CASE STUDY

Meeting HIPAA and PCI DSS requirements in Windows environment

syslog-ng™ Premium Edition

"I RECOMMEND ONE IDENTITY'S SYSLOG-NG™ PREMIUM EDITION BECAUSE IT IS A MATURE PRODUCT WITH PROVEN SUCCESS, HAS SOME OF THE BEST DOCUMENTATION, IS CONTINUALLY BEING DEVELOPED, AND HAS A RICH FEATURE SET."

- Mr. Thomas Robbins , IT Project Manager, DataPath

DataPath

DataPath, founded in 1984, is a management-owned, privately held company based in Little Rock, Arkansas, that produces software solutions for administering employee benefit plans. DataPath takes vague regulatory guidance and creates the most concrete administration systems on the market. The company is determined to provide flexible solutions to allow its clients to market, propose, install, administer, test, and report employee benefit plans. Their clients include employers, third party administrators, benefit consultants, plan service providers, banks, certified public accountants, insurance companies, and insurance agencies.

Learn more

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

The Challenge

Industry compliance and cross-platform support

DataPath needed a solution to transmit system logs over its networks while maintaining compliance with regulations which govern the healthcare and credit card industry, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS). These standards require the use of encryption to protect health information, as well as account data. It was one of DataPath's main technical problems - to work out a way to send log data to a central location by using TLS mutual authentication and encryption. In addition, they needed a solution capable of transferring logs to their Intrusion Detection System (OSSEC) in a custom format. DataPath predominantly uses Windows servers, but different versions of Debian and Ubuntu Linux also run at the company. Consequently, their additional requirement was to find a logging client supporting all of these operating systems. They tested scenarios which incorporated multiple products in combination to meet these goals; however, they found that this greatly increased the difficulty of maintenance. So, they started to look for a new solution which could also provide them additional features for the future as their infrastructure and requirements grow.

Key Benefits of syslog-ng™ Agent for Windows

- Reads messages from event log groups and log files.
- Transfers log messages using TCP.
- Supports TLS encryption and mutual authentication with the server.
- The format of event log messages can be customized.
- Supports multiple destinations both in parallel and fail-over modes.
- Can be managed from a domain controller using group policies.

The Solution

Logging based on syslog-ng™ agent for Windows

Selection took several days of researching various vendor solutions. “In the selection phase, we also looked at rsyslog because it has a rich feature set. However, in order to use TLS authentication with rsyslog, the messages must be in the new IETF syslog protocol. Since we need to use the SNARE protocol for our IDS, we could not implement rsyslog. To sum up, we were unable to find a Windows syslog client on the market that provides TLS authentication and use the SNARE protocol other than the syslog-ng™ Agent for Windows. Consequently, we chose One Identity syslog-ng™ Premium Edition suite because it was able to solve every problem we faced without having to resort to using multiple tools.” - says Mr. Thomas Robbins, IT Project Manager of DataPath.

Migrating to syslog-ng™ was a proactive decision. The company wanted to better protect and monitor its environment by introducing new tools and by being able to utilize WORM media to store logs. Some of the key features they utilize consist of TLS mutual authentication, disk buffering, flow control, SQL database hooks, and message parsing. On the server side, syslog-ng™ provides an easy-to-use parsing syntax to further classify messages. DataPath uses this feature to parse incoming Windows messages in SNARE format. “In addition, the quality of the product documentation is superb and there is an ample community support.” - adds Mr. Robbins.

DataPath performed all system analysis, design and implementation in-house. They are currently using syslog-ng™ Premium Edition 4.0.1 server running in a VMware ESXi VM environment on a 64-bit Debian Linux version 6.0.1. The logs are stored in flat files and in a MySQL database which resides on a fiber channel SAN. Log source hosts consist of Windows Server 2003, 2008 SP2 and 2008 R2 SP1 machines running the syslog-ng™ agent for Windows application.

The Results

Meeting all demands in one package

“We are currently in productive operation and we have not had to make any changes to the system since it went live. We are currently monitoring 25 Windows servers with syslog-ng™ Premium Edition that require TLS mutual authentication for compliance reasons, but we expect more as our infrastructure grows.” - says Mr. Robbins.

The best technical benefit that One Identity offers for DataPath is a product that is capable of meeting all of their demands in one package. This greatly simplified the implementation and maintenance of the logging infrastructure. Since the logs are being delivered to a central location near real-time, they can react faster to situations which could affect uptime. “The competitive advantage of One Identity is the rich documentation of its products. In addition, One Identity seems to be one of the few or possibly only company to offer a combination of a syslog server with a Windows client.” - concludes Mr. Robbins.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com