思科 Stealthwatch

改善企業環境內的能見度

掌握每台主機

記錄每個對話

瞭解正常行為

接收異動警示

快速回應威脅

安全數位業務需要更好的能見度

現今的企業網路快速擴張，並連結了多個分支、行動使用者、雲端和資料中心。組織正逐漸從傳統 IT 基礎架構轉型成數位型網路基礎架構，以改變其執行業務的方式。從簡化作業和庫存管理到提供全新加值服務，許多企業已感受到數位化所帶來的重要優勢。

不過，隨著公司將業務數位化，並採用新作法和新技術，他們也會需要更好的能見度，以維持安全性。

76% 的 IT 專業人員表示能見度是最大的挑戰。
資料來源：Ponemon 研究機構

優勢

- **能見度涵蓋所有網路**的對話，包括東西南北流量，可偵測內部和外部威脅
- **執行進階安全性分析**並取得深入情境，以偵測可能意味著攻擊的廣泛異常行為
- **加速並改善整個網路內的威脅偵測**、事件回應及鑑識，包括加密流量
- 具有網路活動的稽核記錄，可進行更深入的**鑑識調查**
- **簡化**網路分段、效能監控及容量規劃
- **確保企業遵循法規**，方式是辨識網路的加密程度以及其品質
- 藉由全域和本地流量相互關聯，**達到更好的能見度及異常行為偵測能力**
- 從雲端服務取得背景資訊，**藉此辨識內部威脅**

思科 Stealthwatch

監控 · 偵測 · 分析 · 回應


延伸的網路


資料中心


分支機構


雲端

思科 Stealthwatch 可持續即時監控所有網路流量，並提供涵蓋範圍更深入的資料檢視；進而大幅改善了延伸網路的能見度，並縮短發現可疑事件時的回應時間。此外，思科 Stealthwatch 可為網路主機建立正常網路及網路活動的基準，並套用環境感知分析以自動偵測異常行為。Stealthwatch 可識別廣泛的攻擊行為，包括惡意軟體、零日攻擊、分散式拒絕服務 (DDoS) 嘗試、進階持續性威脅 (APT) 及內部威脅。

現在有了認知分析（雲端式威脅偵測和分析功能），思科 Stealthwatch 可取得額外的背景資訊，進一步找出延伸網路中的新威脅，並為其排定優先順序。具備認知分析功能的 Stealthwatch 可提供全域及本地流量的額外能見度和背景資訊，並利用機器學習技術持續分析及偵測命令和控制通訊。現在，您可偵測到能繞過現有安全控制項的威脅，並識別對合法雲端服務的資料竊取事件。

分析加密流量以改善安全性

加密技術對於資安防護至關重要；雖然您可使用加密技術保護資料與隱私安全，但攻擊者也可能利用加密隱藏惡意軟體，甚至規避網路安全產品的偵測。透過思科 Stealthwatch 及其增強的分析功能，您可進一步瞭解網路上的加密流量是否為惡意威脅。Stealthwatch 運用機器學習，並針對內部流量中繼資料採用統計模式（又稱加密流量分析），以增強 NetFlow 分析能力。認知分析可從偵測到的結果進行學習，並隨著時間因應不斷變動的網路行為。

具備認知分析功能的 Stealthwatch 可讓您在管理主空台集中管理整個網路及網路流量，有效改善流量能見度。具備認知分析功能的 Stealthwatch 採用的方式並非解密流量，而是找出加密流量中的惡意模式，進而辨識威脅並加速適當的回應程序。

透過加密流量分析，Stealthwatch 還可確保企業遵守加密協定，並且洞悉和瞭解網路上要加密和未加密的內容。

將能見度延伸到雲端

工作負載正逐漸遠離內部部署，轉移到雲端環境。雖然這樣給予了組織更多彈性空間，但也會妨礙您檢視數個虛擬執行個體內流量的能力。不過採用 Stealthwatch 後，您即可取得所有網路能見度、威脅偵測及分析功能，無論在公有雲、私有雲或混合雲環境皆適用。您可在整個基礎架構中獲得即時情境感知和增強型安全。

將能見度延伸至端點

在連網世界中，行動力掌控一切。比起過去，有越來越多使用者從更多地點使用更多裝置連線到公司網路。但若要真正監控所有網路活動，資安專業人員必須查看從網路邊緣一直到遠端裝置上發生的應用程式和處理序。透過思科 Stealthwatch 端點授權，資安專業人員可對出現可疑行為的使用者電腦進行更有效率且情境資訊完整的調查，並且加速事件回應、快速修復政策違規情況。

延伸能見度至分支機構

若想取得分支機構網路的網路能見度，特別是涵蓋多個地點的分散式分支機構網路，程序可能會很複雜，且需要高昂成本。思科 Stealthwatch 網路學習認證是一套符合成本效益的解決方案，專為延伸至分支機構及遠端的網路提供安全防護。您可以運用思科裝置產生的 NetFlow 資料來充分利用現有的思科網路調查資源，改善您網路上的能見度及安全性；思科會在網路元素本身內建安全性異常活動偵測功能，運用封包擷取搭配智慧型偵測器，從而識別、減輕並修復威脅。此解決方案可在不影響頻寬的情況下提供能見度，而且僅在需要採取行動時才要求互動並移動資料。

「每當我走進公司，我就知道我必須對發生的情況擁有基本的瞭解，**Stealthwatch** 總是能為我解圍。…對我的團隊而言，**Stealthwatch** 最有利的優勢，就是在無人關注的情況下，**Stealthwatch** 仍在背景中悄然運行，持續眼觀四方，不斷觀察。」

Phil Agcaoili。
Elavon 資訊長 深入瞭解

專為協同合作而設計的資安防護

思科 Stealthwatch 可利用您現有的網路基礎架構，增強整個企業網路的能見度；此外，還能將 NetFlow 資料整理成可操作的情報，並將您的網路化為感應器。您將獲得所有網路流量的深入能見度，進而識別潛在的網路威脅。

透過整合 Stealthwatch 及其他思科安全解決方案，您可取得涵蓋延伸網路、分支機構、資料中心和雲端的分段、威脅偵測和鑑識增強功能。

思科 Stealthwatch 和思科身分識別服務引擎相互整合後，可協助組織全方位檢視延伸網路的情況。現在您可將現有網路當作感應器，以取得整個企業的唯一能見度，且能透過集中控制項和政策實施簡化網路分段，並藉由主動偵測威脅及透過進階鑑識功能進行追溯，進而更快速地因應威脅。

思科現已合併 NetFlow 分析及封包分析功能。我們已整合思科 Stealthwatch 和思科安全封包分析器。這兩種技術都有助於疑難排解資安和網路事件，但常因預算考量或缺乏資源的緣故擇其一而捨其一。我們的目標式方法可讓您僅儲存關注的封包來減少儲存成本，同時提供網路上所發生事件更詳盡、情境豐富的記錄。將 NetFlow 提供的能見度與更精準、更符合成本效益地取得封包層級資料的方式結合，有助於您視需要來對特定問題進行調查。

後續步驟

若要深入瞭解，請造訪 http://www.cisco.com/go/stealthwatch 或諮詢當地思科客戶代表。

思科 Stealthwatch

- 橫跨網路周邊、內部、資料中心及私有雲和公有雲，一直到達端點的深入能見度
- 以 NetFlow 建立可精準指出異常行為的基準，讓瞭解正常網路行為的過程更簡單
- 持續監控遍佈於分散式網路的裝置、應用程式及使用者
- 進階安全性分析和情報，用於偵測可能意味著攻擊的廣泛行為
- 以即時威脅偵測縮短事件回應時間
- 出色的鑑識調查及全方位的網路稽核途徑
- 網路分段、法規遵循驗證及疑難排解和診斷的簡化功能