Hybrid Cloud

主機防護偵測

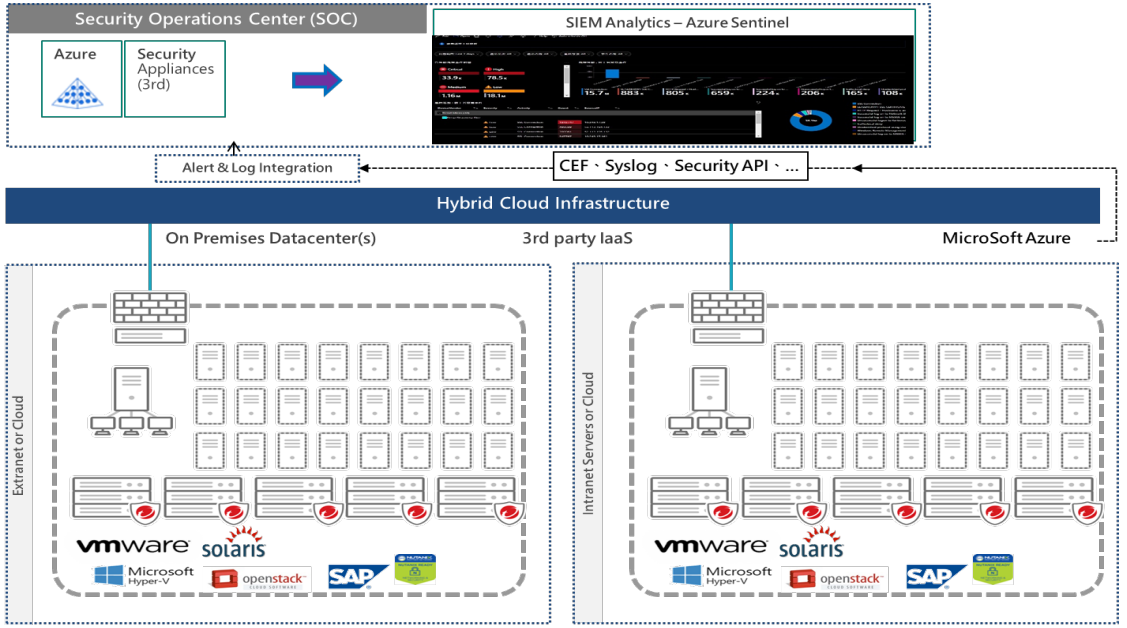
Hybrid Cloud 主機防護偵測

情境說明

- 藉由單一代理程式和平台來部署並整合實體、虛擬、多重雲端環境的資安防護。
- 能保護虛擬桌面和伺服器，防範零時差惡意程式，包括：勒索病毒、虛擬加密貨幣挖礦攻擊以及網路攻擊，並且盡可能減少資源利用效率不佳或緊急修補所帶來的營運衝擊。
- 利用 IPS 所提供的虛擬修補來保護已終止支援的系統，確保老舊系統的安全，防範目前及未來的威脅。

使用產品 TrendMicro Deep Security + Azure Sentinel

情境架構



效益

- 提供進階的資安控管來保護您的關鍵伺服器與應用程式，例如：入侵防護 **(IPS)**、一致性監控、機器學習、應用程式控管等等。短時間內部署與拓展
- 即時偵測及攔截威脅，卻不影響效能。

防禦模組介紹

單一代理
多重防護

Known
已知威脅

1 Anti-Malware

即時偵測、阻擋惡意程式
(網頁威脅、病毒、蠕蟲、木馬)

Web Reputation

2 Firewall

降低攻擊表面，防止 DoS 攻擊 、網路探測掃描

偵測或阻擋已知攻擊、應用程式漏洞

Intrusion Prevention

網頁應用程式防護

應用程式網路連線控制

Unknown
未知威脅

3 Integrity Monitoring

監控目錄、系統、檔案、應用程式、機碼值變更

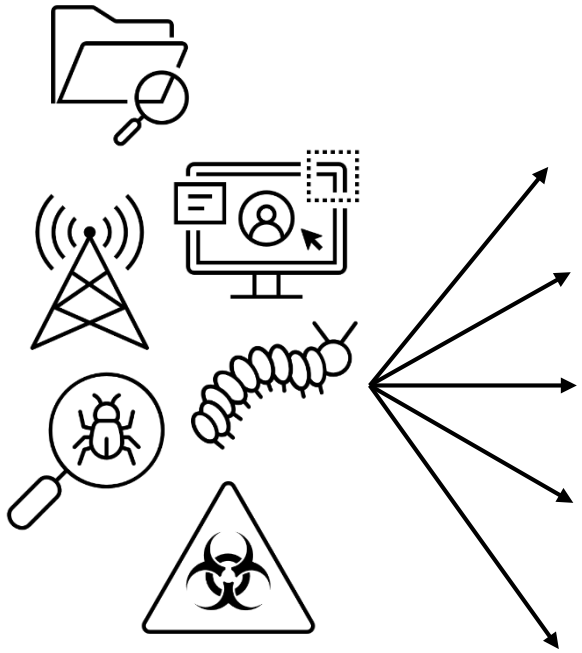
Application Control

防止未經授權之應用程式或可執行檔運行

4 Log Inspection

收集日誌紀錄並從中辨識安全事件

多層式伺服器防護架構



網路層級安全

- 未知的連線與橫向移動
- 系統、應用程式弱點攻擊
- 主機漏洞掃描與探測

系統層級安全

- 可疑的應用程式或可執行檔
- 系統重要參數的設定與變更
- 應用程式與系統事件紀錄收集

惡意程式防護

- 即時監控與防禦
- 防止惡意程式執行與擴散
- 病毒碼與規則更新
- 可疑物件分析

主機式防火牆
主機式入侵防護

惡意程式防護
網頁信譽評等

防禦模組一覽

Firewall | 防火牆
- 主機式雙向防火牆
- 網路偵查掃描 (Reconnaissance)
- 阻擋DoS攻擊、未經授權連線

Web Reputation | 網頁信譽評等
- tap/inline mode
- Smart Protection Network

Application Control | 應用程式控制
- 白名單
- 自動建立應用程式清單
- 支援維護模式

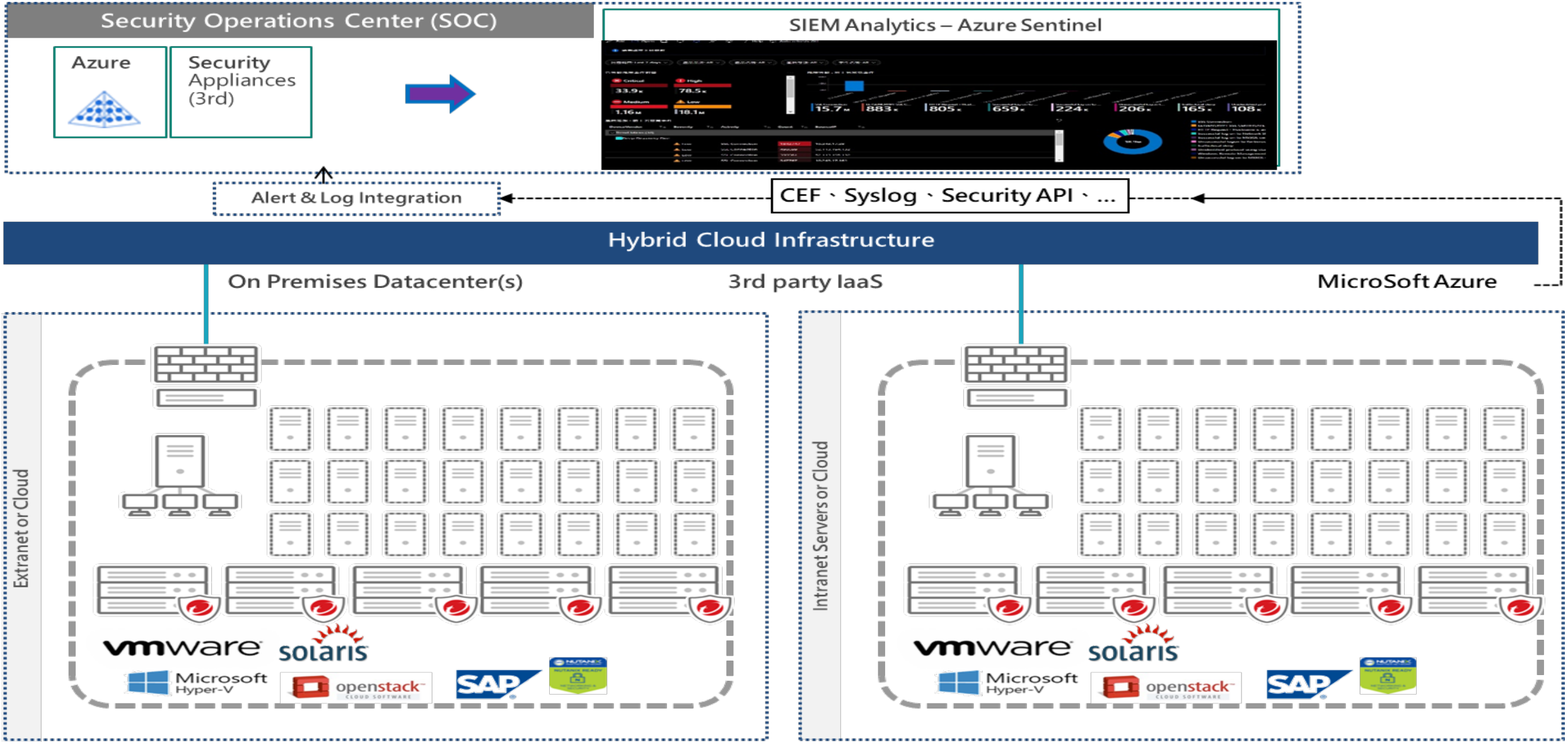
Intrusion Prevention | 入侵防護 (IPS)
- tap/inline mode
- 過濾封包、檢查出入流量
- 偵測、攔阻弱點攻擊
- 虛擬補丁技術 (Virtual Patch)

Anti-Malware | 惡意程式防護
- 病毒、木馬、間諜、惡意程式
- 支援零代理模式 (Agentless)
- 雲端大數據資料庫 (Smart Protection Network)
- 預判式機器學習引擎

Integrity Monitoring | 完整性監控
- 偵測異常事件、可疑活動
- 系統檔案、服務、機碼監控
- 可自訂監控範圍
- 自我建議評估掃描 (Recommendation)

Log Inspection | 安全日誌管理
- 收集、分析作業系統和應用程式日誌
- 可疑行為、帳號偵測
- 收集主機事件資訊
- 支援事件紀錄轉送

情境架構


Security Operations Center (SOC)
Azure
Security Appliances (3rd)
SIEM Analytics – Azure Sentinel
Alert & Log Integration
CEF、Syslog、Security API、...
Hybrid Cloud Infrastructure
On Premises Datacenter(s)
3rd party IaaS
MicroSoft Azure
Extranet or Cloud
Intranet Servers or Cloud
vmware
solaris
Microsoft Hyper-V
openstack
SAP


The Best
is Yet to Come !