corero [NETWORK SECURITY]

SMARTWALL ONE™

產品規格表_

突破平凡，盡在 SmartWall ONE

SmartWall ONE 以高度延展性為核心設計，系統全自動化，操作簡單直覺，讓你輕鬆自信地防禦最猛烈的 DDoS 攻擊。它不只是防禦工具，更是為你的企業量身打造的堅固堡壘，全面守護網路安全與穩定企業的營運。

多地備援能力

DDoS 防護，應該與你的網路一樣堅韌可靠。SmartWall ONE 提供具備彈性調整能力的多站點韌性防禦，可在各地即時執行防禦策略。即使發生光纖中斷、斷電，甚至整個站點故障，無需人工重新設定或延遲反應，防禦機制依然不中斷。

具前瞻性的擴充與靈活性

想像你的資安防護就像堆積木一樣靈活。透過我們的模組化設備，你可以依照業務需求彈性擴充，不論是吞吐量的授權，或實體 400GE/100GE 模組都可隨你的需求靈活配置。擴充不代表重來，而是讓你的防禦能力隨著業務一起成長。

高解析度流量的可視性

深入駭客思維，掌握攻擊及網路的全貌。我們領先業界的分析能力，讓你深入剖析攻擊模式。不單單只是數據，而是可行的資訊，協助你精準強化防禦策略。

全方位防護

我們將全面守護你的網路，抵禦各類威脅，包括大流量攻擊、連線耗盡（state exhaustion）、高速短時攻擊、IoT 殭屍網路、地毯式攻擊（carpet bombing）、間歇性、有節奏的流量攻擊戰術（Pulsing tactics），以及 DNS Flood 攻擊。除此之外，我們先進的混合雲防禦架構，能抵擋最嚴峻的攻擊，確保你的網路不僅安全無虞，更能持續穩定運作，毫無中斷。

DDoS 專用防禦裝置

SmartWall ONE，讓你始終領先威脅一步

每年，DDoS 攻擊都變得更狡猾、更複雜。他們不僅規模越來越大，手法也更陰險，同時持續變換策略、鎖定各式各樣的通訊協定發動攻擊。這些攻擊通常來得快、退得也快，但該攻擊卻讓「現有的DDoS即時偵測與立即防禦設備」壓力倍增。那麼，你的應對之道是什麼？你需要的不只是功能強大的防護，而是一套能隨時保持警覺、立即應變的 DDoS 防禦系統。

這就是為什麼你的網路及安全需要配備 SmartWall ONE。

SmartWall ONE 是一套快速、極致靈敏且全自動化的 DDoS 防禦解決方案，提供實體設備與虛擬機版本，滿足不同部署的需求。其彈性化、軟體導向的架構設計，能無縫整合至你的現有網路與基礎設施中。不論你的網路架構如何轉變，SmartWall ONE 都能為你帶來高度防護的安心體驗，讓你專注於核心業務發展，無須擔心服務中斷的風險。

強大擴充能力，助你從容應變

我們的 SmartWall ONE解決方案採用speed-agnostic架構設計，該架構支援各種速率，且不受限於單一設備的固定吞吐量授權，可隨企業成長而靈活擴充，真正實現彈性擴展。

令人振奮的是，我們推出全新一代 400G Network Threat Defense（NTD）防禦設備，大幅提升整體效能與部署彈性。這些先進設備支援 SmartWall ONE 在本地部署，不論是實體硬體設備或虛擬化軟體形式，都能完美整合至現有網路架構中，與高速網路發展無縫接軌。 這代表不只是滿足頻寬需求，而是以無與倫比的敏捷性，超越當前與未來的流量挑戰。

支援軟體與虛擬環境部署

適合雲端或資料中心環境，DDoS 防護可透過軟體形式部署於虛擬機或雲端實例中，提供具高度延展性與彈性的防禦解決方案。

這種部署方式不僅可快速導入、輕鬆擴充，同時可有效降低營運成本，免去專用硬體設備的需求，節省機櫃空間並降低能源消耗。更重要的是，它能因應保護需求的變化快速調整，無須修改實體基礎架構，是希望提升資源使用效率，同時維持高防護水準的企業最佳選擇。

削減開銷，防護不打折

自動化防禦讓你不再為 DDoS 頭痛費神，省時又省錢。SmartWall ONE 的防護效能穩定流暢，讓你不禁懷疑：過去怎麼會容忍比這更差的解決方案？

輕鬆部署，持續守護

DDoS 攻擊交給我們自動處理，無需你動手干預，網路依然穩定暢通、不中斷。

支援 On-Prem 與 Hybrid 架構

強化你的純雲端防護架構，結合我們高精準、即時反應的本地部署防護能力。混合式防護無縫整合，無感部署，效能依然強勁，讓你幾乎感受不到它的存在但始終在線，持續守護。

靈活對應各種使用情境

無論採用哪種部署模式，SmartWall ONE 都能靈活配合你的環境。不論是實體、虛擬、主動線上防護（Inline）或部署於側線監控，我們都能全面守護，在攻擊造成任何損害之前即時攔截，將風險降到最低。

強化服務，同步提升營收表現

如果你是服務提供商，SmartWall ONE 將是你提供高階即時 DDoS 防護服務的黃金利器。不僅能強化你的營收來源，還能有效保障客戶的營運不中斷及不影響正常流量。

穩定無縫的服務連續性

自動化在各分散式據點執行 DDoS 緩解防禦，無延遲、無需重新設定，且沒有單點故障風險。

你的 DDoS 中控中心，狀況全都掌握

SmartWall ONE 的 SecureWatch Analytics 就是你面對 DDoS 攻擊時的全方位監控之眼。它不只是監控儀表板，更能從混亂中理出頭緒，精準指出你該如何應對，用最簡單明瞭的方式讓你重要資訊一目了然，不用再辛苦過濾雜訊。

全時監看不中斷

資訊可透過即時或歷史圖表與儀表板呈現，讓你全面掌握流量與攻擊趨勢。

精準調校防護策略

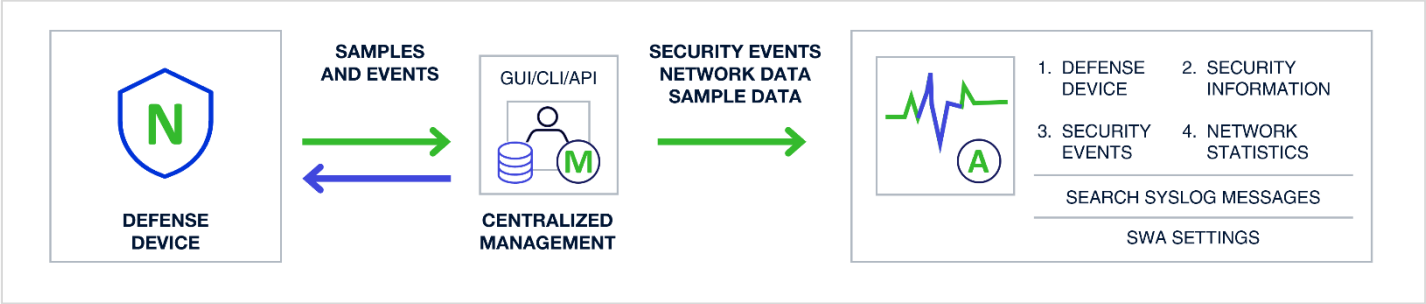
轉化數據為行動依據，全面提升資安策略效能。

深入剖析攻擊模式

深入鑽研攻擊期間的詳細流量資訊，掌握被封鎖與允許的流量細節。

升級版威脅情資分析

所有事件都會被安全儲存與索引，並可透過 API 與 syslog 提供給其他資安工具進行外部分析，強化整體整合的能力與事件的可視性。



N Corero Network Defense Device | **M** Provider Service Management | **W** DDoS Traffic Analysis

設備安全防護範圍

靈活的資安防護功能

- 可防禦針對單一或多個 IP 與子網段的攻擊
- Smart-Rules：專利的高效能啟發式引擎，可自動偵測並封鎖大流量 DDoS 攻擊，包含零時差（zero-day）威脅
- Flex-Rules：可客制化過濾規則，採用 Berkeley Packet Filter（BPF）語法，並加入 Corero 強化功能
  -應對各類型大流量攻擊向量，從反射型（Reflective）攻擊到特定應用負載（如 TeamSpeak、RIPv1、NetBIOS
- DDoS Intelligence 主動式防禦情報饋送
- 殭屍網路與來源泛洪（source flood）偵測與封鎖機制
- 智慧型自動封鎖異常封包片段（fragment）
- 基於 TCP/UDP 埠號的精準防護
- 支援頻率限制（Rate Limiting）策略設定
- 支援雲端緩解及 BGP RTBH / FlowSpec 訊號回傳整合

資源耗盡型攻擊（Resource Exhaustion）

- 異常格式與截斷封包（例如：UDP 炸彈攻擊 / UDP bombs）
- IP 封包分段／重組規避技術（AETs）
- 無效的 TCP 封包段識別碼（Segment ID）
- TCP/UDP 封框中的錯誤檢查碼與非法旗標（Flags）
- 無效的 TCP / UDP 埠號
- 針對 DNS 基礎架構的 NXDOMAIN water torture

頻寬及資源耗盡型 DDoS 攻擊

- TCP flood（TCP 洪水攻擊）
- UDP flood（UDP 洪水攻擊）
- UDP fragmentation（UDP 封包碎片攻擊）
- SYN flood（SYN 洪水攻擊
- ICMP floods（ICMP 洪水攻擊）
- Carpet bombing（地毯式攻擊）

反射放大式 DDoS 攻擊（Reflective Amplification DDoS）

- NTP monlist 回應放大攻擊
- DNS query 查詢放大攻擊
- 無連線式 LDAP（CLDAP）反射攻擊
- SSDP/UPnP 回應放大攻擊
- SNMP 封包反射攻擊
- CHARGEN 回應放大攻擊