Cyber Attack 手忙腳亂，AMF-SECurity 自動阻斷

針對感染惡意軟體 / 勒索軟體的終端設備，利用終端交換器 (Edge Switch) 中斷連線隔離！防止受害擴散！

AMF-SEC(Autonomous Management Framework SECurity)

在傳統閘道式防火牆的架構中，遭遇網路攻擊時只能靠防火牆 (Firwall) 進行阻擋及防禦，對於內部攻擊就算注意到病毒的入侵，通常也已經漫延到企業整個網路環境。面對這樣的狀況，管理者也僅能被動及耗時地找出受感染設備再加以進行處理，這樣的處理方式成效不彰，並且各廠牌防火牆、交換器及資安設備操作方式不同，難以用傳統網管方式進行聯合及終端防禦管理。因此，Allied Telesis 開發出 AMF-SEC ，可和不同廠牌防火牆、資安設備及應用程式整合，在偵測到攻擊行為時自動關閉受感染的終端設備與網路，以阻止病毒感染的擴散！
此外，除了提高整體網路安全性外，網路管理者也無須時時刻刻的關注網路狀態，進而可以減輕企業營運負擔和成本。

透過與應用程式協作實現企業 SDN

SDN 是一項突破性技術，透過軟體集中控管網路設備，可以更靈活、動態地更改網路設定與配置，有助於改進資料中心的設計和營運。然而，若只是將資料中心的 SDN 直接應用於企業網路是不會產生足夠的安全性效果。因此，Allied Telesis 開發出 AMF-SEC 用來作為優化企業網路營運安全的解決方案。

AMF-SEC 四大優點

大幅強化網路安全

- 與資安應用程式連結，控制網路存取
- 防止資安事件的擴散
- 支援多樣的應用程式，如：端點安全、IT 資產管理和人力資源管理等

大幅降低資安措施的營運負擔及營運成本

- 檢測受感染的終端或可疑行為，並自動將可疑終端與網路進行隔離
- 透過自動控制關閉可疑終端電源或中斷網路連接，減輕管理人員的工作負擔和營運成本

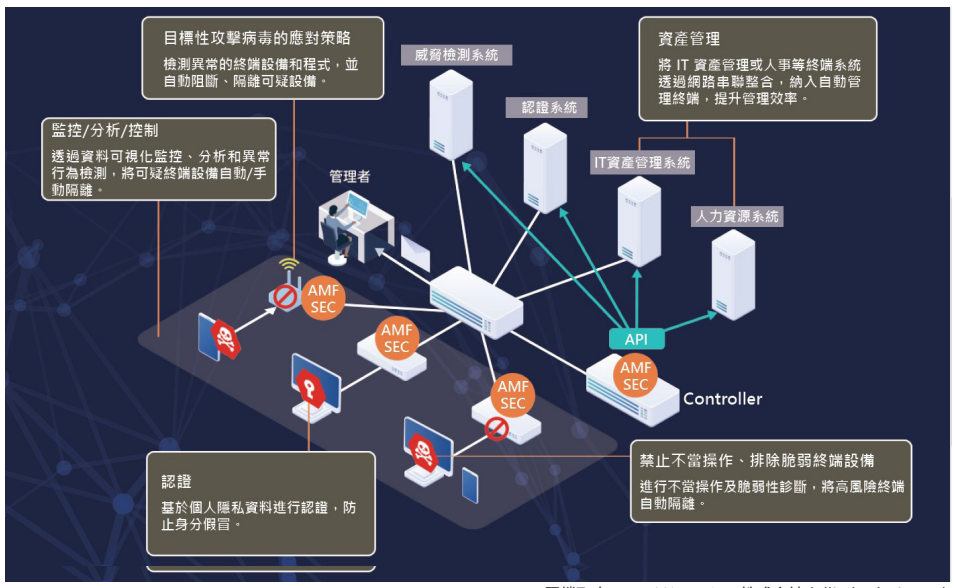
易於事件發生的調查和系統恢復

- 因為是利用自動控制進行網路隔離，進而大幅縮短調查事件原因的時間
- 調查結束並消除感染原因後，只需一個動作即可將被隔離的終端恢復到原有的網路狀態

多樣化的使用方式

- 透過多種方式控制使用者流量，且應用於各種使用場景
- 初期導入成本低，僅部署支援 AMF-SEC 功能的終端交換器即可達到自動化

Allied Telesis 自 2014 年起就有與各家應用程式廠商 (例如 : 趨勢科技資訊安全系統公司、人力資源雲端服務 Lacras 公司，以及 IT 資產管理系統 QualitySoft 公司) 等企業合作，提供提升網路營運管理效率和加強資訊安全的解決方案。
此外，Allied Telesis 還致力於辦公室節能解決方案、大樓自動化解決方案以及與這些解決方案之安全性相關聯的次世代網路解決方案，未來會持續推進各種應用程式的合作，擴大與更多合作夥伴結合的聯盟。



圖檔取自 アライドテレシス株式会社 (Allied Telesis K.K.)

AMF-SEC 與其他產品的搭配

TREND MICRO · paloalto · FORTINET · Barracuda · Sky株式会社 · MOTEX · QualitySoft · D-Link · HITACHI Inspire the Next · DDS · Lacrasia · WatchGuard · SOPHOS · SONICWALL · FFRI · FireEye · SECURITY MATTERS · Zingbox · Soliton · STG-i · ORIZON · 秀 · DigitalArts · CORE SECURITY · RAD · Doktor · IMPERVA · lastline · i3Solution

AMF-SEC × Deep Discovery Inspector 之新解決方案

這是一套 Allied Telesis SDN/AMF-SEC 結合 Trend Micro 的目標式 Cyber 攻擊對策產品「Deep Discovery Inspector」的解決方案，其主要目的在於針對可能感染惡意軟體 / 勒索軟體，或受到網路攻擊之可疑終端設備，透過終端交換器實施連線中斷 / 端點動態隔離等方式，以防止資料外洩、受害擴散。
在 Deep Discovery Inspector 的威脅偵測功能當中，AMF-SEC 結合以下的偵測功能，並利用終端交換器所檢測到的有受到網路攻擊或感染病毒的終端設備，將其之間的網路連線中斷 / 隔離，以防止受害範圍的擴散。

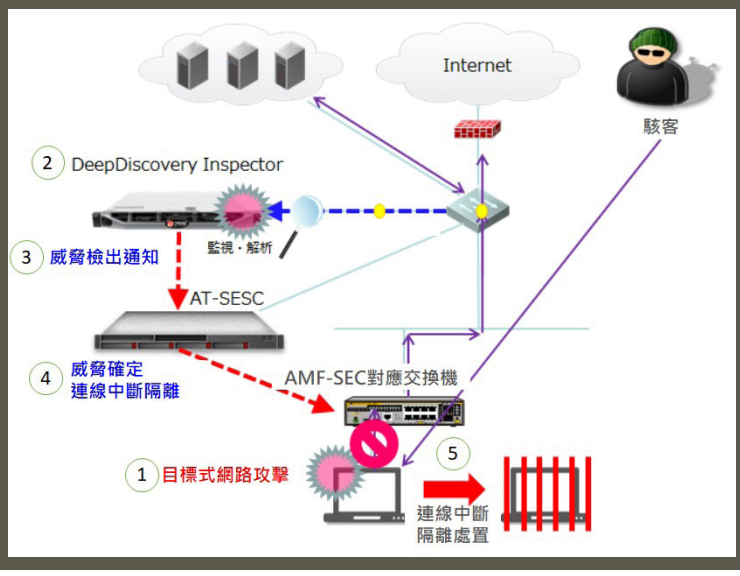
- 透過 WEB Reputation Service
- C&C 伺服器類別的連線的檢出
- 既知惡意軟體的檢出
- 在沙箱中確定為高風險之檔案的檢出

Allied Telesis AMF-SEC 與終端交換器四種聯防方式 :

- Drop Discard (L2 阻擋 MAC 方式)：針對可疑終端設備的連線，邊緣交換器經由 MAC 位址執行封包丟棄動作。
- Port invalidation (link-down) (網路埠關閉)：將可疑之終端設備與終端交換器連接之網路埠轉換成禁用狀態。
- IP filter Discards (L3 阻擋 IP 方式)：針對可疑之終端設備的 IP 位置進行封鎖。
- Quarantine (隔離) (VLAN 隔離)：將可疑之終端設備移送至其它 VLAN 網斷進行隔離。

模擬情境說明

① 終端主機受到目標式網路攻擊。
② Deep Discovery Inspector 即時監控 / 解析網路流量內容。
③ Deep Discovery Inspector 檢測到威脅，發出威脅檢出通知給 AT-SESC。
④ AT-SESC 確定是威脅後，發出防護指示給支援 AMF-SEC 功能的終端交換器。
⑤ 終端交換器依照指示對受到網路攻擊之終端設備進行連線中斷或端點隔離。

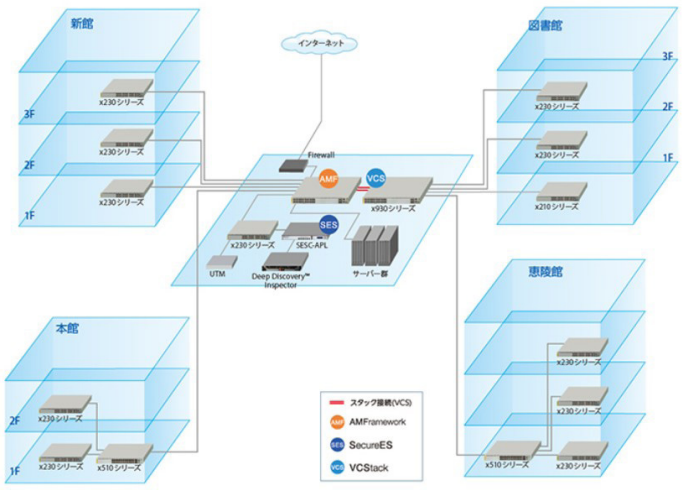


成功案例 - 日本名寄市立大學

原文取自 アライドテレシス株式会社 (Allied Telesis K.K.)

● 導入契機 - 為何要導入 AMF-SEC ？
新聞中充斥著目標式郵件攻擊與勒索軟體等各種威脅訊息，企業與組織都追求加強資訊安全。日本名寄市立大學雖然在傳統的網路中有採取了一定的資安措施，但從 2017 年開始，決定全面重新檢討資安政策並進行修補與加強。日本名寄市立大學專案負責人表示：「以往雖然已導入防火牆和病毒防護軟體，但此次不單只有硬體及軟體，連整體運用面都要重新檢視。」NTT 東日本對名寄市立大學提出了從設備、軟體、策略重新組織與運用等的各種提案，其中包括 Allied Telesis AMF-SEC 解決方案。
Allied Telesis AMF-SEC 可與各種應用程式搭配使用，提供在終端使用者上自動建立虛擬網路，以及行為檢測等安全強化功能的高效率化 OpenFlow/SDN 技術，又可以與趨勢科技的 Deep Discovery Inspector (以下簡稱 DDI) 聯動，針對 DDI 在網路上偵測到的目標式攻擊與 Zero-day 攻擊進行連線中斷與網路隔離。

● 客戶感想 – 感受到 AMF-SEC 的導入效果，日後也將持續採用
系統導入後，DDI 實際上都會檢測到威脅和可疑的行為，而 AMF-SEC 也會隨之中斷網路連線。當初為了加強資安而導入 DDI，利用 DDI 檢測出威脅並且發出告警通知，但如果管理者未注意到該訊息或延遲對應，則即使 DDI 檢測到威脅，等到真正處理時受害範圍可能已經都擴散開了。現在結合了 AMF-SEC，就算一時忽略了 DDI 所檢測的威脅訊息，也不會造成任何損害。AMF-SEC 會自動地中斷連線防止損害擴散，讓我們可以更放心地使用 DDI 進行偵測。



(網路示意圖)

威雲科技股份有限公司
台北總公司：114 台北市內湖區瑞光路 335 號 5 樓 / (02)7721-8168
台中分公司：403 台中市西區忠明南路 62 號 6 樓之 2 / (04)2328-5588

威雲科技製作