E-SOFT
曜 祥 網 技

SIP

Security Intelligence Portal

全方位資安智慧平台

零信任解決方案 ZTA

精準落實　資安治理

ZTA零信任資安框架

Security Intelligence Portal(SIP)全方位資安智慧平台

全面落實零信任防禦

全方位資安智慧平台(Security Intelligence Portal)簡稱 SIP，提供企業全方位自動化盤點、合規檢查及矯正機制，透過業界最完整的盤點技術將企業既有資安管理系統，以獨家的關聯式分析技術，提供全環境資訊資產的可視性，進一步達到風險透明化，結合企業流程並落實資安管理政策，提高資安治理成熟度。
透過SIP管理平台能夠極大化企業既有資安投資綜效，強化資訊基礎建設的防禦力。

產品特色

- 支援客戶各種不同需求之部署架構且不需更改既有網路架構
- Agentless及最小權限之設計
- 提供完整的網域設備之資安組態稽核
- 可針對用戶端進行資安合規檢查
- 多種存取控制合規檢查政策設定(Pre-Check & Re-Check)，並提供自動化矯正程序
- 平台內建資通安全法稽核所需之報表
- SIP以法規為根基，企業全網資安為核心，進而整合外部網路資安聯合防禦，可以做到事前的預防、事中的因應及事後的處理

零信任架構之設備存取控制流程

Security Intelligence Portal (SIP)
全方位資安智慧平台

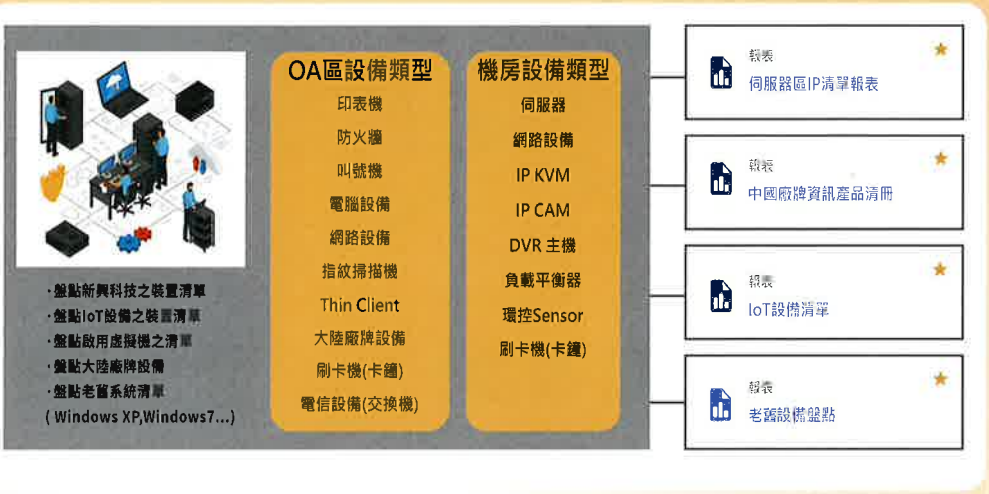
Dr. IP IP 資源管理系統

#Zero Trust Architecture

連網設備全面盤點及自動化管理

Dr. IP IP資源管理系統提供業界最完整的 IP 生命週期控管流程，採用旁路式及 Agentless的架構，無需改變企業既有的網路架構即可自動偵測環境中所有的連網裝置，透過多種的識別技術有效掌握設備類型(Windows、Linux、Switch、IoT Device、中國製設備等)，並使用專利的阻斷機制來建構一套完整的零信任網路存取控制流程。提供多種 IP/MAC 管理政策，系統有效的提供資安法規要求之所需，相關應用場景如下:

1.伺服器區IP資產登錄管理
2.全公司設備盤點登錄管理
(PC、NB、IoT)
3. 私接設備控管
4. IP有效性控管
5. 設備未關機控管



Smart AD組態盤點管理系統

#Privileged Management

1 Smart AD 本機組態盤點管理模組

強化企業Windows平台之管理，透過Agentless及最小權限的方式進行Windows網域相關資料收集，有效的掌握Windows設備網域的部署率及設備使用人員帳號進而達到設備實名化管理之目的，針對Windows設備能有效的收集每台本機的資安稽核相關項目之資料，簡化管理者作業，相關的應用場景如下:

1.Windows設備網域符規檢查
2.AD帳號登出入稽核軌跡(如本機Local Admin之軌跡查核)
3.Windows設備本機資安查核
- 本機人員帳號盤點
- 本機最高權限成員盤點
- 分享資料夾啟用及權限盤點
- SID重複稽核
- GPO套用檢查

4.本機組態異動告警
- 本機提權告警

2 Smart AD 網域組態盤點管理模組

提供企業因應整體資安治理成熟度提升之需求，有效的掌握網域控制站重要物件異動，並提供管理者因應法規下之資安查核所需，相關的應用場景如下:

1.網域帳號及權限群組盤點查核
2.網域帳號生命週期管理查核
3.網域帳號異動查核
4.網域帳號提權告警
5.網域群組原則異動告警

政府機關資安弱點通報機制VANS資訊資產系統 for Windows、Linux

#Risk Assessment Visibility

企業內網軟體風險評鑑系統提供完整的軟體漏洞盤點及管理機制，能夠針對Windows、Linux 及 macOS進行軟體資產盤點，進一步整合外部CVE情資資料庫，進行軟體資產CPE格式正規化及CVE漏洞比對，可依據不同角度(設備、軟體、CVE)有效的快速掌握企業軟體資產之CVE漏洞，並可針對Windows的軟體資產進行相關的升級矯正，相關的應用場景如下:

1.政府機關因應法規VANS 系統軟體資產上傳
2.軟體漏洞通報快速之因應
3.自建軟體漏洞通報機制(VANS)
4.軟體升級矯正

GCB/FCB進階稽核管理(政府組態)

#GCB

GCB進階管理系統提供企業能夠依據國家資通安全研究院或F-ISAC公告之GCB及FCB範本，有效的查核其套用的完整性及有效性，GCB查核範本至少包含Windows、Linux、Office瀏覽器及網通設備(防火牆...)等，系統採用群組化的設計方式，建立相關的設備群組及需檢查的GCB/FCB項目，簡化管理者查核作業，提高GCB/FCB套用之完整性，相關應用場景如下:

1.政府機關GCB套用完整性查核
2.金融機構FCB套用完整性查核

NAC++ 內網資安智慧部署管理系統

#Agentless

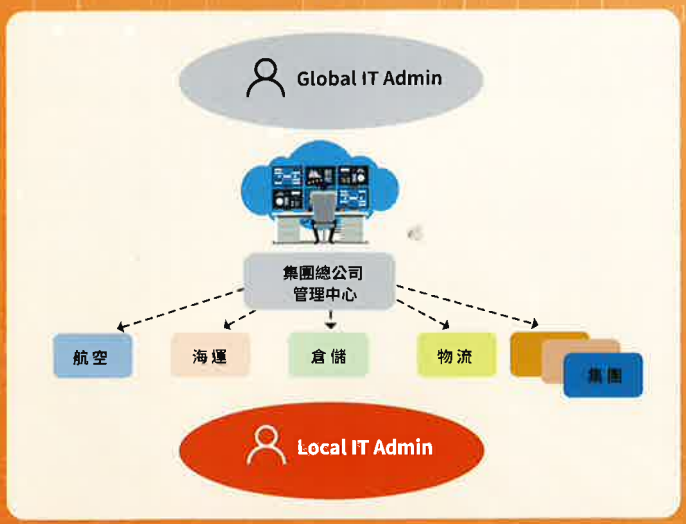
NAC++系統基於IP資源管理系統之機制，能夠整合至少40種以上的資安管理系統，包含防毒軟體、DLP軟體、資產管理軟體、EDR軟體...等，協助企業建立資安管理政策之完整性及有效性的檢查覆核機制，透過Dr.IP獨家的封鎖技術進一步建立Pre-Check及Re-Check管理流程，提高企業資安治理成熟度，相關應用場景如下:

1.提供企業資安管理KPI指標檢核
2.建立設備進機健康檢查流程
3.零信任網路下之設備健康檢查(信任推斷)
4.重要嚴重事件告警
5.部署完整性：全面監控企業內部電腦是否都依公司規範安裝Agent，透過NAC++協同防禦管理，讓資安防護更完善

6.部署有效性：管理者能輕鬆掌握資安軟體部署率與政策執行落實度，大量節省管理人員檢核的時間
7.自動化矯正方案：橫向整合矯正機制，整合資產軟體達成自動派發機制

內外網資訊安全聯防系統

1.可與各大品牌之SIEM資安事件管理產品進行整合而做到內外聯防，將SIEM系統具備資安事件與記錄整合管理功能，提升為具備主動防禦能力的資安管理平台
2.可與多種品牌之防火牆、IPS、防毒牆之產品進行整合而達到動態防禦的系統協防運作模式，降低管理員單台設定之負擔
3.對於IT部門在人力資源與資安管理知識均有限，又需面對日益升高的資安攻擊事件的壓力下，SIP所具備操作簡易、快速佈署、擴充性強、內建全方位的報表與內網稽核軌跡，協助輕鬆因應主管機關檢核，將資安防護從網路可視度出發，與現有IT系統及維運全方位整合，提升整體資安治理的成熟度



SIP中控平台

SIP中控平台可以整合企業內部多台SIP伺服器，提供三層式的架構，總部可透過單一Console統一掌握全球各區之資安管理政策的完整性及有效性，如防毒部署率、Hotfix派送率...等，即時掌握各區之健康狀態

資安防護戰略已從資安設施部署
走向採取零信任協同作戰防護
Security Intelligence Portal(SIP)

各自獨立的資安系統
透過SIP串聯設備資訊
資產全面掌握

各資安系統之關鍵
管理資訊做關聯及
交叉分析自動矯正

管理者能
輕鬆的掌握做
最有效的行動

導入 SIP 的效益:

- 協助企業改善內網的設備可視性
- 協助企業落實各項端點資安軟體部署率
- 快速定位發生資安事件設備之所在，有效縮短資安事件反應時間
- 協助企業將資訊安全風險評估由被動反應轉化為主動預防
- 事先掌握高風險設備挖掘企業資安管理安全點讓企業即早因應防禦
- 零信任資安框架支援整合

E-SOFT 曜祥網技

客服專線: 0800-333-077
e-mail: sales@e-soft.com.tw
http://www.e-soft.com.tw