Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT
硬體設備

2017

目錄

CHECK POINT
硬體設備

次世代威脅防護

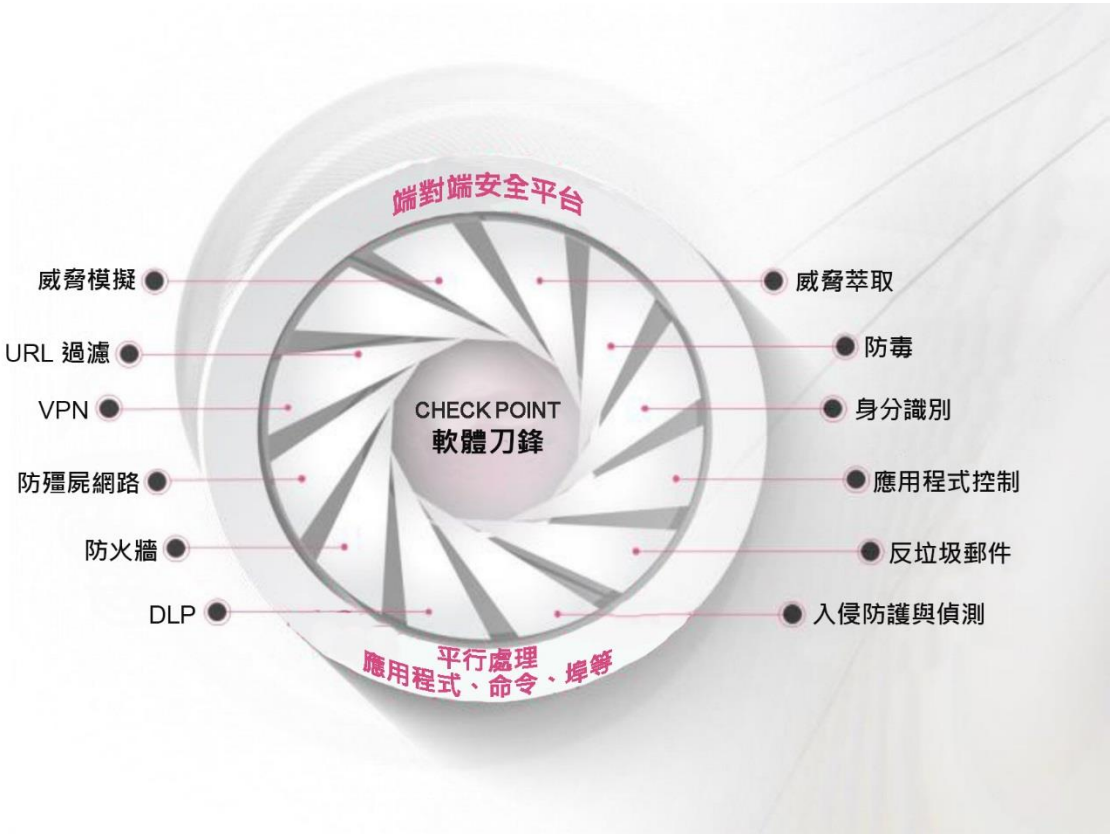
完善的威脅防護

面對惡意軟體快速成長、駭客變得愈加老練及新型未知零時差威脅日漸增多的情況，我們必須採取不同的方法，來保障企業網路和資料的安全。Check Point 提供完全整合的完善威脅防護，以協助您對抗這些新興威脅，同時降低複雜性並提高運作效率。Check Point 威脅防護解決方案包括強大的安全功能，如防火牆、IPS、防殭屍網路、防毒、應用程式控制和 URL 過濾，以對抗已知的網路攻擊和威脅；現在更結合了獲獎肯定的 SandBlast™ 威脅模擬和威脅萃取，功能更加強大，可徹底防範最複雜的威脅和零時差漏洞攻擊。

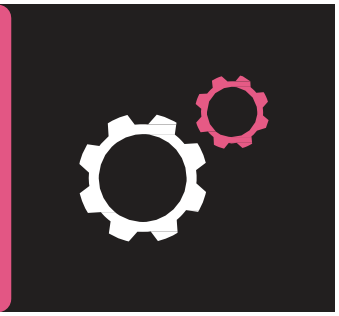
防止已知和零時差威脅

作為 Check Point SandBlast 零時差防護解決方案組成部分的雲端型威脅模擬引擎，可在惡意探索階段，甚至在駭客套用規避技術試圖繞過沙箱之前，便發現惡意軟體。另外透過在虛擬沙箱中運行，還可迅速隔離並檢查檔案，提前發現惡意行為，防止其入侵您的網路。此創新性解決方案結合雲端型 CPU 級檢查及作業系統 (OS) 級沙箱，以防止遭到最危險的入侵程式感染及零時差和鎖定目標攻擊。

此外，SandBlast 威脅萃取技術可移除可遭利用的內容 (包含主動式內容和內嵌物件)、重建檔案以消除潛在威脅，並且立即將處理過的內容傳送給使用者，以維持商流。



為您量身打造的安全次世代作業系統



GAIA - 統一安全作業系統

Check Point GAiA™ 是所有 Check Point 硬體設備、開放式伺服器和虛擬閘道適用的次世代安全作業系統。客戶可因使用高效率的 64 位元作業系統、改善的硬體設備連線功能及簡化的運作流程而獲益。GAiA 透過啟用角色式管理功能，針對具備不同權限的使用者進行職能分工，從而簡化管理流程。自動化軟體更新功能可提高運作效率，而直覺式和功能豐富的網路介面則能供使用者快速搜尋任何命令或內容。透過加速和叢集技術確保 IPv4 與 IPv6 網路的安全性，且支援最新的單點傳播和多點傳播路由通訊協定。

善用虛擬化功能

Check Point 虛擬系統讓組織得以在單一硬體裝置上建立多個虛擬化安全閘道，藉此強化其基礎設施。此外，組織也能藉由無縫的安全技術和基礎設施之強化，而節省大量的成本。簡化的虛擬化閘道管理流程可進一步提升資源不足之 IT 部門的運作效率，使網路安全獲得所需的簡單性。

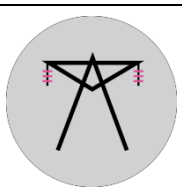
計算安全硬體設備實際效能的全新方法

與提供效能數值 (以最佳測試條件為基準，並使用只有一種規則 (Accept Any) 的安全原則) 的其他供應商不同的是，Check Point 安全硬體設備是以實際的客戶流量、多重安全功能以及典型安全原則為基礎。SecurityPower™ 提供有效衡量標準以選擇適當的硬體設備，從而更精準預測日常運作中遭到安全攻擊的目前與未來行為。客戶絕對能夠獲得符合目前需求的安全硬體設備，而且還可獲得成長空間。

SecurityPower

安全閘道

Check Point 在整合式次世代威脅防護平台中，為各種規模的客戶提供最新資料和網路安全防護功能，既可減輕複雜性，又可降低總擁有成本。不論是資料中心、大型企業、小公司或是家庭辦公室，只要需要次世代安全功能，Check Point 都有適合您的解決方案。

 分公司辦公室	部署	分公司或小型辦公室	1100
	機型	桌上型	1400
	介面	1 GbE、802.11n/ac Wi-FI、3G/4G、PoE	2200
	FW 輸送量	750 Mbps 至 14.5 Gbps	3100、3200
	特殊功能	DSL、網路管理	5100
 企業	部署	企業	4200、4400
	機型	1RU	4600、4800
	介面	1、10、40 Gb	5200、5400
	E FW 輸送量	3 至 52 Gbps	5600、5800、5900
	特殊功能	彈性 IO 選項、LOM	12200
 資料中心	部署	大型企業、資料中心	12400、12600
	機型	2RU	13500、13800
	介面	1、10、25、40、100 GbE	15400、15600
	FW 輸送量	25 至 128 Gbps	21400、21700、21800
	特殊功能	25/40/100 GbE、DC 電源、LOM	23500、23800
 底座系統	部署	資料中心、電信業者、電訊廠商	44000
	機型	6RU 至 16RU	64000
	介面	1、10、40、100 GbE	
	FW 輸送量	80 至 880 Gbps	
	特殊功能	刀鋒式、可調式平台	
 加固型設備	部署	惡劣環境	1200R
	機型	桌上型、DIN 安裝	
	介面	1 GbE、3G/4G 支援	
	FW 輸送量	2 Gbps	
	特殊功能	AC/DC 電源	

1400 硬體設備

分公司辦公室安全機制

1430-1450
(WI-FI 選項)

1470-1490
(WI-FI 選項)

概覽

若企業範圍延伸至遠端和分公司辦公室，其中僅少數幾乎不具備 IT 專業知識的使用者，那麼要在企業上下實施一致的網路安全措施就極具挑戰性。遠端和分公司辦公室也需要與主要企業辦公室一樣等級的防護，才能對抗複雜的網路攻擊和零時差威脅。Check Point 1400 硬體設備是簡單、實惠且易於部署的多功能合一解決方案，可提供領先業界的安全功能，以利保護企業網路中最脆弱的環節，也就是遠端分公司辦公室。

您現在可以藉助獲獎肯定的 Check Point 威脅防護來保護整個網路，從企業總部到遠端辦公室全面覆蓋。1400 硬體設備是小型辦公室的理想選擇。我們提供簡易的直覺式本機管理介面，以方便小型辦公室環境的本機管理和支援。想要從中央辦公室管理安全性的企業，也可利用 Check Point 安全管理或多網域安全管理功能，從遠端進行管理，並將一致的安全原則套用至各個外地辦公室的成百上千台裝置。

全包式安全機制

威脅防護

Check Point SandBlast™ ZERO-DAY PROTECTION

威脅防護 + SANDBLAST

重點概述

我們有各式各樣的網路介面選擇，包括 1GbE 網路連接埠、PoE、802.11b/g/n/ac WiFi (具備訪客存取功能)、3G 和 4G 無線連線。

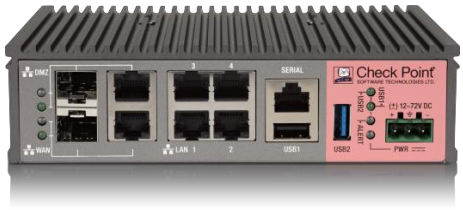
最大能力	1430	1450	1470	1490
防火牆輸送量[1]	900 Mbps	1.1 Gbps	1.6 Gbps	1.8 Gbps
威脅防護輸送量[1]	90 Mbps	150 Mbps	175 Mbps	220 Mbps
1 GbE 埠	1 個 WAN、1 個 DMZ、6 個 LAN 開關		1 個 WAN、1 個 DMZ、16 個 LAN 開關	
Wi-Fi 選項	802.11 b/g/n/ac、單頻 2.4 或 5GHz		802.11 b/g/n/ac、雙頻 2.4 和 5GHz	
PoE 選項	✖		✓	

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/1400-security-appliances

1200R 加固型硬體設備

惡劣環境適用的安全機制



1200R

概覽

保護重要基礎設施免遭網路攻擊，會面臨到特別的挑戰。環境可能很惡劣，且系統經常使用特殊化通訊協定。Check Point 的 ICS/SCADA 網路安全解決方案提供先進的威脅防護功能，並搭配加固型硬體護備選擇及完善的通訊協定支援，從而確保如發電設施、交通控制系統、淨水系統及工廠等重要資產決不受駭。

1200R 硬體設備使我們廣泛的硬體設備產品系列趨於完備，以支援各式各樣的部署環境，並滿足特別的需求。例如，1200R 符合關於耐熱、抗振和電磁抗擾性 (EMI) 方面的工業規格，如 IEEE 1613 和 IEC 61850-3。在極端溫度下 (從 -40°C 到 75°C)，其他硬體設備會故障失效，只有這款硬體設備能保障您的安全。

全包式安全套件

威脅防護

Check Point SandBlast ZERO-DAY PROTECTION

威脅防護 + SANDBLAST

重點概述

內含銅製和光纖 1GbE 網路連接埠，透過相容 USB 數據機提供 3G 和 4G 無線連線支援。

最大能力	1200R
防火牆輸送量 (Mbps) [1]	700
IPS 輸送量 (Mbps) [1]	60
WAN	1 個 10/100/1000BaseT RJ45 或 1 個 1000BaseF 埠
DMZ	1 個 10/100/1000BaseT RJ45 或 1 個 1000BaseF 埠
LAN	4 個 10/100/1000BaseT RJ45 埠
安裝選項	DIN 導軌或機架安裝
工業認證	IEEE 1613、IEC 61850-3
電源	AC 或 DC

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/industrial-control-systems-appliances

3000 硬體設備

分公司辦公室適用的企業安全機制

3100

3200

概覽

所有地點均採用一致的防護措施才能獲得無縫的安全性，僅主要企業網路採用防護措施無濟於事。遠端和分公司辦公室需要採用相同的防護等級才能構成一致而全面的潛在威脅防護網。Check Point 3000 硬體設備是為小型和分公司辦公室提供安全防護的理想解決方案。

3000 硬體設備採用精巧的桌上型，可提供企業級安全性，且毫無任何漏洞。多核技術、6 個 1 GB 網路連接埠及先進的威脅防護功能，可輕鬆地將健全的安全機制散佈到遠端分公司地點和小型辦公室。雖然機型小巧，但這些強大的硬體設備卻可提供高達 2.1 Gbps 的實際防火牆輸送量，及高達 160 Mbps 的實際威脅防護輸送量。

全包式安全套件

威脅防護

Check Point SandBlast ZERO-DAY PROTECTION

威脅防護 + SANDBLAST

重點概述

3000 硬體設備設計精簡、採用多核技術且具備 SandBlast 零時差防護功能，從而使這些閘道理想適合於小型辦公室和遠端分公司辦公室部署。

最大能力	3100	3200
防火牆輸送量 (Gbps) [1]	2.1	2.1
NGFW (防火牆、應用程式控制、IPS) 輸送量(Mbps) [1]	220	260
威脅防護輸送量 (Mbps) [1]	130	160
1 GbE 埠 (銅製)	6	
記憶體	8 GB	
儲存空間	1 個 320GB (HDD) 或 1 個 240GB (SSD)	
機箱	桌上型	

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/3000-security-appliances

5000 硬體設備

企業級安全性、彈性網路選項

5100 5200 5400 5600 5800 5900

概覽

您的安全決策再也不必在功能和效能之間抉擇。為特定目的建置的 Check Point 5000 硬體設備提供最先進的威脅防護安全機制，即使在要求嚴苛的中小型企業網路中也毫無破綻。

Check Point 5000 硬體設備將多重網路介面選項與高效能多核功能兩相整合，從而提供優異的多層安全防護而又不影響效能。5000 硬體設備配備多達二十六 (26) 個 1 GB 網路連接埠、備援熱交換電源供應器及可供選購的頻外 LOM 模組，以精巧的 1U 機架掛接式機型容納所有以上功能。這些硬體設備支援高達 26 Gbps 的實際防火牆輸送量及 1.7 Gbps 的實際威脅防護輸送量，效能屬同級產品最佳。

全包式安全套件

威脅防護

Check Point SandBlast ZERO-DAY PROTECTION

威脅防護 + SANDBLAST

重點概述

5000 系列的硬體設備具備模組式設計及多種網路選項，不只為這些閘道提供豐富多元的系列連線選項，也賦予閘道高度的可自訂性，從而適合於在任何網路環境中部署。

最大能力	5100	5200	5400	5600	5800	5900
防火牆輸送量 (Gbps) [1]	4.2	5.3	10	17.5	22	26
威脅防護輸送量 (Gbps) [1]	250 Mbps	290 Mbps	395 Mbps	645 Mbps	1.035	1.7
1 GbE 埠 (銅製)	14	14	18	18	26	26
1 GbE 埠 (光纖)	4	4	4	4	8	8
10 GbE 埠 (光纖)				4	8	8
記憶體	16 GB	16 GB	32 GB	32 GB	32 GB	32 GB
儲存空間	1 個 500GB (HDD) 或 1 個 240GB (SSD)					2 個磁碟機
AC 或 DC 電源供應裝置	1	1	1	2	2	2
無人值守管理模組	✓	✓	✓	✓	✓	✓
網路擴充槽	1	1	1	1	2	2

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/5000-security-appliances

15000 硬體設備

大型企業威脅防護

15400

15600

概覽

大型企業對效能、運作時間和可擴充性有嚴格需求。15000 硬體設備整合了最全面的安全防護功能及為特定目的建置的硬體。這些強大的安全硬體設備經過最佳化調整，可提供高達 3 Gbps 的實際威脅防護輸送量，從而保障最重要資產安全無虞。

Check Point 15000 硬體設備理想適合於需要高效能和彈性 I/O 選項的大型企業網路。若您準備從 10 GbE 升至 25、40 或 100 GbE，15000 硬體設備亦可隨之擴充。這些 2U 硬體設備提供三個 I/O 擴充槽 (以增加埠容量)、備援的 AC 或 DC 電源供應器、2 個 1TB (HDD) 或 2 個 480GB (SSD) RAID1 磁碟機陣列，以及無人值守管理 (LOM) 模組 (適用於遠端管理)。

全包式安全套件

威脅防護

Check Point SandBlast ZERO-DAY PROTECTION

威脅防護 + SANDBLAST

重點概述

15000 系列的硬體設備具備模組式設計及多種網路選項，不只為這些閘道提供豐富多元的系列連線選項，也賦予閘道高度的可自訂性，從而適合於在任何網路環境中部署。

最大能力	15400	15600
防火牆輸送量 (Gbps) [1]	30	30
威脅防護輸送量 (Gbps) [1]	1.695	3
1 GbE 埠 (銅製)	26	26
10 GbE 埠 (光纖)	12	12
40 GbE 埠 (光纖)	4	4
100/25 GbE 埠 (光纖)	4	4
記憶體	64 GB	64 GB
儲存空間	2 個 1TB (HDD) 或 2 個 480GB (SSD)	
AC 或 DC 電源供應裝置	2	2
無人值守管理模組	✓	✓
虛擬系統	40	80

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/15000-security-appliances

23000 硬體設備

資料中心威脅防護

23500

23800

概覽

資料中心對效能、運作時間和可擴充性有嚴格需求。23000 硬體設備整合了最全面的安全性防護功能及為特定目的建置的硬體。這些強大的安全硬體設備經過最佳化調整，可提供高達 4.5 Gbps 的實際威脅防護輸送量，從而保障最重要資產安全無虞。

Check Point 23000 硬體設備理想適合於需要高效能和彈性 I/O 選項的資料中心網路。若您準備從 10 GbE 升至 25、40 或 100 GbE，23000 硬體設備亦可隨之擴充。這些 2U 硬體設備提供五個 I/O 擴充槽 (以增加埠容量)、備援的 AC 或 DC 電源供應器、2 個 1TB (HDD) 或 2 個 480GB (SSD) RAID1 磁碟機陣列，以及無人值守管理 (LOM) 模組 (適用於遠端管理)。

全包式安全套件

威脅防護

Check Point SandBlast ZERO-DAY PROTECTION

威脅防護 + SANDBLAST

重點概述

23000 系列的硬體設備具備模組式設計及多種網路選項，不只為這些閘道提供豐富多元的系列連線選項，也賦予閘道高度的可自訂性，從而適合於在任何網路環境中部署。

最大能力	23500	23800
防火牆輸送量 (Gbps) [1]	34	43
威脅防護輸送量 (Gbps) [1]	2.9	3.6
1 GbE 埠 (銅製)	42	42
10 GbE 埠 (光纖)	20	20
40 GbE 埠 (光纖)	4	4
100/25 GbE 埠 (光纖)	4	4
記憶體	128 GB	128 GB
儲存空間	2 個 1TB (HDD) 或 2 個 480GB (SSD)	
AC 或 DC 電源供應裝置	2	2
無人值守管理模組	✓	✓
虛擬系統	125	250

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/23000-security-appliances

44000、64000 安全系統

可調式、多刀鋒效能

44000 和 64000 安全系統

概覽

一旦涉及對資料中心、電訊和雲端服務供應商之要求最嚴苛的網路環境進行保護，則安全性和效能必然是兩個完全不能妥協的重要因素。44000 和 64000 安全系統中的多刀鋒硬體及軟體架構是這些環境的理想選擇。44000 的平台提供高達 240 Gbps 的可擴充實際防火牆輸送量，64000 平台則提供高達 539 Gbps 的輸送量。

全包式安全套件

全包式次世代威脅防護 (NGTP)：由使用者識別並控制應用程式，然後掃描內容以將威脅阻擋在外。

重點概述

電訊廠商級 ATCA 機座從基礎開始設計，可滿足資料中心和服務供應商對穩定性、可用性和可維護性的需求；單一底座內的多個安全閘道模組可在高可用性和負載分攤模式下運作。新增另一個在高可用性模式下運作的底座，以進一步提升備援能力，從而確保重要任務資產總是處於可用狀態並受到保護。

最大能力	44000	64000
防火牆輸送量 (Gbps) [1]	高達 240	高達 539
100 GbE 埠 (光纖)	高達 4 個	高達 4 個
40 GbE 埠 (光纖)	高達 12 個	高達 12 個
10 GbE 埠 (光纖)	高達 64 個	高達 64 個
安全交換模組	1 到 2 個	2 個
安全閘道模組	1 到 6 個	2 到 12 個
電源供應裝置	4 個 AC	6 個 AC

[1] 實際流量混合、傳統規則式、具備 NAT 和記錄功能及最安全威脅防護環境下的效能

詳情請見：www.checkpoint.com/products/41000-61000-security-systems

虛擬硬體設備

公有雲與私有雲安全

企業希望藉由轉型發揮更大的效率、更快的速度、更高的敏捷性以及更有效益的成本控制，因而促進了雲端架構 (公有雲、私有雲或混合雲) 的普遍採用。雖然雲端能夠提供傳統架構所不能及的許多優勢，但也會使您的公司面臨全新的安全挑戰。Check Point 提供完備的公有雲與私有雲安全性產品組合，可順暢地將安全防護延伸至任何雲端環境，使得其與實體環境一樣安全，讓您可以高枕無憂。

公有雲安全挑戰

當您將運算資源和資料移至公有雲時，安全責任便由您和雲端服務供應商共同承擔。將應用程式和資料從企業移出至雲端供應商 (如 Amazon Web Services 或 Microsoft Azure) 後失去掌控，以及隨之產生的資源監控與管理挑戰，都會產生各種安全隱憂。具有匿名、多租用戶性質的公有雲尤其如此。

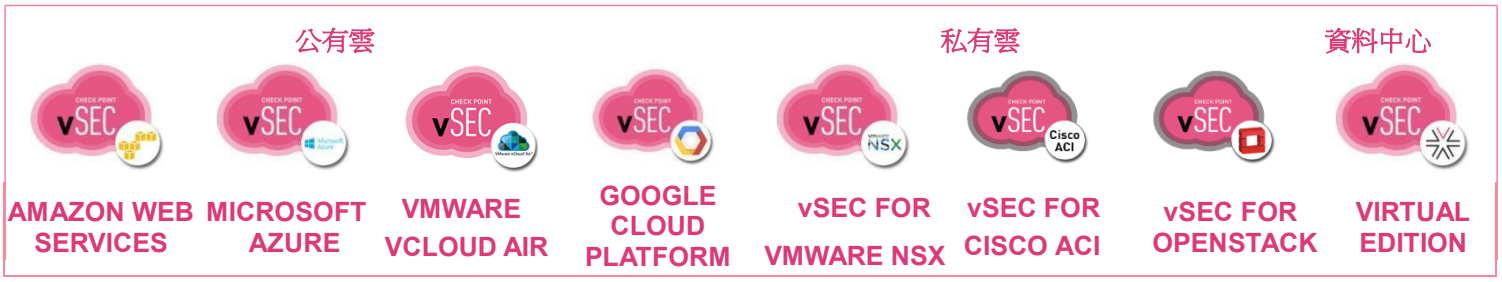
許多公司使用混合雲以保有對私有雲架構的控制并保護機密資產，同時將其他各方面外包至公有雲。使用混合雲會面臨到一項新挑戰：在企業和公有雲之間來回移動資料時，如何保護資料的安全。

Check Point vSEC 提供先進的威脅防護和單一控制台管理，以利輕鬆擴大安全防護範圍，從而使公有雲環境內的資料和資產獲得保護。

私有雲安全挑戰

企業採用軟體定義網路和私有雲環境後，即因更高的敏捷性和效率而獲益，但也導致資料中心內東西向網路流量遽增。流量模式的轉變帶來了新的安全挑戰。由於缺乏對東西向流量安全的足夠控制，威脅一旦進入資料中心，即可暢行無阻；而傳統的安全防護方式無法與多變的虛擬環境 (系統不斷在其內外佈建應用程式) 保持一致的步伐。

Check Point vSEC 可順暢地為私有雲架構提供先進的威脅防護功能，並提供可視性與控制力，從而有效管理實體和虛擬環境內的安全性 - 所有這些只需單一統合管理解決方案即可輕鬆解決。



詳情請見：www.checkpoint.com/products-solutions/private-public-cloud

SMART-1 硬體設備

巨量資料時代的網路安全管理

SMART-1 205、210、225、3050、3150 硬體設備

概覽

為有效而實際地管理安全環境，組織也需要有效實際的安全管理解決方案，從而透過比以往更快的方式處理資料。Check Point Smart-1 硬體設備將安全管理 (包括記錄、事件管理和報告) 整合到單個專用管理硬體設備中。組織現在可有效因應巨量資料時代中的資料管理與事件管理要求，集中檢視數十億筆的記錄、查看風險警示並能夠快速調查潛在威脅。

統合的智慧型安全管理

- 單一網域安全管理
- 多重網域安全管理
- 多重網域記錄管理
- SMARTEVEN 事件管理

重點概述

組織可運用 Smart-1 硬體設備管理 5 到 5,000 個閘道。藉助 Smart-1 多重網域管理功能，可將網路分割成多達 200 個獨立網域。此外，Smart-1 硬體設備還提供高達 12 TB 的內建儲存空間，以及連至儲存區域網路 (SAN) 的高效能光纖通道連線，以作為額外的儲存空間。

最大能力	205	210	225	3050	3150
管理式閘道	5	10	25	50	150+
最大網域數 (多重網域管理)[1]	×	×	×	50	200
索引式記錄數/秒	3,000	5,000	11,000	26,000	44,000
SmartEvent 記錄檔大小/日 (GB)	3.5	6.5	13	40	100
HDD	1 個 1TB	1 個 2TB	2 個 2TB	4 個 2TB	12 個 2TB
記憶體	4 GB	8 GB	32 GB	256 GB	256 GB
光纖通道 SAN 卡	×	×	✓	✓	✓

詳情請見：www.checkpoint.com/products/smart-1-appliances

DDOS PROTECTOR

數秒內停止阻斷服務攻擊

506/1006/2006

4412/8412/12412

10420/20420/30420/40420

概覽

近年來，阻斷服務 (DoS) 和分散式阻斷服務 (DDoS) 攻擊變得數量更多、速度更快也更為複雜。這些攻擊相對易於發動，而且會對仰賴網路服務運作的公司造成嚴重損害。許多 DDoS 防護解決方案是由網路服務供應商部署，只針對網路層級攻擊提供一般性防護。然而，現今的 DDoS 攻擊變得愈來愈複雜，駭客會在網路和應用程式層發動多重攻擊行動。成功的 DDoS 解決方案會賦予公司自訂防護功能的能力，以因應變化多端的安全需求、讓公司在遭受攻擊時能快速回應，並可選擇部署選項。

DDoS Protector 專屬硬體設備提供可輕鬆保護任何規模企業的彈性部署選項、可進行即時流量分析的整合式安全管理功能，以及應對 DDoS 攻擊之先進防護的有關威脅管理情資。Check Point 也提供專屬的 24/7 全天候支援服務與資源，以確保隨時提供最新的防護。

多層防護

網路和流量洪水攻擊

應用程式式 DOS/DDOS

重點概述

Check Point DDoS Protector™ 專屬硬體設備具備多層防護功能和高達 40 Gbps 的效能，可在瞬間封鎖阻繼服務攻擊。DDoS Protector 可擴大公司的安全範圍，以便在造成損害之前封鎖破壞性 DDoS 攻擊。

最大能力	企業	資料中心	電訊廠商
輸送量 (Gbps) [1]	500 Mbps 到 2 Gbps	4 到 12 Gbps	10 到 40 Gbps
最大同時連線數	2,000,000	4,000,000	6,000,000
最大 DDoS 洪水攻擊防護率 (pps)	1,000,000	10,000,000	25,000,000
延遲時間		< 60 毫秒	
10/100/1000 銅製乙太網路	4	8	
10 GbE (SFP+)			20
40 GbE QSFP			4
網路運作		透明 L2 轉送	
高可用性		主動-被動叢集	

[1] 輸送量是使用 eCommerce 防護設定檔，依據行為 IPS 防護力和重點 IPS 防護力計算而成

詳情請見：www.checkpoint.com/products/ddos-protector/

SANDBLAST 硬體設備

私有雲零時差威脅防護


TE100X


TE250X


TE1000X


TE2000X

概覽

隨著網路威脅愈趨複雜，許多針對式攻擊行動從攻擊已下載檔案和電子郵件附件中的軟體漏洞開始。這些威脅包括新入侵程式，甚至是已知入侵程式的變體，它們幾乎每天竄出，無既有簽章，因此也沒有標準的解決方案可以偵測這些變體。從未出現過的新威脅需要偵測能力超出已知威脅簽章的新解決方案。

具備防規避惡意軟體偵測功能的 Check Point SandBlast 零時差防護可提供完善的防護能力，即使是危害性最大的攻擊也無法得逞，同時還確保能將安全內容快速地傳送給使用者。我們解決方案的核心在於兩大獨特功能 - 讓威脅防禦更上層樓的威脅模擬和威脅萃取。

停止新的和未知的威脅


威脅模擬


威脅萃取

重點概述

我們提供各種 SandBlast 硬體設備；最適合因為有法規方面或隱私權的顧慮而無法使用 SandBlast 威脅模擬雲端式服務的客戶。

最大能力	TE100X	TE250X	TE1000X	TE2000X
建議檔案數/月	100K	250K	1M	2M
建議使用者數	多達 1,000 名	多達 3,000 名	多達 10,000 名	多達 20,000 名
輸送量	150 Mbps	700 Mbps	2 Gbps	4 Gbps
虛擬機器數	4	8	28	56
10/100/1000Base-T RJ45	13	17	14	14
10 GBase-F SFP+	-	-	6	8
機箱	1U	1U	2U	2U
HDD	1 個 1TB		2 個 2TB RAID1	
電源供應裝置	1	2	2	2

詳情請見：www.checkpoint.com/products-solutions/threat-prevention-appliances-and-software

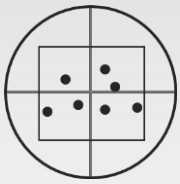
備受肯定的領導者

請放心購買 Check Point 產品，我們可以保證您購買的是安全產業領導者出品的產品，而且是受主要測試和分析公司肯定的產品。

GARTNER

企業網路防火牆

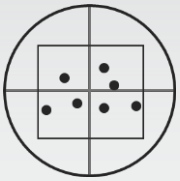
1997 年以來持續領先[1]



GARTNER

統合威脅管理

連續 5 年領先業界[2]



NSS LABS

推薦

- 防火牆
- 次世代防火牆
- IPS
- 漏洞攻擊偵測系統

NSS Labs RECOMMEND

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED IPSEC - BASIC

FIPS VALIDATED 140-2

Common Criteria

其他認證包括：NATO Information Assurance Product Catalogue、Common Criteria Medium Robustness、Defense Information Systems Agency (FW、VPN、IDS 和 IPS DoD 認證)、Commercial Solutions for Classified Program、IPv6 Ready、V PN Consortium。詳情請瀏覽 www.checkpoint.com。

[1] Gartner, Inc., Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Greg Young, Jeremy D'Hoinne，2015 年 4 月 22 日。

[2] Gartner, Inc., Magic Quadrant for Unified Threat Management, Je remy D'Hoinne, Adam Hils, Greg Young, Rajpreet Kaur，2016 年 8 月。

立刻聯絡 Check Point

www.checkpoint.com/about-us/contact-us

美國地區聯絡電話：1-800-429-4391

1-650-628-2000

聯絡我們

全球總部 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | 電話：972-3-753-4555 | 傳真：972-3-624-1100 | 電子郵件：info@checkpoint.com
台灣分公司 | 臺灣臺北市大安區信義路 4 段 6 號 6 層 | 電話：886-2-2703-2798 | 傳真：886-2-2703-2796 | www.checkpoint.com

