Version 2 台灣二版
www.version-2.com.tw

組合型產品解決方案 X 專業化在地售後服務

資安解決方案

資安防護首選

銷售專線：02-7722-6899　網站：www.version-2.com.tw　業務部門：enterprise@version-2.tw　技術支援：support@version-2.tw

2024.5.13 版

Version 2 台灣二版
www.version-2.com.tw

台灣二版 Version 2 Limited

資安解決方案 專業代理商與領導者

Version 2 代表再進化，藉由不斷成長蛻變，可以一直與時俱進，不斷進化；

Version 2 是西方勝利的象徵並同時蘊含東方雙數的吉祥，兼具東西方思維，彈性不僵化。

台灣二版 (Version 2) 是亞洲其中一間最有活力的 IT 公司，多年來深耕資訊科技領域，致力於提供與時俱進的資安解決方案 (如 EDR、NDR、漏洞管理)，工具型產品 (如遠端控制、網頁過濾) 及資安威脅偵測應變服務服務 (MDR) 等，透過龐大銷售點、經銷商及合作伙伴，提供廣被市場讚賞的產品及客製化、在地化的專業服務。台灣二版 (Version 2) 的銷售範圍包括香港、中國、台灣、新加坡、澳門等地區，客戶涵蓋各產業，包括全球 1000 大跨國企業、上市公司、公用機構、政府部門、無數成功的中小企業及來自亞洲各城市的消費市場客戶。

台灣二版代理產品總表

資安解決方案

- ATERA — IT服務管理解決方案
- Parallels — Parallels Secure Workspace 企業行動辦公環境解決方案
- BULLWALL — 防勒索軟體解決方案
- cloudm — 雲端轉移解決方案
- Comet — 備份解決方案
- eset — 企業資安解決方案
- jumpcloud — 雲端身份驗證目錄解決方案
- keepit — 雲端備份&復原解決方案
- PANDORAFMS ENTERPRISE — 網路監控解決方案
- portnox™ — 網路存取控管(NAC)解決方案
- runZero — 資產調查與管理解決方案
- SCADAfence — OT高端網路安全解決方案
- SCALE COMPUTING — 超融合解決方案
- senhasegura — 特權帳號管理解決方案
- vRX — 漏洞管理解決方案

工具型軟體

- NordLayer — 遠端安全存取解決方案
- NordLocker — 雲端儲存加密解決方案
- NordPass — 企業密碼管理解決方案
- SAFEDNS — 網路過濾(WebFiltering)解決方案
- SupRemo — 遠端控制解決方案

資安服務

- UnderDefense — 資安威脅偵測應變服務(MDR)

台灣二版 代理產品 目錄

資安解決方案

ESET 企業資安解決方案

工具型軟體

資安服務

資 安 解 決 方 案

Atera · IT 服務管理解決方案

Atera 為新一代專業 IT 管理平台，讓管理服務供應商 (MSP) 和 IT 專業人員隨時掌握和管理複雜資訊，無論身在何處，也能為戶提供高質量、即時的服務。因應遠端工作的需求，協助企業建立和支援強大的混合工作環境，並有效地為遠端工作人員提供服務。

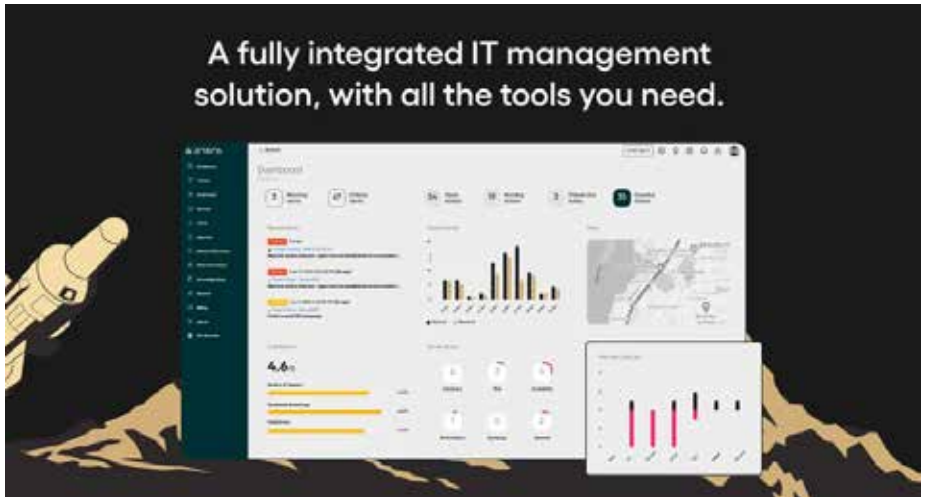
擁有完整的遠端監測與管理 (RMM) 控制權，可內建熟悉的工具組合，及智能自動化設定，讓您在提升業務的同時，也能輕鬆跟上用戶的需求。

▼主要功能

1. 全方位的遠端監測與管理（RMM）和 PSA（Professional Services Automation）平台，讓管理服務供應商 (MSP) 和 IT 專業人員隨時掌握和管理複雜資訊
2. 依技術人員的數量計價
3. 部署簡單，五分鐘即可啟動
4. 省時自動化
5. 具認證的嚴密安全性

▼介面說明

▼示意圖



▼ Atera 指標客戶

▼獎項

Parallels Secure Workspace・企業行動辦公環境解決方案

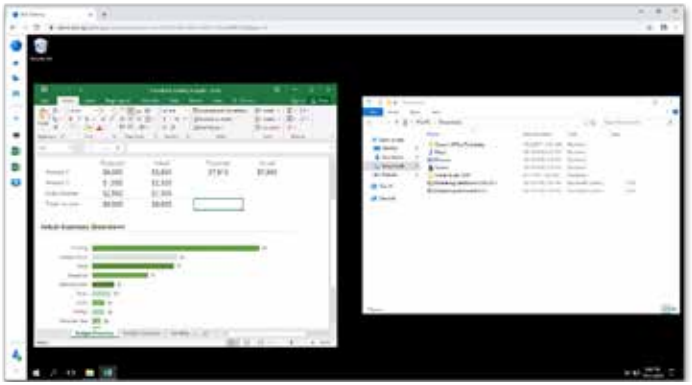
根據 IDC 預估，超過 50% 的企業組織員工在後疫情時代，有部分時間將採取遠距工作，但無論疫情是否結束，如何為混合辦工場域打造 24x7 不間斷連線，已經成為企業將面臨的問題。【Parallels Secure Workspace 企業行動辦公環境解決方案】(舊名：Awingu) 為雲服務，不需安裝額外的硬體或閘道器，就能將企業等級的內部環境延伸到遠距工作場所，保護企業資訊安全，也讓員工能夠享有良好工作效率；除此之外，亦能提供以身分為基礎的存取控制 (Role-based access control) 服務，確保每個遠距端點受到安全防護。

▼主要功能

1. 可隨時隨地透過一般網路瀏覽器與任何設備連接 (無需管理員或考慮 client 端設備)
2. 易於部署和維護，使用 Active Directory，30 分鐘內完成設定，且系統資源占用少及低頻寬 (僅為 VPN 需求的十分之一)
3. 高度安全的遠端連接：
   - 內建 Session Recordings，掌握所有存取記錄
   - 可追溯所有已完成的存取並進行稽核
   - 監控異常及使用者存取
   - 可進行區域限制、IP 限制等控制性設定
   - 內建 MFA 認證機制
4. 支援舊版、Web 和 SaaS 應用程式及任何公有雲 (AWS / Azure / GCP)
5. 可做為 VDI(特定情境) 之替代方案

▼示意圖

▼介面說明



▼ Parallels Secure Workspace 指標客戶

proximus　Port of Antwerp　NHS　the Y　AVIAPARTNER
東方・花旗 citi ORIENT　Politie Police　UDLAP　telenet　BZL

BullWall・防勒索軟體解決方案

BullWall 的 RansomeCare (RC) 專利技術是目前唯一針對檔案 (文件) 方面的解決方案，通過機器學習 (ML) 分析檔案 (文件) 活動，並使用檢測傳感器來識別威脅 -- 無論檔案 (文件) 類型或活動如何；無論檔案 (文件) 是重新命名、修改、建立還是刪除。一旦 RC 檢測到惡意加密，就會在幾秒鐘內隔離任何受影響的用戶或設備，防止對文件共享的重大損害及影響。

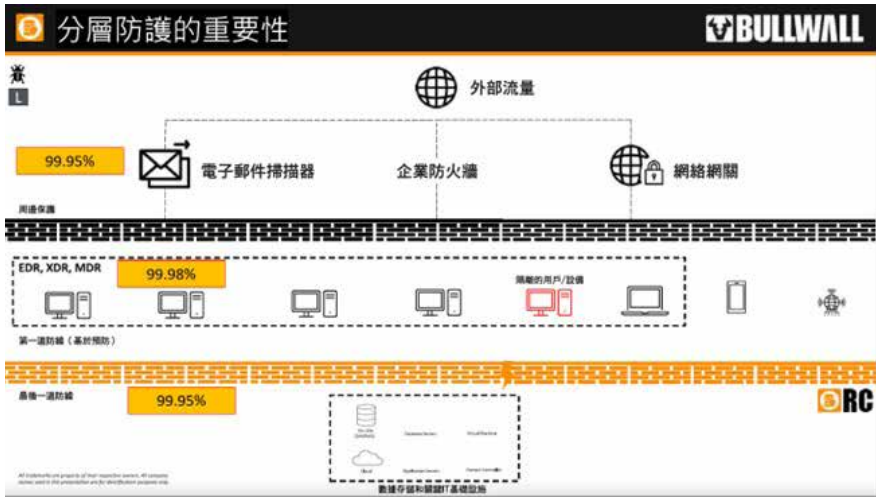
▼主要功能

1. 實時 (Real-Time) 偵測檔案變更
2. 利用多種方法偵測加密行為
3. 即時回應遏制勒索軟體
4. 列出受影響檔案清單快速還原損毀檔案
5. 產出通報機制要求報告快速通知相關機構

▼介面說明

RC RansomCare

▼示意圖



▼ BullWall 指標客戶

TEMPUR +SEALY　RICOH imagine. change　Bank of Ireland

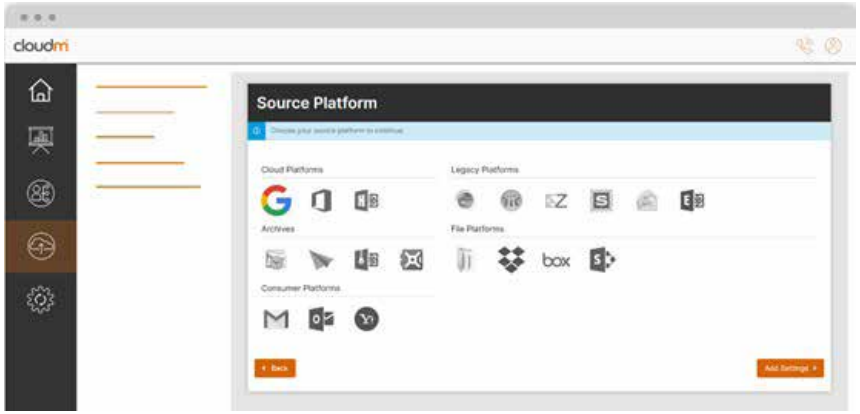
CloudM · 雲端轉移解決方案

CloudM 於 2018 年成立，位於英國曼徹斯特，是一家屢獲殊榮的 SaaS 公司，為適用於 Microsoft 365 和 Google Workspace 的全球領先之雲端轉移工具，協助全球 40,000 多家客戶進行超過 7,500 萬次的轉移，包括 Spotify、Netflix 和 Uber 等世界知名公司皆是 CloudM 的客戶。

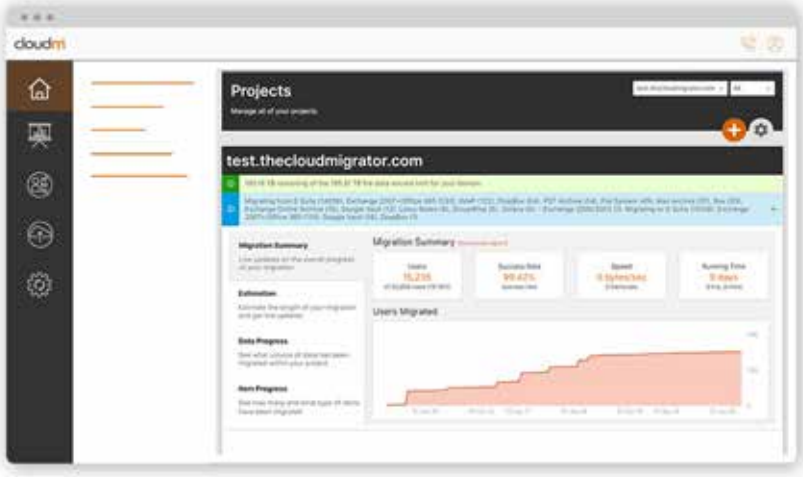
▼主要功能

1. 能從數十個原先平台輕鬆轉移到新平台
2. 全面的轉移前環境掃描
3. 多個伺服器進行轉移
4. 即時查看轉移進度
5. 可簡單進行轉移的設置
6. 轉移到雲存儲 / 從雲存儲轉移

▼介面說明



▼示意圖



▼ CloudM 指標客戶

GROUPON　HomeServe　Spotify　Carrefour
TELUS International　NETFLIX　THG IDEAS WITH MOMENTUM　SALSIFY　RSPCA
Booking.com　Kempinski　Uber

▼獎項

computing
Cloud Excellence Awards 2021 Winner

Comet・備份解決方案

Comet 成立於 2015 年，於 2017 年 2 月推出此款備份軟體，為跨平台並具有高效、靈活及多功能的備份和復原解決方案，可以支援企業和一般用戶，執行伺服器備份到選擇的雲端儲存服務，或協助完整複製整個伺服器環境至雲端。

▼主要功能

1. **為災難復原和企業運營提供資料保護**

   無論雲備份、電腦備份還是資料備份，都能提供保護和復原磁碟機代號 (分區)、資料庫、伺服器、文件和文件夾，支援 Windows、MacOS 和 Linux。

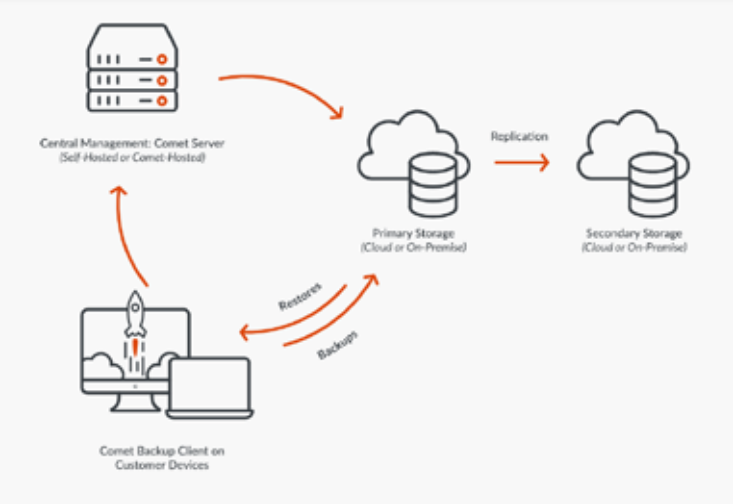
2. **快速、安全、加密**

   藉由刪除重覆資料，將資料分解成壓縮的加密區塊，進而提高寬頻和存儲空間效率。在進行第一次備份後，不必再次重新上傳完整文件。

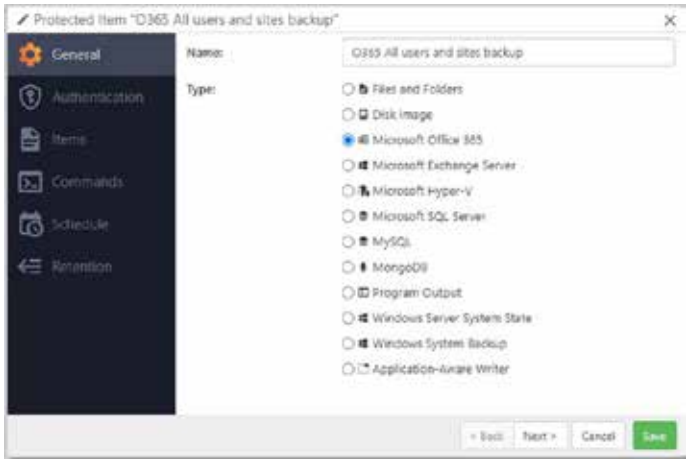
3. **可跨平台**

   能備份於 Amazon AWS、Google Cloud Storage、Microsoft Azure、Backblaze B2、Wasabi、Let'sEncrypt、OpenStac 等平台。

▼示意圖



▼介面說明



▼獎項

中大型企業安全解決方案 雲端版 ESET BUSINESS SOLUTIONS

專為 5 台以上之企業防護設計，與本地端解決方案不同，雲端版將主機放置在 ESET 維護的雲端環境中執行，用戶端可依照用戶需求靈活運用及搭配，節省大量資源及成本。版本內結合了端點、伺服器，利用遠程集中管理方式，為企業資訊安全提供便利又多重的保障。

組合配置說明	ESET PROTECT ENTRY 標準雲端版	ESET PROTECT ADVANCED 進階雲端版	ESET PROTECT COMPLETE 旗艦雲端版	ESET PROTECT Elite 企業雲端版 (最低25台)
ESET PROTECT CLOUD 雲端中控台	●	●	●	●
ESET ENDPOINT ANTIVIRUS 端點防毒	●	●	●	●
ESET SERVER SECURITY 檔案伺服器安全	●	●	●	●
ESET ENDPOINT SECURITY 端點網路安全	●	●	●	●
ESET LIVEGUARD ADVANCED 動態威脅防禦		●	●	●
ESET FULL DISK ENCRYPTION 全硬碟加密		●	●	●
ESET CLOUD OFFICE SECURITY 雲端辦公室安全			●	●
ESET MAIL SECURITY 郵件安全			●	●
ESET INSPECT CLOUD 端點進階威脅偵防系統				●
ESET CLOUD MOBILE DEVICE MANAGEMENT 行動設備管理	●	●	●	●
ESET Vulnerability & Patch Management 漏洞和修補程式管理				●

中大型企業安全解決方案 ESET BUSINESS SOLUTIONS

專為 5 台以上中大型企業防護設計，可依照用戶需求靈活運用及搭配，節省大量資源及成本。版本內結合了端點、伺服器、行動裝置，利用遠程集中管理方式，為企業資訊安全提供便利又多重的保障。

組合配置說明	ESET PROTECT ESSENTIAL PLUS On-prem 簡易加強版	ESET PROTECT ENTRY On-prem 標準版	ESET PROTECT ADVANCED On-prem 進階版	ESET PROTECT COMPLETE On-prem 旗艦版
ESET PROTECT 本地端中控台	●	●	●	●
ESET ENDPOINT ANTIVIRUS 端點防毒	●	●	●	●
ESET SERVER SECURITY 檔案伺服器安全	●	●	●	●
ESET ENDPOINT SECURITY 端點網路安全		●	●	●
ESET LIVEGUARD ADVANCED 動態威脅防禦	●		●	●
ESET FULL DISK ENCRYPTION 全硬碟加密			●	●
ESET MAIL SECURITY 郵件安全				●

小型企業安全包 ESET BUSINESS SECURITY PACKS

適合小型企業、家庭辦公室，台數在 5-20 台電腦以內，依品項不同內含檔案伺服器安全、郵件伺服器安全，並提供行動裝置防護，為小型企業提供最經濟實惠的資安防護包。

★ 此組合包為固定台數販售，無法增加或減少授權台數。

組合配置說明（單位：台）		可使用裝置數	電腦	檔案伺服器	行動裝置	郵件伺服器
家庭辦公室資安包		5 U	5	1	5	
		10 U	10	1	5	
		15 U	15	1	5	
		20 U	20	2	5	
小型公司資安包		5 U	5	1	5	8
		10 U	10	1	5	15
		20 U	20	2	5	25

ESET V11 中控台（EP）ESET PROTECT

論及這幾年來，最讓人倍感威脅的攻擊，就是以加密使用者電腦檔案，並要使用者支付贖金，才能復原檔案的勒索軟體（Ransomware）。ESET 企業產品 V10 則針對這個部份加強了防護，可抵禦所有已知的勒索威脅，並且阻止零日漏洞攻擊，隨著各式新型勒索軟體變種不斷湧現，升級至 ESET 新版 V11，就可助您遠離災害。

▼重要功能說明

1. **靈活的安裝機制**

   可安裝於 Windows、Linux 或虛擬設備上，完成安裝後，管理者可透過 Web 控制台，而且從任何一台設備或操作系統輕鬆登錄進行所有管理。

2. **更新美化用戶介面（UI）**

   為了讓管理者易於閱讀及操作，主要功能表、使用者介面、圖示皆做了更新及美化。

3. **可以建立多個用戶的權限群組**

   可以建立多個用戶的權限群組，分層設定其登錄 / 管理範圍之權限，簡化大型企業團隊的職責。

4. **硬體資訊管理**

   可以從 Windows、macOS 和 Linux 系統收集已安裝的硬體資訊。

5. **可客製報表及通知系統**

   通知系統具有完整的 WYSIWYG（所見即所得）編輯器，您可以自行設定想要收到的格式內容。另外有 170 多種內置報表，讓您輕鬆快速地客製報表。

6. **支援虛擬桌面架構（Virtual Desktop Infrastructure，簡稱 VDI）**

   每次機器連線到伺服器，就會從其硬體指紋建立一個項目，在重新安裝機器之後，此指紋不會改變，可用來比對新連線的機器與先前連線的機器，讓您輕鬆解決複製電腦之間的衝突。

7. **強化勒索軟體防護功能（Ransomware Shield）**

   這項功能是 ESET 所開發的『主機入侵防禦系統（HIPS：Host-based Intrusion Prevention System）』的一部分，可保護電腦免於勒索軟體的威脅。

8. **標籤**

   使用任意數目且使用者可完全定義的標籤來標記相關物件，輕鬆地用來識別並尋找相關的物件集。

9. **支援 ESET 新的資安產品（為提供的付費服務，需額外購買。）**

   - ESET 動態威脅防禦（ESET LiveGuard Advanced）
   - ESET 端點進階威脅偵防系統（ESET INSPECTOR）
   - ESET 全硬碟加密（ESET FULL DISK ENCRYPTION）

▼系統支援

Windows Server：
2022、2019、2016、2012 R2、2012

Linux Server：
RHEL、CentOS、Ubuntu、SLED 等主要發行版

虛擬設備：
VMware vSphere/ESXi
VMware Workstation
VMware Player
Hyper-V
Oracle VirtualBox、Citrix

硬體需求：
記憶體：4GB
硬碟空間：100GB
硬碟 IOPS：500 MBps
處理器：4 核心；2.1GHz 或以上
網路連線：建議 1Gbit/s

＊詳細資訊請依官網為主

▼介面說明

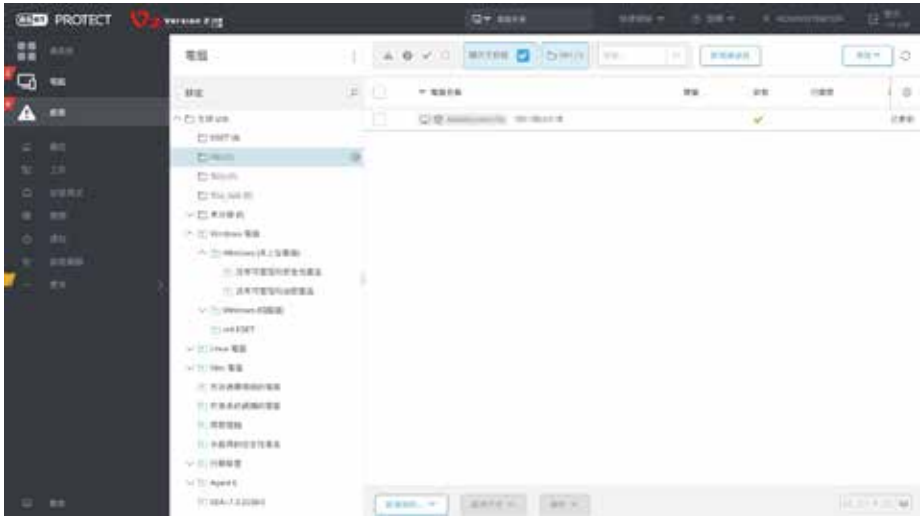
1. Web 介面重新設計：

新的主要功能表、精美的使用者介面、新圖示、重新設計的快速連結和說明連結。

2. 靜 / 動態群組分類：

靜態群組：手動移除或新增特定的用戶端電腦至該資料夾。

動態群組：依據自訂的特定條件自動篩選至該資料夾。



3. 報告：

可依據管理者需求，自訂各式報表及報表呈現方式。

企業端點網路安全 (EES) ESET ENDPOINT SECURITY
企業端點防毒 (EEA) ESET ENDPOINT ANTIVIRUS

專為企業開發的網路安全產品，ThreatSense® 掃描引擎技術結合了雙向防火牆與反垃圾郵件模組，加快速度及精確度確保電腦安全。此產品擁有完整的安全解決方案，結合最強防護與低系統使用量，基於人工智慧的進階技術，能夠主動消除病毒、間諜軟體、特洛伊木馬、蠕蟲、廣告軟體、rootkit 及其它網際網路型入侵攻擊，且不妨礙系統效能或中斷電腦運作。 ★ 此為解決方案支援之產品，不單獨販售報價。

▼主要功能

1. **防毒 / 反間諜**

   遠離網路威脅，透過識別碼及基因碼，偵測未知變種或已知威脅，並清除所有類型病毒包括：病毒、隱藏惡意程式、蠕蟲和間諜軟體。

2. **釣魚網站防護**

   防範假冒網站竊取個人及企業帳戶資料。

3. **裝置控制**

   依使用者權限不同來設定為拒絕存取、讀取或讀取與寫入，也可將其設為白名單。

4. **進階記憶體掃描器**

   針對多層加殼及隱藏偽裝的惡意軟體，藉由快取記憶體中的程式行為分析，準確判斷並阻擋惡意程式。

5. **HIPS 主機入侵防禦偵測**

   藉由代碼行為規則，精準阻擋未知型病毒威脅，並可透過自主規則設定，加強系統防護能力。

6. **防禦程式漏洞**

   針對網路瀏覽器（IE、Google …等網頁瀏覽器）、PDF 閱讀器、JAVA、Flash 及其它 web2.0 相關技術進行漏洞偵測，防止惡意程式或其它威脅攻擊。

7. **ESET Live Grid 雲端偵測**

   為雲端的預早警告系統，利用從「雲端」技術所提供的相關資訊即時串流，將防護功能維持在最新狀態。

8. **防禦殭屍網路**

   防範殭屍網路等惡意軟體入侵，預防企業內部的電腦發出垃圾郵件、網路攻擊、駭客對外攻擊，避免造成更大的損失。

9. **雙向防火牆（僅限 ESET ENDPOINT SECURITY 適用）**

   防止未授權的遠端連線至公司網路，提供反駭客防護及預防機密資料外洩。

10. **網頁監控（僅限 ESET ENDPOINT SECURITY 適用）**

    允許管理者封鎖可能包含潛在冒犯性資訊的網站。

11. **垃圾郵件防護（僅限 ESET ENDPOINT SECURITY 適用）**

    垃圾郵件過濾器能與系統搭配運作來預防威脅，針對廣告信件或大量寄發之郵件伺服器進行有效過濾，防止使用者接收電郵的風險。

12. **安全的瀏覽器（僅限 ESET Endpoint Security 適用）**

    零信任的方式，假設電腦或其防護功能都已遭破解或不足，同時不允許篡改瀏覽器的記憶體空間，因而無法篡改瀏覽器視窗的內容。（預設不啟用）

13. **WMI 和完整登錄檔掃描**

    改善登錄檔掃描，在登錄檔或 WMI 存放庫中尋找並消除惡意參照或危險內容。

▼系統支援

Windows：	macOS：	Linux：	Android：
11、10	10.15 以上	(only ESET Endpoint Antivirus) Ubuntu、Red Hat	Android 5 以上

＊詳細資訊請依官網為主

▼介面說明

1. 防護狀態：

顯示關於 ESET 軟體的防護資訊。

2. 電腦掃描：

可自行調配所需的掃描類型，也可用拖拉式的方式將檔案個別掃描。

3. 設定：

可調配該用戶的電腦、網路 或 Web 和電子郵件安全性設定，適合進階用戶使用。

4. 工具：

可協助簡化程序管理，因應管理者不同的需求，為進階用戶提供額外選項的模組。

檔案伺服器安全（ESS）ESET SERVER SECURITY

完全相容於中控台（ESET PROTECT）工具，能簡單有效地滿足伺服器之網路需求，對所有類型之惡意攻擊提供主動威脅偵測、高速掃描及檢測率，只需占用極低的系統資源即可完成。

▼主要功能

1. **防毒 / 反間諜**
   遠離網路威脅，透過識別碼及基因碼，偵測未知變種或已知威脅，並清除所有類型病毒包括：病毒、隱藏惡意程式、蠕蟲和間諜軟體。

2. **HIPS 主機入侵防禦偵測**
   藉由代碼行為規則，精準阻擋未知型病毒威脅，並可透過自主規則設定，加強系統防護能力。

3. **裝置控制**
   依使用者權限不同來設定為拒絕存取、讀取或讀取與寫入，也可將其設為白名單。

4. **Web 存取防護**
   掃描 HTTP / HTTPS 等通訊協定，並可設定 URL 位址管理。

5. **支援叢集環境（Cluster）**
   本基礎架構可讓 ESET 伺服器產品彼此互相通訊及交換資料，例如配置和通知及同步化產品執行個體群組中正確作業所需的資料。

6. **支援 Hyper-V**
   支援微軟虛擬化技術。

7. **自動排除**
   偵測已知服務（DC、SQL Server、IIS 等）並自動依照最佳建議排除相關資料夾檔案。

8. **占用系統資源低**
   提供強大防護性能同時，為日常應用程序預留了更多的系統資源。

9. **ESET Live Grid 雲端偵測**
   為雲端的預早警告系統，利用從「雲端」技術所提供的相關資訊即時串流，將防護功能維持在最新狀態。

10. **OneDrive 掃描**
    可用於掃描放置在 OneDrive 雲端儲存空間中的檔案。適用於 Office 365 商業帳戶。

▼系統支援

Windows Server：	Server Core ：	Linux Server：
2022、2019、2016、2012 R2、2012	2022、2019、2016、2012 R2、2012	RHEL 7 (x64) 以上 CentOS 7 (x64) 以上 Ubuntu Server 18.04 LTS (x64) 以上 Debian 10 SLES 12(x64) 以上

＊詳細資訊請依官網為主

ESET 動態威脅防禦 ESET LIVEGUARD ADVANCED

近年 APT 進階持續性威脅（Advanced Persistent Threat）攻擊事件猖獗，無論是惡意郵件、勒索病毒或是釣魚信件的威脅與日俱增，ESET 動態威脅防禦專門解決未知威脅，為付費型雲端服務，此方案會協助企業將可疑文件自動提交給 ESET 雲端伺服器，由進階惡意軟體檢測引擎進行分析，並提供關於惡意行為的報告給客戶（授權數需達 1,000 台），該報告則提供觀察到的樣本行為的摘要，能更有效的偵測到 APT 攻擊及勒索病毒，幫助企業對抗詭譎的網路威脅。 ★ 此為解決方案支援之產品，不單獨販售報價。

▼產品優勢

1. **多重防禦，層層篩選過濾更透澈**

   新型態的攻擊行為與勒索軟體都是經過一次又一次的變種與演化的版本，ESET 動態威脅防禦，運用三種不同的機器學習模式處理上傳的文件樣本並在完全沙箱進行模擬分析，而惡意軟體試圖蒙蔽或逃避檢測等技巧，都將無所遁形。

2. **深度學習偵測引擎，平均分析 5 分鐘內搞定**

   ESET 動態威脅防禦採用高效率設計，將多數樣本的分析時間控制在 5 分鐘以內，對於原先已分析過的樣本，只需要幾秒鐘便可反饋結果，令公司所有設備均可及時得到防護。

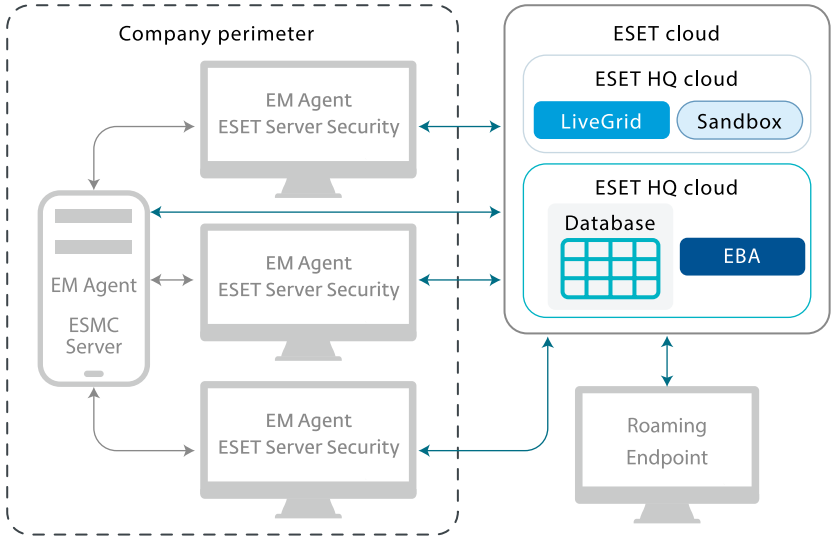
3. **訊息完整並即時同步**

   ESET 動態威脅防禦所分析的每個樣本，皆可在中控台（ESET PROTECT）讀取，另外 ESET 雲端防護系統（ESET LiveGrid®）的全部資料，也都會同步更新於此，企業可即時做好資安攻防。

▼主要功能

1. 行為分析檢測
2. 機器學習技術
3. 零日威脅防禦
4. 雲端沙箱

▼流程說明



▼系統支援

ESET Endpoint Antivirus（第 7 版及更新版本）
ESET Endpoint Security（第 7 版及更新版本）
ESET Mail Security（第 7 版及更新版本）
ESET File Security for Windows Server（第 8 版及更新版本）

＊詳細資訊請依官網為主

全硬碟加密（EFDE）ESET FULL DISK ENCRYPTION

提供由 ESET 遠程管理控制台本地管理的強大加密功能，並提高組織的數據安全性，可從 ESET PROTECT Cloud 或 ESET PROTECT 管理使用，由於熟悉現有的管理環境和概念，可幫助管理員節省時間。實現法律合規性的基本加密解決方案。不僅可以保護企業免受數據丟失的影響。還可以幫助其遵守 GDPR 等數據保護法規。

★ 此為解決方案支援之產品，不單獨販售報價。

▼主要功能

1. **通過一個控制台管理所有產品**

   ESET FULL DISK ENCRYPTION (EFDE) 在 ESET V10 中控台（ESET PROTECT）中工作，由於熟悉現有的管理環境和概念，可幫助管理員節省時間。

2. **全面驗證**

   專利技術可為各種規模的企業保護數據。ESET FULL DISK ENCRYPTION (EFDE) 是經過 **FIPS 140-2 驗證的 256 位 AES 加密**。

3. **強大的加密**

   ESET FULL DISK ENCRYPTION (EFDE) 對系統磁盤，分區和整個驅動器進行加密，以確保存儲在每台 PC 或筆記本電腦上的所有東西都被鎖定和保護，以防止丟失或被盜。

4. **跨平台覆蓋**

   通過單個儀表板管理 Windows 計算機上的加密和本機 macOS 加密（FileVault）。

5. **一鍵式部署**

   從基於雲的控制台管理整個網絡上的全磁盤加密。中控台（ESET PROTECT）單一窗格可讓管理員單擊一下即可在其連接的端點上部署，開通和管理加密。

6. **隨時添加其他設備**

   您可以隨時增加許可證涵蓋的設備數量。

▼端點加密（EEE）& 全硬碟加密（EFDE）差異

功 能 / 特 色	全硬碟加密 (EFDE)	端點加密 (EEE)
全硬碟加密	●	●
可攜式媒體加密		●
文件與文件夾加密		●
電子郵件與附件加密		●
虛擬磁碟與檔案加密		●
授權方式	每個裝置附加於 ESET PROTECT	每個使用者單獨購買
購買方式	每個裝置附加於 ESET PROTECT	每個使用者單獨購買

▼系統支援

Microsoft Windows：
7、8、8.1、10、11

macOS：
10.14（Mojave）及更高版本
※ 需在雲端或本地部署的中控台（ESET PROTECT）

＊詳細資訊請依官網為主

雲端辦公室安全（ECOS）ESET CLOUD OFFICE SECURITY

主要目標是保護 Microsoft 365，透過易於使用的雲管理控制台，為 Microsoft 365 應用程序提供針對惡意軟件，垃圾郵件和網絡釣魚攻擊的高級預防性保護。

▼主要功能

1. **反垃圾郵件**

   屢獲殊榮的引擎來提高性能，可以過濾所有垃圾郵件，並使用戶郵箱中不會出現未經請求或不想要的郵件。

2. **反惡意軟體**

   掃描所有傳入的電子郵件和附件以及所有新的和更改的文件，這有助於使用戶的郵箱免受惡意軟件的侵擾，並防止惡意軟體通過雲存儲在多個設備上傳播。

3. **反網路釣魚**

   阻止用戶造訪被稱為網路釣魚站點的網頁，電子郵件中可能包含導致網路釣魚網頁的連接。

4. **通知事項**

   通知消除了經常檢查儀表板的需要，從而大大提高了管理員的效率。

5. **自動保護**

   啟用此選項，管理員可以確保在 Microsoft 365 用戶中新增用戶時，自動受到保護，而無需轉到控制台分別添加它們。

6. **查核管理員**

   管理員可以檢查此存儲部分中的對象，然後決定刪除或同意，此功能提供對由我們的安全產品隔離的電子郵件和文件的簡單管理。

▼系統支援

瀏覽器：

Mozilla Firefox , Microsoft Edge , Google Chrome , Opera , Safari

Microsoft 365 plans：

Microsoft 365 enterprise plans：

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3, E5, F3
- Office 365 E1, E3, E5

Microsoft 365 business plans：

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Microsoft 365 Education plans：

- Microsoft 365 A3, A5

Exchange Online plans：

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

OneDrive plans：

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

＊詳細資訊請依官網為主

郵件伺服器安全（EMS）ESET MAIL SECURITY

因惡意軟體犯罪者經常利用電子郵件擴散感染，故企業郵件伺服器成為重要的第一防線。

ESET MAIL SECURITY 替多個平台提供最佳的反惡意軟體與主動掃描，更快的效能、整合反垃圾郵件及占用系統資源低等特性可處理高流量郵件伺服器工作。

▼主要功能

1. **防毒 / 反間諜**
   掃描所有進出資訊，支援 POP3、SMTP 與 IMAP 協議，從閘道層過濾電郵威脅，含間諜軟體在內。
2. **垃圾郵件防護**
   過濾垃圾郵件與釣魚郵件，攔截率高。
3. **主機防護**
   全方位伺服器防護，包括即時防護與手動掃描功能。
4. **寄送隔離區報告**
   可設定定期寄送郵件隔離區報告給使用者，並提供 Web 介面讓使用者自行管理已隔離郵件。
5. **自訂訊息處理規則**
   可設定多種條件規則過濾郵件，例如自動將附件為執行檔的郵件隔離。
6. **實現集中管理**
   支援 ESET 遠程管理伺服器，透過 Web 控制介面全方位管理。
7. **Office 365 信箱掃描**
   對於使用混合 Exchange 環境的企業，掃描雲端信箱。
8. **網路釣魚防護**
   可防止使用者存取已知是網路釣魚網頁的功能。(含 mail 內容通往網路釣魚網頁的連結)
9. **郵件隔離區報告**
   隔離區報告是傳送至選定使用者或系統管理員的電子郵件，以提供所有已隔離電子郵件的相關資訊。其也可讓他們遠端管理已隔離的內容。
10. **匯出至系統日誌伺服器 (Arcsight)**
    允許信箱伺服器防護記錄的內容以常見事件格式 (CEF) 複製到系統日誌伺服器，以搭配 Micro Focus ArcSight 等防護記錄管理解決方案使用。

▼系統支援

ESET Mail Security for Exchange Server：

Microsoft Windows Server 2019、2016、2012 R2

Microsoft Exchange for Server：2019、2016、2013、2010 SP3

ESET Mail Security for IBM Lotus Domino：

Microsoft Windows Server 2019、2016、2012 R2、2012

IBM Domino Server 6.5.4 以上

＊詳細資訊請依官網為主

端點進階威脅偵防系統（EI）ESET INSPECT

端點為絕大多數 APT 以及指定目標攻擊的入侵點。防護這類攻擊需要即時監控及評估網路中所有的活動，以及在必要時採取對應的動作。ESET INSPECT (EI) 是一個端點偵測及回應工具，應用進階技術監控和評估端點所有可疑程序、違反原則，以及高危險行為。並且在發生異常的時候提供詳細報告以及可採取的動作選項。

★ 此為解決方案支援之產品，不單獨販售報價。

▼主要功能

1. **蒐集情資**

   ESET INSPECT (EI) 會持續收集端點上所有活動的詳細資料。這些資料將會集中並上傳至控制伺服器即時評估，並提供高效能的搜尋以及過濾選項。

2. **解讀資料**

   ESET INSPECT (EI) 可自動將所有線索串聯起來，找出所有看似安全的程序，檔案以及活動中間的關聯性，並透過進階的評估機制抓出隱藏威脅以及弱點。

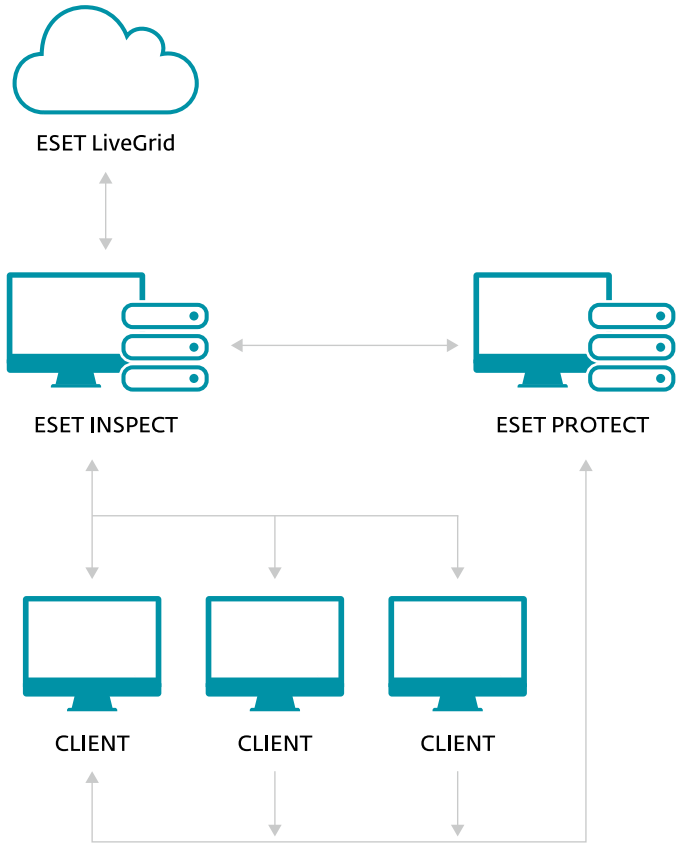
3. **因應措施**

   所有可疑程序都可阻擋，已被入侵的端點可在第一時間隔離，將網路通訊限制在內部系統或者是 ESET INSPECT (EI) 管理伺服器。

4. **可用性**

   ESET INSPECT (EI) 儀表板提供一目了然的網路活動資訊。視覺化的資料呈現方式幫助您簡單看出入侵點，影響範圍，存取到的檔案等等。讓您了解這些資料的關聯性在哪裡，程序第一次在哪裡被執行等等調查資安事件時所需要的重要資訊。

▼流程說明



▼系統支援

用戶端：
Microsoft Windows：10、11
macOS 10.15 (Catalina) +

伺服器：
Microsoft Windows Server 2012、2012R2、2016、2019、2022

MS SQL：
Microsoft SQL Server 2017+

MySQL：
MySQL 5.7.41+、MySQL 8.0.32

＊詳細資訊請依官網為主

雲端行動裝置管理 ESET CLOUD MOBILE DEVICE MANAGEMENT

保護企業行動裝置免於惡意軟體威脅，即使裝置遺失或遭竊也能確保資料安全，管理員可監視已安裝的應用程式，或依照類別、權限及程式來源，封鎖應用程式存取，並提醒用戶解除安裝危險之應用程式，降低其暴露風險。支援中控台（ESET PROTECT）。

★ 僅適用於中大型解決方案（雲端版）

▼主要功能

1. **即時防護**

   採用 ThreatSense® 掃描引擎技術，其專為行動設備設計，能即時保護所有應用程式及檔案。

2. **釣魚網站防護**

   阻止假冒網站竊取機密資料，例如 : 用戶名、密碼與網路銀行資料…等。

3. **簡訊與來電過濾**

   保護用戶免受未知號碼或指定聯絡人電話及簡訊騷擾，更可針對指定時段設定免騷擾功能。

4. **集中管理功能**

   裝置的設定不符合公司安全策略時，程式會自動通知用戶與管理員，提出調整建議。

5. **應用程式控管**

   替管理員提供已安裝程式監控、阻止連線及提示用戶移除特定程式等功能。

6. **防盜功能**

   可設定信任 SIM 卡保護及鎖屏、資料刪除、警報器…等遠端命令。

▼系統支援

Android 5 (Lollipop) 和更新版本

※ 不支援雙 SIM 卡智慧手機裝置及通話功能的平板電腦之無法使用如防盜、SMS 和通話過濾等功能。

＊詳細資訊請依官網為主

雙重認證安全（ESA）ESET SECURE AUTHENTICATION

提供公司網路與資料安全、易用的遠端連線雙重認證功能，其採用一次性雙重密碼認證機制（2FA-OTP），密碼隨機而成無法預測或重覆使用，可廣泛搭配各類 VPN 應用與商業工具，包含 Microsoft SharePoint 與 Microsoft Dynamics CRM 等，透過登錄遠程桌面或 VMware Horizon View，大幅提高外出辦公時遠端連線至公司設備瀏覽機密資料的安全性。

▼主要功能

1. **2FA 輕鬆上手**

   身份驗證很容易：只需回覆發送到手機的提示即可，適用於 iOS 和 Android 設備，以及所有平台和服務。

2. **多種驗證方式**

   支援 APP、推播通知、硬體令牌，FIDO 安全密鑰以及自定義方法。

3. **雲端支援**

   除本地 APP 外，透過 ADFS 3.0 或 SAML 協議支援 Web / 雲服務，例如 Office 365，Google Apps，Dropbox 等。

4. **遠程管理**

   使用其自己的簡化管理控制台，可透過 Web 瀏覽器造訪。

5. **安裝設定簡單有效率**

   無論企業員工多寡，皆能夠同時安裝設定並且不需要花費太多時間，就算公司沒有 IT 人員，依舊很有效率。

6. **無需專用硬體**

   只需在伺服器上安裝並開始設定即可。

▼系統支援

伺服器端：

Microsoft Windows Server 2008、2008 R2、2012、2012 R2、2016、2019、2022

Windows Small Business Server 2008、2011

Windows Server 2012 Essentials、2012 R2 Essentials、2016 Essentials、2019 Essentials

用戶端：

Windows 7、8、8.1、10、11

行動設備用戶端：

iOS 12 ~ 16 以上（iPhone）、

Android 4.4 ~ 13 以上版本 (Google Play Services 10.2.6)

＊詳細資訊請依官網為主

郵件加強版（EPMP）ESET PROTECT MAIL PLUS

防止垃圾郵件和惡意軟體到達用戶的郵件信箱，利用多層反垃圾郵件，反網路釣魚和主機服務器保護技術，保護用戶及其電子郵件（最被利用的威脅媒介）。該解決方案包括雲沙箱技術，防止零日威脅和勒索軟體防護。並可透過雲端管理控制台進行管理。一鍵安全部署，無需購買或維護其他硬體即可提供網路可見性，進而降低成本。

▼主要功能

1. **一鍵式管理**

   單擊即可進行新增或排除，提交文件以進行進一步分析或啟動掃描之類的操作。

2. **查核管理**

   隔離郵件後，將向用戶發送電子郵件，並且可以自行處理。 管理員可以決定從中央隔離區刪除或同意該郵件。

3. **定義通知**

   使用預定義的通知或新增自己的通知。 通知系統具有完整的 " 所見即所得 " 編輯器。

4. **反垃圾郵件**

   可以防止垃圾郵件到達用戶的郵箱。包括 SPF 和 DKIM 驗證，反向散射保護和 SMTP 保護。

▼系統支援

伺服器：

Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007
Microsoft Small Business Server 2011
IBM Domino 6.5.4 及更高版本

＊詳細資訊請依官網為主

端點加密軟體（EEE）ESET ENDPOINT ENCRYPTION

資料為企業重要資產，但隨著員工出差、企業網路傳輸而導致外洩，讓企業面臨重大安全危機，簡單易用的資料加密軟體，適用於所有類型之企業，利用軟體既有的優化配置，加快管理員佈署時間，採用單一 MSI 安裝檔，只需幾個動作，即可增強用戶規範性、強化公司資料安全管理。

▼主要功能

1. **全面驗證**

   專利技術可為各種規模的企業保護數據。採用美國國家安全局認可最高安全進階加密標準 AES 256 位元加密技術進行 FIPS 140-2 驗證。

2. **無需伺服器**

   不需安裝在伺服器，並且可以無縫支援遠程用戶。

3. **內建 TPM 安全晶片**

   以獨立的安全晶片利用公開金鑰架構（Public Key Infrastructure，PKI）產生無法複製的數位簽章，來驗證存取資料的平臺與硬碟的身份。

4. **依數據粒度防護**

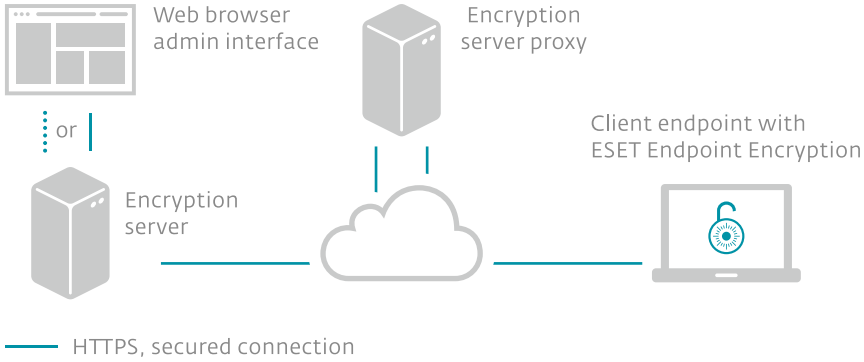
   協助企業增強保護特定文件，文件夾，虛擬磁盤或檔案的能力。

5. **保護傳輸中的數據**

   電子郵件包含三種加密方式：立即加密、發送時加密及加密並發送，保護電子郵件在傳送同時，避免遭受惡意干擾。

6. **集中管理**

   管理員透過控制台統一部署加密方案，並可以按照需求，為整個公司、管理團隊及當前加密項目建立共享密鑰，分層管理權限。



▼系統支援

用戶端：

Windows：11、10、 8.1、8、7 SP1

伺服器端：

Windows Server 2019、2016、2012 R2、2012、2008 R2、2008

Windows：11、10、8.1、8、7

＊詳細資訊請依官網為主

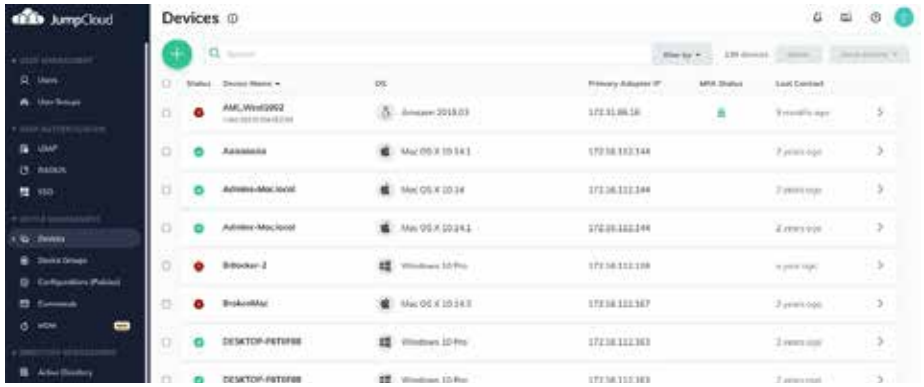
JumpCloud・雲端身份驗證目錄解決方案

JumpCloud 於 2012 年在美國科羅拉多州創立，為提供雲端目錄即服務 (Directory as a Service) 的軟體公司，它旨在協助簡化具有多個用戶目錄或不想自己安裝目錄的企業進行目錄管理；也是可以提供核心身份和存取控制服務、行動式裝置管理、多因素驗證 (MFA)，單點登錄（Single Sign On，簡稱為 SSO）等的雲目錄平台。JumpCloud 擁有超過 180,000 個組織的全球用戶，以及 5,000 多個付費客戶，是建構具彈性的目錄驗證服務，或者想替代地端 AD 目錄的最佳選擇。

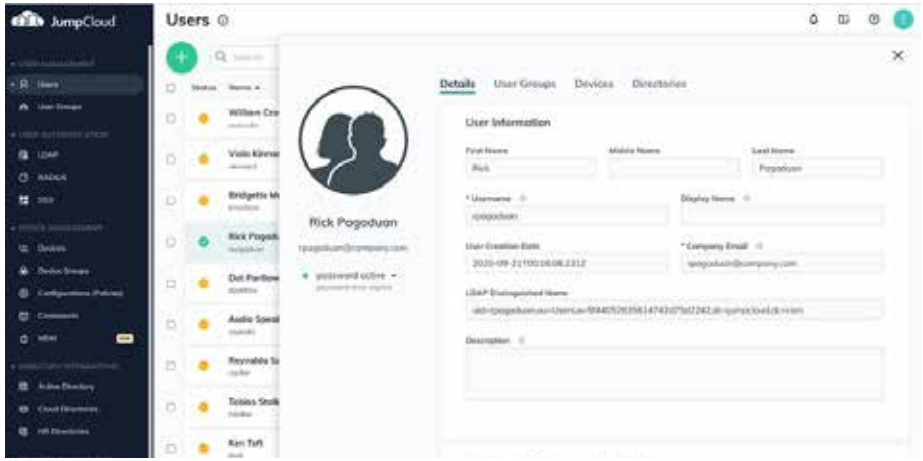
▼主要功能

1. 雲端目錄服務
2. 集中身份管理
3. 靈活管理
4. 實現零信任架構之安全遠程訪問（Secure Remote Access）
5. 合規及管理

▼介面說明



▼示意圖



Keepit · 雲端備份 & 復原解決方案

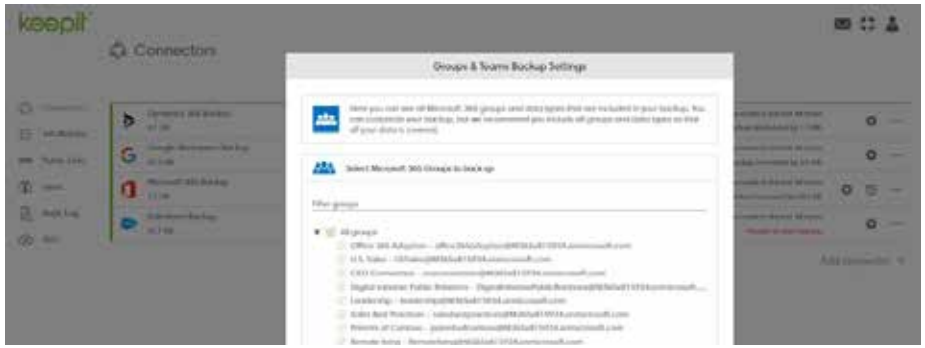
Keepit 成立於 2007 年，總部位於哥本哈根，是一家軟體即服務 (SaaS) 公司，為資料 (數據) 儲存於雲端的企業，以區塊鏈驗證解決方案為架構，提供保護 SaaS 資料 (數據) 安全及管理服務的中立及獨立雲端供應商；Keepit 可確保在包括 Microsoft 365、Azure Active Directory、Salesforce、Google Workspace 和 Dynamics 365 等的資料 (數據) 之安全，在全球設有辦事處和資料 (數據) 中心，擁有數千個企業用戶，並獲得國際標準化組織 (簡稱：ISO) 及國際電工協會 (簡稱：IEC) 之資訊安全管理系統 (簡稱：ISMS) 的國際標準 --27001:2013 認證及得到研究和評論平台 TrustRadius 的最高評價的肯定。

▼主要功能

1. 7x24 確保企業重要資訊系統持續提供服務，不會受到天災人禍、駭客攻擊等事件影響
2. 以區塊鏈驗證解決方案為架構，確保資料 (數據) 之安全
3. 遵守監管機構要求 (如 GDPR)，將風險降至最低
4. 操作簡單，數分鐘內與原先系統接軌
5. 快速的協助企業資料 (數據) 復原，僅需幾秒鐘
6. 符合成本效益並兼具未來的彈性擴充需求

▼示意圖

▼介面說明



▼ Keepit 指標客戶

SAXO BANK · GOLDBECK · Danish Cancer Society · ORIFARM · SKIVEKOMMUNE · THE OCEAN CLEANUP · INNOVATION · OXFORD · Innovation Norway · PILGRIM · HAARSLEV Processing Technology · RATHGEBER

▼獎項

TrustRadius	Capterra	Gartner peerinsights	G2
4.5	4.8	5.0	5.0

PandoraFMS・網路監控解決方案

Pandora FMS 為業界熟知且專業的最佳網路監控工具之一，為首席執行官兼創始人 Sancho Lerena 的個人項目，經過不斷的發展，成為公司監控套件，跨越國界和語言，並提供市場上最完整的解決方案之一；Pandora FMS 的目標是為公司提供集成的橫向監控解決方案，結合來自不同來源和部門的訊息，提供單一的控制平台。

▼產品特色

1. **多合一監控**

   為監控 IT 基礎設施、網路、應用程式及服務的平台，協助用戶整合監控工作並降低監控設置的複雜性。

2. **靈活性**

   用戶能夠根據自己的特定需求進行設定，可支援廣泛的技術、協議和資料來源，能夠適應不同的環境。

3. **具彈性**

   能夠從單個伺服器監控數萬台設備和服務，還支援分佈式監控，用戶能在多個伺服器上擴展監控基礎設施。

4. **高延展性**

   具有模組化架構，用戶能透過插件和模組，添加新的監控功能和特性，更容易整合其他系統和工具。

5. **多元化報價**

   提供包括企業版及依雲端需求的計價方式，無論企業規模或任何預算，都可以選擇使用。

▼示意圖

▼介面說明

▼獎項

Portnox・網路存取控管 (NAC) 解決方案

企業內部網路防禦，長久以來乙太網路已成為基礎網路的標準，但是同時也因先天上簡單的設計，沒有任何管理或控制連網設備的機制，造成不易管理、無法有效監控上線設備的問題；又隨著 BYOD（Bring Your Own Device）各種移動設備的盛行，需求不斷地成長，再加上內網安全與管理需求不斷地增加，NAC（Network Access control）解決方案主要的功能就在於解決設備在連上企業或組織內部網路的第一時間，如何來判斷其是否合法，有無權限進入網路的問題。

▼產品優勢

1. **集中管理裝置連線狀態**

   能全面偵測並隨時偵測有哪些人持有哪些裝置（設備），透過何種方式欲存取企業網路，無論是公司員工、外來訪客、遠端上下游合作廠商或在家工作的員工…等，不同身分的使用者有不同的網路存取權限。

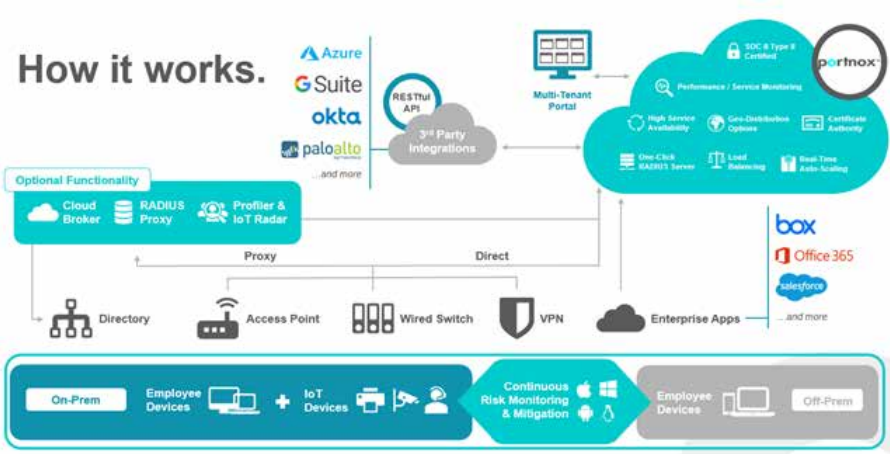
2. **整合無線網路管理機制**

   不論是透過內部區域網路（LAN）、無線區域網路（WLAN）、遠端透過虛擬私人網路（VPN）、廣域網路（WAN）等何種管道連線進入企業網路，所有的進入點都能夠全面偵測。

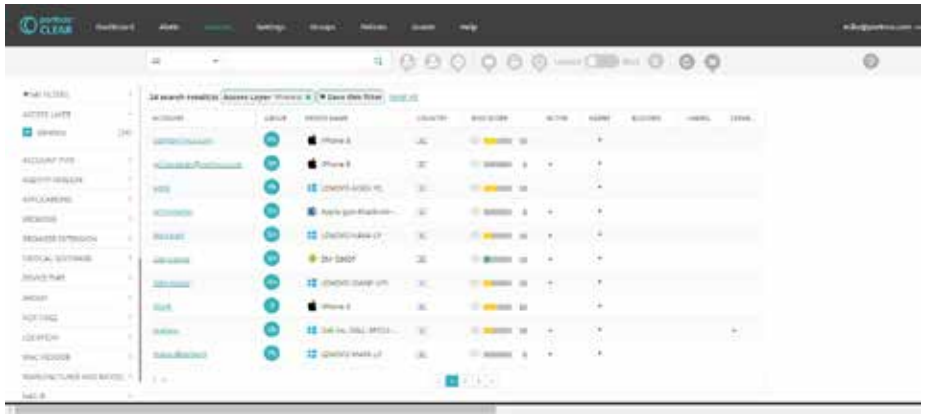
3. **支援多種身份驗證來源**

   支援包括 RADIUS、DHCP、微軟 AD 架構等多種不同後端身分認證方式。

▼示意圖



▼介面說明



▼ Portnox 指標客戶

ArcelorMittal　aunalytics　ROIVANT SCIENCES　Scottish Water　VISA

▼獎項

runZero・資產調查與管理解決方案

runZero 由 Metasploit（安全測試框架）的建立者 HD Moore 於 2018 年創立，是 HD Moore 發想的一種創新積極的資產調查與管理解決方案，此方案可以在沒有任何資料依據的情況下，協助企業查找和識別網路上的所有資產；作為一名資安研究和滲透測試人員的他，因長期需要運用不同方式查找並整合設備的資訊，故累積了大量關於安全滲透測試的應用研究及技術，所以建立了 runZero。

▼產品特色

1. **部署簡單快速**

   在任何地方、任何平台上，只需部署 runZero Explorer（輕量級掃描引擎）即可執行掃描操作，並於數分鐘內將數據上傳到控制台。

2. **完整且準確資產清單資料**

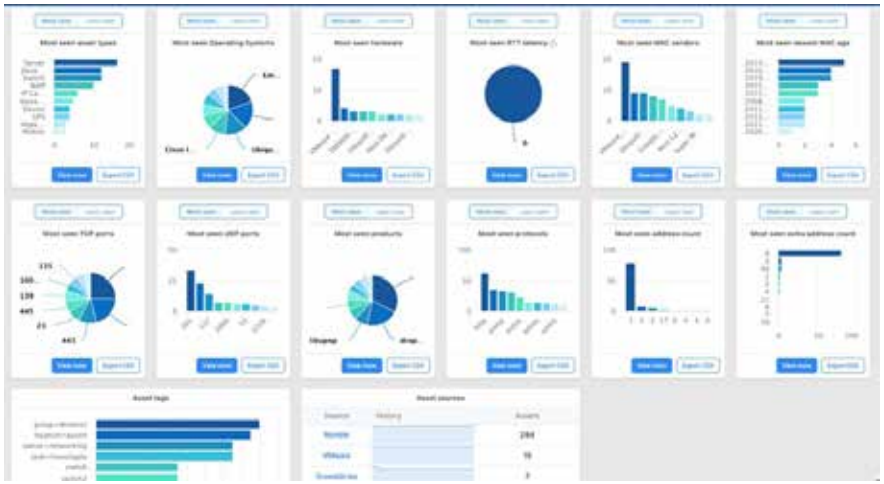
   能提供事件回應和資安團隊快速決策所需的關鍵資產清單資料，無需知道 IP 地址，直接在資產清單資料搜尋即可。

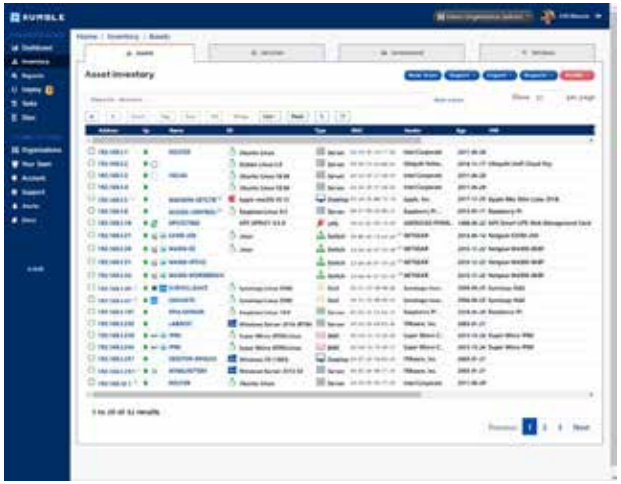
3. **具彈性及相容性**

   可單獨或與其他資安解決方案一起使用（如 CMDB、MDM 和 EDR），更可大大提昇網路中所有資產及服務的可視性。

▼示意圖

▼介面說明





▼ runZero 指標客戶

Capgemini　PRESIDIO　Recorded Future

GREYNOISE INTELLIGENCE　THE NATIONAL WWII MUSEUM NEW ORLEANS

▼獎項

G2 4.0

Capterra 4.9 / 5

Software Advice 4.9 / 5

SCADAfence・OT 高端網路安全解決方案

SCADAfence

近年來 ICS 工業控制系統（Industrial Control System）資安攻擊事件頻傳，而與 IT（Information Technology）系統有顯著的差異，就是 OT（Operational Technology）網路控制的是影響國家關鍵基礎設施（如石油、水、電廠等），鑒於越來越多的關鍵基礎設施依賴網路設備進行控制運行，這使得針對於此的攻擊破壞力愈加增大，未來需要提防由其引發的大規模 DDoS 攻擊、勒索軟體及 APT 等網路攻勢，並有效針對 OT 網路進行資安分析與威脅偵測，預警惡意程式的攻擊，進而提供有效的防護資訊，來避免關鍵性基礎設施與互聯網造成嚴重的影響。

▼產品優勢

1. **提高安全評估的準確性**

   透過 OT 網路清單，識別、查找出可疑的通訊模式，以及檢測出資安漏洞和可能的風險，並分析其威脅，最後產出詳細的調查結果報告和補救建議；由於平台會分析所有相關活動，加上過程全自動化，故可以減少人力時間並提高結果的準確性。

2. **實現高效的架構設計**

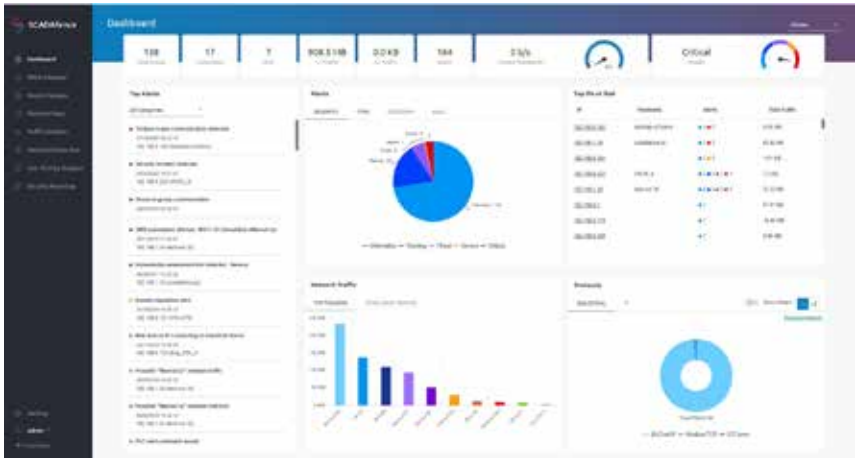
   可透過資產清單和網路圖提供對網路的準確視圖，有助於發現和反映關鍵資產和區域、識別攻擊媒介以及定義安全要求；該平台還可洞察流量模式和應用程式行為，從而大大改善區隔和其他項目的設計。

3. **持續降低風險**

   對 OT 網路的持續監控，為用戶提供了網路安全狀況的清晰畫面，並提供了帶有修復建議的警報通知；可降低了網路攻擊的風險，並最大程度地減少了事件反應時間；該平台允許管理員和管理人員不斷檢視其重大風險，並分析他們為降低風險所採取之措施的效益（能）。

▼示意圖

▼介面說明



▼ SCADAfence 指標客戶

TARO　VESTEL　MITSUI FUDOSAN

▼獎項

Cutting Edge
ICS/SCADA Security

Cutting Edge
Compliance

Next Gen
Critical Infrastructure Protection

Scale Computing · 超融合解決方案

透過集中儲存設備、將伺服器進行虛擬化工程，並整合相關資源於設備上，不僅無須更換或廢除現有的設備，相反地還能透過集中化與虛擬化的方式，讓新舊兩套架構並存，以互補方式大大降低導入時的壓力，可有效降低資料中心內的設備複雜度，縮短停機而造成服務中斷時間；此外，因為超融合基礎架構（HCI）需要的空間很小，這也意味著企業無須另外釋出空間來容納相關設備，也無須提供額外的電力與空調，讓企業能夠維持低成本的營運狀態。

▼產品特色

1. **簡單**

   易於部署及管理，只要一個人一小時內完成部署，而該平台能將自我修復與智能自動化相結合，使客戶能夠在基礎設施維護上花費更少的時間，專注於主要策略項目及發展其業務。

2. **高效**

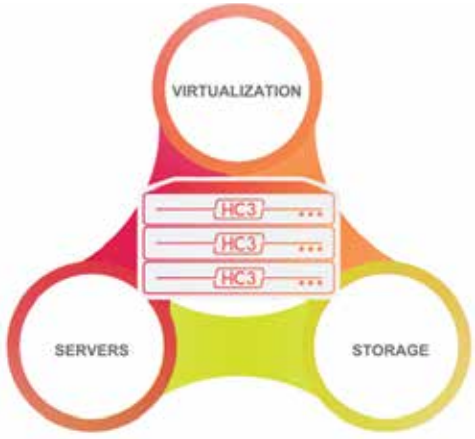
   能將傳統虛擬化軟體、災難恢復軟體、伺服器和來自不同供應商的共享儲存整合在一起，以建立虛擬化環境的需要，HC3 多合一的設備架構讓「開箱即用、輕鬆部署」得以真正實現。

3. **創新**

   擁有獲專利的 HyperCore™ 技術，可以實時自動識別、緩解和糾正基礎架構中的問題，即使在 I.T. 資源和人員短缺的情況下，也可以使應用程式獲得最大的正常運行時間。

▼介面說明

▼示意圖



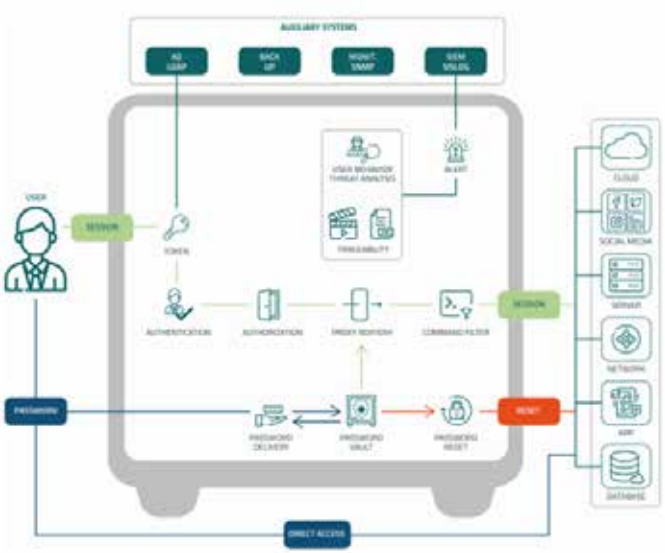
senhasegura・特權帳號管理解決方案

IT 部門對於系統的登入帳號及存取權限的管控，管理政策涵蓋的範圍大多針對一般的使用者，像是執行例行工作內容的公司內部員工，政策內容包含帳號命名方式、密碼設定與變更原則、登入錯誤次數的鎖定等。但是像系統管理者、網管人員、DBA（Database Administrator，資料庫管理員）、AP 開發人員、及 AP 執行時的專用存取帳號等對於系統有高存取權限之帳號，常常將特權帳號排除於管理政策之外，但如果持有特權帳號人員對企業有不法之意圖，企圖利用特權身分帳號取得重要資料或是癱瘓系統，造成的傷害的後果將無法想像。

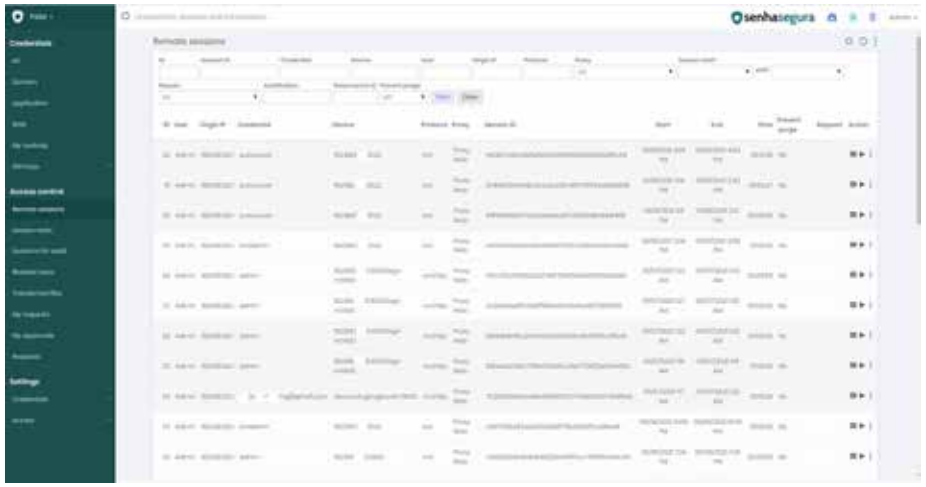
▼產品特色

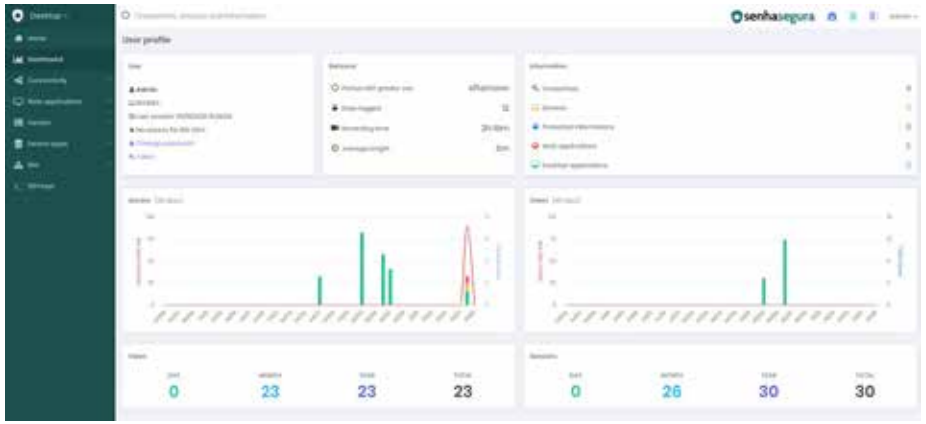
1. 部署簡易高效，免除了一般部署自動化特權存取管理的傳統複雜性，在 7 分鐘內即可完成部署，易於使用。
2. 可進行各種角色定義及使用者權限設定，協助企業集中管理及實施分層分級存取控制。
3. 可產生稽核記錄及存取歷史記錄，以確保遵守政府及業界法規。
4. 涵蓋了特權存取管理的完整週期：前期的身份審核及升級 >> 中期的行為跟進及監測 >> 後期的管理及稽查

▼示意圖



▼介面說明





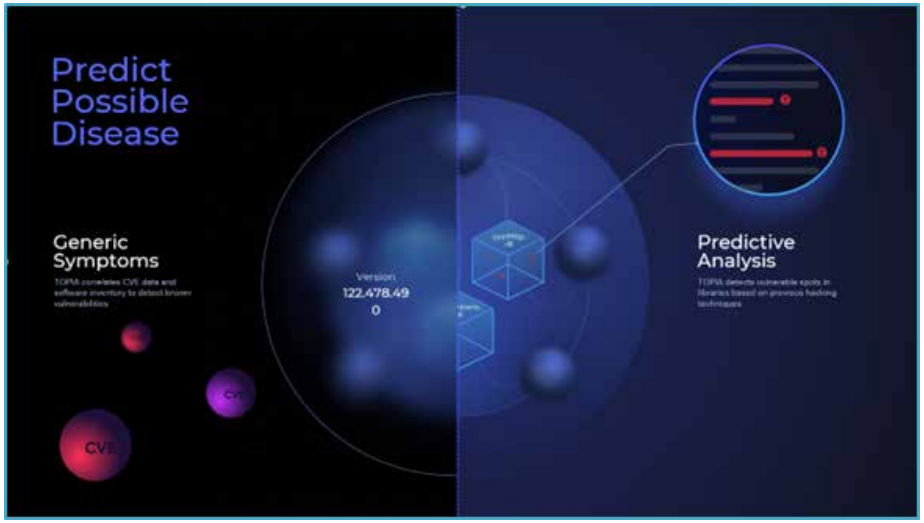
vRx・漏洞管理解決方案

面對每年被揭露 1 萬多個新漏洞，許多企業 IT 管理人員看到軟體廠商公告的漏洞訊息早已麻痺；而企業典型的漏洞管理工作流程通常費時費工，識別漏洞與修復漏洞的工作中間存在巨大的鴻溝。【vRx 漏洞管理解決方案】(舊名：TOPIA) 協助企業結合當前漏洞威脅情報、風險持續監控，進而為後續的漏洞提供快速應急、風險預警的高效率管理流程，並在各個環節，提供優化分析後的技術建議，最大程度加快漏洞修復效率，在漏洞被利用前完成修補。

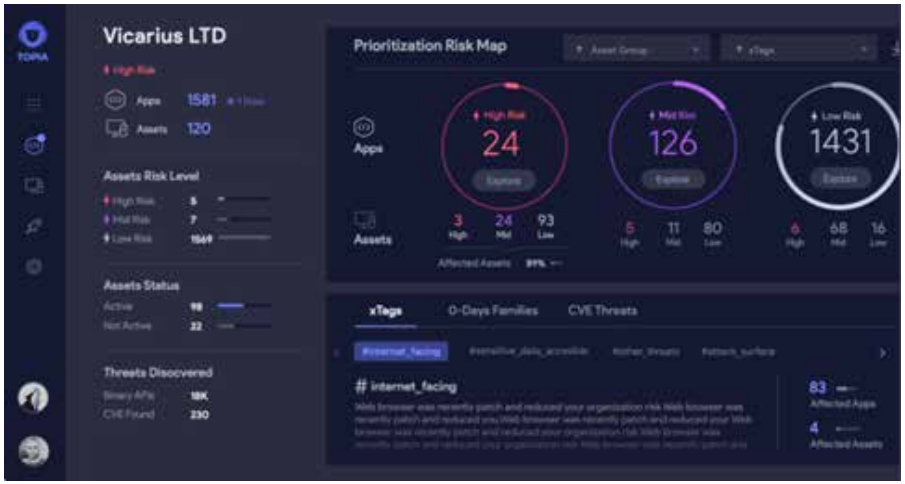
▼產品特色

1. 可自動搜尋設定模組、分析漏洞及自動修補
2. 能發現並防堵尚未通報之漏洞
3. 提供企業風險管理、依漏洞嚴重程度級別處理與排序建議

▼示意圖



▼介面說明



▼ vRx 指標客戶

NHS　ADAMA　INGRAM MICRO　HCC　Ingecom

▼獎項

GetApp BEST FUNCTIONALITY & FEATURES 2021
Capterra BEST VALUE 2021
Software Advice MOST RECOMMENDED 2021


工具型軟體

NordLayer・遠端安全存取解決方案

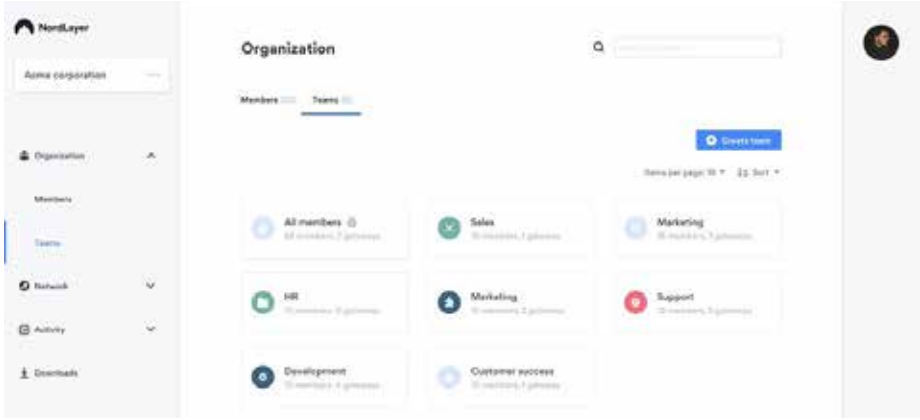
NordLayer

Nord Security 為企業和個人資安 / 隱私解決方案的全球領先供應商之一，致力於為每個人創造一個安全的網路未來，旗下產品已被全球數百萬客戶使用，並受到網絡安全專家和媒體的好評，自 2012 年以來，Nord Security 一直在創造屢獲殊榮的產品：NordLayer / NordLocker / NordPass 等。

▼產品特色

1. 適用於現代企業的調適性網路存取安全解決方案，前身為 NordVPN Teams，幫助各種規模的組織在打造現代安全遠端存取解決方案時應對擴充和整合挑戰。
2. 在現有基礎設施的情況下快速且易於實作，無需硬體，並且在設計時考慮到易擴充性。
3. 符合今日敏捷企業和分散式勞動力的不同成長速度和特殊網路安全需求，並獲選為 2021 年最佳的企業 VPN 供應商。

▼介面說明



▼示意圖

▼ NordLayer 指標客戶

HOSTINGER　SOUNDCLOUD　Calendly

shutterstock　whatagraph　U S MOBILE

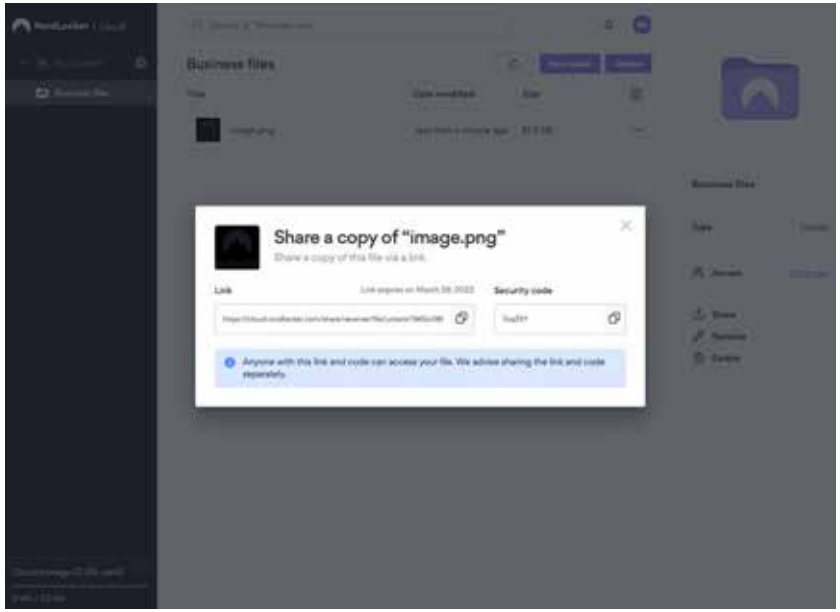
NordLocker・雲端儲存加密解決方案

Nord Security 為企業和個人資安 / 隱私解決方案的全球領先供應商之一，致力於為每個人創造一個安全的網路未來，旗下產品已被全球數百萬客戶使用，並受到網絡安全專家和媒體的好評，自 2012 年以來，Nord Security 一直在創造屢獲殊榮的產品：NordLayer / NordLocker / NordPass 等。

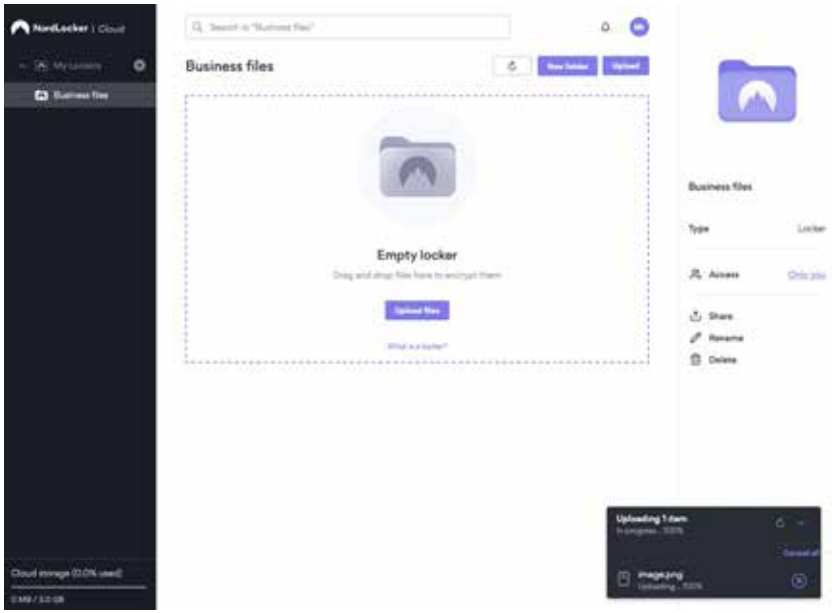
▼產品特色

NordLocker 是全球第一款使用私有雲的端到端檔案加密工具。NordLocker 適用於 Windows、macOS、iOS 和 Android，支援所有檔案類型，提供快速直觀的介面，並保證裝置之間的安全同步。使用 NordLocker，檔案可以免於遭受駭客攻擊、監控和資料收集。獲選為 2021 年度消費者加密解決方案。

▼示意圖



▼介面說明



▼獎項

Consumer Encryption Solution of the Year 2021

Cloud-Based Product of the Year 2021

Cutting Edge ICS/SCADA Security

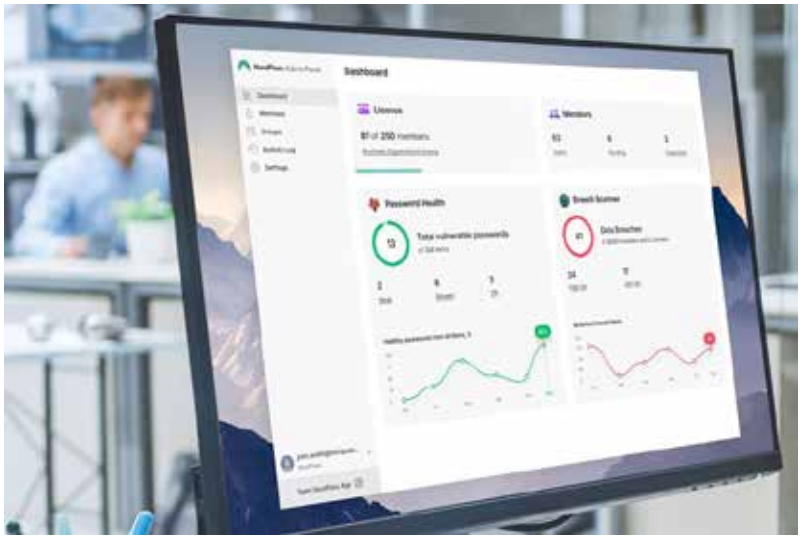
NordPass・企業密碼管理解決方案

Nord Security 為企業和個人資安 / 隱私解決方案的全球領先供應商之一，致力於為每個人創造一個安全的網路未來，旗下產品已被全球數百萬客戶使用，並受到網絡安全專家和媒體的好評，自 2012 年以來，Nord Security 一直在創造屢獲殊榮的產品：NordLayer / NordLocker / NordPass 等。

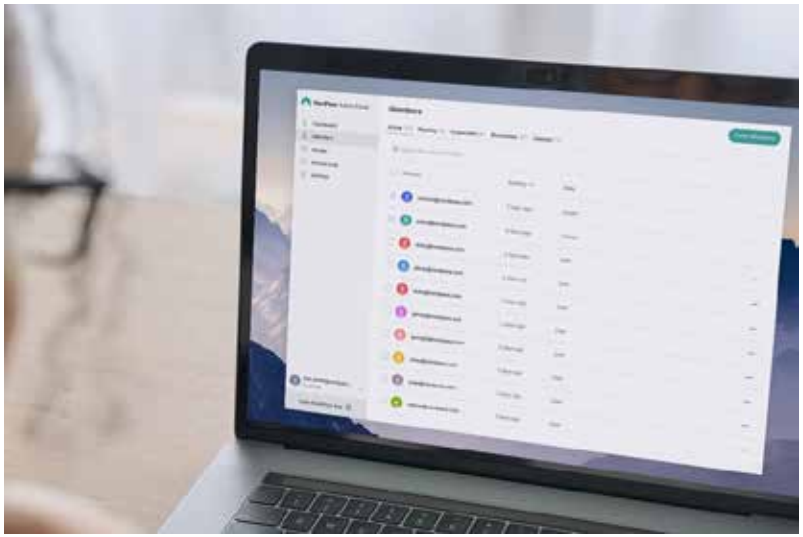
▼產品特色

NordPass 是一款適用於商業和消費者客戶的密碼管理器。使用最新技術開發，可提供最大程度的安全性。NordPass 的開發考慮到經濟性、簡單性和易用性，允許用戶在桌上型電腦、行動裝置和瀏覽器上安全存取密碼。 所有密碼都在裝置上加密，因此只有用戶才能存取密碼。2022 年獲選最佳的密碼管理器之一及 2021 年最容易設定的密碼管理器。

▼示意圖



▼介面說明



▼ NordPass 指標客戶

HOSTINGER　boredpanda　evergrowth.io

CUSU　BIZIMPLY　eneba

SafeDNS．網路過濾 (WebFiltering) 解決方案

在企業環境中，想要享受使用網際網路帶來的便利以及生產力，卻往往難以防範的誤觸惡意網站或被植入惡意程式，使敏感的重要資料或個人隱私暴露在危險之中；另外近年來勒索軟體的散播管道，也延伸至網頁，故在過濾網路流量之後，企業針對上網的內容，也需要進一步的透視，來減少員工經由瀏覽網頁的情況下，遭到有心人士下手，發動攻擊的機會。【SafeDNS 網路過濾 (Web Filtering) 解決方案】，藉由整合一系列全方位安全防護技術，來協助企業防範新興及現有 Web 威脅，並同時管理網際網路資源的使用情形，以增強員工產能及阻擋來自網頁的威脅或攻擊。

▼產品特色

1. **人工智慧過濾技術**

   利用人工智慧 (AI)、機器學習 (ML) 來分析和處理企業的所有網路過濾，提供了最準確和最完整的網路分類；除了效能快及節省時間外，並確保使用者其網路安全且不會過度阻塞。

2. **惡意軟體和殭屍網路防護**

   SafeDNS 持續的更新惡意軟體網站名單，藉以協助企業阻止使用者存取惡意軟體內容或危險網站。

3. **內容過濾**

   阻止所有不受歡迎或不適當的網站，如色情、賭博及您設定的其他內容類別；SafeDNS 的資料庫超過 1.09 億個網站（涵蓋數十億個網頁）的資訊，並分為 61 個類別，且持續增加中；也能阻止大部份不同形式的在線廣告干擾。

4. **易於部署、管理及成本實惠**

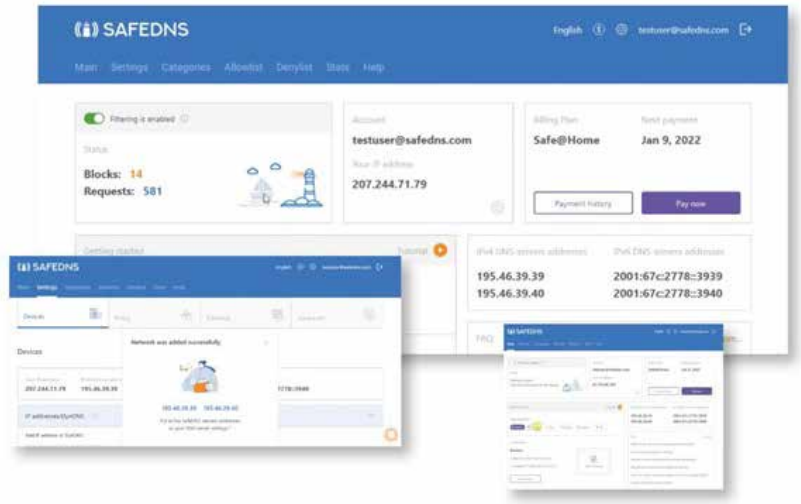
   SafeDNS 為雲服務，故無需額外在 Client 端、伺服器或電腦上購買任何硬體設備或安裝其他軟體。

5. **安全及更快的互聯網**

   SafeDNS 的 DNS（Domain Name System）伺服器分佈於美洲、歐洲、澳大利亞和遠東等地區，並透過邊界網關協議 (Border Gateway Protocol，簡稱 BGP) 及任播（Anycast）架構，協助客戶在全球的任何位置都能快速並安全地存取。

▼示意圖

▼介面說明



▼ SafeDNS 指標客戶

▼獎項

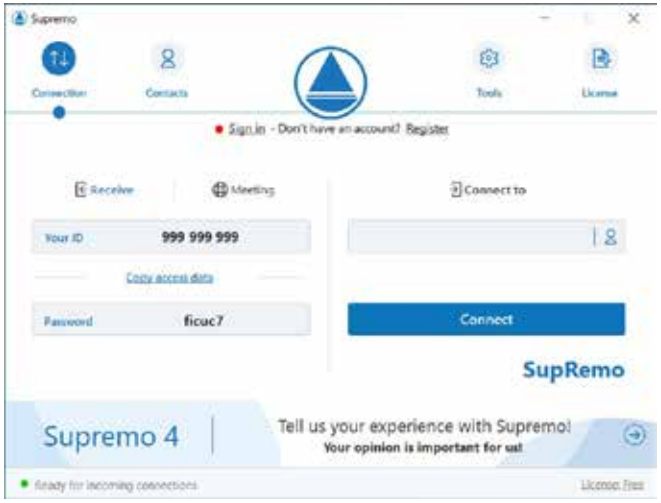
SupRemo・遠端控制解決方案

SupRemo 是一款來自於義大利的遠端桌面控制軟體，適用於 Windows、macOS、iOS、Android 和 Linux 多平台，允許多個用戶連接到同一台電腦，其使用強大的數據傳輸協議，允許用戶連接到路由器和防火牆後面的遠程電腦，並無需任何配置。最重要的是，Supremo 提供用戶極高的安全保障，通過網路傳輸的所有數據都使用 AES256 位算法進行加密。此外，每個控制會話都會生成隨機的 4 位密碼。還可以指定更強大的密碼來保護用戶的電腦並阻止指定的 ID。

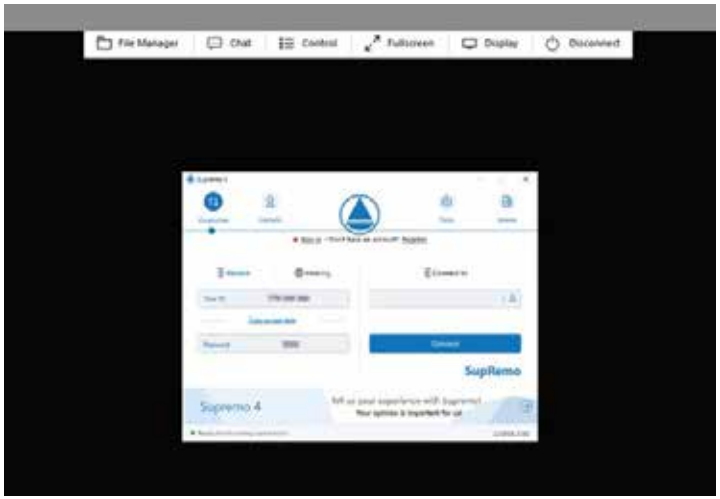
▼產品特色

1. 可跨 (多) 平台存取設備
2. 可多人線上會議功能
3. 可多用戶 / 設備群組管理
4. 免安裝、成本低 (性價比高)
5. 可及時線上交談與文件傳輸詳細紀錄報表
6. 可透過 GPO 大量部署 (*Group Policy Object，群組原則物件)

▼介面說明



▼示意圖



資安服務

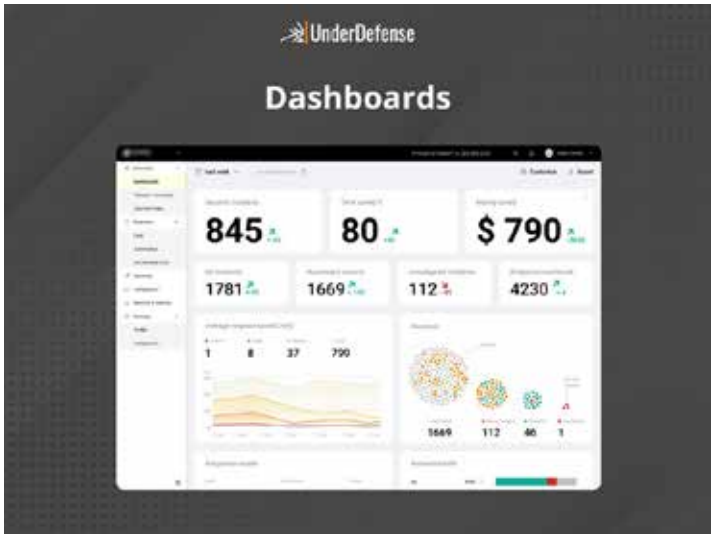
UnderDefense・資安威脅偵測應變服務 (MDR)

UnderDefense 於 2016 年在紐約成立，為歐洲頂尖的道德駭客 (Ethnical Hacker) 團隊之一，在多次國際駭客大賽中名列前茅，近幾年在 Clutch 排名中均是第一 (Clutch 為美商服務業評比機構)，Gartner 用戶評價亦為 5 星滿分；UnderDefense 業務遍及美國和歐洲，具備豐富的實戰經驗，且擁有大量的專業認證，每年處理數以百計的滲透測試服務 (Penetration Test，簡稱 PT)，對於專案處理非常嫻熟，除滲透測試服務外，亦操作專業 SOC，為企業提供各層級的 MDR，以及 SIEM(安全性資訊與事件管理)、Incidence Response(安全事件應變) 等服務。

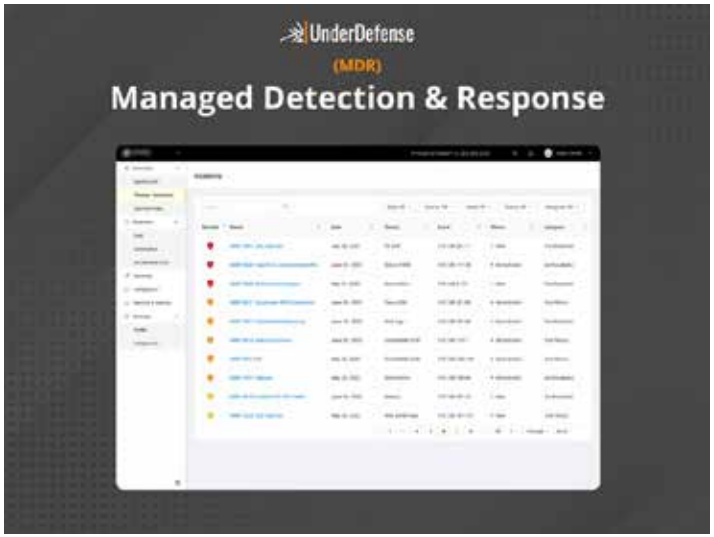
▼產品特色

1. 24x7x365 託管威脅回應
2. 由專業的資安團隊協助企業監視網路並保護企業免受惡意攻擊、勒索軟體和資料遺失
3. 事件取證和資料洩露復原
4. 能快速有效地調查、控制和補救關鍵安全事件，並協助企業回應及復原
5. 滲透測試
6. 協助企業定期檢查，防止駭客攻擊

▼介面說明



▼示意圖



Version 2 台灣二版
www.version-2.com.tw

獨家總代理產品

ATERA
Awingu.com
One Workspace. Any Device. Anywhere.
BULLWALL
cloudm
Comet
eset
jumpcloud
keepit
NordLayer
NordLocker
NordPass
PANDORAFMS ENTERPRISE
portnox™
runZero
SAFEDNS
SCADAfence
SCALE COMPUTING
senhasegura
SupRemo
TOPIA
UnderDefense

銷售專線：02-7722-6899　網站：www.version-2.com.tw　業務部門：enterprise@version-2.tw　技術支援：support@version-2.tw