產品規格文件

# Contoso CipherGuard Sentinel X7

# 1. 產品概觀

## 1.1 簡介

Contoso CipherGuard Sentinel X7 是一款先進且具高彈性的安全性產品，經過精心設計，可強化電腦網路基礎架構，以抵禦各種威脅和弱點。本文件詳細說明 Contoso CipherGuard Sentinel X7 的技術規格、特色與功能。

## 1.2 主要特色

* **防火牆保護：** Contoso CipherGuard Sentinel X7 使用具狀態檢視防火牆，並採用深度封包檢測技術。其可在應用程式層檢查並分析網路封包，提供對資料流的精細控制。此防火牆會根據持續變化的網路情境動態調整其規則集，以降低與應用程式層攻擊相關的風險。
* **入侵偵測與防禦系統 (IDPS)：** 我們的 IDPS 由機器學習演算法驅動，可持續監控網路流量模式與異常情況。其運用簽章式偵測、異常偵測和啟發式分析，以識別並阻止潛在威脅。此系統採用威脅情報饋送機制，確保能持續更新以應對最新的已知攻擊模式。
* **虛擬私有網路 (VPN) 支援：** Contoso CipherGuard Sentinel X7 支援業界標準的 VPN 通訊協定 (例如 IPsec 和 OpenVPN)。其透過加密傳輸中的資料，來促進公用網路上安全通訊的實現。此 VPN 模組採用進階加密演算法 (包括 AES-256)，可為遠端使用者和分支機構確保強固且安全的通訊通道。
* **端點安全防護：** 我們的端點安全模組採用多層式防禦方法，整合了防毒、反惡意軟體及主機型入侵防禦功能。其可執行即時行為分析與啟發式掃描，確保能主動偵測並抑制惡意活動。此外，其亦與威脅情報平台整合，以便迅速回應新興威脅。
* **記錄與監控：** 記錄與監控子系統會擷取關於網路活動的全面資料。其包含流量模式、使用者驗證事件及安全政策違規的詳細記錄。此功能與 SIEM (安全性資訊與事件管理) 整合，有助於集中監控及分析，讓安全管理員能夠迅速回應潛在的安全事件。
* **使用者驗證與存取控制**：Contoso CipherGuard Sentinel X7 支援多重要素驗證 (MFA) 機制，包括生物辨識驗證及智慧卡整合。存取控制原則是以使用者角色為基礎，並運用 LDAP 及 Active Directory 整合。動態原則強制執行可確保僅有經授權的使用者能存取敏感資源。

# 2. 技術規格

## 2.1 硬體需求

* **處理器：** 四核心 2.5 GHz 或更高時脈，支援硬體加速功能
* **RAM：** 最低 16 GB，建議使用 ECC (錯誤校正碼)
* **記憶體：** 最低 200 GB，建議使用 SSD 以獲得最佳效能
* **網路介面卡 （NIC）：** 雙連接埠 Gigabit 乙太網路，支援巨型訊框

## 2.2 軟體需求

* **作業系統：** 相容於 Windows Server 2019 及更新版本、CentOS 8 或同等版本
* **資料庫：** PostgreSQL 13 (用於資料儲存)，已針對高效能索引進行最佳化
* **安全性更新：** 自動更新威脅情報饋送及定期安全性修補程式

## 2.3 網路相容性

* **通訊協定：** 支援 TCP/IP、UDP、ICMP、IPv6
* **整合：** 與 BGP 及 OSPF 路由通訊協定無縫整合
* **相容性：** 可與 Cisco、Juniper 及其他主要網路廠商的設備互通運作

# 3. 實作計劃

## 3.1 部署步驟

1. **部署前評估：** 執行全面的網路弱點評估，包括滲透測試與風險分析。
2. **安裝：** 將 Contoso CipherGuard Sentinel X7 部署於專用伺服器或虛擬機器上，確保最佳的硬體使用率與資源分配。
3. **設定：** 根據組織需求自訂安全政策、存取控制及防火牆規則。微調入侵偵測參數，以達到最高的準確度。
4. **測試：** 執行完整的測試計畫，包括模擬攻擊情境與負載測試，以驗證解決方案的有效性及效能。
5. **訓練：** 為 IT 人員提供深入的訓練課程，內容涵蓋日常維運、事件應變程序及維護工作。

## 3.2 維護與支援

* **定期更新：** Contoso 保證產品的持續更新，其中包含最新的威脅情報與安全強化功能。
* **技術支援：** Contoso 提供專屬的全年無休 (24/7) 支援團隊，確保針對任何與 Contoso CipherGuard Sentinel X7 相關的技術問題或洽詢，均能提供迅速的協助。