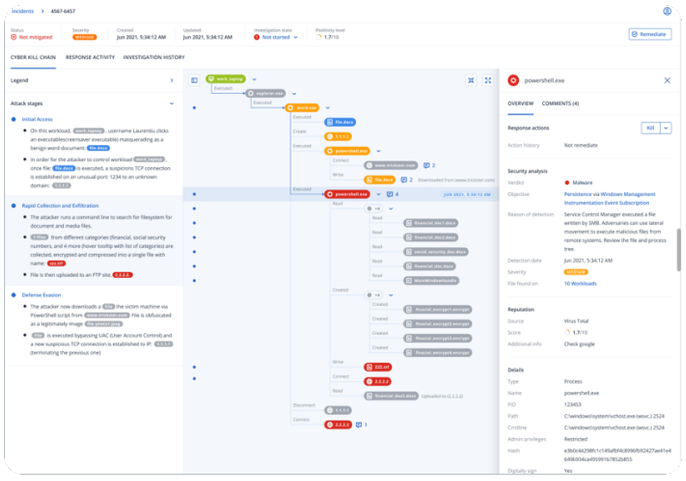
★ 獨家

Acronis 支援勒索軟體偵測和資料復原、挖礦程式偵測、即時防護和隨需掃描。領先業界的 AI 型 Acronis Active Protection，引入靜態分析器與行為分析，可不斷觀察電腦上資料檔案的變動狀況。一組行為是正常且為預期中的情況；另一組行為可能會發出訊號，通知有可疑的動作正在對檔案進行敵對行動。Acronis 的方法會觀注這些行動，並將其與惡意行為模式對比，識別勒索病毒的攻擊，即使是來自從未被發現的勒索病毒變種，亦無法閃避。




## 端點偵測及回應 (預計2023年上市)

Acronis 的端點偵測及回應 ( EDR ) 功能，可使用基於行為和病毒碼簽章的自動化引擎、URL 過濾、新興的威脅情報回饋、事件關聯和 MITRE ATT&CK® 持續進行監控作業。然後安全地從遠端連接工作負載，或檢查備份中自動保存的鑑識 ( forensic ) 資料，進行威脅調查與後續的稽核，並藉由阻絕、殺死流程、隔離等方式完成清除作業。



## 資料外洩管控

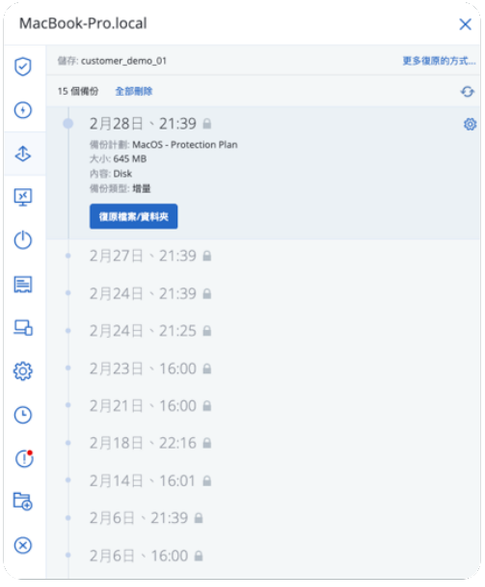
Acronis Advanced DLP 透過分析資料傳輸的內容和上下文並執行原則型預防控制措施，防止資料透過週邊裝置和網路通訊從工作負載中外洩，進而保護客戶的敏感資料。此外，借助自動產生的基準 DLP 原則，可以準確、高效地為組織建立業務特定原則，以便在系統執行原則之前對其進行驗證以保護客戶資料。

# 3. 無毒備份 事後回復

## 連續資料備份 / 快速復原

能實現業界最佳復原時間目標 ( RTO ) 的 Acronis Instant Restore 專利技術，可直接從現有 Microsoft Hyper-V 或 VMware vSphere ESXi 主機上的備份儲存裝置，啟動任何 Windows 或 Linux 系統 ( 實體或虛擬 )，讓使用者在短短幾秒內復原系統，無需移動資料。

此外，Acronis 能為使用者工作時最常用的每個裝置定義關鍵應用程式清單，並監控所列應用程式中進行的每個變更。如果發生惡意軟體感染，使用者可從上次備份還原資料並套用最新收集的變更，以避免資料遺失。




## 遠端裝置與資料抹除

IT 人員可從遠端操作任何端點，如同在裝置旁一樣。IT 人員無需變更防火牆設定或建立其他 VPN 通道，即可安全連接至遠端機器 ( 即使位於私人網路上的防火牆後方 )， 檢視使用者的螢幕，為特定工作提供支援或修正問題，也可以執行端裝置清除，防止資料因裝置遺失而外洩。


## 安心復原 / 備份檔掃毒

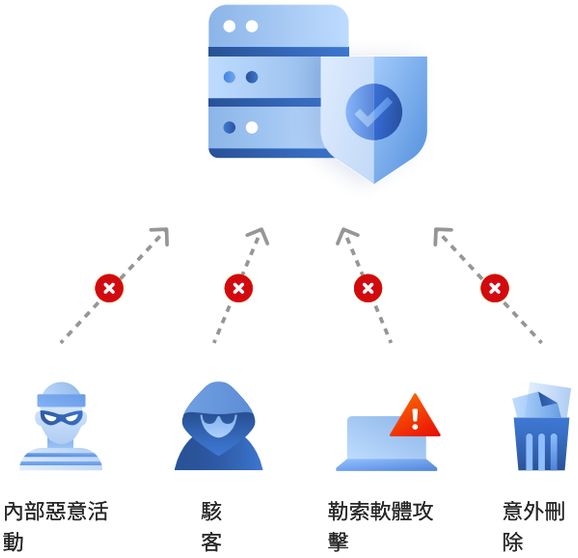
★ 獨家

Acronis 將防惡意軟體掃描和防毒軟更新整合至復原程式中。藉由更新防病毒定義檔，並對備份映射檔進行防惡意軟體掃描，找出潛在的惡意軟體感染，可讓使用者快速輕鬆地還原無惡意軟體的作業系統映射檔，並減少重複感染的機率。


## 不可刪除竄改之備份

★ 獨家

不可變動儲存空間可以在指定的保留期間內存取已刪除的備份。從備份中復原內容，但無法變更、移動或刪除。當保留期限結束後，已刪除備份將會永久抹除，確保業務關鍵資料不會遭到篡改。



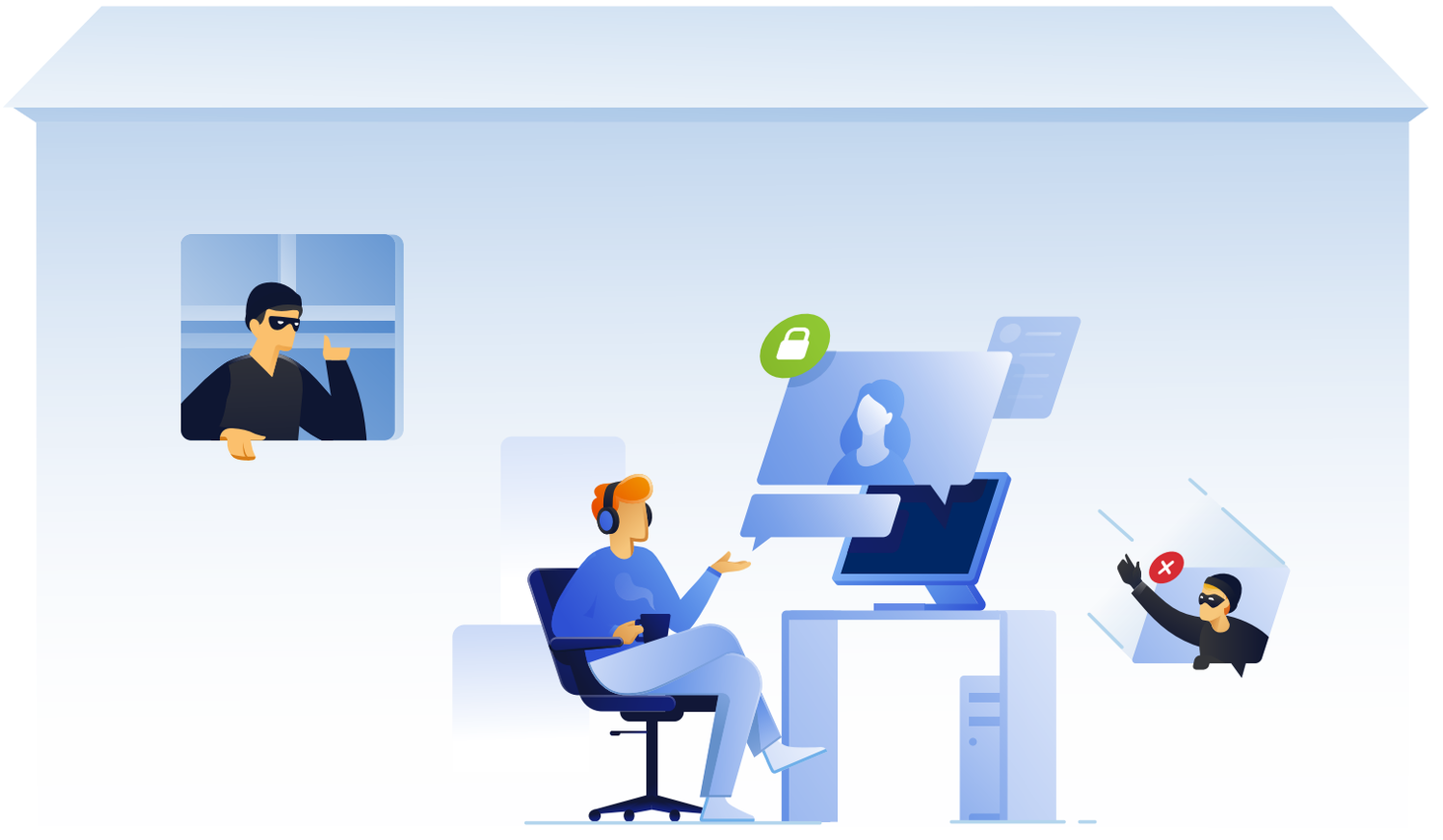
## 資安鑑識資料備存

透過啟動產品中特殊的「鑑識模式」，可以收集磁區層級的記憶體傾印和完整的硬碟映射檔，除備份重要資料，確保備份中的關鍵證據安全性，也提供了日後進行分析和調查所需的資訊，使日後調查作業更容易、花費更少。


## 異地備援服務

★ 獨家

Acronis 一流的全球資料中心，提供零疏失、零篡改、零誤刪、零勒索、零病毒等絕對安全的備份儲存及異地備援空間。相關服務包括當地端平臺受到攻擊時 15 分鐘內可故障還原 ( Failover )資料，備份備援整合移轉至雲端，修復資料後再回復 ( Failback ) 資料，以及發生災難時可最快獲得雲端復原服務。

# 成功案例分享

## F1 威廉斯車隊利用 Acronis Cyber Protect Cloud 增加新的保護層

**標誌性的一級方程式車隊擴大與 Acronis 的技術合作範圍**

作為世界領先的一級方程式（Formula 1）車隊之一，威廉斯車隊（Williams Racing）40 多年來持續贏得大獎賽（Grands Prix）。威廉斯車隊由弗蘭克・威廉斯爵士創立，1977 年首次進入 F1，從那時起，威廉斯車隊已經贏得了 16 個 FIA 一級方程式世界錦標賽冠軍，成為賽車隊中最成功的第三支車隊。

幾年前威廉斯與 Acronis 建立了技術合作關係，為其基礎架構提供網路保護（cyber protection）。透過 Acronis Cyber Backup，威廉斯公司將備份作業所需的時間從幾天縮減到幾分鐘，IT 部門則藉由這些生產力的提高，提升其處理和解決全公司所有 IT 服務的水準。

### 主要挑戰和需求

- 將網路保護擴展到 Microsoft 365 信箱和 SharePoint 站點
- 保護所有工作人員和工作負載，不受地點限制
- 降低 IT 管理的複雜性

### 受保護的資源

- 600 台 伺服器
- 1,200 個 Microsoft 365 信箱
- 1,500 個 端點
- 0.5 PB 的 資料

### 主要效益

- 一個代理程式即可執行備份、反惡意軟體、URL 過濾和修補程式管理
- 對最常用的應用程式提供持續的資料保護
- 使用者可放心地從遠端創建敏感性資料

「無論我們的員工在哪裡工作，Acronis 都能提供保護 .....
我們讓所有使用者能夠安心地在家工作，並從遠端創建敏感性資料。」

Graeme Hackland
Williams Group 資訊長

# BlueBerry 選擇 Acronis Cyber Protect Cloud 保護 Microsoft 365

**紐西蘭服務供應商 BlueBerry 在其備份產品中增加 Microsoft 365 保護，並加強對客戶的支援**

BlueBerry 是一家位於紐西蘭的託管服務供應商 ( Managed Servicer Provider, MSP )，提供系統設計、營運持續規劃、技術發展管理以及電腦軟硬體供應等解決方案。該公司與該地區約 300 家中小型企業合作，其中 23 家是託管服務客戶。BlueBerry 是微軟公司的銀級合作夥伴，專精於 Microsoft 365 和 SharePoint。該公司之前建議客戶的備份方案之一是 SolarWinds 的 Managed Backup ，但 SolarWinds 不支援 Microsoft 365 信箱。

改用 Acronis Cyber Protect Cloud 之後，BlueBerry 能透過集中的管理主控台，管理所有的備份，以及復原個別的檔案、應用程式資料、Microsoft 365 信箱或整個虛擬平台。由於 Acronis Cyber Protect Cloud 支援 20 多個虛擬、實體和雲端平台，以及混合的備份和復原功能，使得 BlueBerry 能協助其客戶復原到類似或不同的硬體，同時從一個集中位置輕鬆管理資料。

## 主要挑戰和需求

現有的備份解決方案
不支援 Microsoft 365

一個支援
所有資料、應用程式
和設備的單一備份和
復原解決方案

## 受保護的資源

- 7 台 伺服器
- 10 TB 資料
- 17 個 工作站
- 151 個 信箱

## 主要效益

- 創造新的收入來源
- 為客戶提供更高水準的服務

「Acronis 不但為公司創造新的收入來源，
更重要的是，讓我們能提供更高品質的客戶服務。」

Allan Willoughby
BlueBerry 總經理

# 台灣實際案例 - 政府機構

## 政府單位引進 Acronis Cyber Protect Cloud 強化資安、發歸遵循一次達成

### 挑戰與需求

因應資安等於國安的思維，行政院資通安全處在資通安全管理法中明定，政府機關在初次受核定或等級變更後之一年內，需完成相對應的威脅偵測機制建置，並持續維運及依主管機關指定之方式，如端點偵測及應變機制、資通安全防護等法規，提交相關的監控管理資料。只是對於 IT 以及資安維運人力吃緊的政府部門來說，要符合資通安全管理法要求的難度非常高，儘管已採購各種類型的資安防護軟體，但因為得分別安裝相對應的管理工具、代理程式等，反而造成資訊人員在管理上的工作負擔，且不一定能成預期的防護效果。

### 解決方案與效益

某政府機構為提升自身防護能力、迎合法規需求，選擇涵蓋事前預防、事中防護、事後回復等三大功能的 Acronis Cyber Protect Cloud，實現以下效益：

運用 Acronis 雲端資安服務及台灣全球資料中心，確保符合

**台灣資安法規要求**

**僅在用戶端安裝一個代理程式**

即享有資安情資及自動執行對應防護、弱點掃描、更新管理 、上網安全管控、郵件安全管控、惡意軟體防護、零時差勒索軟體防護等資安防護。

可在閘道端透過多層次資安防禦機制

**阻擋惡意程式入侵**

也能在內部網路中察覺新型態惡意程式入侵之後，依照事先設定參數採取自動化作為，如阻斷網路連線、保全現場環境，以

**快速回應威脅**

**降低受害範圍**

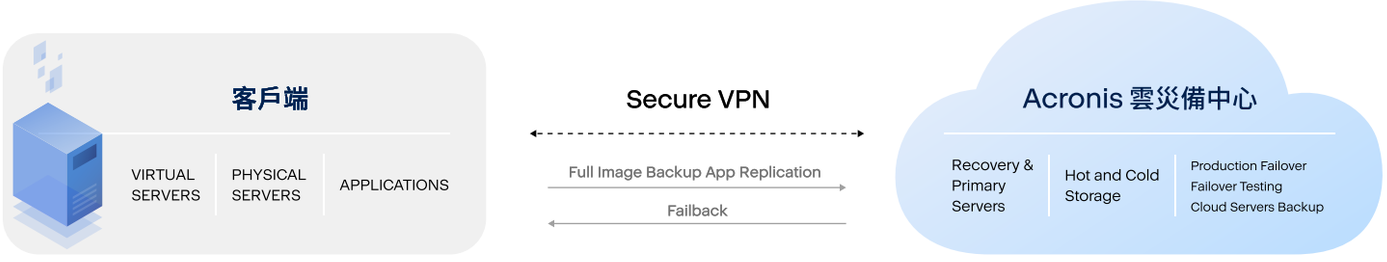

「Acronis Cyber Protect Cloud 是市面上唯一整合惡意程式防堵、端點防護、備份與備援等整合式多層式資安防護平台，讓用戶能在單一環境中獲得最完善的保護。Acronis 的整體資安防護力，讓用戶可即時掌握端點設備的健康狀態，迎合資通安全管理法的要求。」

**Sean Wang**
Acronis 大中華區首席技術顧問

# 台灣實際案例 - 傳統產業

## Acronis 助傳統產業提升防護力，Cyber Protect Cloud 雲端服務快又穩定

Acronis 的雲端災難備援中心：一鍵啟用 DR、一鍵還原




最低維運成本：VPN 網路架構不計價、上傳 / 下載流量不計價

## 挑戰與需求

在各種天災事件頻傳下，無論是高科技產業或傳統產業，都必須強化營運韌性，才能維持在商業市場中的競爭力，以及保護得來不易的商譽。某知名台灣傳統產業的台北總部會將資料備份到本地的單一台 NAS 設備，也會定時將 NAS 設備中的備份資料，傳送到南部分公司的 NAS 設備，但如果總公司出現資訊系統異常的狀況，僅有備份資料的南部分公司，將因沒有相對應的資訊架構而無法在短時間內接手運作，帶來潛在的營運風險。

## 解決方案與效益

該公司 IT 部門與營運團隊討論後，最終選擇能在既有資訊預算、享受雲端災難備援中心服務、同時遏制資安威脅發生的 Acronis Cyber Protect Cloud，實現以下效益：

Acronis Cyber Protect Cloud 是市面上少數符合 NIST 規範的超融合多層次防護架構，能

**一次滿足該公司的全方位需求**

獲得最完善的資料保護服務，並免去勒索軟體的威脅。

Acronis 台灣全球資料中心具備低延遲、高頻寬的特色，不僅

**大幅節省資料備份時間**

當需要啟動雲端災難備服務時，也能在最短時間內完成故障轉移作業，讓該公司儘速恢復正常營運。

Acronis 雲端災難備援中心具備操作簡單的特性，只需

**一鍵即可執行**

資料還原、雲端災難備援，減輕 IT 人員的負擔。

「Acronis 台灣資料中心採用在地化的資源，優異的頻寬、連線速度能提供最即時、快速的雲端災難備援服務。目前已吸引許多台灣傳統產業使用，享受以最合理成本實踐保護資料安全、維護商業運作的目的。」

**Sean Wang**
Acronis 大中華區首席技術顧問

# 台灣實際案例 - 大專院校

## 學校借助 Acronis 在預算內同時完成資安防護、資料備份

**AI 智慧型零時差勒索軟體防護 防堵入侵成效絕佳**


## 挑戰與需求

資訊人力不多、工作繁重、預算有限等，是各級學校共同面臨的挑戰。根據 Acronis 公布 2021 政府、學校、企業的資安風險藍圖，社交工程攻擊、勒索軟體、資安漏洞等，均名列衝擊高、可能性高的第一象限。某知名大專院校曾發生系統維護商在維護期間不小心誤刪資料檔及備份檔，導致學生資料及選課資料遺失的憾事。為避免此類事件重演，該校初期原本想將備份資料放在隨手可得的 NAS 設備上，只是近來 NAS 頻頻爆發漏洞遭到駭客入侵、重要資料被勒索軟體加密的事件，因此需要一套既可輕鬆提升整體資安防護能力，又能降低駭客攻擊威脅的解決方案。

## 解決方案與效益

該校在考量預算、使用便利性等因素下，最終決定運用 Acronis Cyber Protect Cloud 服務，一次解決資安防護、資料備份等問題，並實現以下效益：

Acronis Cyber Protect Cloud 內建 AI 智慧型零時差勒索軟體防護功能，可主動監控異常存取行為及檔案變化狀況，找出潛在的未知威脅。

即使是新種勒索病毒變種也能快速揪出，有效保護校園內部網路的安全。

Acronis Cyber Protect Cloud 代理程式可安裝於 Windows、Linux 和 macOS 等環境中，為端點裝置提供完善的惡意軟體防護。

Acronis 可提供零篡改、零誤刪、零勒索、零病毒等絕對安全的備份儲存功能，可針對備份映像檔進行防惡意軟體掃描，從而減少重複感染的機率。

「在安全備份儲存的基礎下，Acronis 也提供一鍵即可執行資料還原、雲端災難備援的機制，讓資訊人員可在最短時間內完成資料復原，而無需手動進行繁瑣的資料復原流程，同時減輕工作人員的負擔。」

**Sean Wang**
Acronis 大中華區首席技術顧問

Acronis

Cyber Protection

**了解更多 Acronis 的產品和服務：**

**最新動態**
https://www.facebook.com/AcronisTaiwan

**詳細資料**
https://www.acronis.com/zh-tw/

**直接連繫我們，**
**我們將隨時為您提供協助：**

Team-Sales-GCR@acronis.com