先進威脅防禦設備

產品概述

Juniper Networks 先進威脅防禦設備（Advanced Threat Prevention Appliance）是分散式軟體平台，結合了先進的威脅偵測、穩固的安全分析，以及單鍵式威脅消除等功能，可保護企業免於遭受網路攻擊，並且大幅提昇資安小組的工作效率。

先進威脅防禦設備可偵測出隱藏於網站、電子郵件和橫向訊務中的威脅。此外，它還可擷取其他安全設備的日誌，以便一窺環境中所有威脅的全貌。

產品說明

全球各地的企業每天都面臨著各式各樣的安全和工作效率挑戰，而零時差（Zero-day）攻擊通常可躲過傳統安全設備的偵測，因為這類設備僅透過特徵值來進行偵測，很難找出 Zero-day 威脅。更雪上加霜的是，資安小組每天都會收到海量的告警，使得辨識重大安全事件並採取對應措施，成為一項艱鉅的任務。

Juniper Networks® 先進威脅防禦設備（前身為 Cyphort 多合一系統）可針對網站、電子郵件和整體網路中橫向傳遞的訊務，進行持續不間斷的多級（multistage）偵測與分析。它可收集來自多個攻擊媒介的資訊，然後使用先進機器學習和行為分析技術，在短短 15 秒內辨認出先進威脅；接著將那些威脅與網路中其他安全工具所收集的資料相結合，並進行分析與關聯性比對，以便針對所有與受感染主機相關的惡意攻擊事件，建立一個易於檢視的時間軸。一旦找到了威脅，便透過「單鍵式」政策更新功能，將資料推播到在線（inline）安全工具，以阻擋重複出現的先進攻擊。

先進威脅防禦設備的偵測元件可監測網路訊務，以便迅速發現正通過殺傷鏈（kill chain）的威脅，並偵測出釣魚攻擊、安全漏洞、惡意軟體下載、命令和控制通訊，以及各種內部威脅。其多級威脅分析程序，包括靜態、負載，機器學習和行為分析，以及惡意軟體信譽（malware reputation）分析，可利用 Juniper 的全球安全服務來因應不斷改變的威脅態勢。這項雲端全球安全服務提供由安全研究員、資料科學家和良心駭客所產生的最新威脅偵測和消除資訊。

先進威脅防禦設備的威脅分析元件讓您能一目了然地查看從各種不同來源收集到的攻擊者身分和威脅活動等資訊，這些來源包括 Active Directory、終端防毒設備、防火牆、安全網路閘道器、入侵偵測系統，以及終端偵測與回應工具。此分析元件先檢視這些來源提供的資料，然後辨識先進威脅特徵，並建立這些事件的關聯性，以便深入洞察殺傷鏈的全貌。資安分析人員會收到完整的主機和使用者時間軸，其中描述主機或使用者所遭遇的威脅事件。時間軸可提高第一線和第二線資安分析人員診斷和調查惡意威脅事件的效率。

先進威脅防禦設備可與其他安全設備整合在一起，以便消除威脅，讓使用者能夠使用 REST API，自動在 Google 和 Office 365 上隔離包含威脅的電子郵件。藉由將惡意的 IP 位址推播到防火牆設備，可有效阻隔被入侵的終端設備、命令及控制伺服器之間的通訊。如與網路存取控制設備整合在一起，還可隔離受感染的主機。先進威脅防禦設備的開放 API 架構使其得以與多家安全設備供應商進行整合，例如 Cisco、Palo Alto Networks、Fortinet、Bluecoat、Check Point、Carbon Black 和 Bradford 等等。

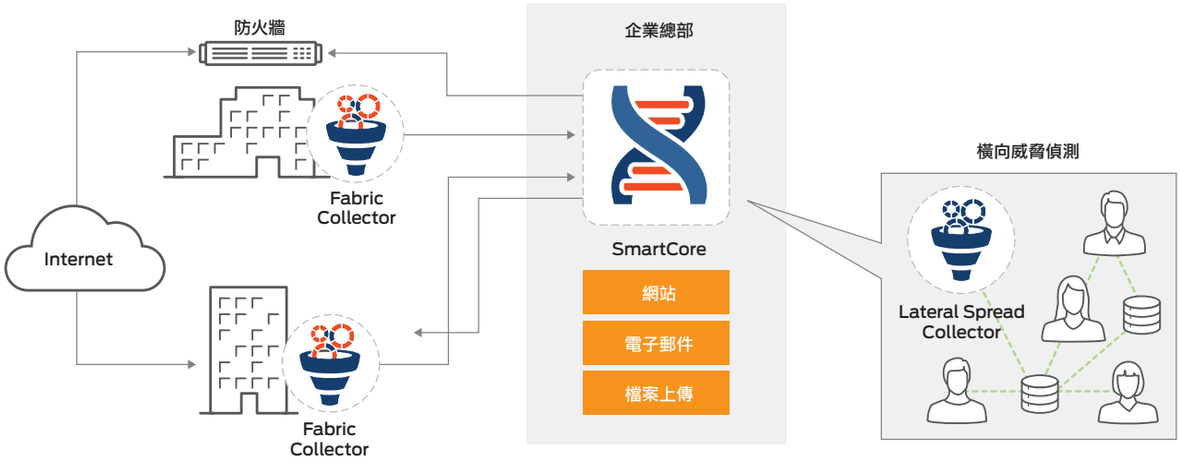

圖 1：Juniper Networks 先進威脅防禦設備架構

架構和重要元件

先進威脅防禦設備架構包括部署於網路重要節點（包含遠端節點）的資訊收集器，它們可作為感應器，負責擷取有關網站、電子郵件和橫向訊務的資訊，並將在整個核心組織中收集到的資料，以及相關的可執行檔，提供給 SmartCore 分析引擎。除了來自資訊收集器的訊務之外，先進威脅防禦設備還可擷取來自其他設備和安全產品的日誌，例如 Active Directory、終端防毒、防火牆、安全網路閘道器、入侵偵測系統，及終端偵測和回應工具等。其他廠商的安全設備可直接擷取日誌，也可經由現有的 SIEM/syslog 伺服器轉送日誌。

利用從各種不同來源收集到的資料，SmartCore analytics 分析引擎可執行以下的多級威脅分析程序：

- **靜態分析：**套用連續更新規則和特徵值，以便找出可躲避在線（inline）安全設備偵測的已知威脅。
- **負載分析：**支援智慧型沙箱（sandbox）陣列，以便藉由偵測可疑的網站和檔案內容，來洞察惡意軟體的行為，避免其鎖定 Windows、OSX 或 Android 等終端設備。
- **機器學習和特性分析：**採用申請專利中的技術來辨識最新的威脅特性（例如長時間的多元件攻擊），並迅速偵測先前的未知威脅。
- **惡意軟體信譽分析：**利用相似的已知威脅來比較分析結果，以便確定最近偵測到的威脅到底是現有威脅的變種，或是前所未見的威脅。
- **排列順序、風險分析、建立關聯性：**在網路、終端環境中，以及在整個殺傷鏈中，根據威脅的嚴重性、鎖定的資產，以及擴散程度，排列處理威脅的先後順序。例如，Mac 系統中高嚴重性的 Windows 惡意軟體，經評估後其風險程度比受保護伺服器的中等嚴重性惡意軟體要低。此外還可根據終端主機名稱和時間，將來自先進威脅防禦設備和其他安全設備的所有惡意軟體事件進行關聯性比對，然後畫出一條主要的時間軸，讓資安小組能夠快速評估威脅風險，以及這些威脅是否需要立即採取對應措施。例如，防毒解決方案遺漏掉，但先進威脅防禦設備偵測出的威脅，其風險評分較高。如此一來，資安小組可及時回頭檢視被感染的主機中發生的所有惡意事件。

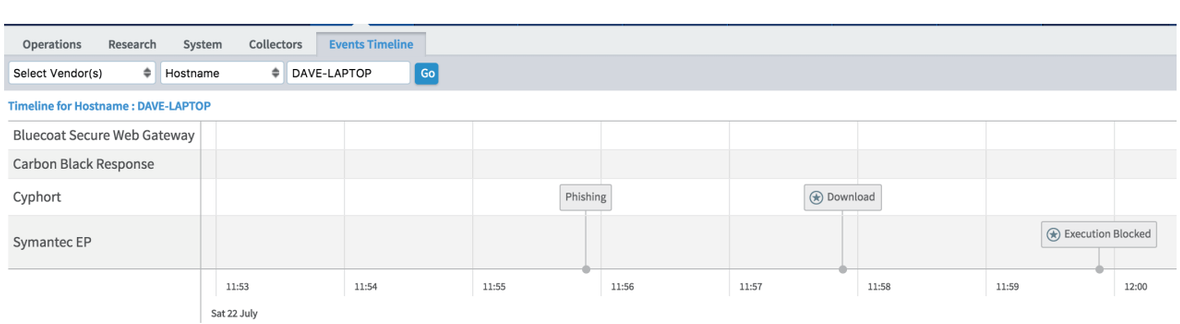

圖 2：先進威脅防禦設備事件時間軸

特色與優點

先進威脅防禦設備具有以下的特色與優點：

- 可檢查多種不同媒介所傳遞的訊務，例如網站、電子郵件和內部傳播
- 透過網路 UI 上傳可疑檔案以便進一步處理
- 支援 Windows 7 和 OSX 10.10 作業系統
- 可分析多種檔案類型，包括可執行檔、DLL、Mach-o、Dmg、PDF、Office、Flash、ISO、ELF、RTF、APK、Silverlight、Archive 以及 JAR
- 包括多項偵測技術，例如弱點偵測、訊務分析、幕後控制（C&C）偵測、YARA，以及 SNORT 規則
- 提供完整且清楚記錄的 API，便於與其他廠商的安全防禦設備進行整合
- 可整合入 Juniper Networks、Palo Alto Networks、Checkpoin、Cisco、Fortinet 和 Bluecoat 解決方案，以便自動阻隔惡意 IP 位址和 URL
- 自動檢查 Office 365 和 Gmail 電子郵件
- 可整合 Carbon Black Protect 和 Response（終端解決方案）以便上傳在終端設備上執行的二進位檔
- 可整合雲端存取安全代理系統廠商 SkyHigh 的系統，以便保護雲端設備
- 透過 Central Managers 管理功能來控管多個 SmartCore 分析引擎
- 支援使用 SAML 和 RADIUS 的存取和認證
- 可比對殺傷鏈（kill chain）中多個事件的關聯性，以便監控威脅進展和風險
- 將惡意軟體活動和群組惡意軟體特徵圖形化，以協助資安小組更深入了解惡意軟體特性
- 根據威脅嚴重度、威脅進展程度、資產價值和其他上下文資料來計算風險，進而排列處理威脅的先後順序
- 提供時間軸檢視圖，以便掌控主機所發生之威脅活動的全貌

產品選項

先進威脅防禦設備可以是實體或虛擬設備方式部署。實體設備可部署為多合一模式（將 SmartCore 和 Fabric Collector 安裝於同一實體設備），也可部署為分散式模式（將 SmartCore 和 Fabric Collector 安裝於單獨的設備中）。虛擬設備只能部署為分散式模式。

硬體

多合一

型號	效能（可辨識的物件）	效能
AIO-R430	每天多達 30,000 個物件	1 Gbps
AIO-R730	每天多達 80,000 個物件	2 Gbps

SmartCore

型號	效能（可辨識的物件）
SC-R730	每天多達 175,000 個物件
AIO-R730	每天多達 80,000 個物件

Fabric Collector

型號	效能
FC-R330	1 Gbps
FC-R730	4 Gbps

虛擬

虛擬 SmartCore 引擎

型號	效能（可辨識的物件）	虛擬 CPU	虛擬記憶體	虛擬磁碟
vSC-8	每天多達 40,000 個物件	8	32 GB	1.5 TB
vSC-24	每天多達 140,000 個物件	24	96 GB	1.5 TB

Virtual Fabric Collector

型號	效能	虛擬 CPU	虛擬記憶體	虛擬磁碟
FC-v50M	50 Mbps	1	1.5 GB	16 GB
FC-v100M	100 Mbps	2	4 GB	16 GB
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64 GB	512 GB

先進威脅防禦設備

訂購資訊

先進威脅防禦設備提供訂閱計費方式。請參見表 1 以查看可用的功能和授權選項。

表 1：先進威脅防禦設備特性和授權選項

標準版（1 或 3 年）	企業版（1 或 3 年）
• 依頻寬和使用者區分的授權，不限地點 • 結合網路、電子郵件、文件上傳和先進威脅分析 • 包括 Windows、Mac	• 依頻寬和使用者區分的授權，不限地點 • 所有標準版特性和先進電子郵件 • 對所有地點進行橫向威脅傳播偵測 • 無限規模的電子郵件和先進威脅分析

如需更詳細的訂購資訊，請洽 Juniper 業務專員。

規格

	AIO-R430	AIO-R730
記憶體	32 GB	96 GB
重量	19.9 公斤	30.8 公斤
體積（寬 X 高 X 深）	48.24 x 4.28 x 60.7 公分，1U	44.42 x 8.73 x 68.37 公分，2U
機箱	19 吋機架	19 吋機架
管理介面（eth0）	(1) 10/100/1000BASE-T 銅纜 Gigabit Ethernet 埠	(1) 10/100/1000BASE-T 銅纜 Gigabit Ethernet 埠
監視介面（eth1）（與核心設備無關）	• （1 個預留的）1000BASE-T 銅纜 Gigabit Ethernet 埠 • Intel Ethernet X520 DP 10Gb DA/SFP+ 伺服器接頭（選配）	• 10/100/1000BASE-T 銅纜 Gigabit Ethernet 埠 • Intel Ethernet X520 DP 10Gb DA/SFP+ 伺服器轉接器（選配）
備用的分析引擎導出介面（eth2）	• 1000BASE-T 銅纜 Gigabit Ethernet 埠（選配） • Intel Ethernet X520 DP 10Gb DA/SFP+ 伺服器接頭（選配；與 Collector 或 AWS 設備無關）	• 1000BASE-T 銅纜 Gigabit Ethernet 埠（選配） • Intel Ethernet X520 DP 10Gb DA/SFP+ 伺服器轉接器（選配；與 Collector 或 AWS 設備無關）
CPU	Intel Xeon E5-2650 v3 2.3GHz，25M cache，9.60GT/s QPI，Turbo，HT，10C/20T (105W) 最大記憶體 2133MHz	雙 Xeon E5-2695V3 14 核心 2.3GHZ 35MB L3 cache 9.6GT/S QPI 插槽 LGA2011 3 120W
交流輸入電壓	自動切換 100-240V	自動切換 100-240V
交流輸入電流	7.4-3.7 Amps	10-5 Amps
交流電源	550 瓦（最大值）	750 瓦（最大值）
電源供應器單元	兩個可熱抽換的 550W 電源供應器	兩個可熱抽換的 750W 電源供應器
頻率	50-60 Hz	50-60 Hz
周圍溫度	-40℃到 65℃，每小時最高溫度梯度為 20℃	-40℃到 65℃，每小時最高溫度梯度為 20℃
HDD（在面板 FRU 之後）	PERC H730 Raid 控制器 - 1 x 500GB 7.2K RPM SATA 3Gbps 3.5 吋可熱插拔硬碟，13G + 2 x 2TB 7.2K RPM SATA 6Gbps 3.5 吋可熱插拔硬碟，13G	PERC H730 - 12 ea. 600 GB SAS 可熱抽換的 2.5 吋 HDD FRU RAID 5
另外的 NIC	1 個雙埠 1 GB	1 個雙埠 1 GB 或 1 個雙埠 10 GB

關於 Juniper Networks

瞻博網路（Juniper Networks）致力於透過多元的產品、解決方案和服務，來改變網路連接的經濟效益，打破了業界一成不變的現狀。我們的團隊與客戶和合作夥伴共同推動技術創新，以提供自動化、可擴充的安全網路，進而提昇網路的靈活性、效能和價值。如欲獲得更多資訊，請瀏覽 Juniper Networks 網站，或是加入 Juniper Twitter 和 Facebook 粉絲團。

Corporate and Sales Headquarters
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

1000627-001-TC Nov 2017