



Admyn™ CVE

—— 弱點掃描服務 ——



資安事件頻傳



近年資訊安全成為全球趨勢，提升了資安管理的重要性，有鑑於駭客攻擊手法日新月異、資安事件不斷風聲，企業該如何做好資安防護？



東元機電與宅配通發生網路資安事件，集團同日發重訊

在7月8日國內傳出兩家上市公司遭遇資安事故的消息，先是老牌電機大廠東元電機發布資安事件重大訊息，同日該公司旗下物流公司台灣宅配通也發布資安重訊。此外，當日還有上櫃公司聖暉工程科技代發布資安重訊，說明子公司聖暉系統集成集團遭受駭客攻擊。



台積供應商擎昊科技更新資安事件說明，提出三大檢討

日前勒索軟體LockBit駭客在6月30日聲稱入侵台積電，當日台積電指出已知悉IT硬體供應商遭駭，而被指為受害者的擎昊科技坦承遭駭，相隔4天，擎昊科技再次針對這次資安事件，說明了更多狀況。

包括該公司是在29日遭到網路攻擊，受影響的範圍是該公司為客戶準備系統安裝環境的工程測試區，同時也表示被截取的資訊中，因使用到特定客戶的公司名稱，因而引起網攻團體的注意，並試圖經此途徑取得客戶之機敏資料。



永信藥品遭駭客攻擊公司發佈資安重訊

業務範圍擴及全球多國的臺灣製藥公司永信藥品工業，昨日傳出遭遇資安事故，上市生技醫療業永信投控在6月17日下午4時32分率先揭露此事，於證交所公開資訊觀測站發布資安重訊，代重要子公司永信藥品工業公告部分資訊系統遭受駭客攻擊，同日傍晚6時，身為公開發行公司的永信藥品工業也發布重訊，公開這起資安事故。

*資料來源:iTome資安事件公告

掌握第一手重大弱點漏洞資訊

現行企業遵循資安法規如:上市資通安全管控指引、資安認證
如:ISO27001,定期進行弱點掃描服務,但往往有些弱點漏洞產生時,已過了弱掃時間,
IT常常無法立即得到相關漏洞資訊,使得企業潛在的資安風險也會提高



IT的聲音，我們聽到了！



「可不可以提供我一套好的工具,讓我能隨時更新弱點漏洞資訊?」



「能不能協助公司及IT全面掌握弱點漏洞資訊 並達到管控預防資安攻擊的發生機率?」



「能夠在第一時間提供圖形化介面的漏洞更新數量狀態,並且由我指定那幾台電腦要進行更新,然後自動派送到每一台電腦進行漏洞修補呢?」

預防勝於治療

坊間現行顧問諮詢弱點掃描SOP 5步驟：

優點：

- 1.資安顧問針對客戶企業環境提供專屬建議與諮詢
- 2.藉由初測及複測的弱點掃描,能確保現階段潛在的弱點漏洞能被完全揭露及更新修補

缺點：

- 1.漏洞更新修補有時間階段性,無法即時掃描更新及呈現相關重大漏洞
- 2.依據客戶規模大小提供專案報價,每次所需花費的掃描費用較高。
- 3.IT無法即時掌握弱點漏洞數量及修補更新狀況

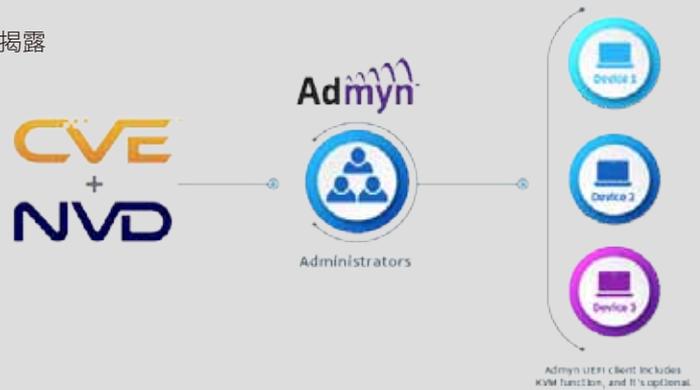


系微提供的解決方案：

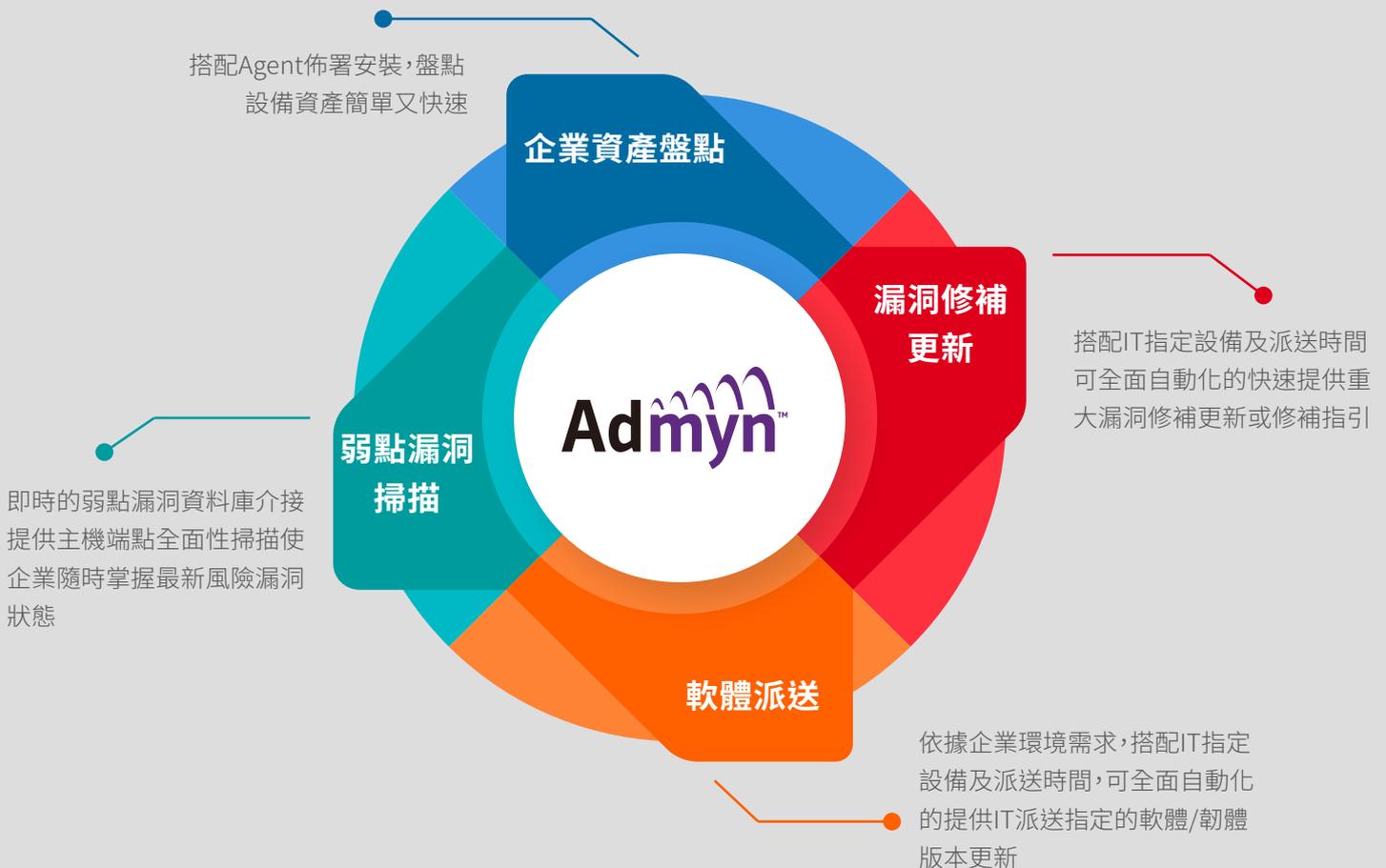
Admyn CVE Architecture Diagram

優點：

- 藉由初測及複測的弱點掃描,能確保現階段的潛在弱點漏洞能被完全揭露及更新修補
- 重大弱點漏洞更新修補快速即時零時差
- 資安顧問針對客戶企業環境提供專屬建議與諮詢
- 計價採訂閱服務,無限制掃描次數,想掃就掃,完全讓你掃好掃滿
- 掃描及修補更新狀態,透過圖形化介面,立即快速呈現
- Client端一次性快速佈署,弱點漏洞更新修補,軟體安裝一鍵自動派送通通做得到!



Admyn CVE 專注功能 覆蓋全面



差異比較：

產品名稱/使用工具	一般弱點掃描工具	Admyn™ CVE
掃描範圍	CVE	CVE
掃描頻率次數	至少2次(初測+複測)	無限制 🚧
掃描結果呈現方式	Report	Report + Dashboard 🚧
漏洞修補	By case報價提供修補服務	自動化修補 🚧

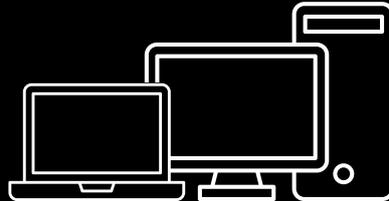
Admyn™ CVE Dashboard

圖形化呈現設備弱點漏洞
現狀修補更新一目了然



清楚掌握企業Top10 高風險
產品一鍵派送修補更新

企業弱點漏洞即時狀態
多維度解析成長趨勢與增減



主機端點安裝Agent硬體需求

作業系統	Windows Server 2016 或 Windows 10 以上之 64-bit 版本
中央處理器	1 GHz 64-bit 相容處理器
記憶體	2 GB
可用磁碟空間	2 GB

* DirectX® 9 顯示裝置具 WDDM 1.0 或更高的驅動程式

* 防火牆需開通 8883 Port