2025台灣二版

企業操作課程-ESET PROTECT On-Prem基礎篇

議程大綱

第一段-ESET PROTECT On-Prem基礎篇

PM1400~PM1530

- ESET PROTECT
  v12.x新功能介紹
- ESET PROTECT架構
- ESET PROTECT規格
- ESET PROTECT安裝

第二段-NordLayer/NordStellar

PM1530~PM1600


ESET PROTECT v12.1新功能介紹

ESET Protect On-Prem新增功能

- **Linux 產品的網路隔離**

我們將此功能擴展到 Windows 和 macOS 安全性產品之外，因此網路隔離現在可用於 Linux。安全性事件發生期間，Linux 端點可以快速進行隔離，防止威脅蔓延並增強跨多平台環境的防護。

- **工作和動態群組範本內容的審核**

我們已啟用對於工作和動態群組範本的審核，進而可以清楚地了解配置變更以及工作和範本的移除。這種增加的透明度對於維護安全性和合規性至關重要。

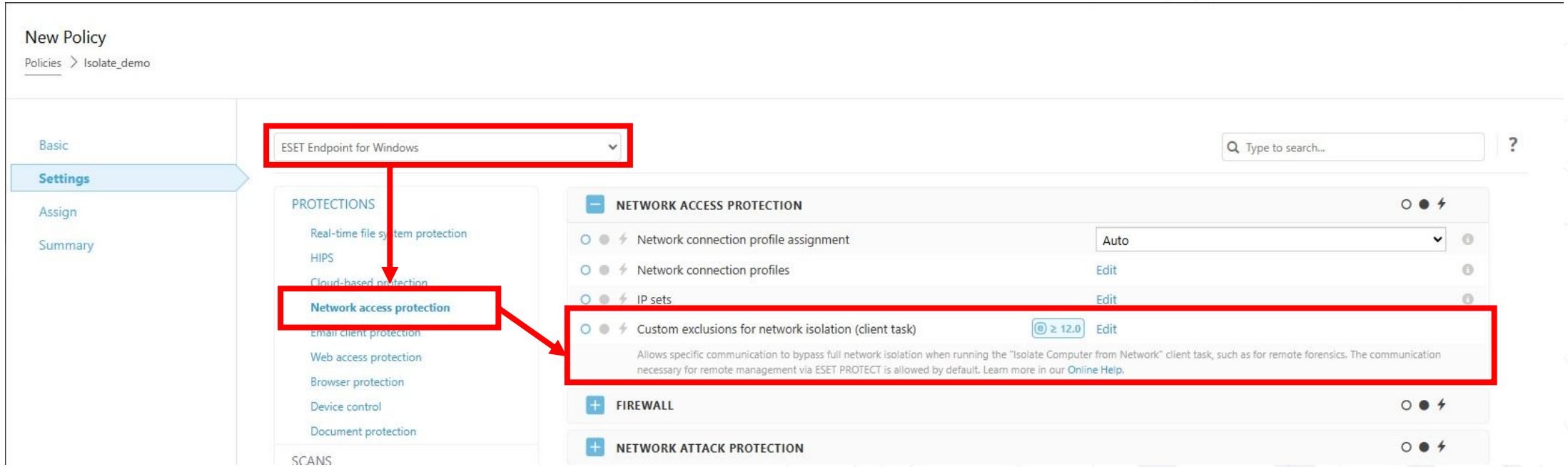
- **Linux 上的 ESET PROTECT 伺服器安裝**

ESET PROTECT 伺服器現在可以安裝在最新的 Linux 發行版上，包括 Ubuntu 22.04 LTS、Ubuntu 24.04 LTS、Debian 12 和 RHEL 9。這確保與現代企業環境的相容性，讓整個更新的平台上的安全性管理更加的無縫。

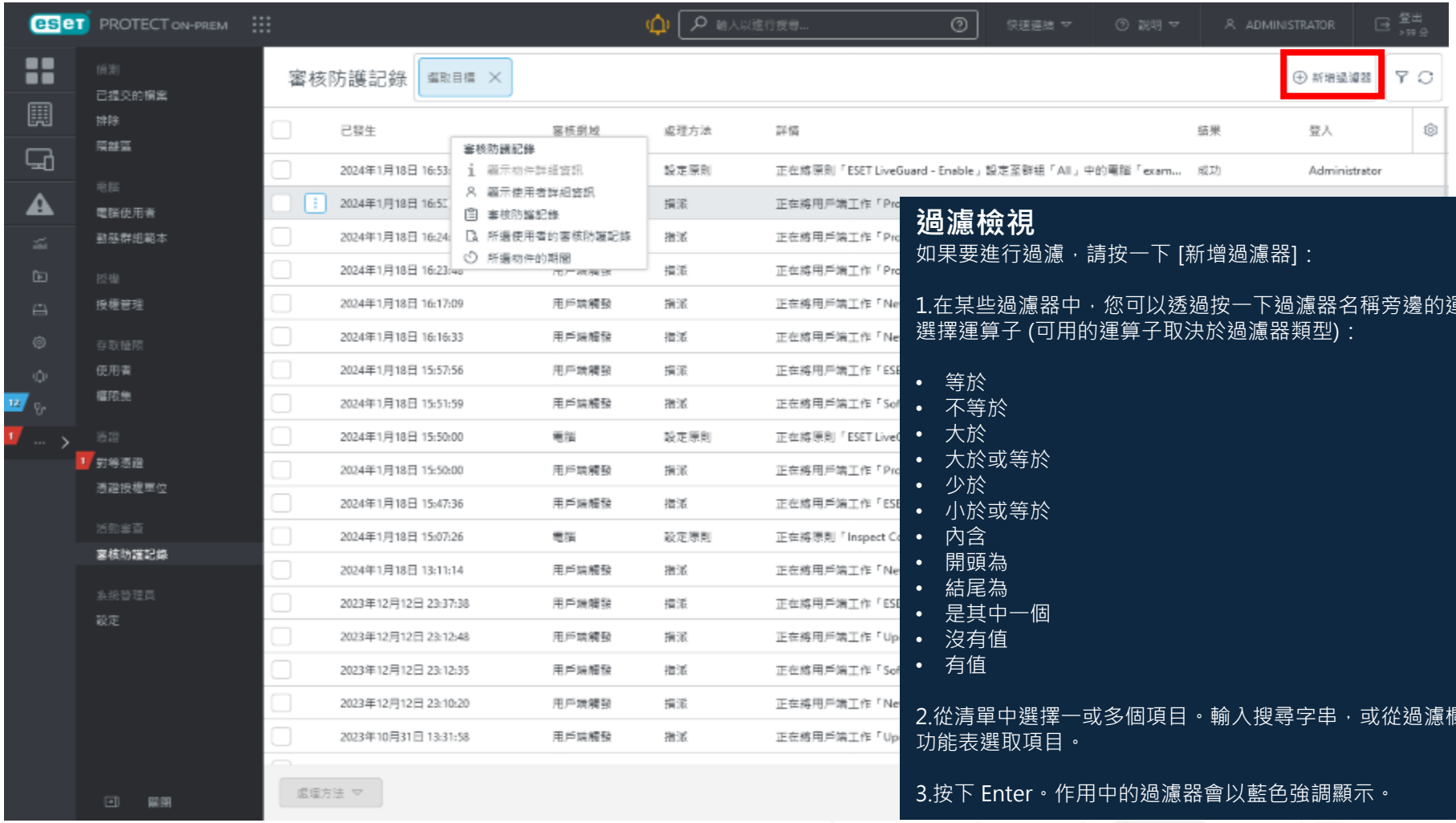
- **ESET Mail Security for Microsoft Exchange Server 的維護模式**

我們已為 ESET Mail Security for Microsoft Exchange Server 新增維護模式的偵測。它表示為一種功能性狀態，可以在動態群組中使用以觸發自動化處理動作，進而增強管理和監視。

ESET Protect On-Prem 網路隔離



ESET Protect On-Prem 審核



過濾檢視

如果要進行過濾，請按一下 [新增過濾器]：

1.在某些過濾器中，您可以透過按一下過濾器名稱旁邊的運算子圖示來選擇運算子 (可用的運算子取決於過濾器類型)：

- 等於
- 不等於
- 大於
- 大於或等於
- 少於
- 小於或等於
- 內含
- 開頭為
- 結尾為
- 是其中一個
- 沒有值
- 有值

2.從清單中選擇一或多個項目。輸入搜尋字串，或從過濾欄位的下拉式功能表選取項目。

3.按下 Enter。作用中的過濾器會以藍色強調顯示。

ESET Protect Cloud

- **主功能表中的新配置區段**

ESET PROTECT 的主功能現在包含一個新的 [配置] 區段 (之前稱為「原則」)。此區段劃分為兩個索引標籤：第一個索引標籤是「設定防護」精靈 (之前位於「快速連結」功能表中)，可讓您快速地配置裝置上的基本設定。第二個索引標籤包含所有現有的原則，並且提供編輯或建立新原則的選項。

- **審核原則變更**

您現在可以追蹤對原則所做的所有變更。您可以在審核防護記錄區段存取此資訊，並在其中比較特定原則的先前設定和目前設定。

- **電腦詳細資料畫面的更新**

我們已經重新設計「電腦詳細資料」畫面以提高可用性。現在，資訊的結構更合乎邏輯、更緊湊、視覺上也更具吸引力。重點詳細資料已反白顯示，以確保您不會錯過任何重要的資訊。

- **新的變更事件狀態**

我們推出一種新的事件狀態："等待輸入內容"。它會通知 ESET MDR 客戶，ESET 或他們的 MSP 正在等待他們就該事件提供意見。

- **改進的 ESET MDR 回應作和儀表板**

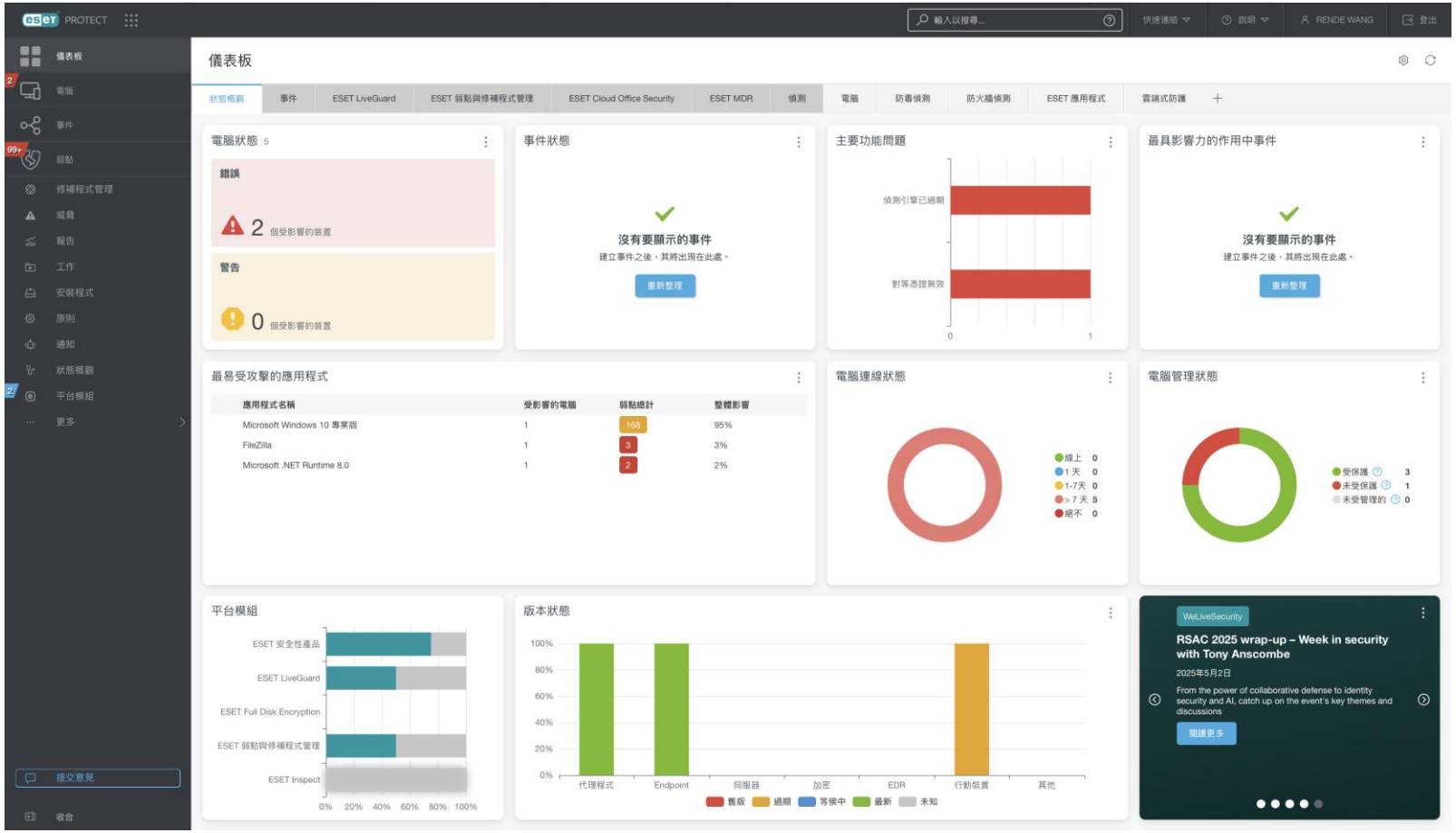
ESET MDR 客戶現在可以指定關鍵資產應該隱藏的回應處理方法。此設定在 [配置] 區段可以使用。

此外，我們已經改進 ESET MDR 儀表板，以提供更好的使用者體驗。使用者現在可以直接瀏覽至 [事件] 區段，而無需重新導向至 ESET Inspect。儀表板還具有經過更新設計的增強型小工具。

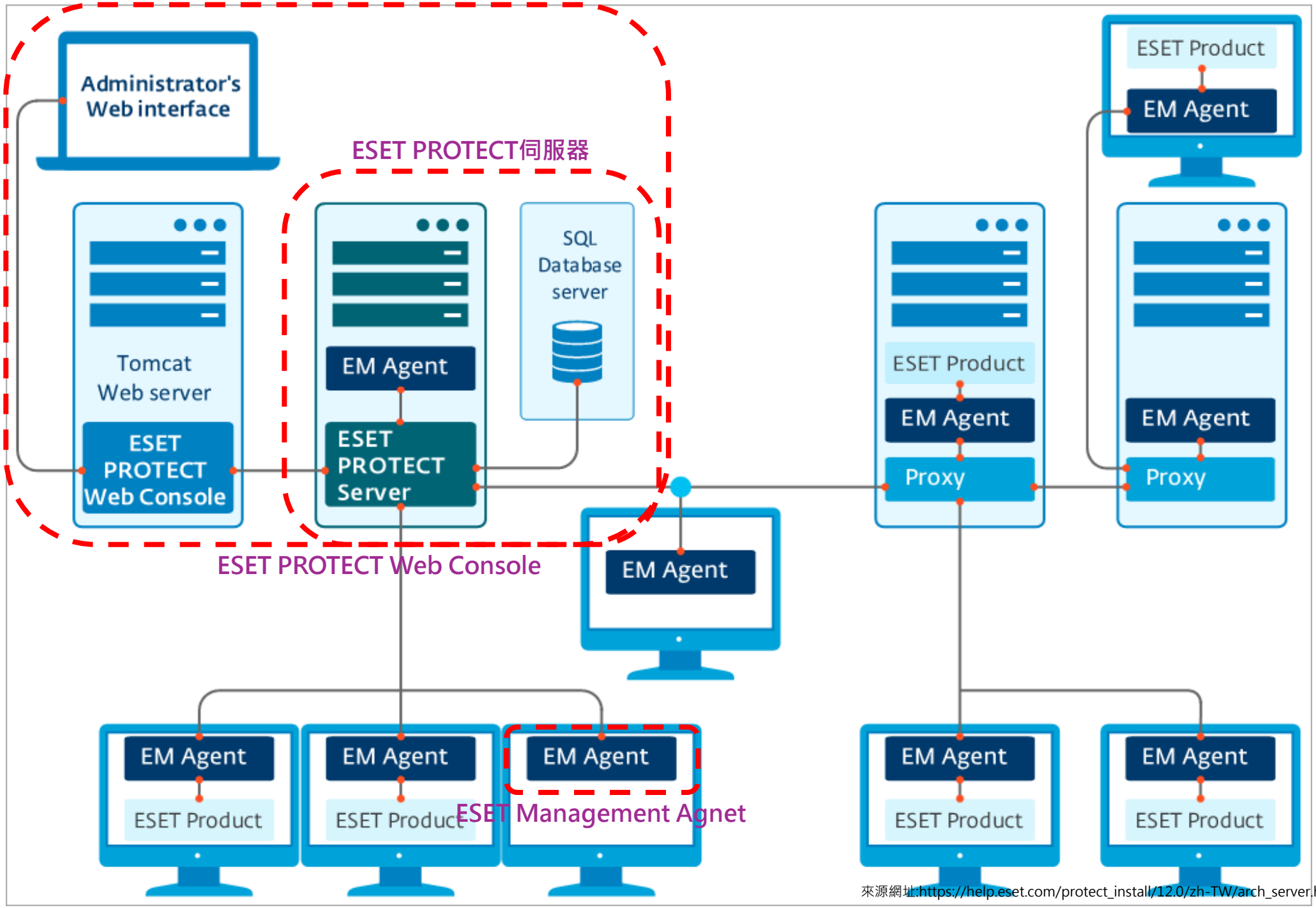
- **其他改進和錯誤修正**

了解已在變更日誌上改進的其他內容。

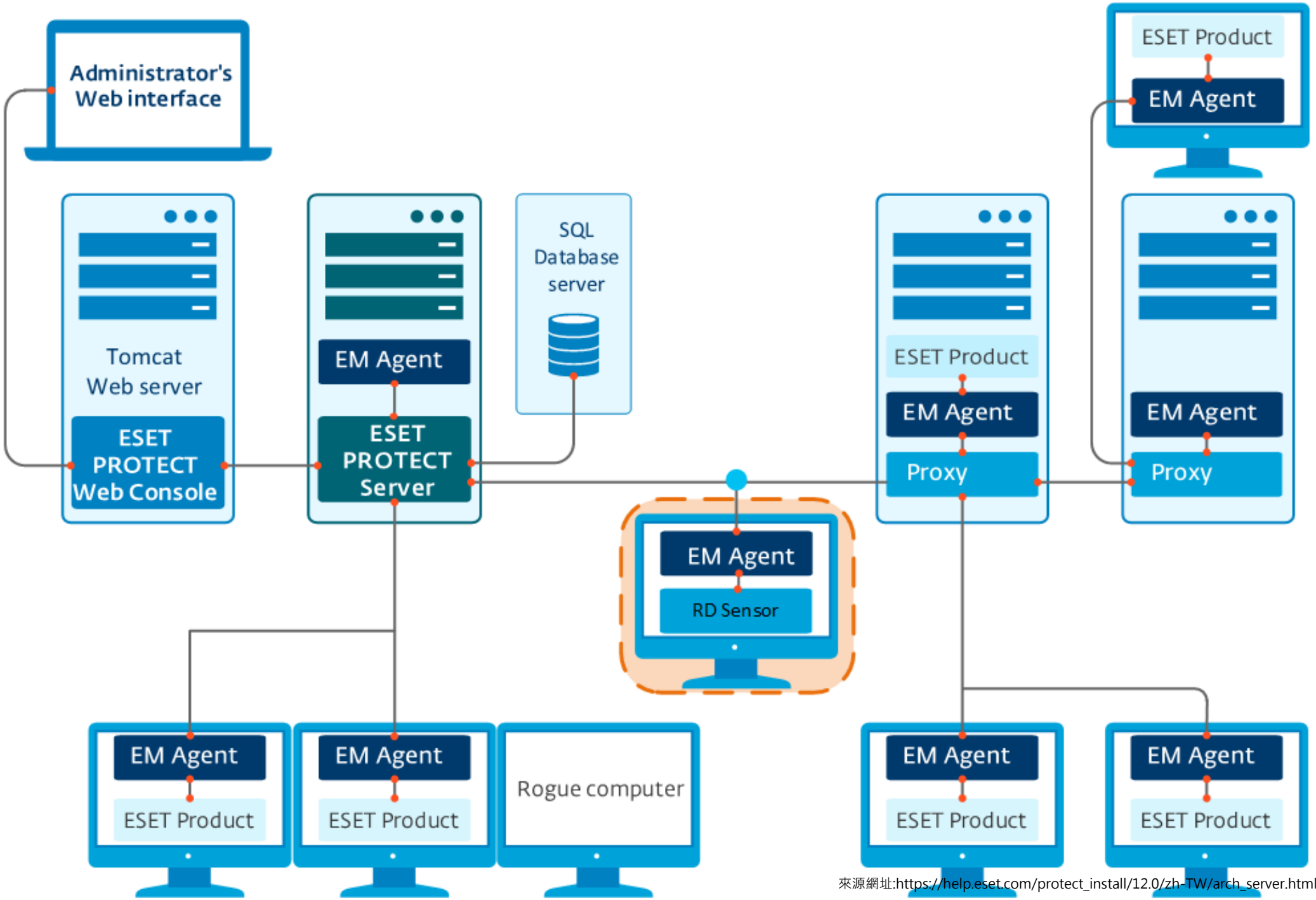
ESET Protect Cloud-狀態概觀儀表板



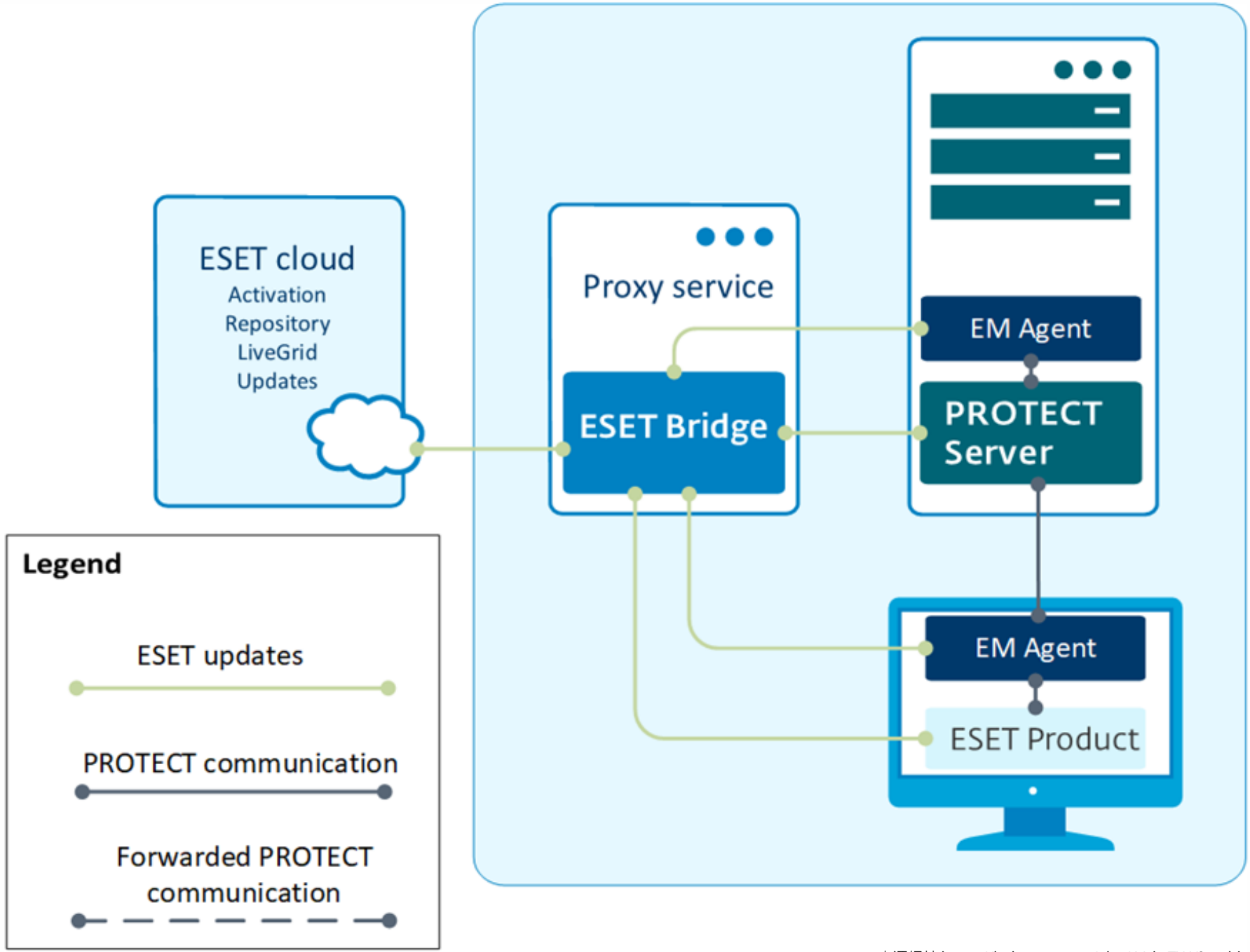
ESET PROTECT架構



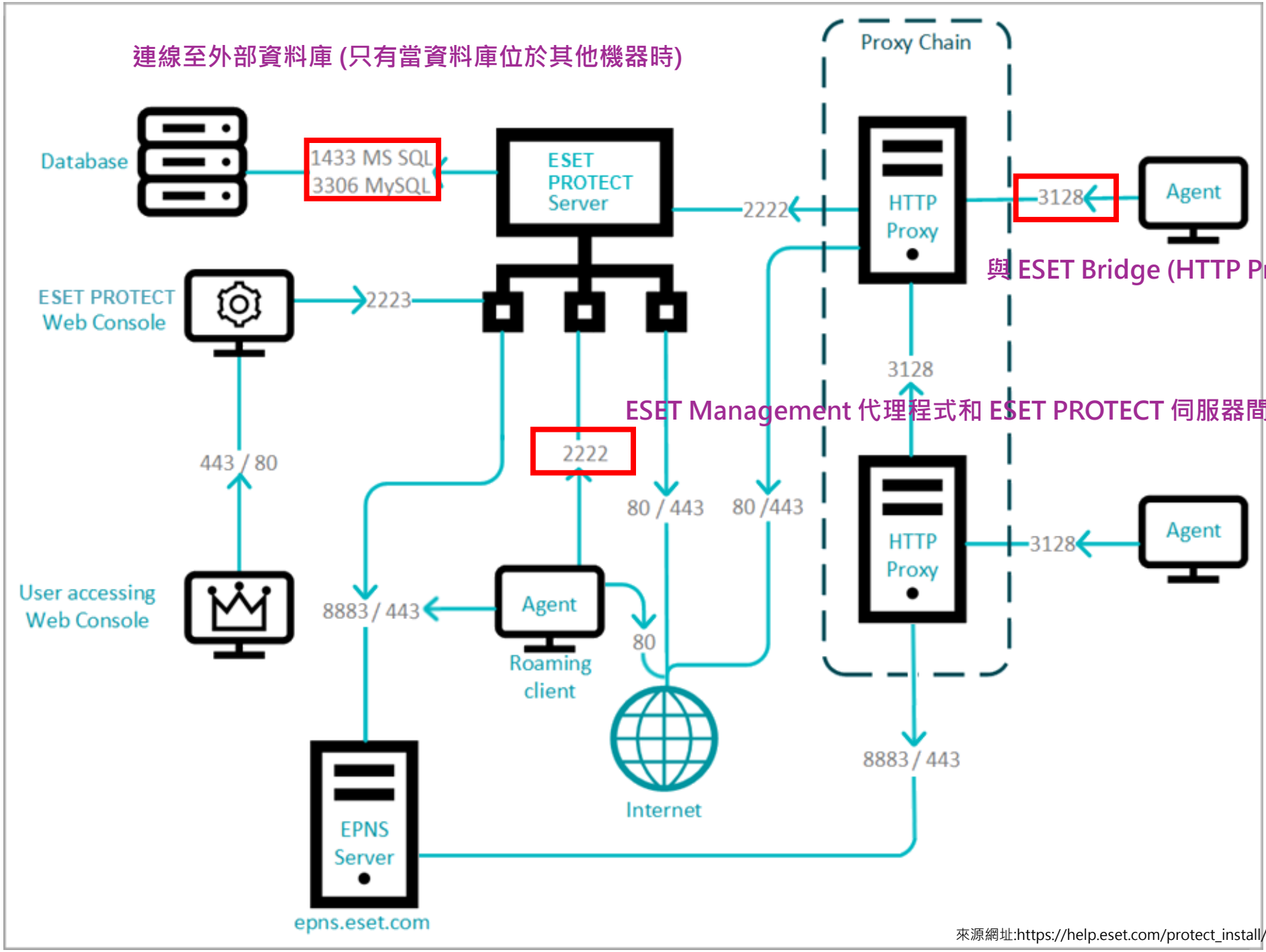
來源網址:https://help.eset.com/protect_install/12.0/zh-TW/arch_server.html?architecture.html



來源網址:https://help.eset.com/protect_install/12.0/zh-TW/arch_server.html?arch_rd_sensor.html



來源網址:https://help.eset.com/ebe/4/zh-TW/?caching_of_downloads_and_updates.html



來源網址:https://help.eset.com/protect_install/12.0/zh-TW/ports_used.html

ESET PROTECT規格

支援的作業系統-Windows

作業系統	伺服器	代理程式	RD Sensor
Windows Server 2012 x64		10.0, 10.1–12.0, 12.3	✓
Windows Server 2012 CORE x64		10.0, 10.1–12.0, 12.3	✓
Windows Server 2012 R2 x64		10.0, 10.1–12.0, 12.3	✓
Windows Server 2012 R2 CORE x64		10.0, 10.1–12.0, 12.3	✓
Windows Storage Server 2012 R2 x64		10.0, 10.1–12.0, 12.3	✓
Windows Server 2016 x64	✓	10.0, 10.1–12.0, 12.3	✓
Windows Storage Server 2016 x64	✓	10.0, 10.1–12.0, 12.3	✓
Windows Server 2019 x64			
Windows Server 2022 x64			
Windows Server 2022 CORE x			
Windows Server 2025 x64			

!!!早期的 Microsoft Windows 系統!!!
•ESET Management 代理程式 10.x 是最後一個支援 Windows 7/8.x 和 Windows Server 2008 R2/Microsoft SBS 2011 的版本。
•一律安裝最新的服務套件，特別是 Windows Server 2012 這類的舊版系統上更要安裝。
•ESET PROTECT On-Prem 不支援執行 Windows XP/Vista/7/8 的電腦管理。

支援的作業系統-Linux

作業系統	伺服器	代理程式	RD Sensor
Ubuntu 18.04.1 LTS x64 Desktop		10.0, 10.1–12.0, 12.3	✓
Ubuntu 18.04.1 LTS x64 Server		10.0, 10.1–12.0, 12.3	✓
Ubuntu 20.04 LTS x64	✓	10.0, 10.1–12.0, 12.3	✓
Ubuntu 22.04 LTS x64	✓	10.0, 10.1–12.0, 12.3	✓
Ubuntu 24.04 LTS x64	✓	11.0–12.0, 12.3	
Linux Mint 20		10.0, 10.1–12.0, 12.3	✓
Linux Mint 21		10.1–12.0, 12.3	✓
Linux Mint 22		11.2–12.0, 12.3	✓
RHEL Server 7 x64		10.0, 10.1–12.0, 12.3	✓
RHEL Server 8 x64	✓	10.0, 10.1–12.0, 12.3	
RHEL Server 9 x64	✓	10.0, 10.1–12.0, 12.3	✓
CentOS 7 x64		10.0, 10.1–12.0, 12.3	✓
SLED 15 x64		10.0, 10.1–12.0, 12.3	✓
SLES 12 x64		10.0, 10.1–12.0, 12.3	✓

作業系統	伺服器	代理程式	RD Sensor
SLES 15 x64		10.0, 10.1–12.0, 12.3	✓
Debian 9 x64		10.0, 10.1–12.0, 12.3	✓
Debian 10 x64	✓	10.0, 10.1–12.0, 12.3	✓
Debian 11 x64	✓	10.0, 10.1–12.0, 12.3	✓
Debian 12 x64	✓	10.1–12.0, 12.3	✓
Oracle Linux 8		10.0, 10.1–12.0, 12.3	✓
Amazon Linux 2		10.0, 10.1–12.0, 12.3	✓
Amazon Linux 2023		11.2–12.0, 12.3	
Alma Linux 9		10.1–12.0, 12.3	✓
Rocky Linux 8		10.1–12.0, 12.3	
Rocky Linux 9	✓	10.1–12.0, 12.3	✓

支援的作業系統-Mac

作業系統	代理程式
macOS Catalina (10.15)	10.0, 10.1–12.0, 12.3
macOS Big Sur (11.0–11.1)	10.0, 10.1–12.0, 12.3
macOS Monterey (12.0)	10.0, 10.1–12.0, 12.3
macOS Ventura (13.0)	10.0, 10.1–12.0, 12.3
macOS Sonoma (14.0)	10.1–12.0, 12.3
macOS Sequoia (15.0)	11.2–12.0, 12.3

支援的 Hypervisor 和 Hypervisor 延伸模組

Hypervisor	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix XenServer	✓	X
Microsoft Hyper-V	✓	✓ (不支援安全開機)
VMware vSphere	✓	✓ (7.0.3.00300)
VMware ESXi	✓	✓ (7.0)
VMware Workstation	✓	✓ (16.2.3)
VMware View	✓	X
Oracle VirtualBox	✓	X
VMware Fusion	✓ x64 X ARM	✓ (12.2.3)
Parallels	X	✓
Hypervisor 延伸模組	**ESET PROTECT On-Prem**	**ESET Full Disk Encryption**
立即可用的 Citrix VDI	✓	X
Citrix XenDesktop	✓	X

硬體與基礎架構大小

用戶端數量	ESET PROTECT 伺服器 + SQL 資料庫伺服器				
	CPU 核心	CPU 時脈速度 (GHz)	RAM (GB)	磁碟機[1]	磁碟 IOPS[2]
最多 1,000	4	2.1	4	單一	500
5.000	8	2.1	8		1.000
10,000[3]	4	2.1	16	單獨	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

部署 ESET PROTECT On-Prem 的最佳做法

用戶端數量	最多 1,000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000+
同一台電腦上的 ESET PROTECT 伺服器與資料庫伺服器	✓	✓	✓	X	X	X
使用 Microsoft SQL Express	✓	✓*	X	X	X	X
使用 Microsoft SQL	✓	✓	✓	✓	✓	✓
使用 MySQL	✓	✓	✓	X	X	X
使用 ESET PROTECT 虛擬設備	✓	✓	不建議	X	X	X
使用 VM 伺服器	✓	✓	✓	選用	X	X
建議的複製間隔 (部署階段期間)	60 秒	5 分鐘	10 分鐘	15 分鐘	20 分鐘	25 分鐘
建議的連線間隔 (部署後，標準使用期間)	10 分鐘	10 分鐘	20 分鐘	30 分鐘	40 分鐘	60 分鐘

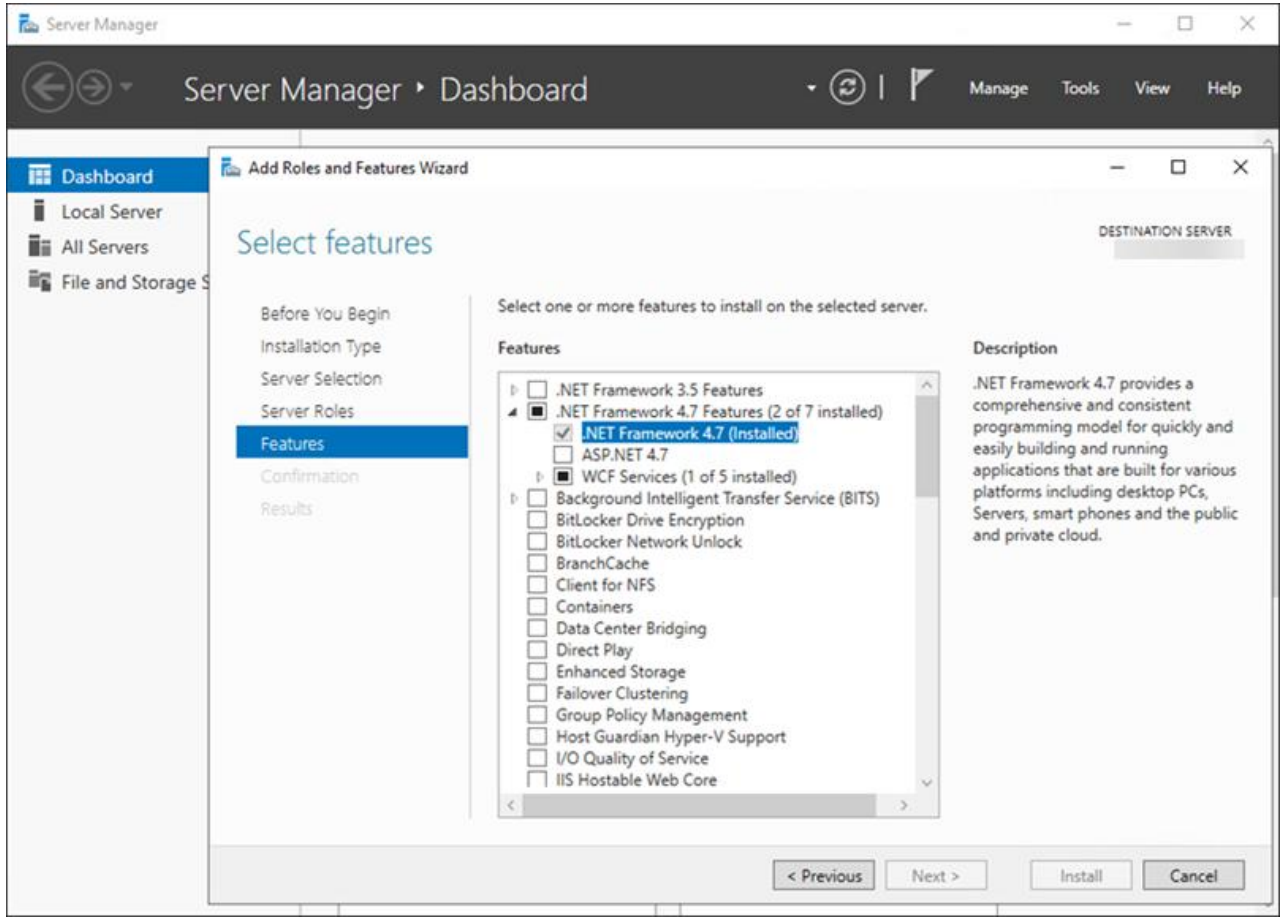
支援的資料庫伺服器和資料庫連接器

支援的資料庫伺服器	支援的資料庫版本	支援的資料庫連接器
Microsoft SQL Server	•Express 和非 Express 版本 •2016, 2017, 2019, 2022	•SQL 伺服器 •SQL Server Native Client 10.0 •ODBC 驅動程式，適用於 SQL Server 11、13、17、18
MySQL	•8.0 •8.1 •8.4 •9	MySQL ODBC 驅動程式版本： •8.x (8.0.x, 8.1.x) •9.2

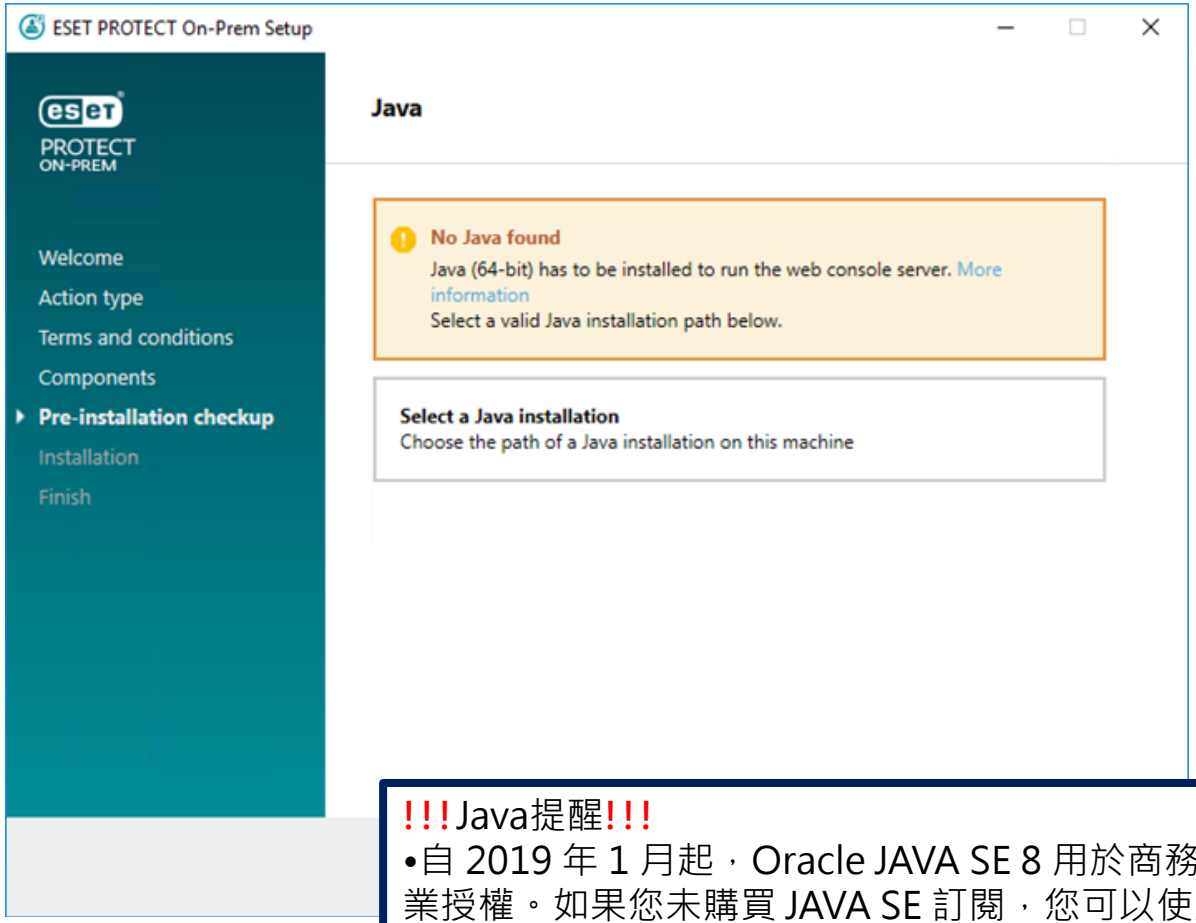
!!!資料庫建議與提醒!!!
•Microsoft SQL Server Express(免費版)的每個關聯式資料庫大小限制為**10**GB。
•ESET PROTECT On-Prem **不支援 MariaDB**。在最新的 Linux 環境中，MariaDB 是預設的資料庫，而且會在您選擇安裝 MySQL 時進行安裝。
•Rocky Linux 不支援 MySQL ODBC 驅動程式 8.x。我們建議在 Rocky Linux 上使用 **mariadb-connector-odbc** 驅動程式版本 3.1.12。

ESET PROTECT安裝

安裝的先決條件-未安裝所需的dotNET版本



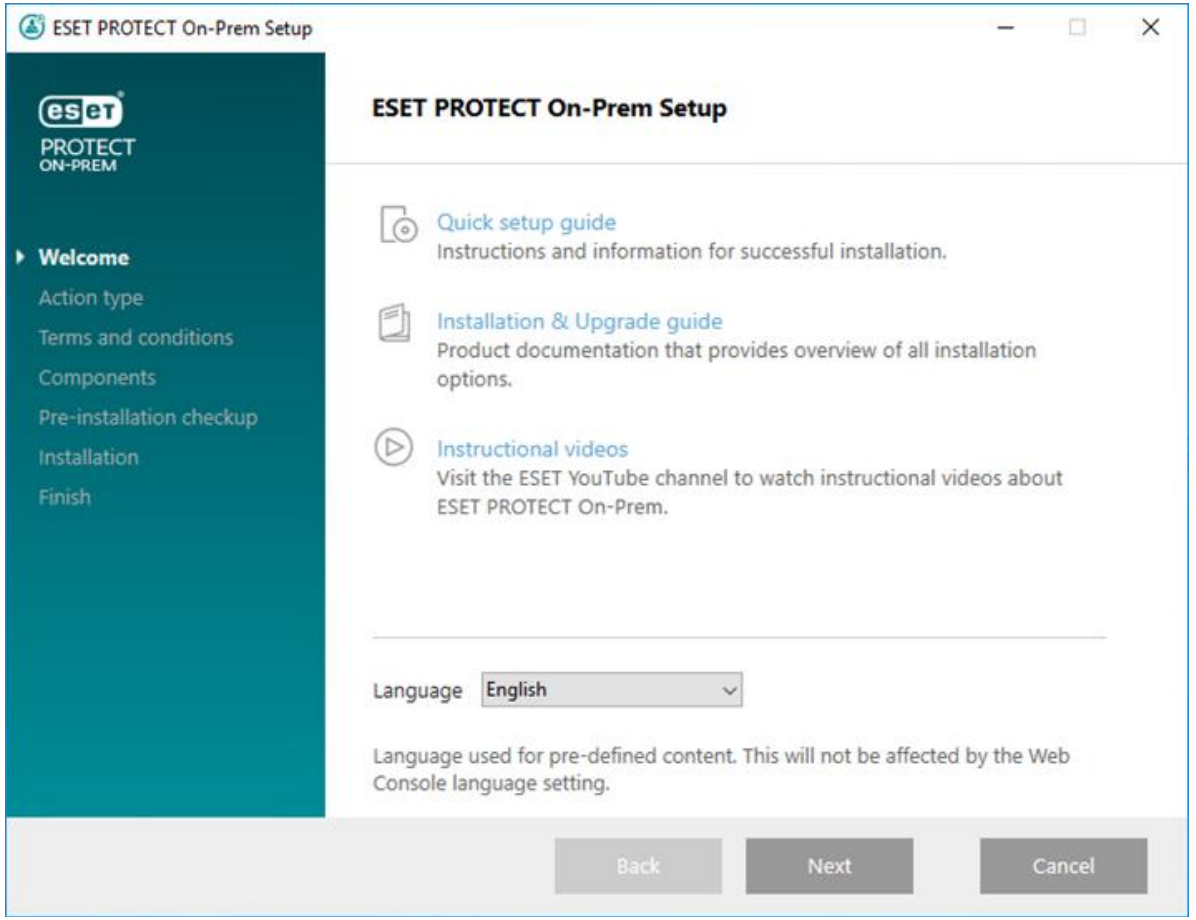
安裝的先決條件-找不到Java



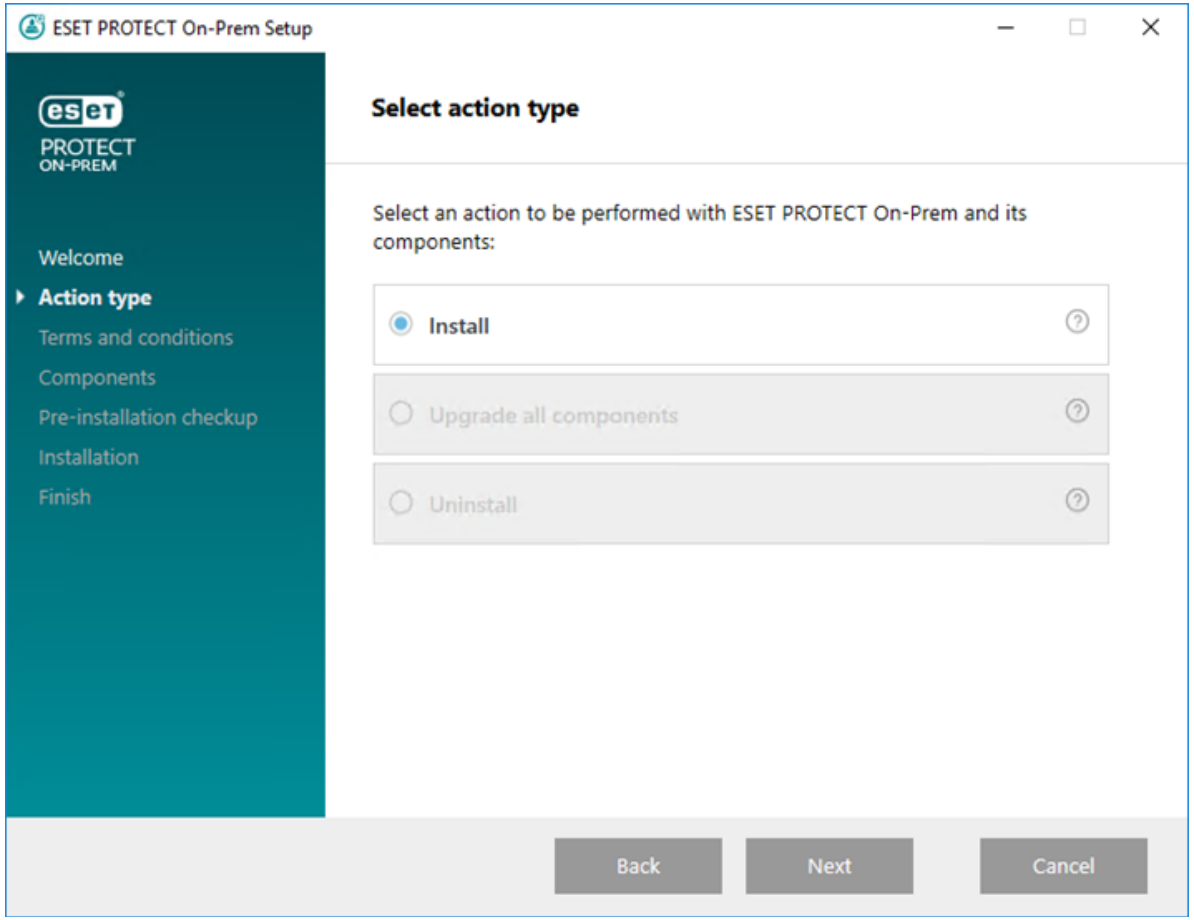
!!!Java提醒!!!

•自 2019 年 1 月起，Oracle JAVA SE 8 用於商務、商業或生產用途的公用更新需要商業授權。如果您未購買 JAVA SE 訂閱，您可以使用本指南轉換為免費的替代項目。請參閱支援的 JDK 版本。

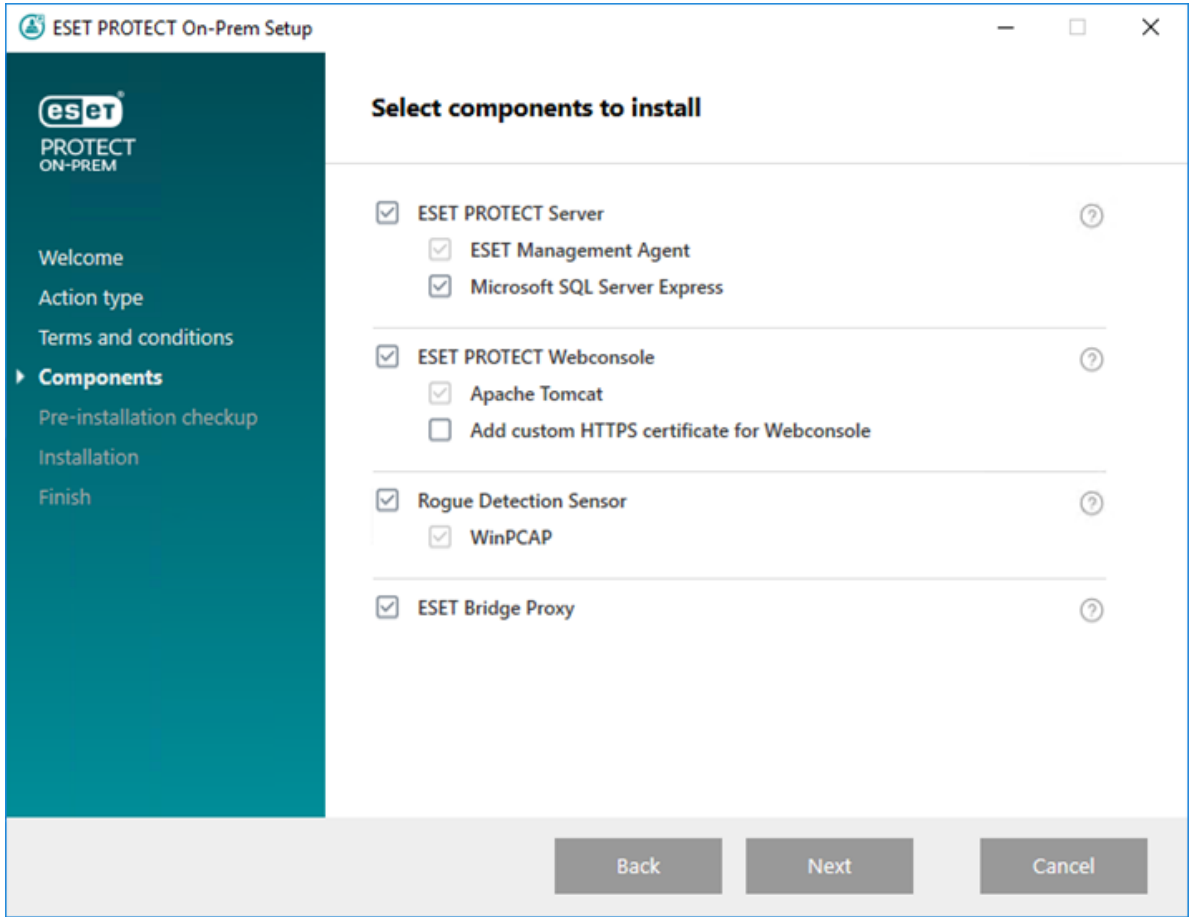
Windows 上的全方位安装



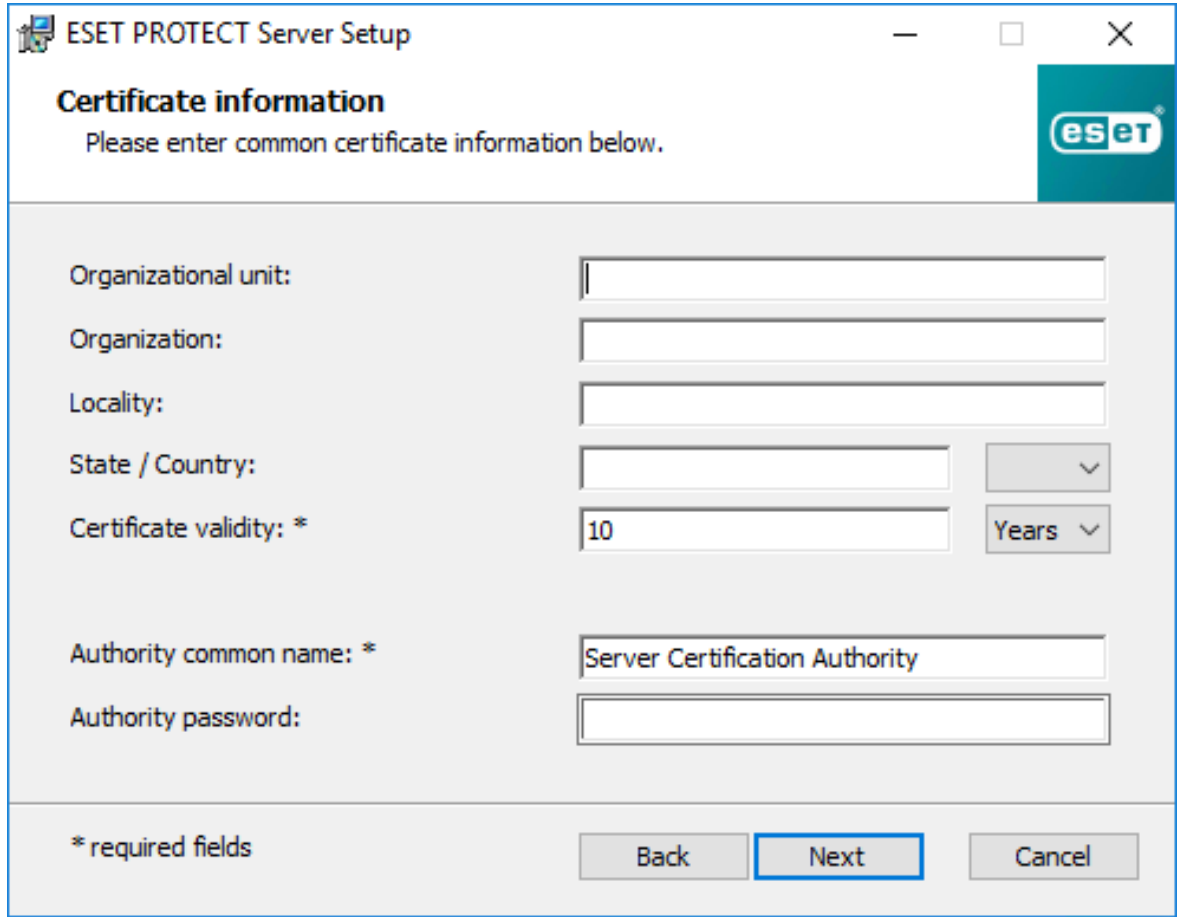
Windows 上的全方位安裝(續)



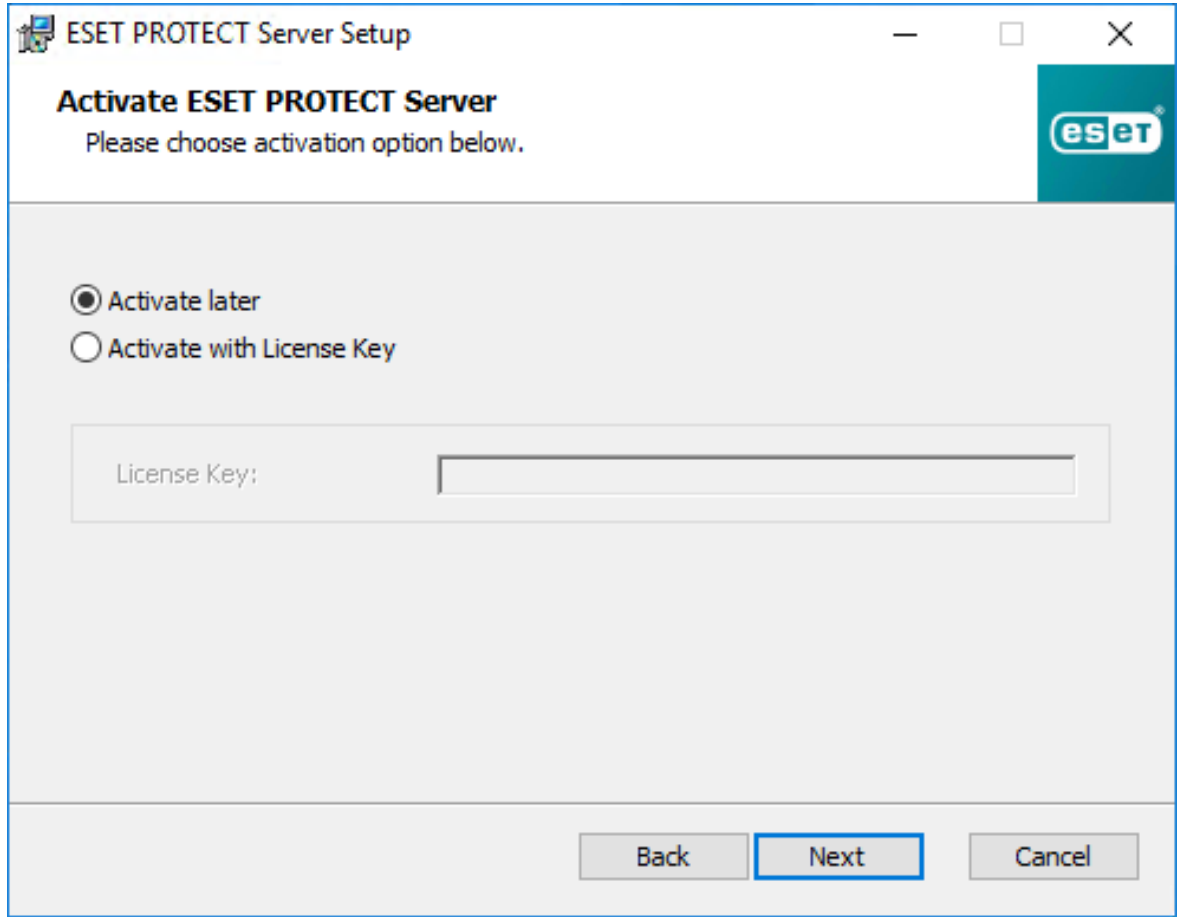
Windows 上的全方位安裝(續)



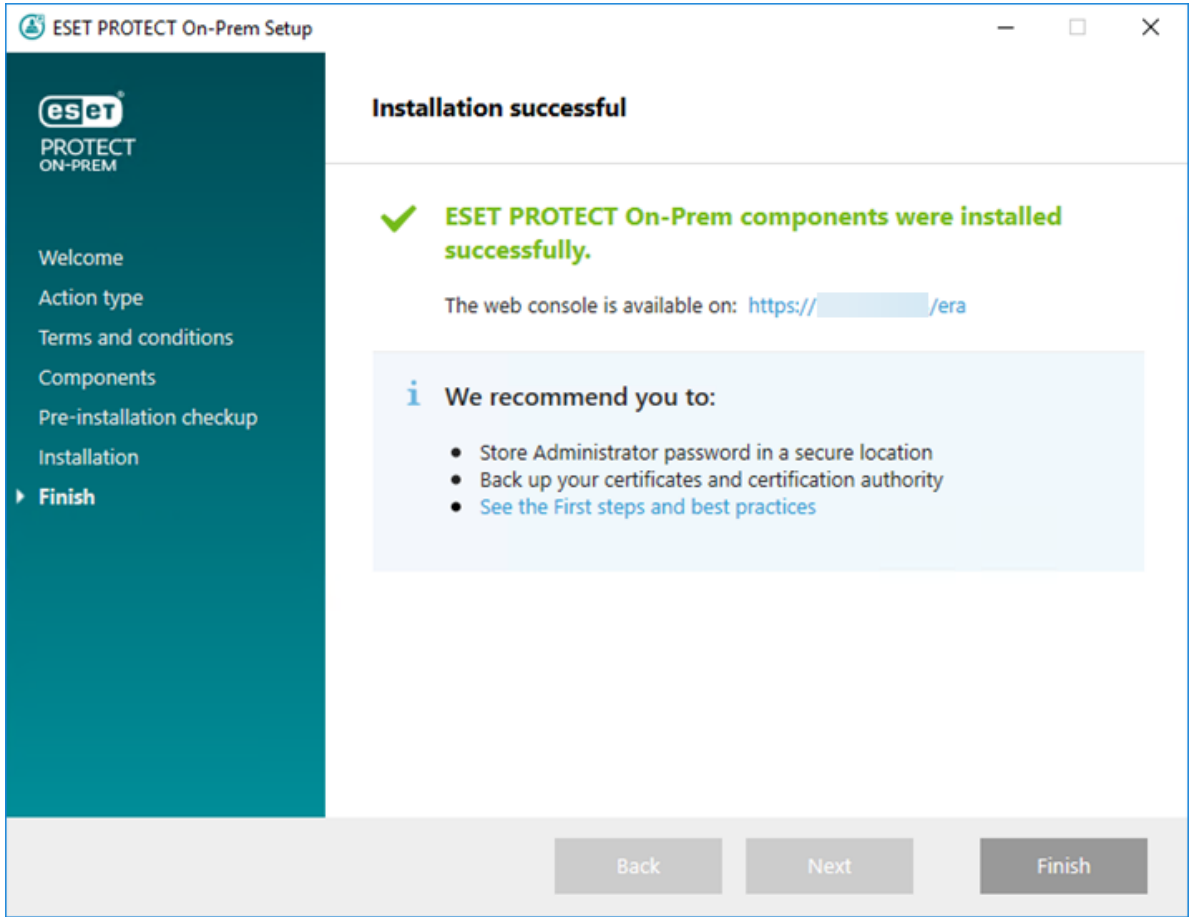
Windows 上的全方位安裝(續)



Windows 上的全方位安裝(續)



Windows 上的全方位安裝(續)



來源網址:https://help.eset.com/protect_install/12.0/zh-TW/arch_server.html?installation.html

結論

產品背景

秉持著ESET超過30年來的專精技術，成功的為企業打造安全防護網，更同時讓企業兼顧管理成本與系統運作效能。

端點安全的重要性

ESET企業安全解決方案（ESET Business Security Solutions）是針對企業複雜網路環境提供最高等級的全面防護規劃。

產品特色

端點偵測與反應系統（EDR）

端點設備防護

雲端沙箱

來源網址:https://cybersec.ithome.com.tw/2025/product-page/5015

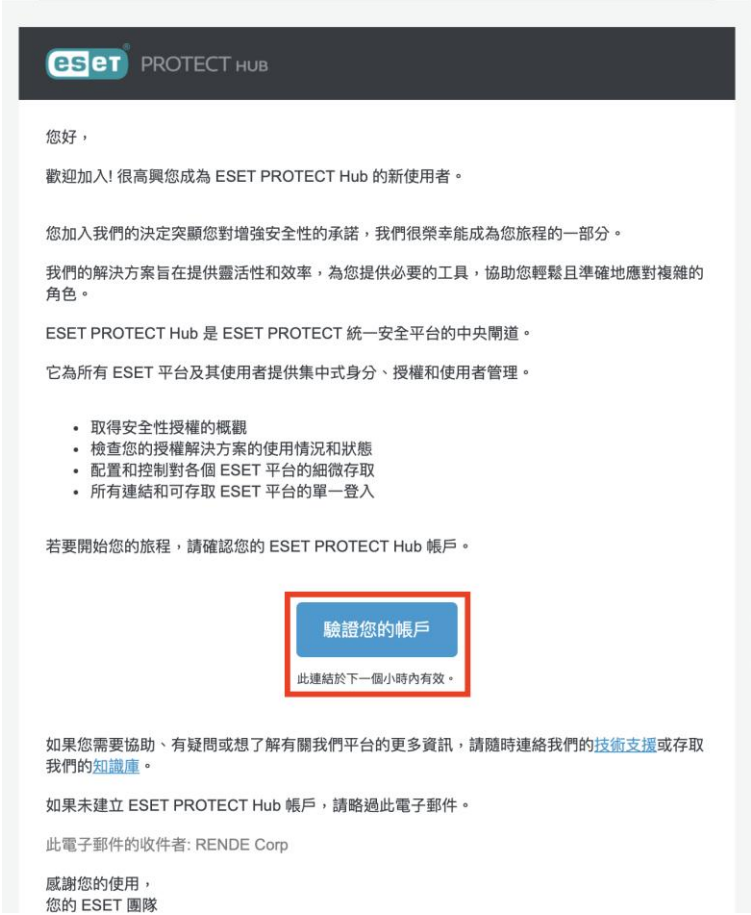
ESET PROTECT On-Prem Demo

ESET PROTECT補充教材

ESET PROTECT Hub註冊

ESET PROTECT Hub註冊(續)

ESET PROTECT Hub註冊(續)



eset PROTECT HUB

您好，

歡迎加入! 很高興您成為 ESET PROTECT Hub 的新使用者。

您加入我們的決定突顯您對增強安全性的承諾，我們很榮幸能成為您旅程的一部分。

我們的解決方案旨在提供靈活性和效率，為您提供必要的工具，協助您輕鬆且準確地應對複雜的角色。

ESET PROTECT Hub 是 ESET PROTECT 統一安全平台的中央閘道。

它為所有 ESET 平台及其使用者提供集中式身分、授權和使用者管理。

- 取得安全性授權的概觀
- 檢查您的授權解決方案的使用情況和狀態
- 配置和控制對各個 ESET 平台的細微存取
- 所有連結和可存取 ESET 平台的單一登入

若要開始您的旅程，請確認您的 ESET PROTECT Hub 帳戶。

驗證您的帳戶

此連結於下一個小時內有效。

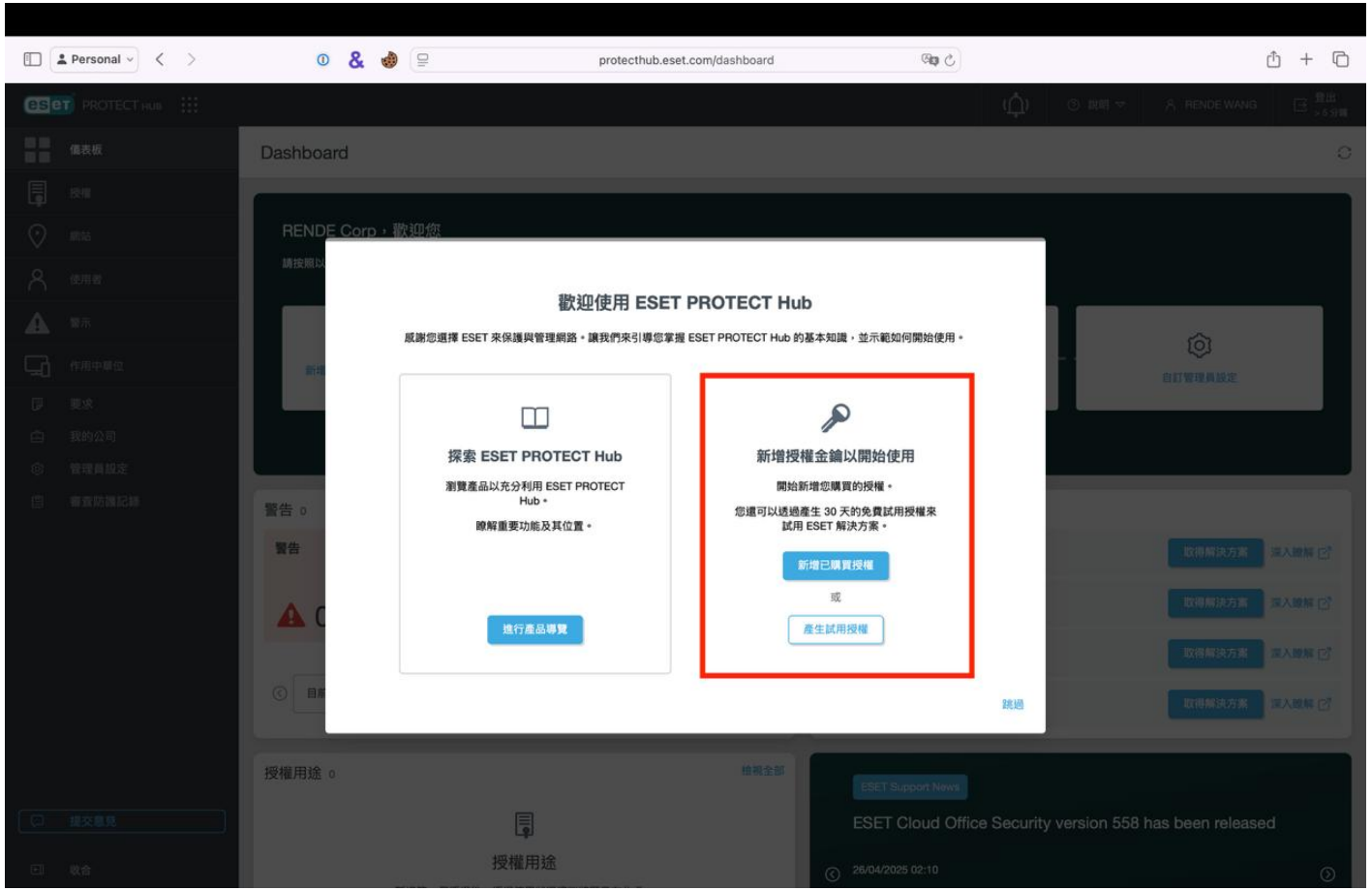
如果您需要協助、有疑問或想了解有關我們平台的更多資訊，請隨時連絡我們的技術支援或存取我們的知識庫。

如果未建立 ESET PROTECT Hub 帳戶，請略過此電子郵件。

此電子郵件的收件者: RENDE Corp

感謝您的使用，
您的 ESET 團隊

ESET PROTECT Hub註冊(續)



ESET PROTECT Hub註冊 Demo


Q&A

2025台灣二版

企業操作課程-NordLayer/NordStellar

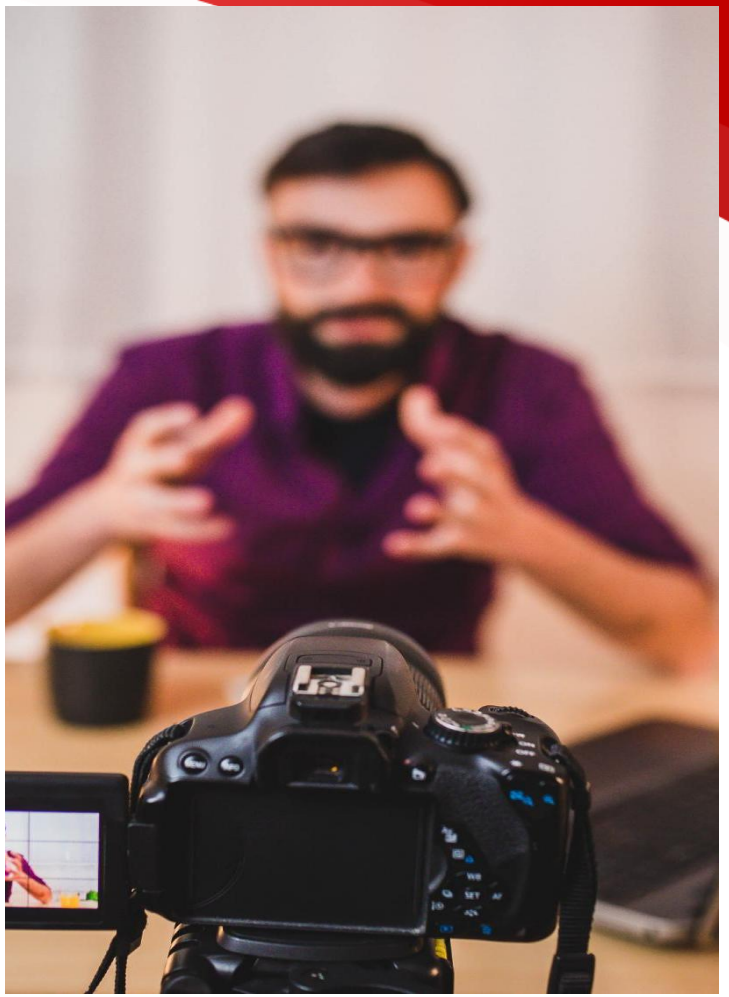
NordLayer/NordStellar 產品介紹

Version 2 台灣二版

- 主講人：

議程內容

- NordLayer產品背景
- NordLayer主要功能說明



NordLayer產品背景

關於NordLayer

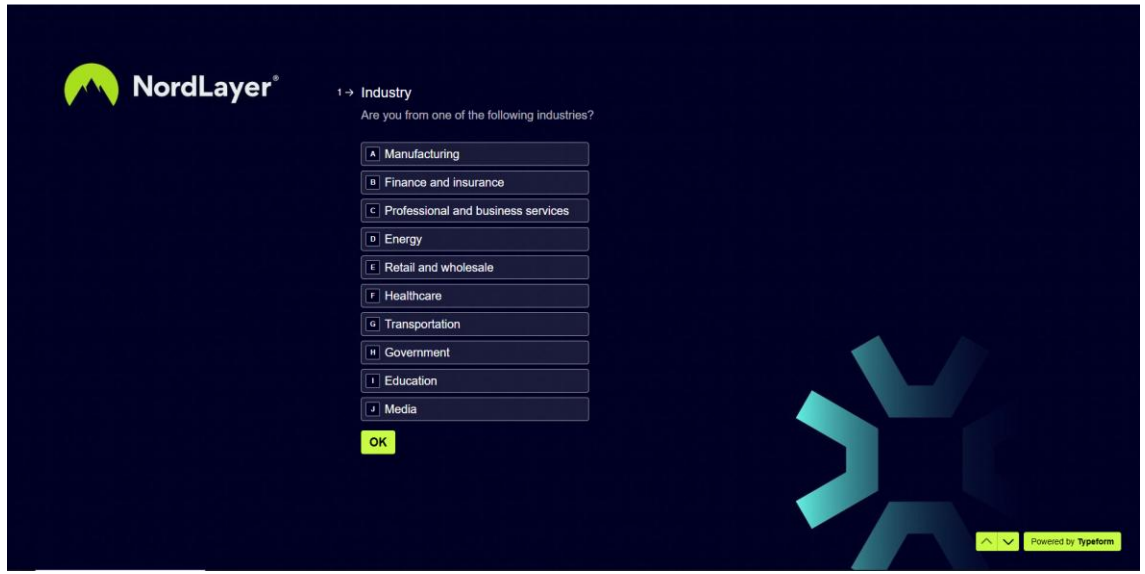
11,000+	10分鐘	30+	4.7/5
受保護的企業	平均部署時間	全球服務據點	**顧客滿意度**

- NordLayer 為任何規模和工作模式的企業提供靈活且易於實施的網路安全工具，這些工具均採用 NordVPN 標準開發。我們幫助企業輕鬆保護網路。 NordLayer 透過符合最佳監管合規標準的技術改進，增強網路安全性，並實現網路和資源存取的現代化。

- NordLayer 專注於網路安全服務的安全服務邊緣，幫助企業採用零信任網路 (ZTNA) 和安全工作小組 (SWG) 原則。 NordLayer 能夠快速輕鬆地與現有基礎設施集成，無需硬件，並且在設計時充分考慮了擴展性，從而滿足當今敏捷企業和分佈式員工不斷變化的增長速度和臨時網絡安全需求。

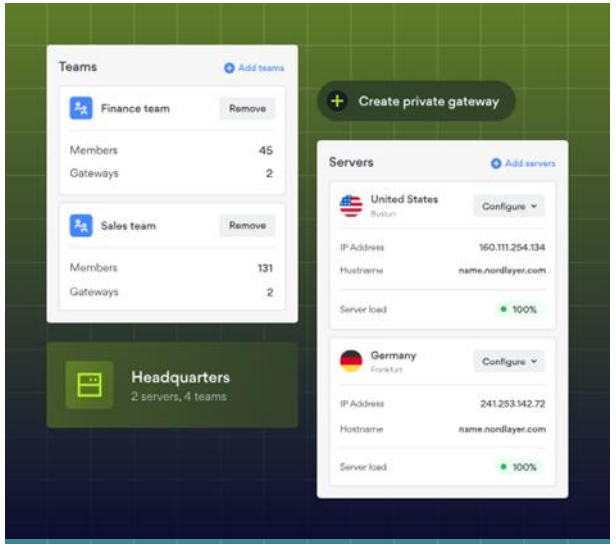
NordLayer主要功能

用於評估解決方案和識別風險的互動式工具



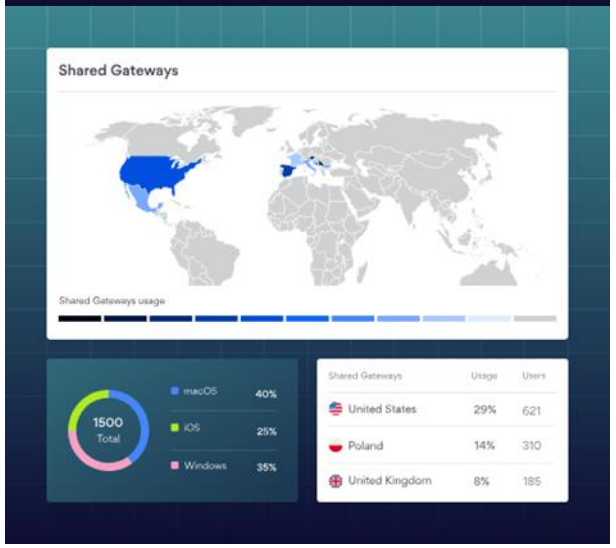
- 風險日益增加
- 規模中立風險
- 敏感數據
- 從哪裡開始

平台組件



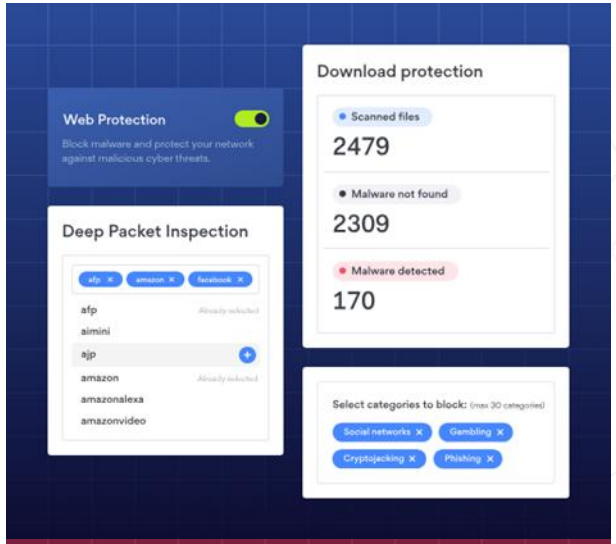
尖端商業 VPN

- 分割隧道
- NordLynx
- 始終開啟 VPN
- 瀏覽器擴充
- IP 允許清單
- 站點連接器



零信任網路訪問

- SCIM 集成
- 多重身份驗證 (MFA)
- 雲端防火牆（FWaaS）
- 設備姿態安全與監控
- 密碼管理器
- 活動/空閒會話逾時



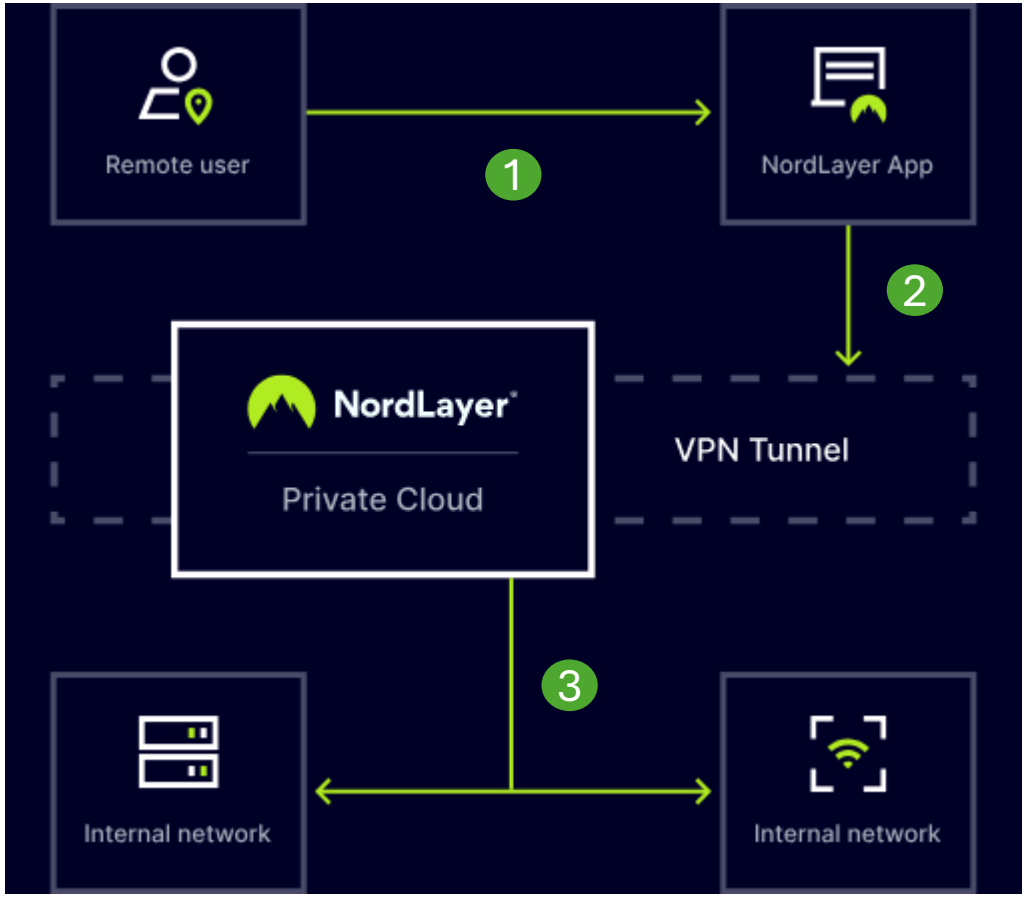
威脅防護

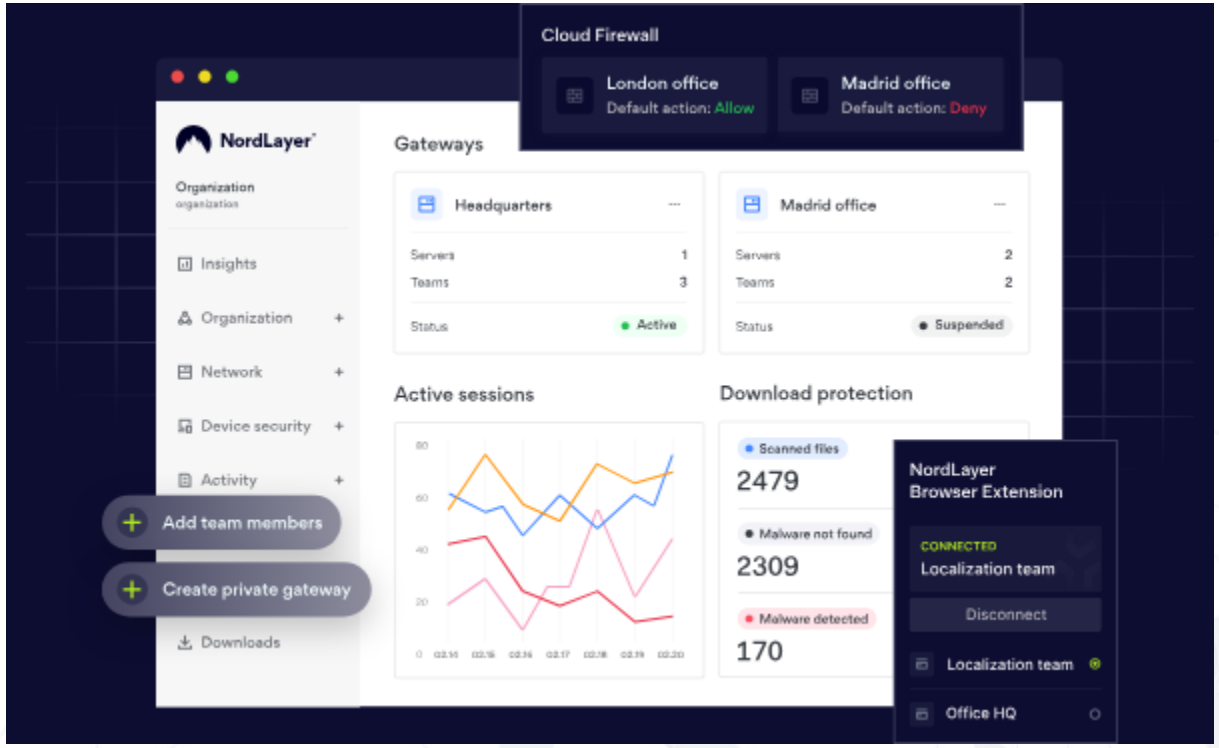
- 深度資料包檢測
- 下載保護
- Web 保護
- DNS 過濾

威脅情報

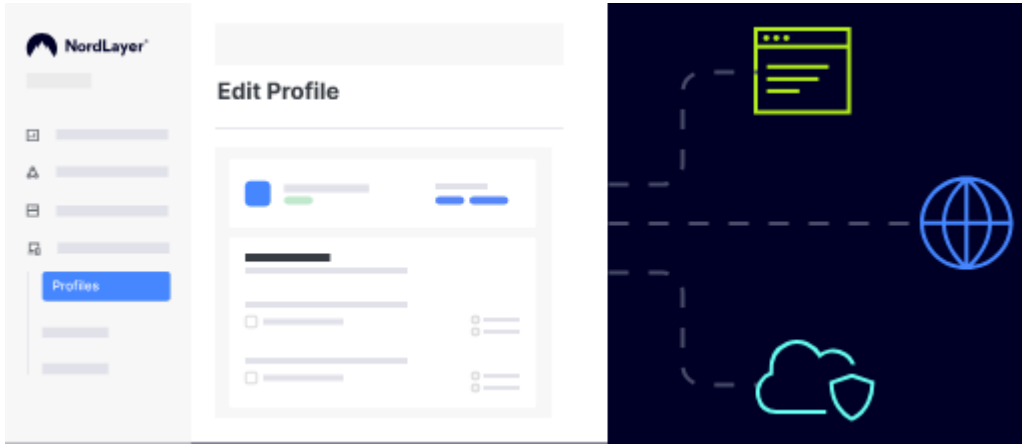
- 暗網監控
- 資料外洩預防
- 資料外洩管理

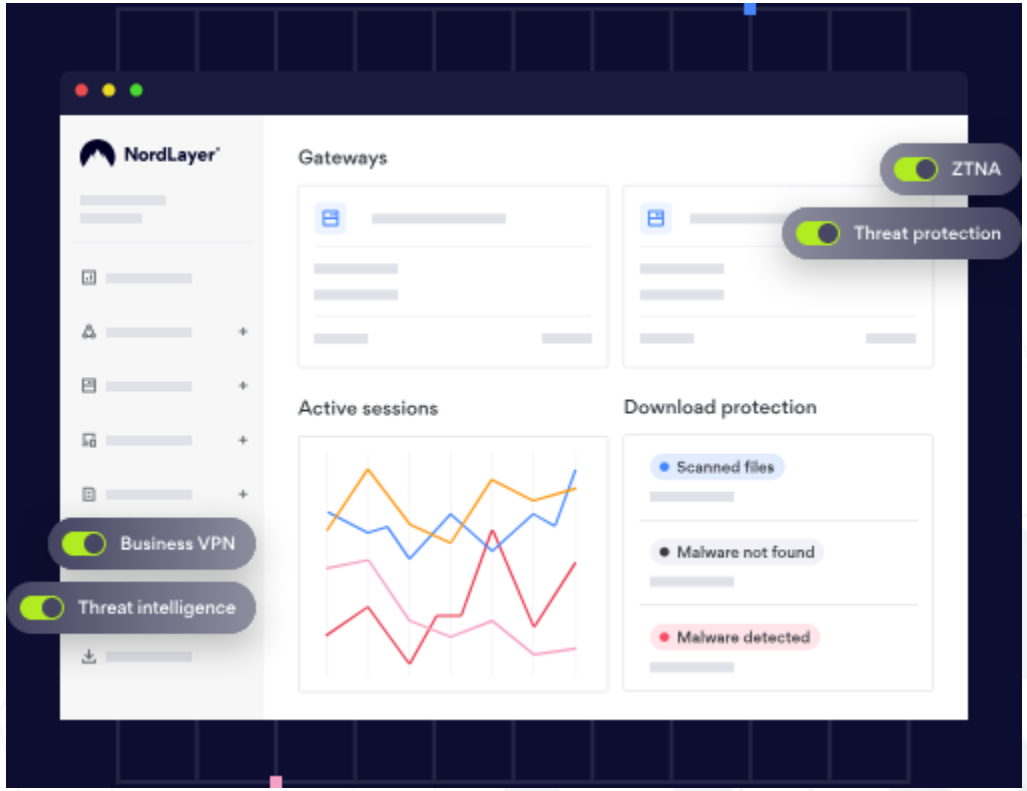
VPN





零信任網路訪問





零信任網路存取 (ZTNA) 以建立安全的存取控制為基礎，並非固有地信任網路內外的任何實體。它運用最佳實踐和技術，在應用程式、設備和資料周圍創建基於身分和上下文的安全邊界。透過利用信任代理，ZTNA 解決方案確保僅在嚴格驗證身分、上下文和策略合規性後才授予存取權限，從而有效地最大限度地減少網路內的未經授權的存取或橫向移動。此策略有助於隱藏關鍵資源，避免其公開暴露，並顯著降低網路攻擊的風險。

威脅防護

增強安全性

NordLayer 的威脅防護為您的營運增添了一層安全保障

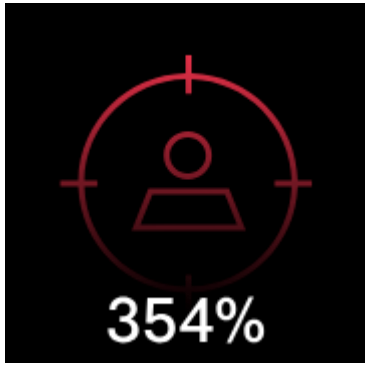
營運連續性

網路威脅會中斷日常運營，造成重大的財務和聲譽損失

監理合規性

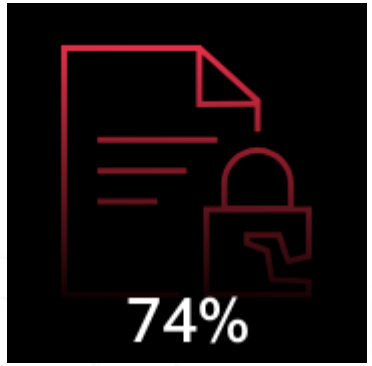
威脅防護措施是 GDPR、HIPAA 和 PCI DSS 等合規標準中的關鍵要求

暗網掃描



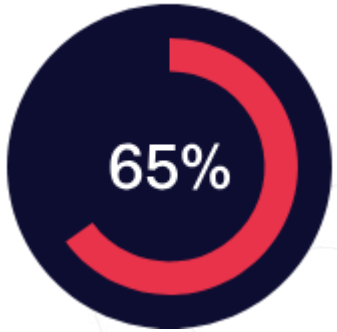
去年帳戶接管（ATO）攻擊激增

外部行為者造成的違規行為，主要是為了經濟利益

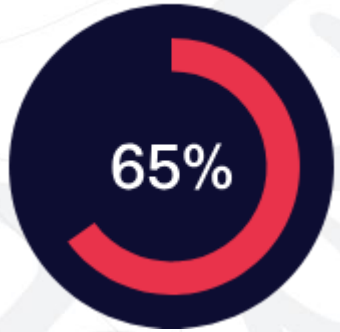


違規行為涉及人為錯誤、社會工程或被盜憑證

的企業在過去一年中遭受了網路攻擊



的公司報告稱資料外洩導致聲譽受損



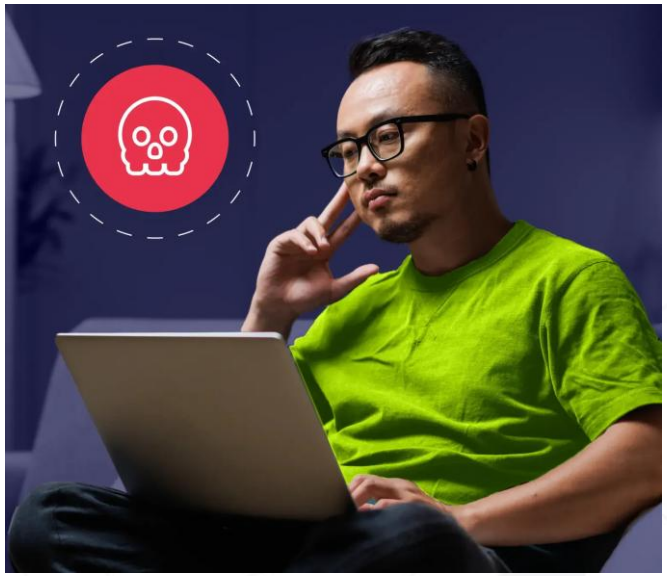
的 IT 管理員表示網路攻擊變得越來越嚴重

暗網掃描(續)

什麼是暗網？

暗網是網路中隱藏的一塊區域，無法透過常規搜尋引擎存取。它運行在 Tor 和 I2P 等覆蓋網路上，但由於潛在的漏洞和追蹤風險，無法保證 100% 的匿名性。雖然有些人用它來保護隱私，但它也是網路犯罪分子交易被盜敏感資料（例如公司憑證和財務記錄）的中心。

如果您的業務資料最終出現在暗網上，則表示駭客或惡意行為者可以存取它，從而使您的公司面臨欺詐、勒索軟體和身分盜竊的風險。



什麼是暗網掃描？

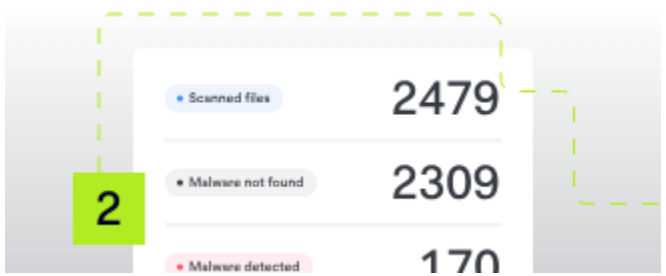
我們為企業提供的暗網掃描服務可協助公司偵測其敏感資料（例如員工憑證或客戶資訊）是否已在資料外洩中外洩。它會搜尋威脅行為者社群（例如暗網論壇和 Telegram 頻道），在這些社群中，網路犯罪分子會交換洩漏的資料、資訊竊取者和憑證轉儲，從而幫助您及早發現風險。

如果發現威脅，公司可以採取行動保護帳戶安全、加強存取控制並防止進一步的安全風險。

NordLayer 多功能防禦法介紹

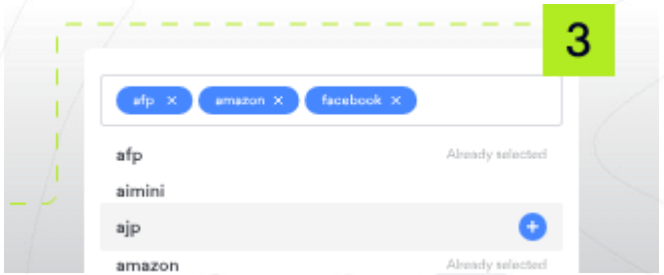
DNS 過濾和 Web 保護

DNS 過濾和 Web 防護是第一道防線。這些工具透過在 DNS 層級評估請求來阻止對惡意網站的存取。此類措施在瀏覽器環境中有效。 DNS 過濾可確保有害內容永遠無法到達員工的裝置。



下載保護

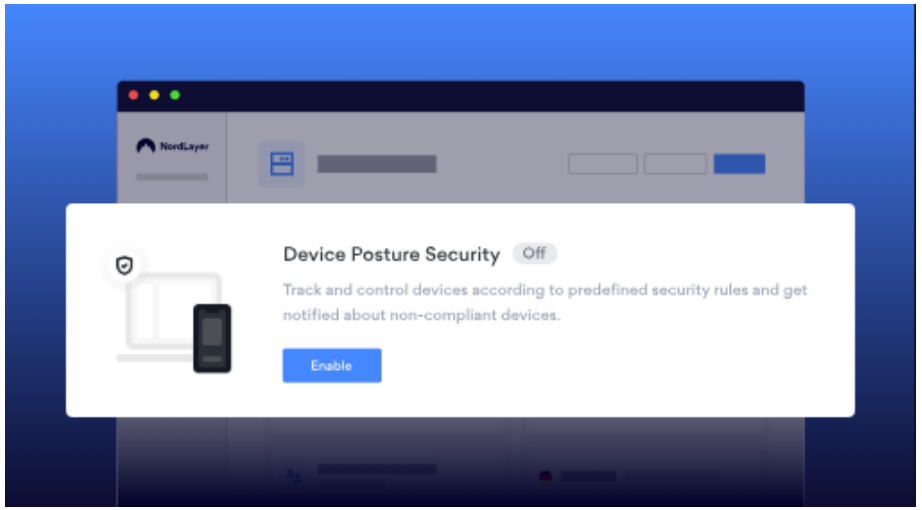
下載保護功能會在下載過程中即時掃描檔案。如果偵測到檔案中存在惡意程式碼，則會立即刪除，從而保護裝置和資料的安全。此功能可確保您的企業免受下載內容引發的惡意軟體攻擊。

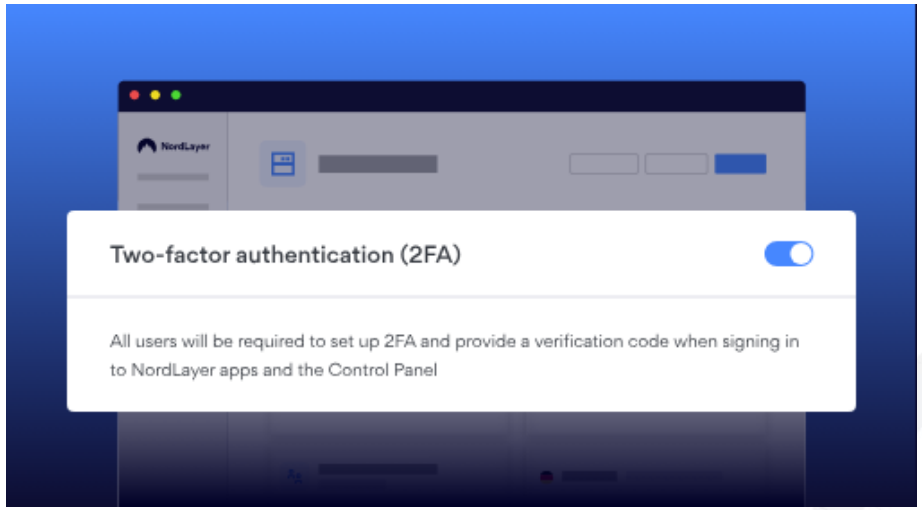


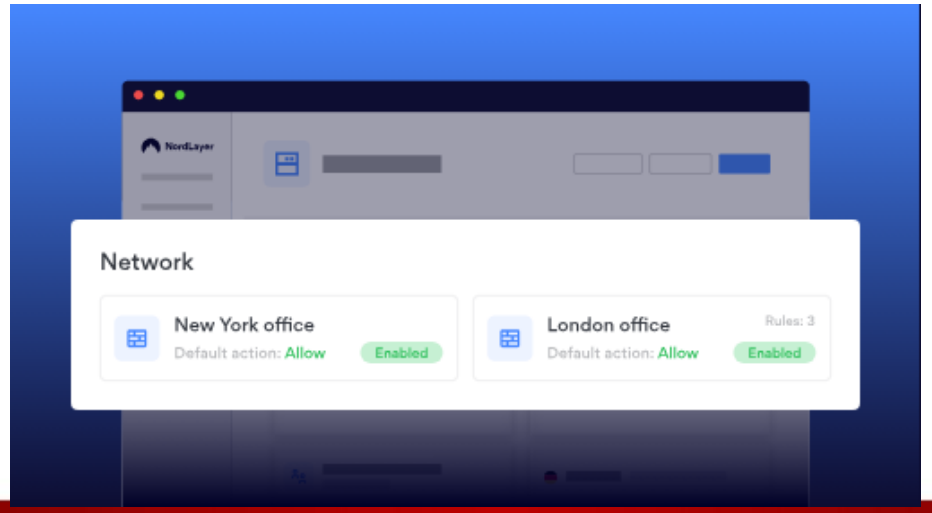
深度包檢測（DPI）

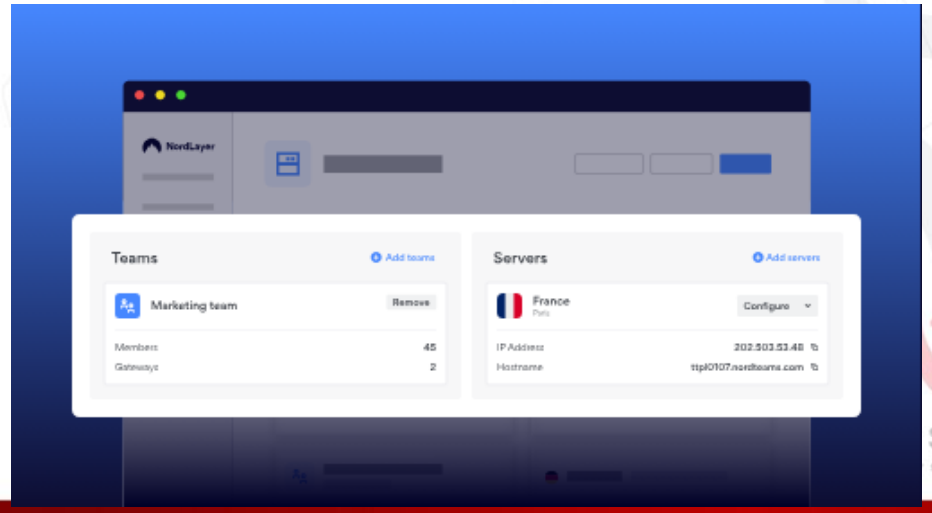
深度套件偵測 (DPI) 會分析網路流量，以阻止未經授權的應用程式和過時的協定。這樣一來，它可以預防漏洞並確保合規性。此功能在設備級別運行，可在不安全活動升級之前識別它們。DPI 也有助於管理流量，以優化網路效能，同時保持嚴格的安全標準。

NordLayer 如何防止商業資料流入暗網





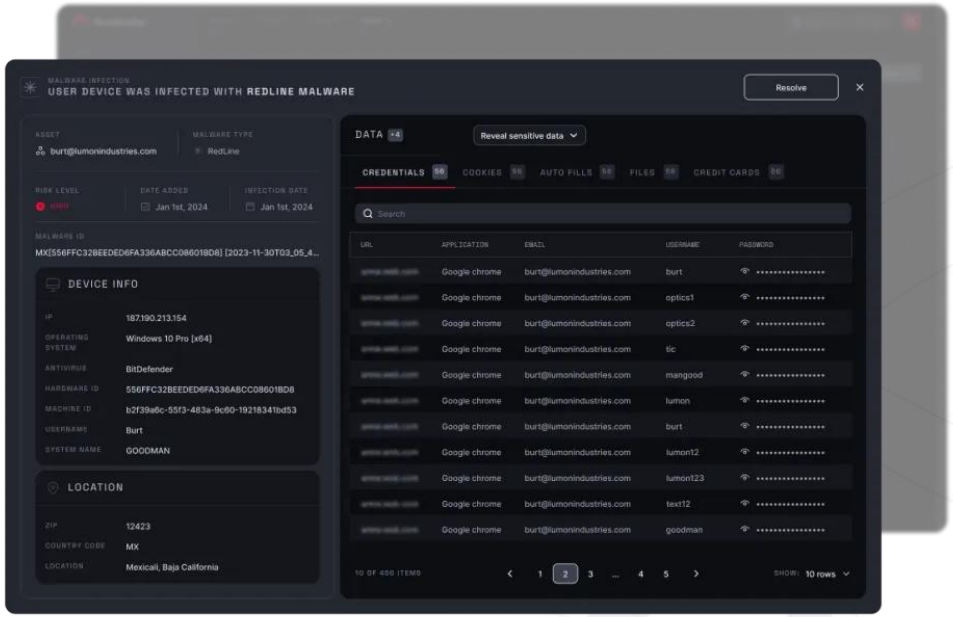




NordSteller功能介紹

帳戶盜用預防

- 即時識別受損帳戶
- 防止針對性地存取高階主管帳戶
- 避免聲譽損害和財務損失



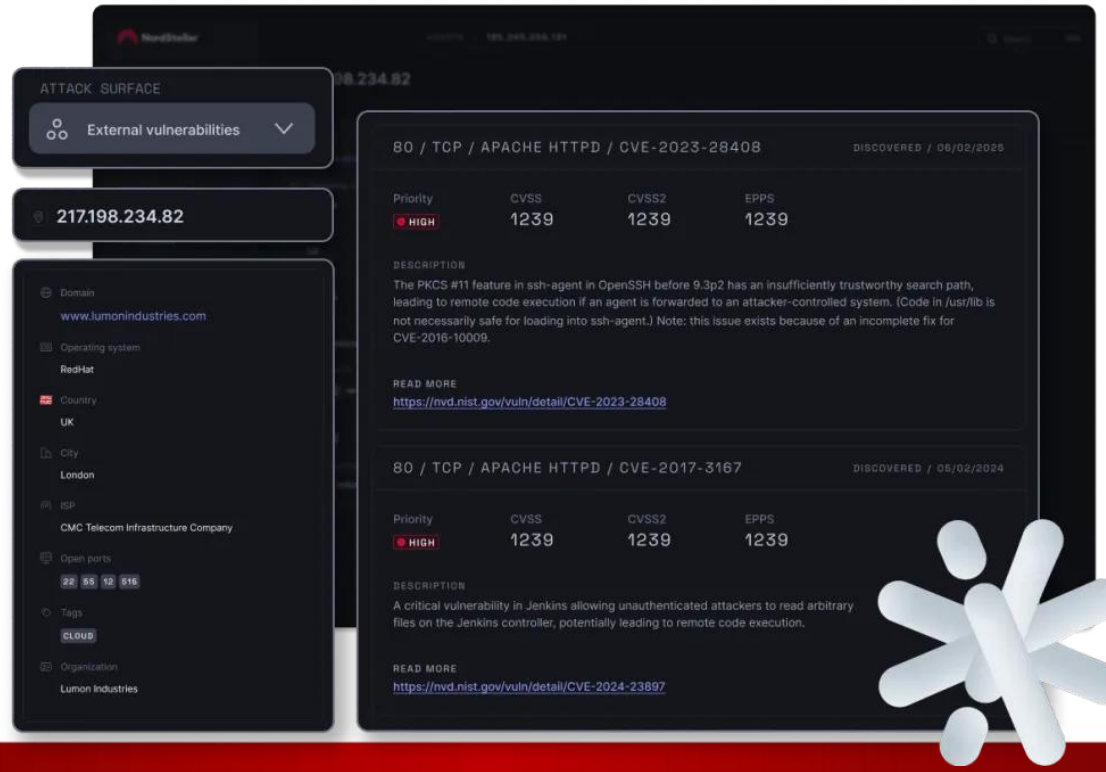
會話劫持預防

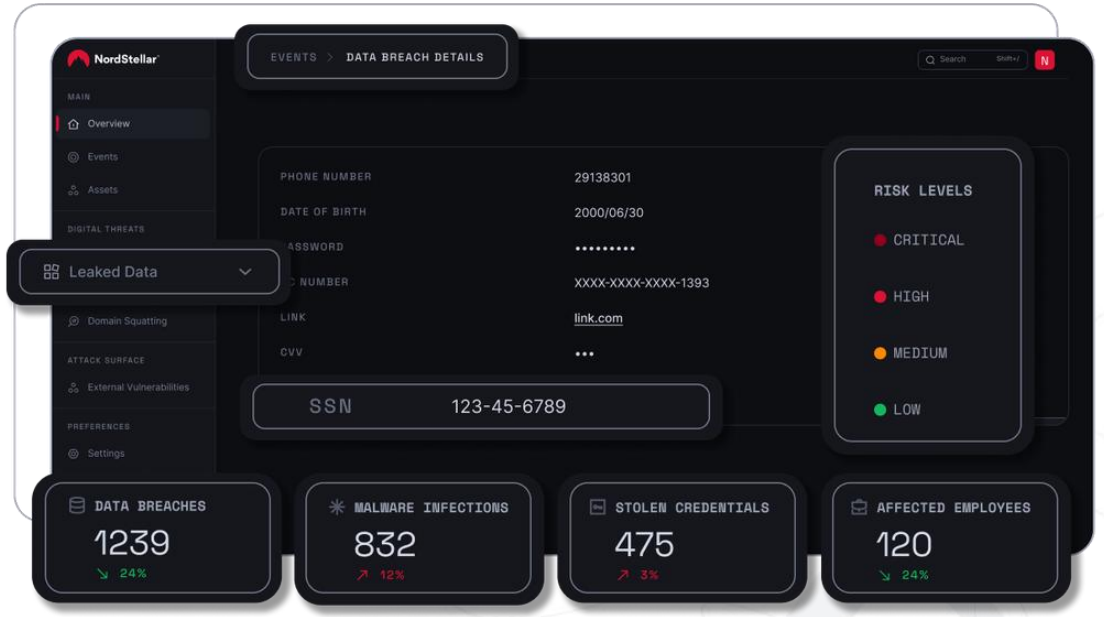
- 識別被盜的活動會話 cookie
- 使受損會話無效
- 檢測受感染的設備

NordSteller功能介紹(續)

為您的領導提供數位高階主管保護

監控並應對針對您領導團隊的威脅，從資料外洩
到惡意軟體感染，
再到可疑的暗網提及，無所不包。取得即時警報，
主動保護您的高階主管和企業。





外部漏洞掃描

- 減少您的業務的攻擊面
- 在漏洞出現時立即進行修補
- 加強您的安全態勢

NORDSTELLAR 漏洞掃描程式的工作原理

1

發現資產

使用 DNS 枚舉、CRT.sh 抓取和其他自動化流程，我們的漏洞掃描器將對應您公司的攻擊面並識別與您的網域相關的資產

2

掃描連接埠

我們會檢查與您的網域相關的所有資產是否存在開放連接埠—這些連接埠通常隱藏著漏洞。如果掃描發現開放端口，也會檢查哪些服務通過該端口運行

3

識別漏洞

下一步是檢查漏洞。我們的平台使用 SHODAN 豐富的漏洞資料庫和豐富的 CVE 資料來查找與開放連接埠相關的任何漏洞

4

確定風險優先級

一旦發現漏洞，我們的平台會使用 CVSS v3、CVSS v2 和 EPSS 評分系統評估每個安全漏洞的嚴重性和影響

5

呈現結果

最後，NordStellar 提供詳細的漏洞掃描結果。為了確保結果盡可能相關，該平台根據風險等級提供了優先級威脅清單。您也可以根據具體需求自訂警報

使用外部漏洞掃描可以偵測到什麼？

開啟連接埠

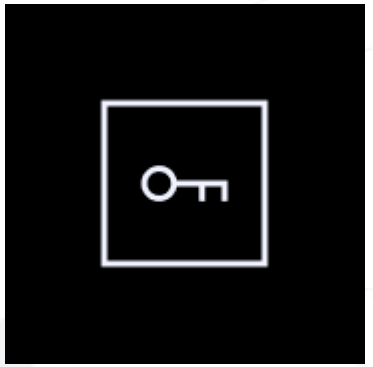
發現開放連接埠並保護透過這些連接埠運作的服務不被暴露

過時的軟體

了解軟體的哪些部分未能更新並修補已知漏洞

配置錯誤

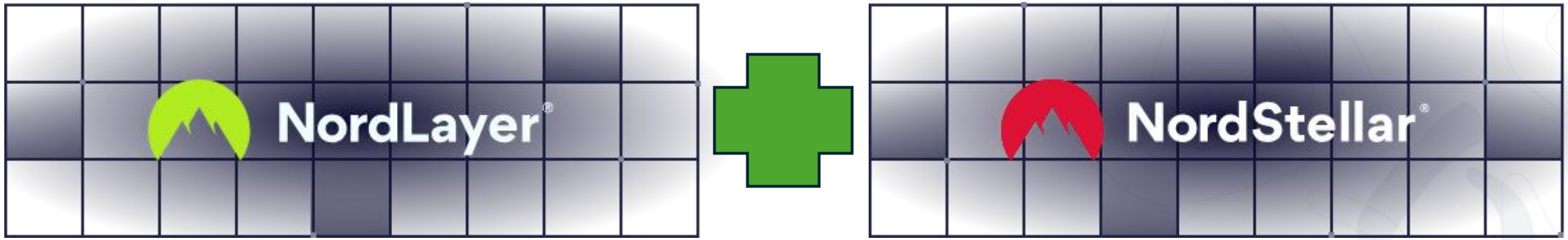
識別並處理身份驗證問題、過於寬鬆的防火牆以及不正確地設定的安全參數



未受保護的 API

尋找有缺陷的 API，並保護駭客無需身份驗證即可從網路存取的 API。

使用 NordLayer + NordStellar 偵測並預防暗網威脅



NordLayer

透過 MFA、設備態勢安全、雲端防火牆和零信任策略防止未經授權的訪問，降低憑證被盜被利用的風險

NordStellar

提供對外部威脅（如暗網）的全天候即時可見性，並幫助保護最重要的事物：您的員工、客戶、基礎設施和品牌

全面的安全保障，多層次的方法

網路防護

透過強大的網路保護解決方案在所有裝置和位置之間實現無縫、安全的連接，整合
VPN 和零信任原則，實現最大程度的防禦

- 共享網關
- 虛擬專用網關
- 具有專用 IP 的伺服器
- 雲端防火牆
- 設備狀態安全

威脅暴露管理

即時威脅情報和暗網監控可在潛在網路威脅影
響您的業務營運之前主動識別並減輕它們

- 帳戶接管預防
- 資料外洩監控
- 深網和暗網監控

遵守

我們的解決方案將積極促進您的安全檢查，並
協助減輕現場和遠端員工的潛在安全威脅

- ISO 27001
- NIS2
- DORA
- SOC 2 type 1 & 2
- HIPAA


Q&A