CASE STUDY

Data Base Factory

syslog-ng™ Store Box

Founded in 1999, Data Base Factory has become a leading outsourcing provider of customer relationship management for many sectors including financial services, telecommunications, energy, and FMCG. The company employs more than 1,800 employees in 10 production locations, including five centers in France, three in Morocco, one in England, and one in Poland.

The Challenge

As a leading outsourcing provider of customer relationship management services, DataBase Factory handles credit card data and therefore must meet the requirements set out in the Payment Card Industry Data Security Standard (PCI-DSS). This industry standard, developed to enhance the security of cardholder data security, consists of twelve major requirements. Requirement 10 of the standard explicitly details which types of logs should be collected, but log messages can be used to meet many of the other requirements by documenting user and system activity such as the monitoring of critical network infrastructure and high-risk devices such as firewalls, active directory servers, core network, and databases.

DataBase Factory was looking for a solution that could reliably and securely collect and manage logs from a variety of devices to help demonstrate full compliance with the standard.

Learn more

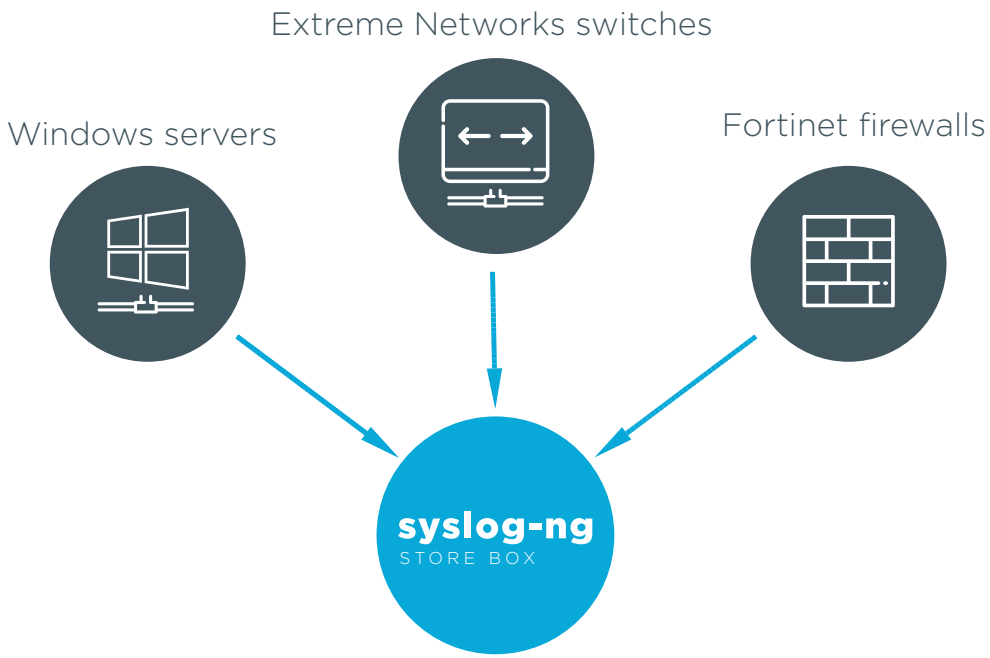
- Read more about syslog-ng™ Store Box
- Request an evaluation
- Request pricing

"THE SYSLOG-NG™ STORE BOX ENABLED US TO RESPOND QUICKLY TO PCI-DSS REQUIREMENTS. WITH THE CENTRALIZED ARCHITECTURE, WE CAN DEPLOY THE SOLUTION FOR ALL HIGH-RISK EQUIPMENT (FIREWALLS, NETWORK CORE, ACTIVE DIRECTORY SERVERS) IN THE INFRASTRUCTURE AT DATA BASE FACTORY SITES."

The Solution

To meet the requirements of PCI-DSS and provide a high level of visibility over critical infrastructure, Database Factory chose to centralize all logs generated by high-risk devices and store them in a secure IT area. DataBase Factory chose to deploy a syslog-ng™ Store Box (SSB) to collect and manage logs from Windows servers, Extreme Networks switches, and Fortinet firewalls. Using SSB's logstore feature, log messages can be archived in an encrypted, time-stamped binary file to prevent access to logs by unauthorized personnel, another PCI-DSS requirement.

Not only does requirement 10 of PCI-DSS call for collecting logs, it also requires that organizations periodically review them. With the help of a One Identity integration partner in France, the Database Factory was able to create dozens of reports that could be run daily, weekly or monthly to not only fulfill PCI-DSS requirements, but has also greatly improved visibility over critical infrastructure. With the advanced filtering, classification and search features of SSB, Database Factory can proactively manage the performance and security of their PCI-DSS infrastructure in real-time.



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