SonicWall Analytics

SonicWall Analytics 將防火牆流量資料轉換為跨使用者、應用程式和網路的可操作洞察，從而幫助以更高的精度和速度降低安全風險——所有這些都通過一個介面。該分析引擎使用高性能雲原生架構構建，可跨數千個防火牆節點大規模豐富大量原始資料，通過執行儀錶板為利益相關者提供完整的可見性和安全透明度。

Analytics 通過使用各種形式的語義圖、時間使用圖表和表格來創建資料模型的知識表示，以幫助減少停留時間並減輕分析師的疲勞。通過增加的向下鑽取功能，安全回應者可以調查關鍵資料點並將其歸零，以暴露隱藏的風險從而進行早期干預，並針對在發現過程中展開的風險用戶活動採取有證據支持的策略行動。

憑藉全面的可視性和控制，安全分析師可以隨時隨地洞察一切，從而成為更好的風險管理者，而回應者可以將寶貴的時間和精力集中在最重要的應用程式和使用者協調快速回應行動上，而不是對每個事件都做出反應。Analytics 以雲敏捷性和雲彈性擴展和執行，從而滿足最苛刻的企業需求。

特點

企業業務

- 獲得完全安全透明度
- 獲取安全態勢的即時快照
- 履行內部合規義務
- 進行準確的網路防禦規劃和預算
- 降低資本支出和運營支出

業務運營

- 一目了然輕鬆瞭解安全指標
- 從每個網路事件、使用者事件和警報中激發洞察
- 制定準確的防禦策略行動
- 以雲敏捷性和雲彈性擴展和執行

安全

- 發現隱藏風險
- 啟用早期干預
- 及時響應不安全的用戶活動
- 幫助分析師成為更好的風險管理者
- 將回應者變成更好的問題解決者

深入瞭解 SonicWall Analytics

www.sonicwall.com/analytics

DATASHEET

隨時隨地洞察一切

Analytics 使您可以全面瞭解租戶、組或設備級別的整個 SonicWall 安全環境。執行儀錶板對通過防火牆生態系統的所有網路流量和資料通信提供靜態和接近即時的分析。所有日誌資料都會被記錄、匯總、情景化，並以有意義且易於使用的方式呈現，讓您能夠根據資料驅動的洞察發現、解讀、分類並採取適當的防禦回應。

Analytics 附帶廣泛的預定義報告，並且可以使用流量資料的任意組合靈活創建特定於您期望用途或意圖的自訂報告，並定期交付它們。它提供長達一年的流量分析、安全性漏洞和異常發現歷史記錄，以說明您跟蹤、衡量和運行安全第一的網路和安全運營中心。

圖 1.0 執行儀錶板

瞭解您的風險

向下鑽取和透視功能使您能夠自信地進一步檢查與入口/出口流量、應用程式使用、使用者和設備訪問、威脅行為等相關的特定模式和趨勢。通過混合使用端點、網路、使用者和應用程式報告和分析，您可以主動分析或響應警報、異常和風險用戶活動。憑藉完全安全透明度，您將獲得情境感知能力，以發現安全風險、協調策略活動、推動一致的安全強制實施並持續監控整個環境的結果。

使用 SaaS、虛擬或 IaaS 選項靈活部署

Analytics 為您提供靈活的部署選擇，完美適合您的運營需求。

為了獲得免維護體驗，Analytics 可作為 SonicWall 託管的 SaaS 產品提供，並可通過互聯網訪問。SaaS 選項為您提供無限彈性以按需擴展，同時可降低運營成本。已去除硬體和軟體採購、定制安裝、定期維護和升級、資產折舊和報廢成本的典型成本，取而代之的是低且可預測的年度訂閱成本。

為實現全面的系統控制和合規性，您可以將 Analytics 內部部署為安裝在您選擇的虛擬平台（例如 VMWare 和 Microsoft Hyper-V）上的軟體。您可以受益於虛擬化的所有運營和經濟效益，包括系統可擴展性、系統組態速度和成本降低。

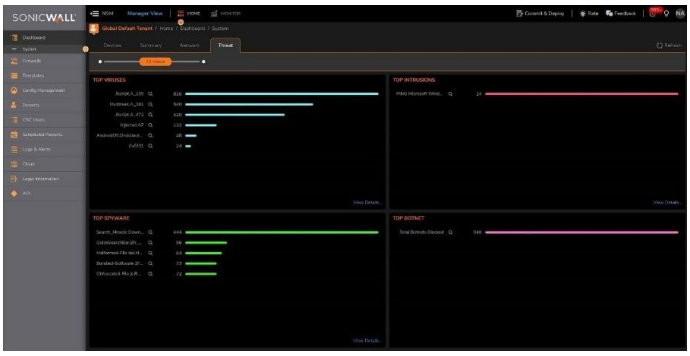

圖 2.0 威脅匯總

功能摘要

功能	描述
數據聚合	自動聚合與規範流經所有防火牆的安全資料。
數據情景化	處理和豐富防火牆資料，並以結構化、有意義且易於使用的方式呈現，使安全團隊、分析師和利益相關者能夠發現、解讀、確定優先順序、制定決策並採取適當的防禦措施。
流分析	網路安全資料流程被連續處理並即時載入，結果顯示在動態的互動式可視儀錶板中。
用戶分析	通過執行儀錶板顯示員工 Web 應用程式和網路使用的綜合視圖。它讓您可以細微性向下鑽取歷史記錄，以針對有風險的用戶 Web 活動建立有證據支持的策略控制措施。
應用程式流量分析	為組織提供對應用程式流量、頻寬利用率和安全威脅的強大洞察力，同時提供強大的故障排除和取證功能。
安全分析	通過快速威脅檢測獲得即時可見性。使安全分析師和事件回應者能夠尋找、識別和調查問題。
即時動態視覺化	通過單一管理平台，安全分析師可以更精確、更快速地對安全資料進行深入的調查和取證分析。
快速檢測和補救	追查不安全活動並通過採取準確行動迅速管理和補救風險的調查能力。
生產力報告 （需要在第 6/6.5 代防火牆上啟用 AGSS/CGSS 許可證，在第 7 代防火牆上啟用基本保護許可證）	提供對組織網路資源利用率的洞察。它可以生成強大的快照以及針對用戶上網行為的深入報告。這些報告收集有關網站位址和訪問使用者訪問日期的資料，並計算使用者在每個網站上花費的時間以及在這些網站上花費的時間是在辦公時間還是非辦公時間。生產力報告將用戶的 Web 活動分為生產力組，例如高效組、低效組、可接受組、不可接受組或自訂群組，以說明組織更好地瞭解網路使用模式並優化員工生產力。 例如，通過瞭解用戶在非業務相關網站上花費的時間，人力資源部門的領導可以管理和應對潛在員工違反行為準則政策的行為。類似用例可以應用於所有其他功能組。
VPN 報告	總結 VPN 隧道中使用了哪些公司資源、它們消耗了多少頻寬以及該流量的使用者是誰（即用戶名和 IP 地址）。網路系統管理員可以利用這些資訊來監控關鍵業務應用程式、控制或整形流量以及規劃容量增長。

功能	描述
流量分析和報告	通過 IPFIX 或 NetFlow 協定為應用程式流量分析和使用資料提供流量報告代理，以進行即時和歷史監控。為管理員提供有效且高效的介面以即時直觀監控其網路，從而能夠識別具有高頻寬需求的應用程式和網站、查看每個使用者的應用程式使用情況以及預測網路遭受的攻擊和威脅。 • 具有一鍵過濾功能的即時報告介面 • 具有一鍵查看按鈕的熱門流量儀錶板 • 具有附加流量屬性選項卡的流量報告介面 • 具有強大關聯和透視功能的流量分析介面 • 用於深入鑽取單個會話和資料包的會話檢視器
綜合圖形報告	提供對防火牆威脅、頻寬使用情況、員工生產力、可疑網路活動和應用程式流量分析的可見性。
Syslog 報告	簡化資料匯總，允許近乎即時地報告傳入的 Syslog 消息。直接訪問底層原始資料進一步促進了廣泛的細細微性功能和高度可定制的報告。
計畫報告	為所有計劃報告提供單一入口點。一份報告可以組合多個單位的圖表和表格。可以計畫報告並以各種格式發送給一位或多位分析師。
清晰報告	提供可自訂的視圖，以在單個頁面上演示多個匯總報告。使用者可以輕鬆流覽重要網路指標，以便快速分析各種報告中的資料。
多威脅報告	收集有關攻擊的資訊，使用 SonicWall Capture ATP、網關防病毒、反間諜軟體、入侵防禦和應用程式智慧與控制安全服務提供對 SonicWall 防火牆所檢測到的威脅活動的即時訪問。
新攻擊情報	報告特定類型的攻擊、入侵企圖和攻擊源位址，使管理員能夠快速回應持續威脅。
惡意無線接入點報告	顯示所有正在使用的無線設備，以及來自主機之間點對點或對等網路的惡意行為以及使用者連接到相鄰惡意網路的意外關聯。
Capture ATP 報告	提供一目了然的威脅分析儀錶板和報告，其中詳細說明了發送到服務的檔的分析結果，包括源、目標和摘要以及引爆後惡意軟體操作的詳細資訊。
僵屍網路報告	包括四種報告類型：企圖、目標、發起者和包含攻擊向量上下文的時間線，例如僵屍網路 ID、IP 地址、國家/地區、主機、埠、介面、發起者/目標、源/目標和使用者。
Geo IP 報告	包含基於流量來源或目標國家/地區的被阻流量的資訊。包括四種報告類型：企圖、目標、發起者和包含攻擊向量上下文的時間線，例如僵屍網路 ID、IP 地址、國家/地區、主機、埠、介面、發起者/目標、源/目標和使用者。
MAC 地址報告	在報告頁面上顯示媒體存取控制 (MAC) 地址。在五種報告類型中包含設備特定資訊（發起者 MAC 和回應者 MAC）： • 資料使用 > 發起者 • 資料使用 > 回應者 • 資料使用 > 詳情 • 用戶活動 > 詳情 • Web 活動 > 發起者
集中式日誌記錄	提供一個用於整合所有受管設備的安全事件和日誌的集中位置，提供單一點來進行網路取證。
雲原生架構	以雲速度和雲彈性從數萬個防火牆節點收集、組合、處理、再處理、提取、關聯和載入大量查詢資料。

許可和包裝

	功能特性	SaaS	On Premises
管理	備份/還原 – 防火牆系統	是	是*
	報告（基於 Netflow/IPFIX）	是	是*
	分析（基於 Netflow/IPFIX）	僅來自本地文件	僅來自本地文件
報告	計畫報告、即時監控器、摘要儀錶板	是	是
	下載報告、應用程式、威脅、CFS、使用者、流量、源目標（1 年流量報告）	是	是
分析（基於 Netflow/IPFIX）	使用向下鑽取和透視進行網路取證和威脅搜尋	是	是
	Cloud App Security – Shadow IT 發現	是	否
	數據保留	30 天	1 年
技術支援		全天候支持	全天候支持**

*需要 AGSS/CGSS 服務或任何付費的 Capture Security Center 服務
**需要全天候支援許可證

最低系統要求

對於通過 Network Security Manager 在 SaaS 模式下的 SonicWall Analytics：

支持的 SonicWall 設備包括：

- SonicWall 網路安全設備：NSA 系列、NSa 系列、TZ 系列設備、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual 設備：NSv 10 至 NSv 400

支持的 SonicWall 固件

- SonicWall SonicOS 6.0 或更高版本

互聯網流覽器

- Microsoft® Internet Explorer 11.0 或更高版本（不使用相容模式）
- Mozilla Firefox 37.0 或更高版本
- Google Chrome 42.0 或更高版本 Safari（最新版本）

對於 SonicWall Analytics 本地部署：

虛擬裝置

- 虛擬機器監控程序：VMware ESXi v5.5 / v6.0 / v6.5 / v6.7、Microsoft Hyper-V Win 2016
- 推薦 RAM：無限（最低 8 GB）
- 硬碟：基礎 OVA 65 GB 需要外部安裝
- vCPU：4/無限
- 網路介面：1
- VMware 相容性指南

支持的 SonicWall 設備包括：

- SonicWall 網路安全設備：SuperMassive E10000 和 9000 系列、NSA 系列、NSa 系列、TZ 系列設備、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual 設備：NSv 系列

深入瞭解 SonicWall Analytics

www.sonicwall.com/analytics

關於 SonicWall

SonicWall 為超分散式時代和每個人都遠端辦公、每個人都移動辦公、每個人都不太安全的工作現實提供了 Boundless Cybersecurity。通過瞭解未知、提供即時可見性並實現經濟學突破，SonicWall 為世界各地的大型企業、政府和中小企業彌補了網路安全業務缺口。有關更多資訊，請訪問 www.sonicwall.com 或在 Twitter、Facebook 和 Instagram 上關注我們。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有關詳情，請訪問我們的網站。
www.sonicwall.com