資安防護稽核分析管理模組/使用授權

網路資訊發達時代常需上網查詢資訊，但如無法自制，可能會消耗太多時間於無效資訊上，需一有效方案實施上網控管功能，並具備稽核能力，以利事後查核統計。

上網流量超越60%以上為SSL加密流量，將導致既有資安設備有60%無法檢測內容與防護，許多惡意攻擊流量皆隱匿其中，需要有效架構解決此一重大資安防護漏洞。

流量加解密模組

可恢復原有資安防護能力，避免每項資安皆升級解密能力，大幅節省預算，避免惡意流量潛藏上網流量中。

完善的解密能力

●具備辨識動態SSL加密能力

彈性的管理機制

●SSL拆解排除設計

搞定複雜的加密行為

●HSTS、HPKP

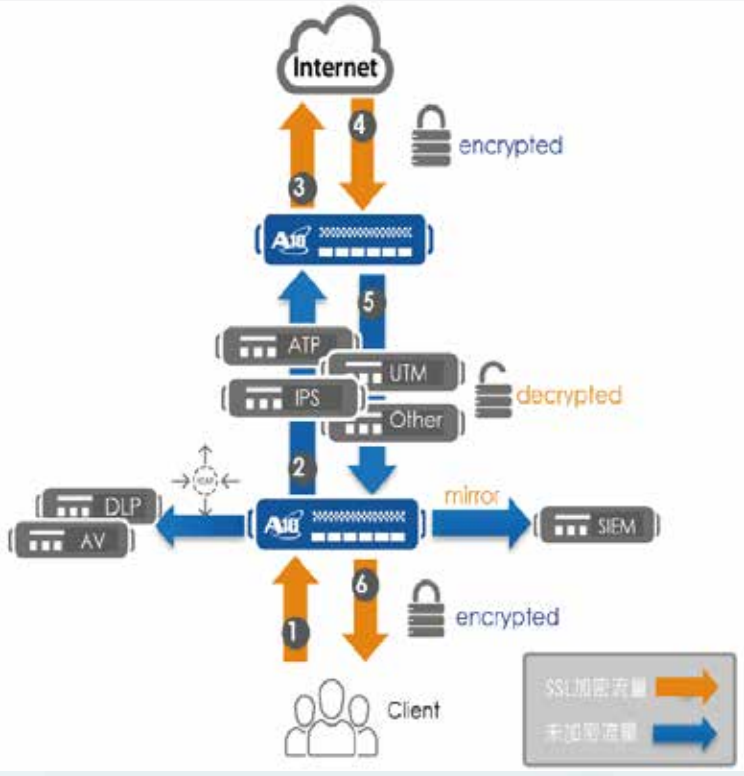
●SDHE/ECDHE Cipher support

動態偵測及拆解使用SSL/TLS加密流量

●Unknown ports (不只 TCP 443)

支援START-TLS拆解

●SSMTP, XMPP, POP3



流量稽核管控模組

導入流量稽核管控，有效控管公務時間允許之應用程式、網站、頻寬，提升公務效率，並提供完整統計報表資訊，以利日後政策訂定。

功能：

身分認證（員工、訪客）

頻寬流量管理

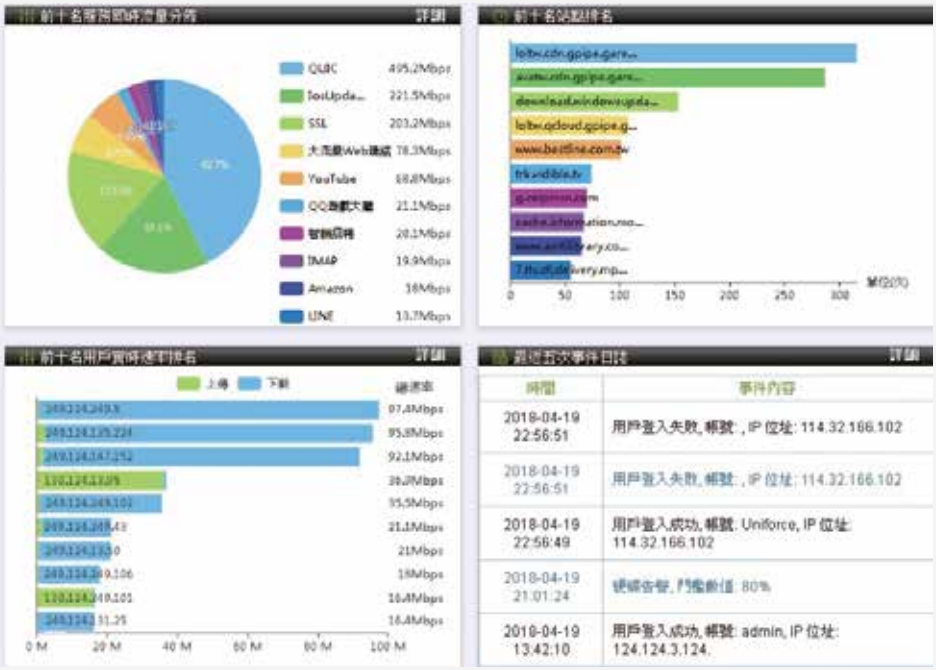
應用服務管制

上網行為稽核

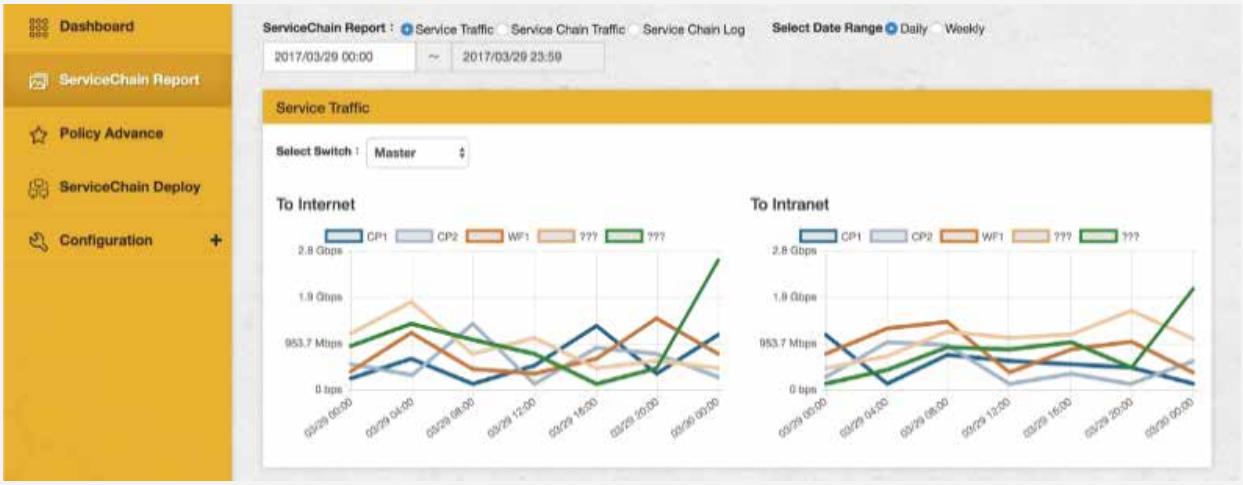
網路流量軌跡追蹤

效益：

提升公務效率，避免惡意網站降低頻寬費用，提供統計資訊，作為評估依據完整報表，以利上網政策制定。



資安檢索分析模組



資安檢索分析模組提供網路流量智慧分流功能，操作人性化、資安設備異常時，可快速排查，無須停機...等。

特色

- 遇網路資安攻擊能有效解決方案
- 汰換設備後，舊設備能沿用，減少預算浪費
- 發揮高可用性之效能
- 延遲時間極少
- 負載平衡和資安設備整合性高
- 網路人工智能慧化
- 提高網路高可用性
- 東西向流量資訊安全防護
- 虛擬化環境資訊安全提高

無人機反制警示模組

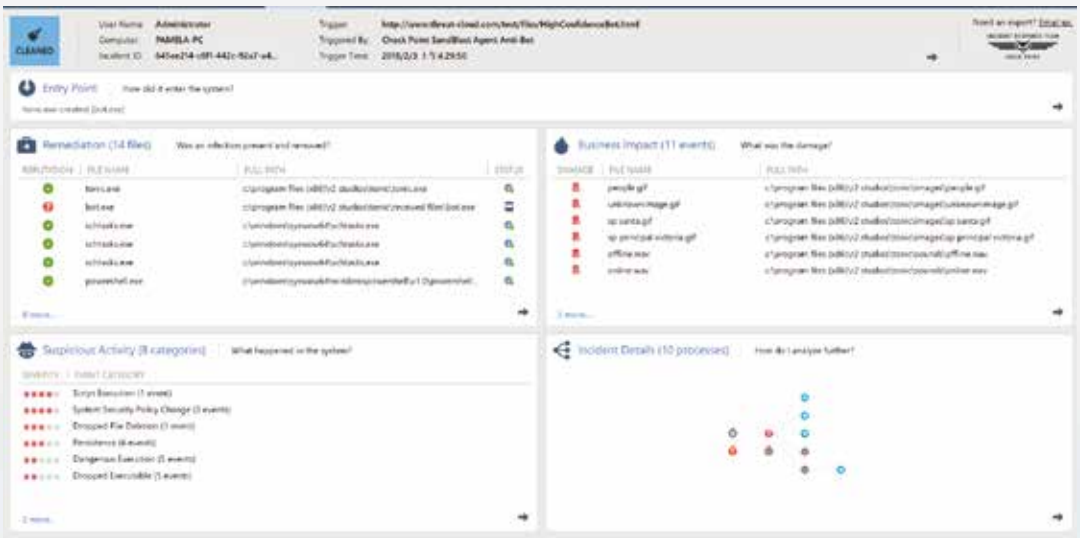
經由建置無人機防制系統軟體，透過制定整合的安全和安防措施，以系統之虛擬區域劃定防制區域範圍，達到警戒偵測及入侵即時警示之區域聯防，達到確保設定區域安全。

特色

- 虛擬禁飛區、虛擬航線、登陸位置。
- 無人機群的發現和緩解。
- 授權無人機的白名單。
- 集成到VMS系統中。

APT攻擊防禦模組

導入新世代資安管理平台暨端點勒索軟體防護，防護APT攻擊、網路入侵、惡意程式、勒索軟體、殭屍網路等複雜網路攻擊，並建立統一管理介面，多樣統計報表，大幅提升機關資安防護能力。



特色

- 大幅提升資安防護能力
- 有效控制應用程式資安防護能力
- 避免勒索軟體攻擊
- 提供統計資訊，作為評估依據
- 完整報表，以利日後政策

DDoS防禦模組

建置DDoS防護系統，可防護府內各式對外服務遭受阻斷式服務攻擊，例如：網站、DNS服務等，除外對內之外也可偵測內對外阻斷服務攻擊,常見於府內電腦中毒感染病毒成為殭屍網路一員。

WAF網站防禦模組

網頁應用程式可說是由外而內的攻擊管道之一，欲防範諸如SQL資料隱碼（SQL Injection）、跨網站指令碼（Cross-Site Scripting）等攻擊行為，大多會在網頁伺服器的前方建置WAF（Web Application Firewall，網頁應用程式防火牆）來抵擋。如今面對駭客組織化、商業化後，促使攻擊手法隨時都在進步，WAF更必須與時俱進，因應攻擊手法的變化，來進行辨識與攔阻。

本模組除管理端外，使用端必須再購買使用授權

經銷商蓋章

華麗得股份有限公司
Brecioso Co., Ltd.
TEL：02-89235035
service@brecioso.com