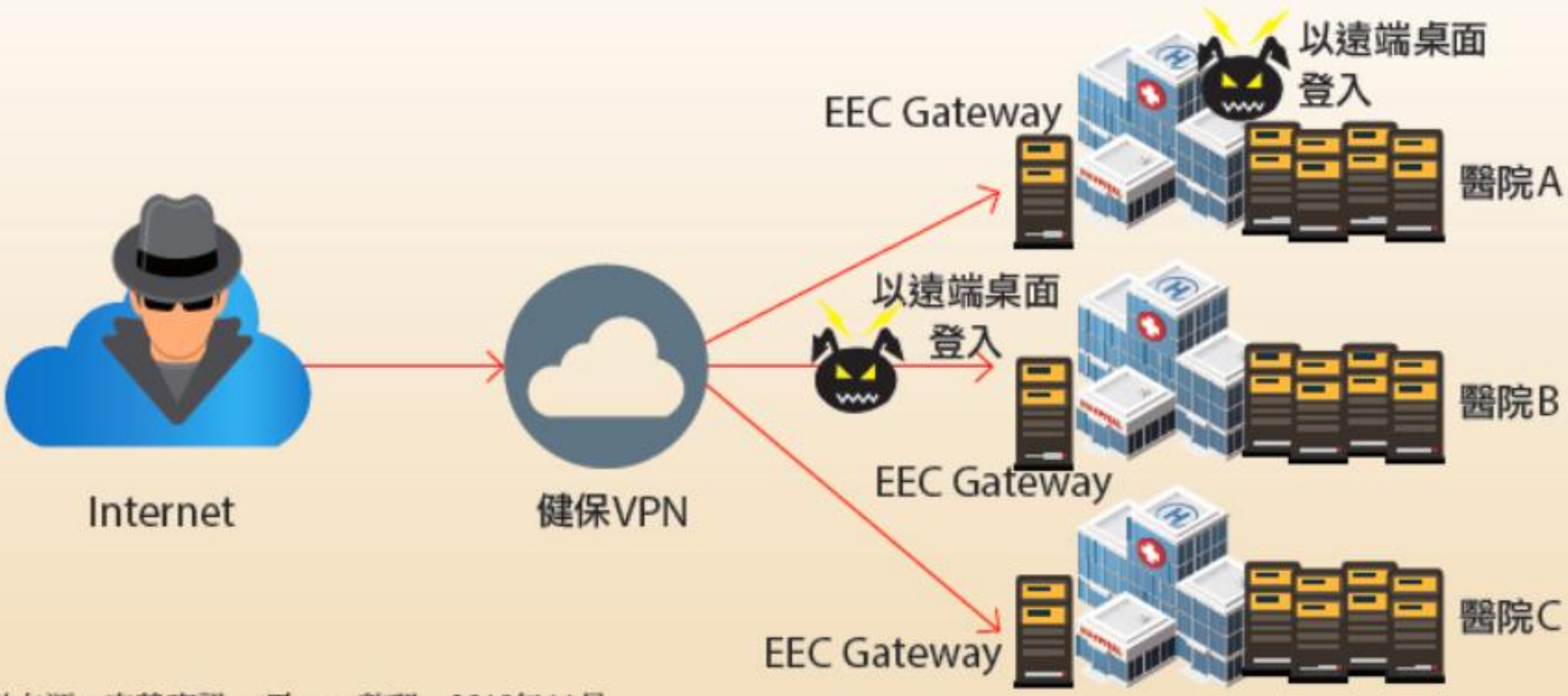
Acronis Cyber Protect Cloud

資安事件頻繁 確定您的防護夠嗎?

勒索軟體攻擊途徑借道健保VPN，同時感染臺灣多家醫院

這次多家醫療院所遭受勒索軟體攻擊，在攻擊途徑上，簡單來說，駭客先是入侵了健保VPN網路，透過衛福部的電子病例交換系統EEC，並透過遠端桌面RDP的管道感染。



資料來源：安碁資訊，iThome整理，2019年11月


ADVANTECH
研華科技
tsmc
國泰人壽
Cathay Life Insurance
群暉科技
Synology
QNAP
威聯通科技
玉山銀行
CHB
彰化銀行
凱基銀行
KGI BANK
DBS
星展銀行
正新橡膠
We Care Family
中國信託銀行
CTBC BANK
台灣大哥大
Taiwan Mobile
台灣高鐵
TAIWAN HIGH SPEED RAIL
凌陽科技
TCE
中華凸版電子股份有限公司
TOPPAN CHUNGHWA ELECTRONICS
中華民國外交部
MINISTRY OF FOREIGN AFFAIRS
REPUBLIC OF CHINA (TAIWAN)
全球頂尖F1賽事,美國職棒,歐洲足球聯賽,日本頂尖賽車 採用Acronis
More than 50 teams use Acronis tech
Arsenal
ROMA
BOSTON RED SOX
AJAX
PFL
Toyota Gazoo Racing
BWT
RACING
WILLIAMS
RACING
DS AUTOMOBILES
TECHEETAH
NIO
333
RACING
ROKiT
VENTURI
ROUSH FENWAY
RACING
Hendrick
MOTORSPORTS

資安威脅態勢越來越複雜

COVID-19 疫情
期間網路犯罪活動突增
300%

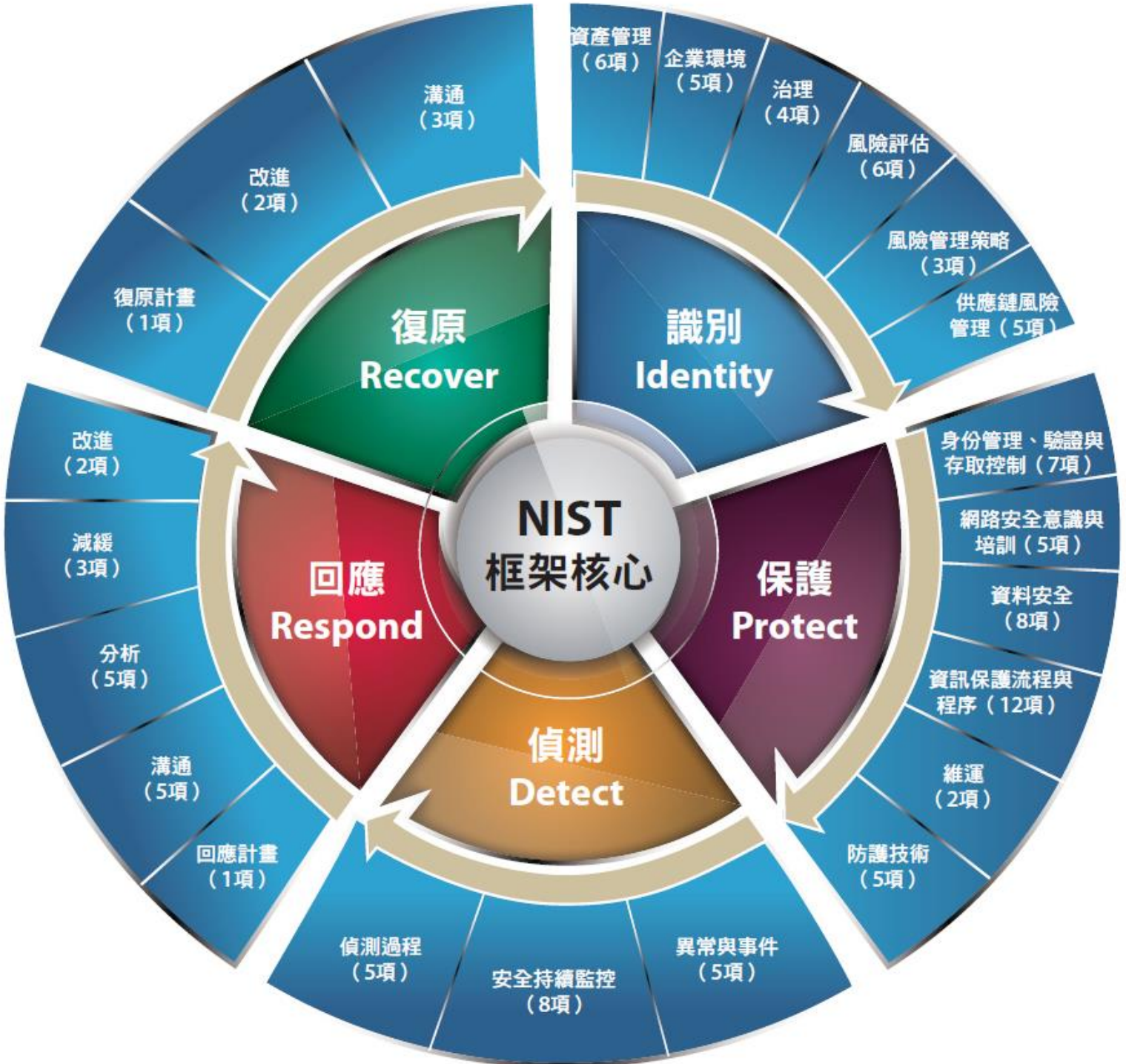
傳統防毒及備份解決方案導
致 **57%** 的攻擊成為漏
網之魚

69% 的管理者
花費更多時間來管理工具
而非抵禦威脅

來源：2020 年 Acronis 網路威脅報告、FBI 2020 年 Acronis 網路警備性報告

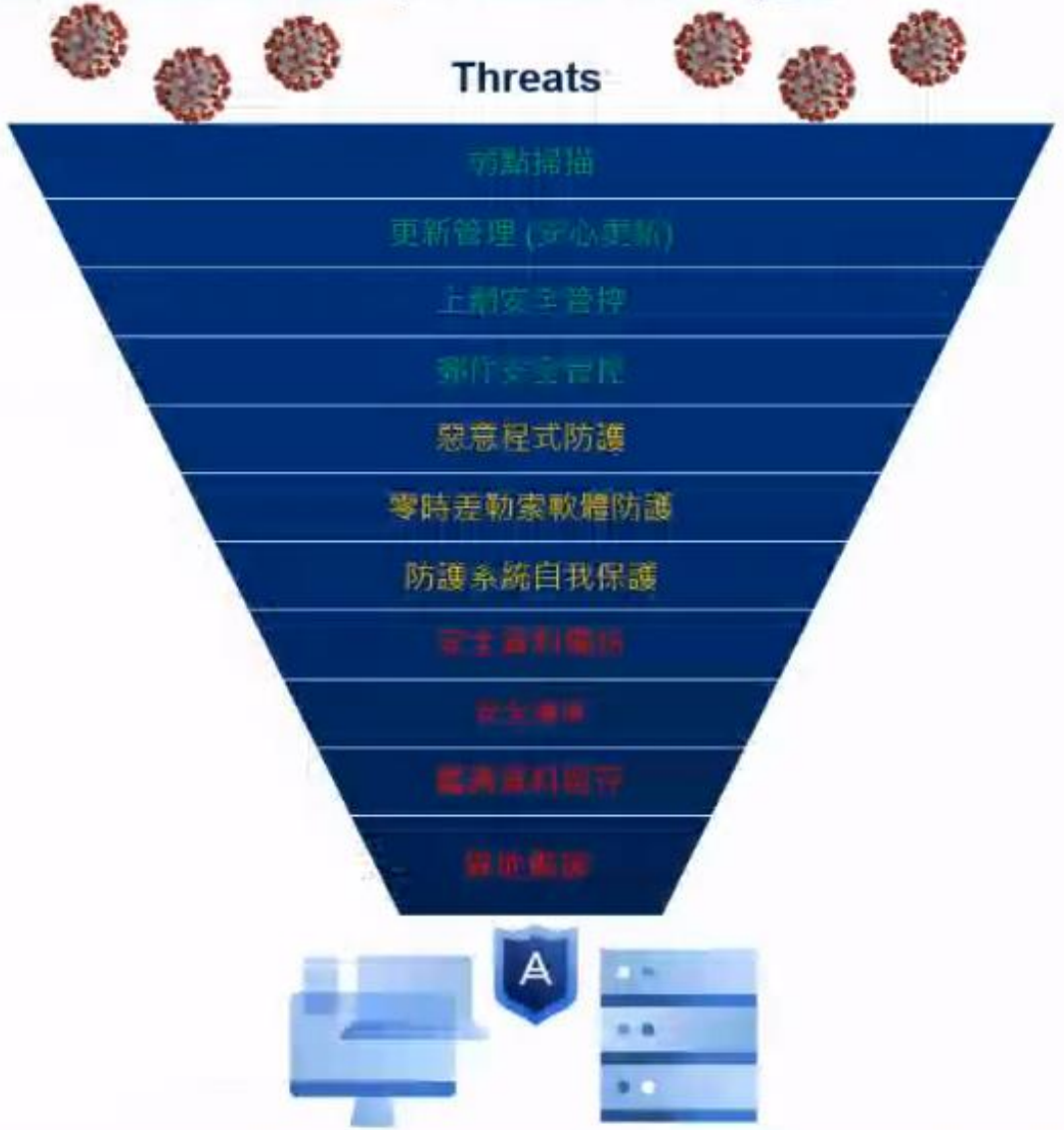
建議企業根據 NIST 資安框架檢視及強化資安管控

- 此框架核心從五大構面評估企業資安防禦現況與目標
- 包含：辨識（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）和復原（Recover）
- 將企業有限的資源應用在目前防護最弱，最需要加強的構面，達到最高效益


NIST
框架核心
識別
Identity
保護
Protect
偵測
Detect
回應
Respond
復原
Recover
資產管理（6項）
企業環境（5項）
治理（4項）
風險評估（6項）
風險管理策略（3項）
供應鏈風險管理（5項）
身份管理、驗證與存取控制（7項）
網路安全意識與培訓（5項）
資料安全（8項）
資訊保護流程與程序（12項）
維運（2項）
防護技術（5項）
異常與事件（5項）
安全持續監控（8項）
偵測過程（5項）
回應計畫（1項）
溝通（5項）
分析（5項）
減緩（3項）
改進（2項）
復原計畫（1項）
改進（2項）
溝通（3項）

Acronis Cyber Protect Cloud 超融合多層次防護

- NIST Identify - 事前預防
  - 資安情資及自動執行對應防護
  - 弱點掃描
  - 更新管理 (**安心更新**)
  - 上網安全管控
  - 郵件安全管控
  - 週邊裝置管控 (資料外洩管控)
- NIST Protect/ Detect/ Respond - 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
- NIST Recover - 事後回復
  - 資料備份 / 連續資料備份
  - 快速資料復原
  - **安心復原 / 備份檔掃毒**
  - 遠端資料抹除
  - **資安鑑識資料留存**

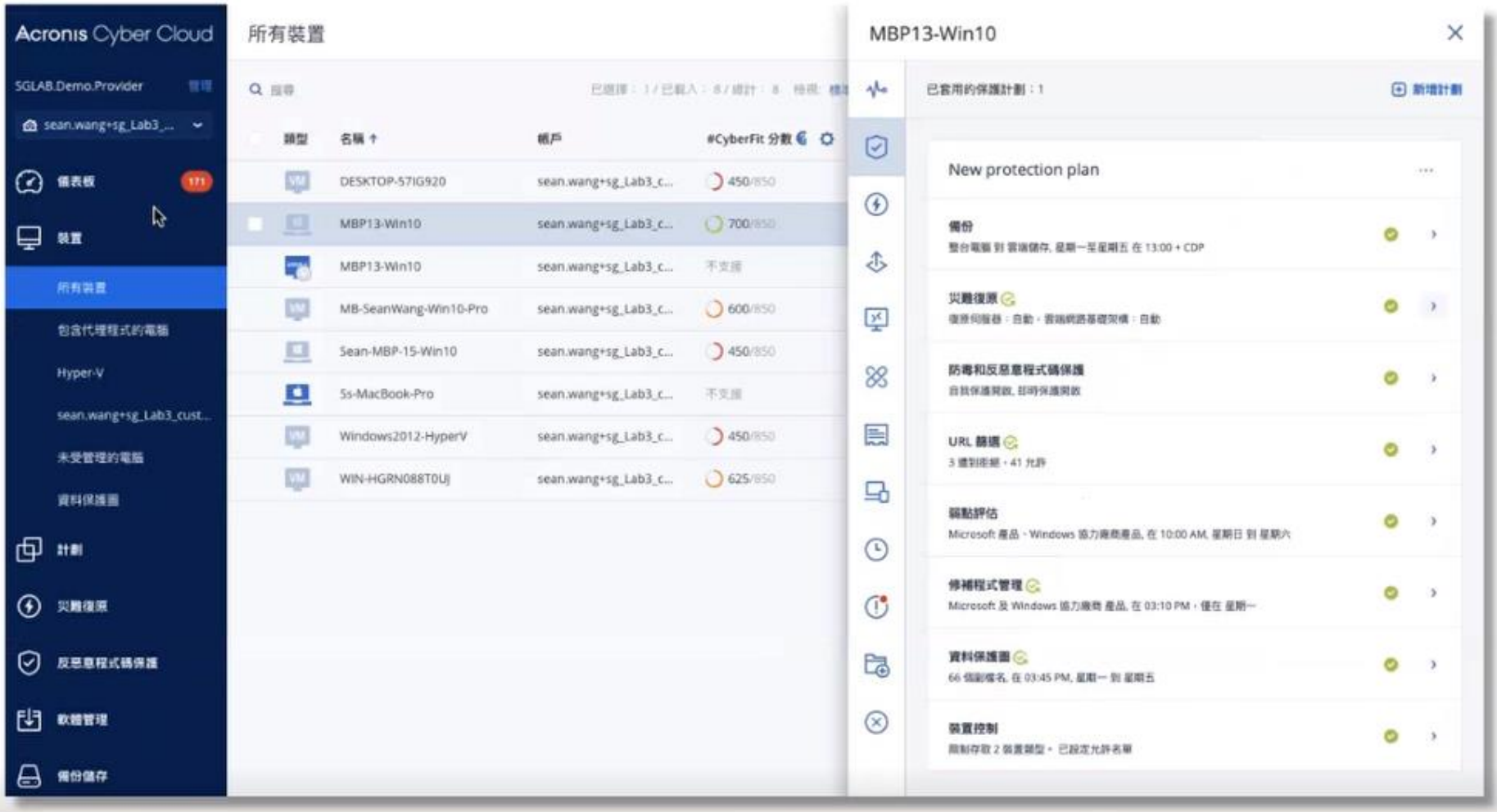


融合為一的力量

獨家

在所有層面進行整合：介面、管理、產品、技術

- 單一 Agent 代理程式
- 單一 Console管理平台
- 單一 Policy防護政策
- 單一後端
- 單一使用者介面
- 單一授權
- 單一廠商支援專線



利用「融合為一」的強大功能，可以：

- 化繁為簡
- 降低成本

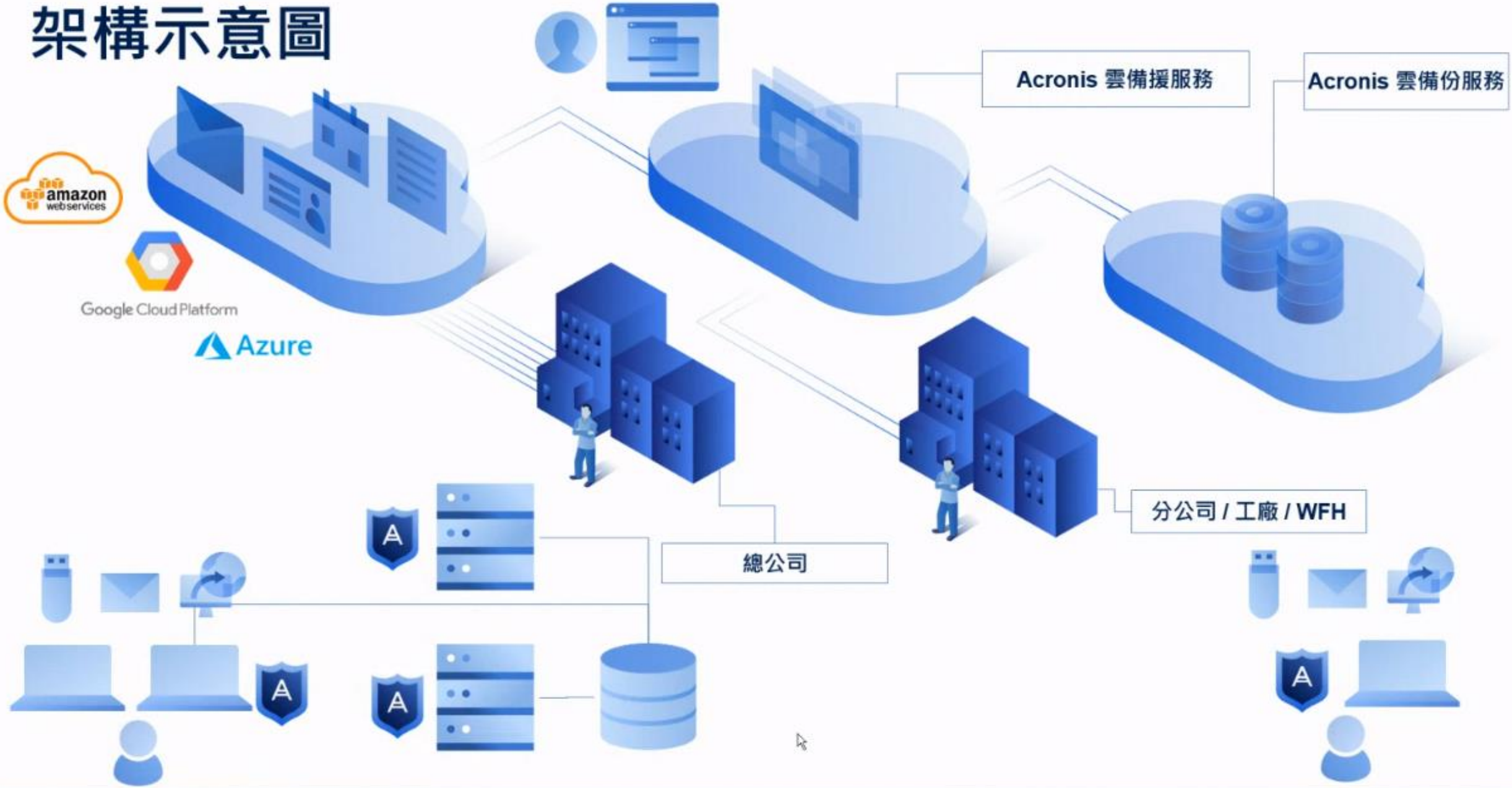
單一防護計畫

所有資安防護層面：

- 備份
- 反惡意軟體防護
- 災難復原
- URL 篩選
- 弱點評估
- 修補程式管理
- Microsoft Defender 防毒軟體和 Microsoft Security Essentials 管理
- 裝置管控

為什麼？ 以較少精力提供更高水準的防護，自動化進行

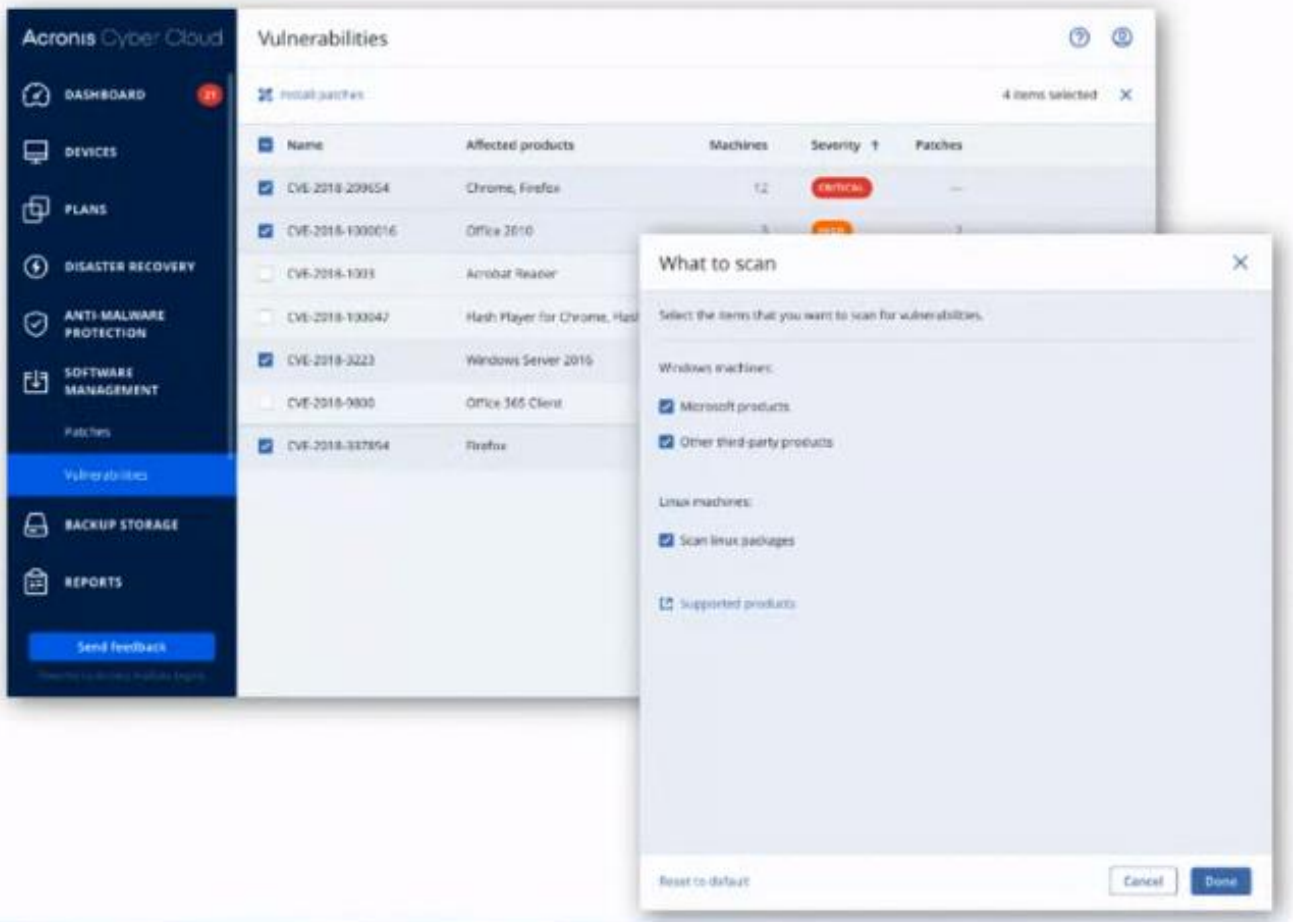
架構示意圖


Acronis 雲備援服務
Acronis 雲備份服務
amazon web services
Google Cloud Platform
Azure
總公司
分公司 / 工廠 / WFH

弱點掃描

在問題出現之前發現問題

- Acronis 的弱點和修補程式管理資料庫持續每日更新
- **支援：**
  - Microsoft：
    a) 工作站 – Windows 7 和更新版本
    b) 伺服器 – Windows Server 2008 R2 和更新版本
    c) Microsoft Office (2010 及其他版本) 和相關元件
    d) .NET Framework 和伺服器應用程式
  - Adobe、Oracle Java
  - 瀏覽器和其他軟體



為什麼？ 減少潛在威脅並防止攻擊

安心更新

Unique

於修補前備份端點，以快速回復至運作狀態

有問題的系統修補程式會導致系統不安全，但修補程式管理回復存在一定的局限性，會很慢。

防故障修補會先建立所選電腦的映像備份，再安裝系統或應用程式修補程式以便快速回復。

- 完整映像備份是回復至可用狀態的最快最簡單的方法

為什麼？ 節省資源，同時支援更快更為可靠的作業

Acronis

事中防護
NIST CSF Protect/ Detect/ Response

AI 智能零時差勒索軟體防護

適用於 Windows、Linux 和 macOS 的惡意軟體防護

- 勒索軟體偵測和自動資料復原
- 挖礦程序偵測
- 即時防護和隨需掃描
- 自我防護：保護 Acronis 元件 (如登錄、服務停止、Acronis 檔案保護)
- Acronis Active Protection 會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 的方法會注視這些行動，並將其與惡意行為模式進行比較。這種方法在識別勒索病毒攻擊方面，非常強而有力，即便是來自從未被發現的勒索病毒變種，亦無法閃避。

Acronis

事後回復
NIST CSF Recover

靈活的儲存選項

雲端儲存

Google Cloud Platform

Acronis Cyber Cloud Storage

Azure

三個全包式雲端儲存選項*

aws

IBM Cloud

Alibaba Cloud

其他公用雲端 *(透過 Acronis Cyber Backup Gateway)*

您自己的第三方雲端儲存

內部部署儲存裝置

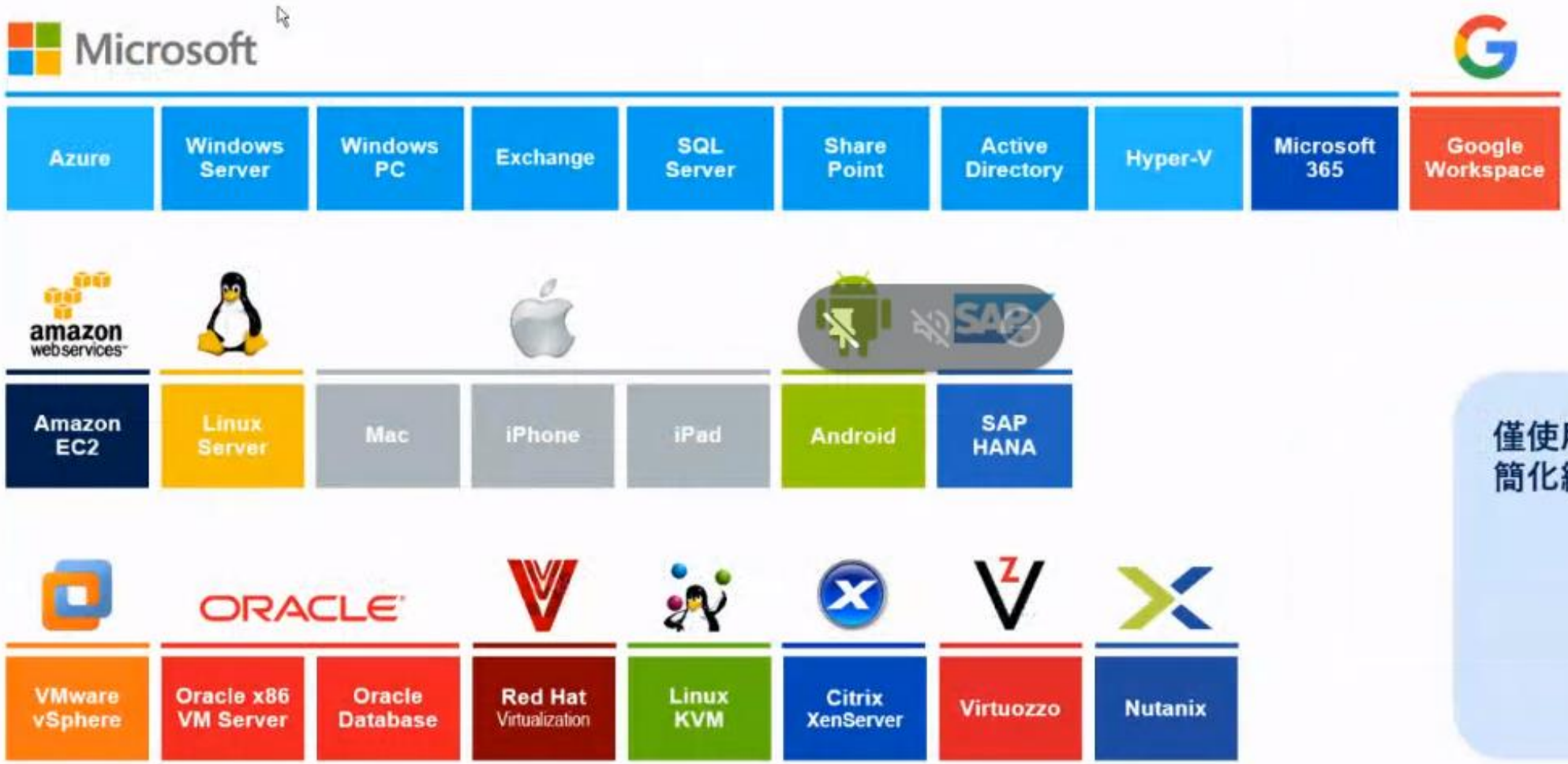
本機磁碟

SMB/CIFS/DFS 和 NFS 共用

Acronis Cyber Infrastructure

> 其他解決方案會使我們陷入不得不告知客戶他們不能做某些事的處境。**Acronis 具有充分的彈性**，這使得我們能夠提供最佳使用者體驗。
>
> **Jason Amato,**
> Centorrino Technologies 的行銷經理

從單一主控台為 20 多個平台提供資料防護



僅使用單一解決方案
簡化網路防護的交付

安心復原

Unique

將惡意程式防護整合至復原程序 避免二次感染

備份中的作業系統映像或應用程式可能含有讓使用者處於風險中的惡意程式

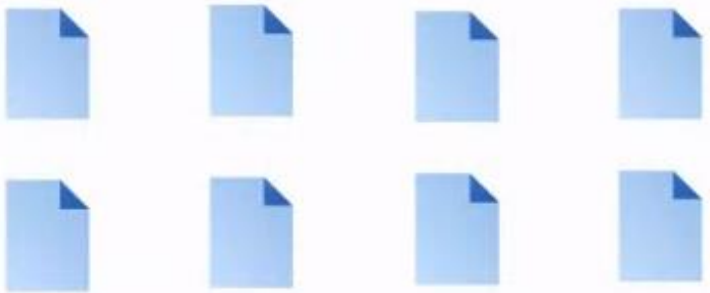
- 更新防惡意程式資料庫 並且自動掃描

為什麼？節省時間、人力。使用乾淨的備份檔快速復原，無需額外步驟

乾淨備份

Unique

備份檔案定期惡意程式掃描 防止還原不乾淨的備份檔



透過在集中位置掃描雲端備份有助於找到潛在的惡意程式，
從而確保使用者還原的是乾淨的備份。

- 提升成功偵測到 Rootkit 和 Bootkit 的可能性
- 還原乾淨資料
- 減少用戶端端點的負載

為什麼？ 以較少精力和資源提供更高水準的防護卸載端點以進行更積極的掃描

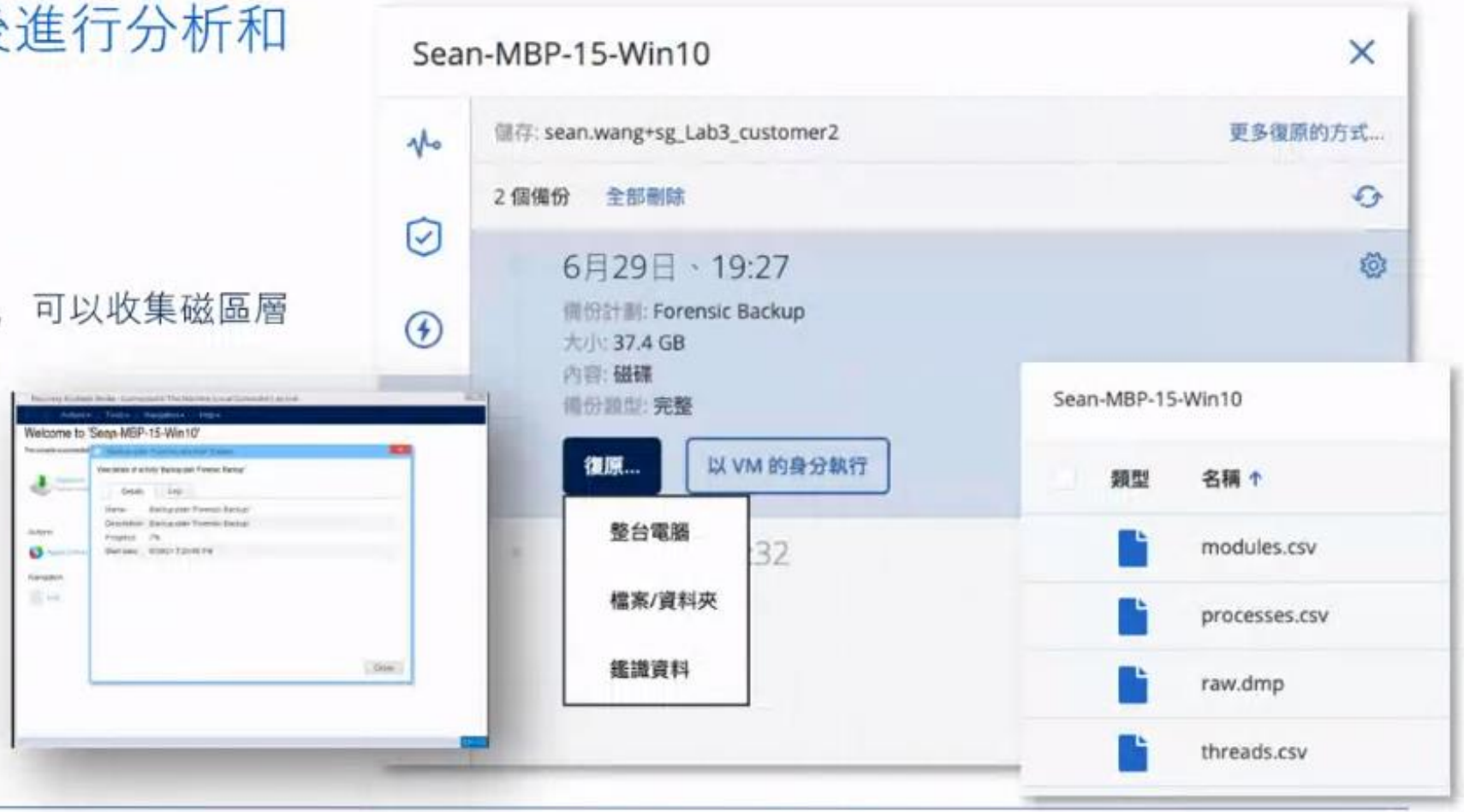
資安鑑識資料備存

Unique

備份重要資料，以及日後進行分析和調查所需的資訊

透過啟動產品中特殊的「鑑定模式」，可以收集磁區層級的記憶體傾印和完整的 HDD 映像。

- 確保備份中的關鍵證據安全
- 使日後調查作業更容易、花費更少



為什麼？ 找出可能影響範圍，降低維運負擔，啟用調查和更佳法規遵循

Acronis

為何選擇 Acronis Cyber Protect Cloud ?

創新的資安防護

與時俱進之自動進化架構

最實用防護整合：反惡意軟體、弱點評估、備份、修補程式管理

多層次防護達到最有效之安控

全面控制受保護系統上的資料生命週期：事前預防、事中防護和事後回復階段

單一代理提供簡單之管理

針對備份和反惡意軟體防護，共用低階攔截的單一代理程式

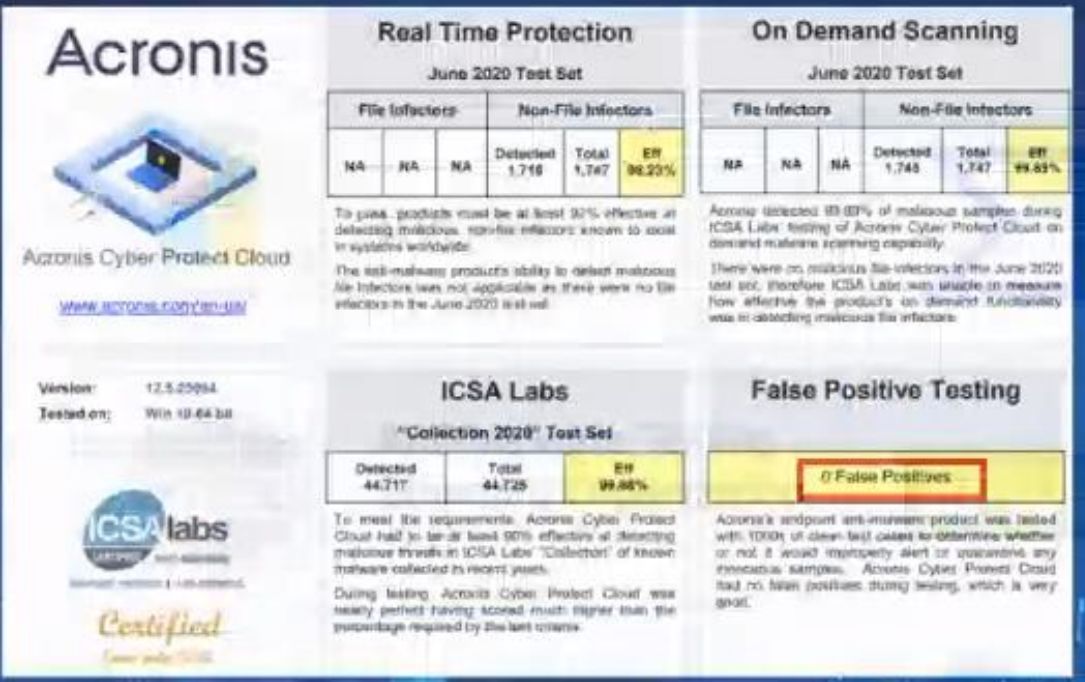
業界最佳技術提供最高之安全等級

在反惡意軟體防護、備份及 AI/ML 方面具有經實證的經驗

簡單的管控減少人力負擔

單一主控台、統一報告、觸控式 UI、單一防護計畫

無數業界資安測試認證



- 最高偵測率
- 零誤判率
- 最佳效能


TAIWAN CYBER SECURITY LANDSCAPE VERSION BETA32
2021 OCT
iThome
Endpoint Prevention
Endpoint Detection & Response
Network Firewall
DDoS Protection
Network Analysis & Forensics
Advanced Threat Protection
Web Security
Risk Assessment & Visibility
WAF & Application Security
Application Security Testing
Managed Security Service
Security Awareness & Training
iThome
臺灣資安市場地圖
TAIWAN CYBER SECURITY LANDSCAPE
VERSION BETA32
Encryption
Data Leak Prevention
Mobile Security
Penetration Testing
Container Security
Cloud Security
GCB
Security Incident Response
NAC
Firewall Management
Secure File Sharing
Authentication
Privileged Access Management
Identity Governance
SOAR
Messaging Security
Security Information and Event Management
Security Analytics
Threat Intelligence
DNS Security
OT Security
《臺灣資安市場地圖》BETA32版，囊括目前熱門的33種資安產品與服務，以及291家廠商，日後將持續更新資訊，以呈現臺灣資安市場完整面貌，歡迎與我們交流討論。
iThome | Version: BETA32(OCT.2021) | Contact:ithomecybenscape@mail.ithome.com.tw

參考資料

- https://www.acronis.com/zh-tw/ Acronis Cyber Protect Cloud全方位網路防護
- https://www.ithome.com.tw/news/133169 【提升企業網路安全新利器】NIST網路安全框架崛起，成為企業資安共通標準
- https://www.ithome.com.tw/tags/%E8%B3%87%E5%AE%89%E4%BA%8B%E4%BB%B6 資安事件列表
- https://www.netadmin.com.tw/netadmin/zh-tw/snapshot/04C60F56343E4625A22F7A944A747301 2021 H1網路資安攻擊數量暴增　勒索病毒仍是企業資安主要威脅
- https://www.knowbe4.com/ransomware-simulator Ransim ransomware simulation tool
- https://www.ithome.com.tw/news/140055勒索軟體攻擊德國醫院導致病患錯失急救黃金期喪命
- https://cloud.acronis.com/login 登入Acronis Cyber Protect Cloud