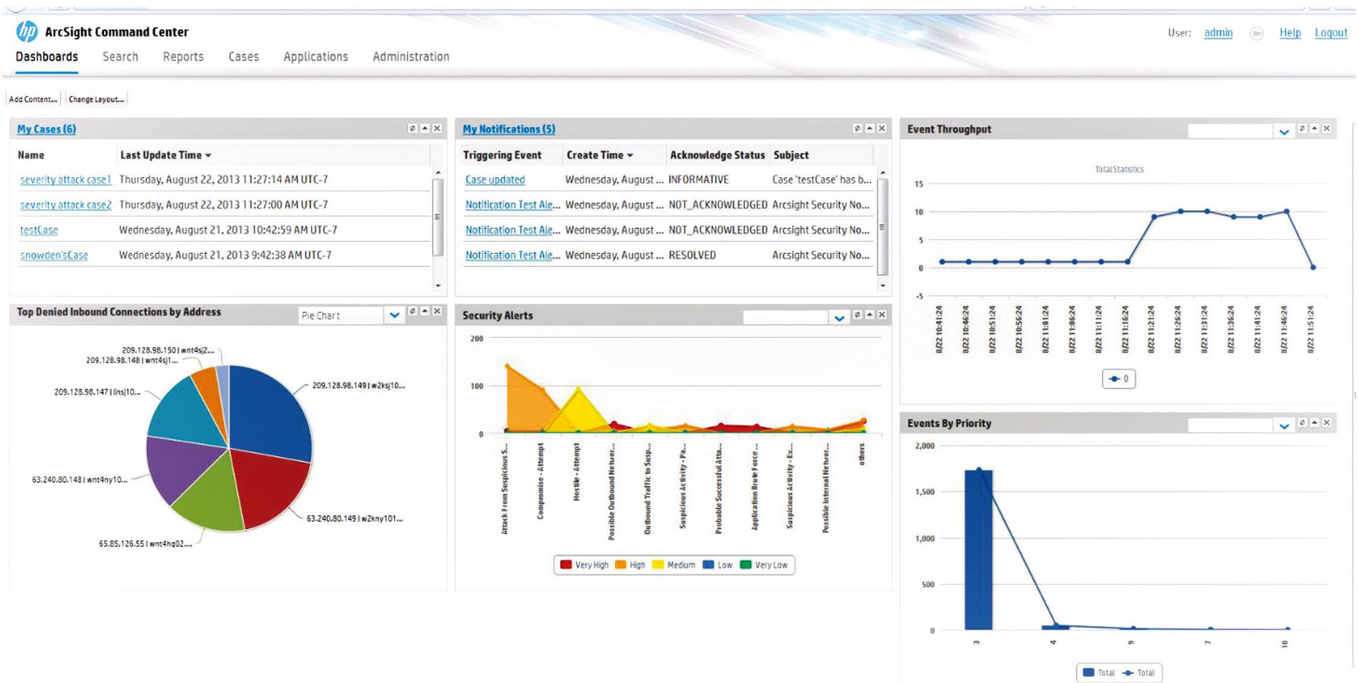
產品介紹

# HP ArcSight Enterprise Security Manager

## 海量資料分析達成資訊安全與合規需求




**即時分析**
HP ArcSight ESM 能協助您快速區隔威脅，讓您能夠選擇最佳回應方式對抗最緊急的問題。

**產品特性**
- 偵測及回應內部和外部威脅
- 保護您 IT 的安全
- 自動化合規狀態監控及報告

HP ArcSight Enterprise Security Manager (ESM) 能為企業安全性提供海量資料分析方法，將海量資料轉換成可據以行動的情報，以降低違規事件的成本，並將企業的風險降至最低。

為了讓企業能保護其重要的資料及智慧資產，資訊安全團隊需要能提供及時、相關性情報的解決方案，以協助他們快速偵測及回應違規事件。隨著資料量呈爆炸性成長，您事件日誌中所存在的高風險異常事件或趨勢也越來越難以辨識。網路犯罪變得越來越精密，攻擊會利用您的大量資料作為偽裝。

若沒有適當的工具，企業組織就無法快速回應，在發生違規事件時因無法有效分析鑑識資料而喪失寶貴時間。公司往往是被第三方通知時才發現遭受侵害，完全不知道系統安全性已受到入侵。

## 即時偵測威脅

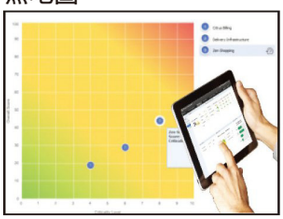
HP ArcSight ESM 是市場上收集、關聯分析及報告資訊安全事件資訊的領導解決方案。HP ArcSight ESM 使用數千種不同的裝置和應用程式連接器，提供一個分析每天商業運作的中心點。藉由這些資料的輔助，HP ArcSight ESM 的即時關聯分析功能可在不尋常或未經授權的活動時發生時立即偵測到情況 。最後，HP ArcSight ESM 的視覺化分析及報告功能支援個人化儀表板並提供系統管理員、管理員或稽核者隨選或排程報告的需求。

## 直覺化的儀表板、可靠的報告

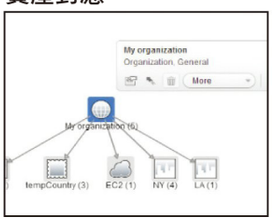
**HP ArcSight Risk Insight**
HP ArcSight ESM 及 Risk Insight 能提供全方位的技術和營運報告，同時透過標準和可自訂的範本，輕鬆製作出合規狀態、商業風險及使用者分析的商業等級報告。除了預先建立的報告和範本之外，本架構還能讓使用者建立新報告和範本，以供即時 (ad hoc) 報告及排程報告之用。

**圖 1.** 使用營業性關鍵 IT 對應模型，區分安全性風險的優先度

**熱地圖**



**資產對應**




**風險指標**


本架構能將相互關聯的大量資訊與全面化檢視進行結合，讓利益關係人可以辨別風險領域、傳達資訊安全性營運的價值及有效性，以及輕易回答關鍵商務問題。趨勢報告能追蹤事件及其長期影響。透過相互關聯技術，趨勢報告也可用來模擬「假設」情境，顯示安全政策變更可能會對企業組織的整體安全性和風險概況產生何種影響。

## 在應用程式層阻止威脅

**HP ArcSight Application View**
應用程式已成為大部分威脅的目標，HP ArcSight Application View 可用來彌平不當的使用者存取及應用程式使用方式所可能造成的安全性缺口。HP ArcSight Application View 將 HP Fortify 的見解運用在應用程式安全方面，直接從應用程式擷取實際的事件，而不需要修改應用程式本身。接著本資料會在 HP ArcSight 平台內相互關聯，協助您的資訊安全管理員立即獲得應用程式的安全性事件情報，而不需要進階的自訂化。

這些情報能快速分析資料庫查詢、錯誤訊息，以及其他可能導致機密資訊損失或身份遭到盜用的應用程式相關威脅。其成效則是應用程式安全性事件的能見度，讓您的 IT 資訊安全團隊不再有盲點。

## 自動化智慧及回應

**HP ArcSight Reputation Security Monitor**
HP ArcSight Reputation Security Monitor (RepSM) 能藉由將威脅情報層疊在網路流量分析上，以篩除惡意網路的通訊，進而提升您 HP ArcSight ESM 平台的功能。本解決方案包括可在每個階段提供偵測及防範協助的腳本。在發生違規事件之前，HP ArcSight RepSM 可偵測聲譽不良網站的危險瀏覽行為。在發生違規事件之後，HP ArcSight RepSM 可辨別受感染的資產或基礎架構，嘗試與聲譽不良的指揮及控制中心通訊。藉由快速偵測這些通訊管道，企業組織即可在其智慧財產從公司外洩之前，提供適當的保護。

**HP ArcSight Threat Detector**
雖然 HP ArcSight ESM 有數百個預先建立的規則和警示，您的資訊安全團隊具備能因應對手而隨時調整的靈活性，才是偵測進階威脅的關鍵能力。Threat Detector ( 威脅偵測器 ) 能讓 HP ArcSight 的關聯分析引擎，處理過往的活動紀錄並發掘出新行為模式。接著關聯分析引擎可以依據這些行為模式自動建立新規則 ,好讓您偵測出零時差蠕蟲及網路裝置、系統和應用程式錯誤設定等新型威脅。

Threat Detector 能為您的分析師提供適當的工具，以便從您網路中的一般事件判別出可疑事件。這可以協助依照您的特定使用案例自訂 ESM，降低維護您資訊安全監控中心所需要的資源數量。Threat Detector 能夠追查出通常只有在發生內部攻擊或帳戶遭到危害的情況下才會發現的可疑行動。Threat Detector 可以偵測這些行為模式，然後建立規則以便未來可以發現這些活動，因此管理者能夠提早解決潛在的問題。

**HP ArcSight Threat Response Manager**
一旦辨識出威脅，就必須和時間競賽，以儘快消除這些威脅。Threat Response Manager (TRM) 能讓您自動化處置及縮短降低威脅所需要的時間。TRM 能為您提供單一、整合式、端對端的網路以及資訊安全事件監控解決方案，讓您使用 HP ArcSight 以及您的內部應用程式所觸發的可行動事件減輕威脅。藉由縮短您的回應時間，您能以更主動的方式管理您的商務風險，讓您可以降低成本及增加佈署系統方式的彈性，以符合您企業組織的獨特需求。

## 讓您的團隊取得自動化安全合規專業知識

依據最佳實務所設計的 HP ArcSight Compliance Insight Packages，能提供一組可協助執行事件及安全性監控的內容套件。它們能協助企業組織符合廣泛的法規遵循需求，並建構強而有力的 IT 治理計劃，包括監控內部控管、存取控制變更、系統管理活動、登入監控，以及變更與風險管理。

它們能自動將這些技術檢查與相關標準原則和作業內容對應，讓企業組織能夠專注於重要服務及商業流程，並致力於處理關鍵的稽核重點。本套件能針對下列法規需求，提供現今 SIEM 市場中最具相關性及全面化的合規內容組合：

- 以 ISO/IEC 27002:2005 為基礎的 IT 治理
- 聯邦資訊安全性管理 (FISMA)
- Sarbanes Oxley (SOX) 和日本 Sarbanes Oxley (J-SOX)
- 支付卡產業資料安全性標準 (PCI DSS)
- 北美電力可靠度公司 (NERC)
- 關鍵基礎建設保護 (CIP) 002-009
- 1996 年健康保險可攜性及責任性法案 (HIPAA)

主動式合規能利用持續的事件收集及管理要求，讓企業組織不再只是以「勾選方塊」的方式來被動因應法規要求。它能啟動全面式、自動化的方法來保護企業、減輕風險，並達成法規要求，同時增加效率及降低成本。

## 單一統一化檢視—由單一位置指揮及控制

**通用日誌管理**
HP ArcSight 的設計能有效地儲存及分析大量的企業日誌資料。此一通用日誌管理解決方案能有效地收集和儲存任何日誌產生來源的機器資料，並統一資料，以供搜尋、製作索引、報告、分析及保存之用。它能支援 Windows® 和 Linux 兩種環境中的應用裝置、軟體、虛擬機器以及雲端等多種不同的佈署。

## HP 服務

**安全監控中心**
若想建構成功的安全性計劃，必須以卓越的技術來配合團隊，以協助運作及實作其資訊安全維運中心 (SOC)。若要偵測及回應來自多重來源的攻擊和違規事件，這些功能性團隊不可或缺。成熟的 SOC 能開發並報告營運指標及關鍵效能指標 (KPI)，以展現出安全性投資的價值。安全性指標應該能夠測量安全性作業的效率及有效性。此外，SOC 具有來自企業的強力支援，可視為企業組織中避免成本及風險降低計劃的重要推手。

惠普科技資訊安全事業處從宏觀角度建構及操作網路 (cyber) 安全防護解決方案和功能，支援所有企業的網路威脅管理及法規遵循需求；結合您和我們的專業維運經驗、實證有效的方法，快速、有效的產出成果，實現最大的投資報酬率。我們使用案例為導向的解決方案，不但具備領導市場的技術，並由訓練有素、條理清晰的專家，執行持續有效的營運和技術流程。

「**HP ArcSight 解決方案提供我們一個更全方位的威脅及風險管理平台，以最佳方式達成整體企業的能見度，進而辨別各種正在進行中的非法活動，並採取迅速的主動預防措施**」。

**- Heartland 付款中心技術長 Kris Herrin**

## 摘要

HP ArcSight 可依據經驗證的攻擊和商業風險，提供公司安全性狀態的單一檢視。我們藉由結合最佳的人員、流程及技術來協助企業推展其安全性作業。透過強化所有三項重要元件，我們可隨時監控您基礎架構的潛在威脅，以協助捍衛您的網路和商務。此外，我們能降低因為網路攻擊所造成的整體損失風險。確保商務安全並非易事。HP ArcSight 所提供的工具，可讓您事半功倍。

## 為何選用惠普科技 (HP)？

許多《財富》(Fortune) 百大資訊安全維運中心均利用 HP ArcSight 技術，惠普科技資訊安全事業處全球服務 (HP ESP Global Servise)。以同業難望項背的經驗，能協助您的企業評估安全性作業功能，開發未來的藍圖。

**請在下列網站了解詳情**
**hp.com/go/ArcSight**

**請在下列網址註冊取得更新**
**hp.com/go/getupdated**

與同事分享　　評分本文件



4AA4-3483ENW，2014 年 6 月，修訂 2