CASE STUDY

在 Windows 環境下滿足 HIPAA 和 PCI DSS 要求

syslog-ng™ Premium Edition

“ 我推薦 ONE IDENTITY SYSLOG-NG™ PREMIUM EDITION，它是一個成熟、已被證明是成功的產品，擁有各種詳細的參考文件，並持續開發中，也具備著豐富的功能組合。”

DataPath IT 專案經理
Mr. Thomas Robbins

DataPath

DataPath 成立於 1984 年，是一家總部位於阿肯色州小石城的私人控股公司，生產用於管理員工福利計劃的軟體解決方案。DataPath 接受了模糊的監管指導，卻建立了市場上最具體的管理系統。公司決定提供靈活的解決方案，以允許其客戶行銷、提議、安裝、管理、測試和彙報員工福利計劃。他們的客戶包括雇主、第三方管理者、福利顧問、計劃服務供應商、銀行、會計師事務所、保險公司和保險代理機構。

Learn more

- Read more about syslog-ng™
- Request an evaluation
- Request pricing

挑戰

行業合規性和跨平台支援

DataPath 需要一個解決方案，以便在其網路上傳輸系統日誌，同時確保符合醫療保健和信用卡行業的法規，例如健康保險流通與責任法案 (HIPAA) 和支付卡產業資料安全標準 (PCI-DSS)。這些標準要求使用加密來保護健康資訊以及帳號資料。加密技術是 DataPath 面臨的問題之一，因此 DataPath 需要一個透過使用 TLS 雙向認證和加密將日誌資料發送到中央站點的方法。此外，他們還需要一種能夠以自定義格式將日誌傳輸到入侵檢測系統 (OSSEC) 的解決方案。

DataPath 主要使用 Windows 伺服器，但公司同時運行不同版本的 Debian 和 Ubuntu Linux，他們的額外需求是找到一個能支援所有這些操作系統的日誌客戶端。他們測試了將多種產品結合以滿足這些需求，然而他們發現這大幅增加了維護的困難度。他們開始尋找一種新的解決方案，可為未來持續增長的基礎設施和需求提供附加功能。

syslog-ng™ Agent for Windows 的主要優勢

- 從事件日誌群組和日誌文件中讀取訊息
- 使用 TCP 轉發日誌訊息
- 支援 TLS 加密和伺服器的雙向認證
- 可以自訂義事件日誌訊息的格式
- 在並行和故障轉移模式下皆支援多個傳輸目的地
- 可以從網域控制器使用群組規範進行管理

解決方案

以syslog-ng™ Agent for Windows 為基礎的日誌紀錄

DataPath 花了幾天時間研究各種供應商解決方案。DataPath 的 IT 專案經理 Thomas Robbins 表示 “ 在選擇階段，我們也考慮了rsyslog，因為它具有豐富的功能組合。但是，為了將 TLS 雙向認證與 rsyslog 一起使用，日誌訊息必須採用新的 IETF syslog 協定。由於我們需要為我們的 IDS 使用 SNARE 協定，所以無法實施 rsyslog。結論就是，除了 syslog-ng Agent for Windows，我們在市場上找不到提供 TLS 雙向認證並使用 SNARE 協定的 Windows syslog 客戶端。因此，我們選擇了One Identity syslog-ng Premium Edition 套件，它可以作為單一工具，解決我們面臨到的所有問題。”

遷移到 syslog-ng™ 是 DataPath 積極採取的決策。該公司希望透過導入新工具以及能夠利用 WORM 媒體儲存日誌來更好地保護和監控其環境。 他們使用的一些關鍵功能包括 TLS 雙向認證、磁盤緩衝、流量控制、SQL Database Hook 和訊息解析。

在伺服器端，syslog-ng™ 提供了一種易於使用的解析語法來進一步對日誌訊息進行分類。DataPath 使用此功能來解析以 SNARE 格式傳入Windows 的訊息， Mr. Robbins 提到 “ 此外，產品文件非常詳細清晰，且有充足的社群平台支援。”

DataPath 在內部執行所有系統分析、設計和實施。他們目前正在使用 syslog-ng Premium Edition 4.0.1 伺服器，在 64 位元 Debian Linux 6.0.1 版本的 VMware ESXi 虛擬環境中運行。日誌儲存在平面檔案 (flat files) 和位於光纖通道 SAN 上的 MySQL 資料庫中。日誌來源端主機由 Windows Server 2003、2008 SP2 和 2008 R2 SP1 所組成，以運行 syslog-ng agent for Windows 應用程式。

結論

一次滿足所有需求

Mr. Robbins 表示 “ 我們目前處於生產運行狀態，自系統上線以來，我們無需對系統進行任何更改。目前正在使用 syslog-ng Premium Edition 監控 25 台 Windows 伺服器，這些伺服器會進行 TLS 雙向認證以確保遵循合規性要求，但隨著我們基礎設施的發展，我們預計會有更多伺服器。”

One Identity 為 DataPath 提供最好的技術優勢是此產品能一次滿足他們所有的需求，大大簡化了日誌基礎設施的實施和維護。由於日誌可幾乎即時的傳遞到集中站點，他們可以對可能影響正常運行時間的狀況做出更快的回應。Mr. Robbins 說 “ One Identity 的競爭優勢在於其產品具有豐富的參考文件，此外，One Identity 是少數可以提供系統日誌伺服器與 Windows 客戶端組合的公司。”

關於 One Identity

One Identity 協助企業建立正確的身分識別與存取管理 (IAM)。我們提供獨特的方案組合，包括身分識別管理組合、存取管理、特權管理、以及身分識別即服務方案，讓企業能夠充分發揮潛能而不會因為安全問題而受到阻礙，同時有效的防範威脅。
更多詳細資訊 OneIdentity.com