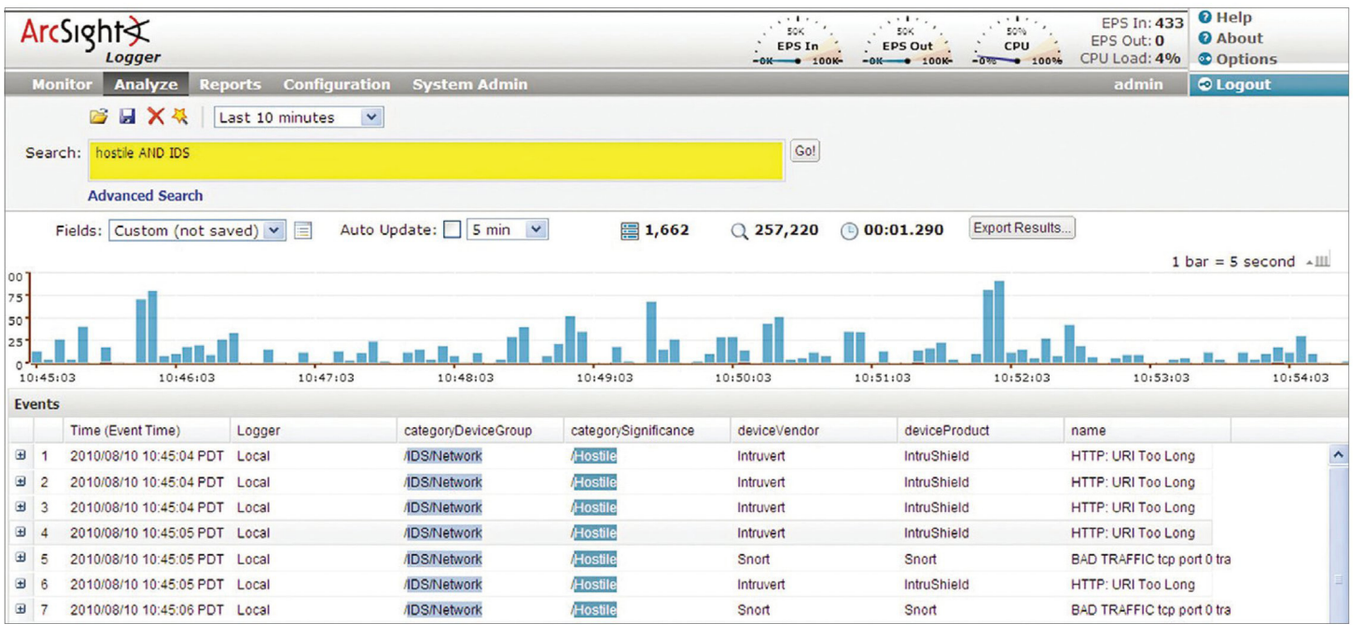
產品介紹

HP ArcSight Logger

通用日誌管理解決方案，能統一 IT 內的所有資料



產品特性

- 全方位收集並儲存超過 350 種廣泛來源日誌
- 超快速日誌全文檢索能力
- 簡化資安鑑識調查
- 內建資安標準及法規遵循的內容
- 支援 IT 營運管理分析
- 偵測可疑威脅行為
- 透過 10:1 高壓縮比，簡易儲存數年份的資料
- 支援擴充收集每天數十億筆事件
- 直接提供日誌管理延伸至資安事件管理 (SIEM) 的解決方案

HP ArcSight Logger 能提供高成本效益通用日誌管理解決方案，可在任何類型的企業計算機資料統一執行搜尋、產製報告、警示及分析。此統一化的計算機資料可用於資安標準及法規遵循、資安鑑識、IT 作業管理及日誌分析。

全方位的收集

針對超過 350 個不同的日誌產生來源進行收集、分類及標準化。HP ArcSight Logger 可從最廣泛的資料來源高速進行資料收集。

輕鬆佈署和管理

HP ArcSight Logger 可透過集中式管理中心 (HP ArcMC) 進行管理，讓您透過單一主控台管理大規模佈署，或是以經濟的資源管理小規模佈署。如此一來可讓您專注於您的使用案例，而非工具本身。HP ArcSight Logger 具備應用設備、軟體或虛擬應用設備等形式，以提供佈署彈性。

透過全文檢索達成超快速資安鑑識

HP ArcSight Logger 採用 HP ArcSight 通用事件格式 (CEF) 以豐富的中繼資料擴充原始計算機資料，可讓您執行全文檢索。亦能將計算機資料製作完整索引並提供此資料，以便透過簡單的搜尋介面執行快速的搜尋及報告。並能輕易將值得注意的事件樣本轉換為即時警示。透過 CEF 事件資料讓您不需要熟知每項日誌來源格式或是產品特定與主題相關的專業知識。

無可比擬的效能

HP ArcSight Logger 是針對海量資料所需要的資料收集廣度、深度及速度而特別打造設計。HP ArcSight Logger 能收集來自數千家廠商、超過 350 種來源的計算機資料，以每秒最多至 100,000 筆事件的速率擷取原始日誌、壓縮並儲存最多至 42 TB 的日誌資料，並以每秒數百萬筆事件的速度執行搜尋。

近乎連續、高成本效益的合規方案

HP ArcSight Logger 隨附許多內建內容，可用於網路安全性、合規、應用程式安全性及 IT 作業監控。另提供額外的內容套件－例如 PCI 和 Sarbanes-Oxley (SOX) 等資安規範專屬的套件，並對應至廣泛認可的標準，包括美國國家標準技術研究所 (NIST) 800-53、ISO-17799 和 SANS。

彈性儲存選項

HP ArcSight Logger 提供多種儲存選項。除了應用設備使用 RAID 功能的內建儲存裝置之外，軟體及應用設備解決方案也都能使用現有的 NAS、直接附加儲存裝置 (DAS) 及 SAN 等現有設備做為主要儲存區。無論儲存裝置為內建或外接，日誌資料皆能以 10:1 的平均壓縮率有效壓縮。

表格 1. HP ArcSight Logger 免費版及企業版功能比較表

功能	HP ArcSight Logger (免費版)	HP ArcSight Logger (企業版)
日誌資料的每日限制	750 MB	無限 (以授權為基礎)
全方位日誌分析	•	•
即時監控及警示	•	•
製作索引、搜尋及報告	•	•
脈絡式向下擷取儀表板	•	•
以角色為基礎的細微存取	•	•
驗證與授權	•	•
HP ArcSight 標準社群支援	•	•
分散式搜尋		•
HP 企業級客服支援		•

關於 HP 企業安全

HP 企業安全 (HP Enterprise Security) 是安全性及合規解決方案的領導供應商，適用於想要減輕環境風險並對抗進階威脅的現代化企業。

藉由領先市場的 HP ArcSight、HP Fortify 和 HP TippingPoint 產品，HP Enterprise Security 獨特提供進階的相互關聯、應用程式保護及網路防護，以建構新一代的資訊安全維運中心 (SOC)。

請在下列網站了解詳情
hp.com/go/HPLogger

HP 服務

惠普科技資訊安全事業處全球服務 (HP ESP Global Services)，從宏觀角度建構及運作網路 (cyber) 安全防護解決方案。透過使用案例為導向的解決方案，支援所有企業的網路威脅管理及法規遵循需求。

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

4AA4-4849ENW，2014 年 6 月，修訂 2