

Database Factory

case study

DATA BASE **FACTORY**

“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.”

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.

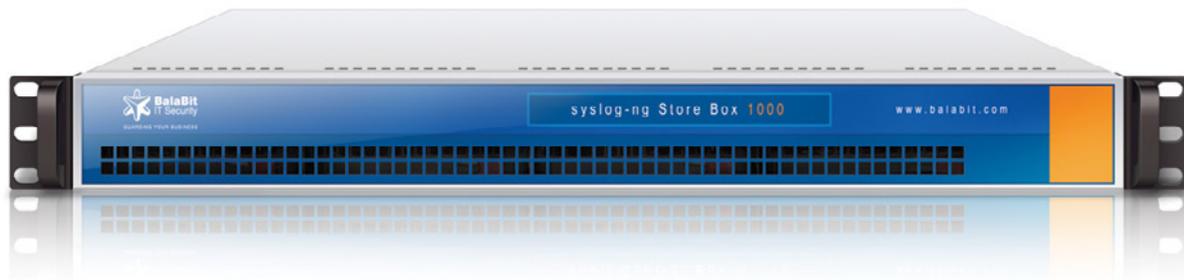
The Challenge

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 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.



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 QUICKSHIFT, a BalaBit 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 BalaBit

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring, trusted logging and proxy-based gateway technologies to help protect customers against internal and external threats and meet security and compliance regulations. BalaBit is also known as “the logging company”, based on the company’s flagship product, the open source log server application, which is used by more than 850 000 companies worldwide and became the globally acknowledged de-facto industry standard.

BalaBit, the fastest-growing IT Security company in the Central European region according to Deloitte Technology Fast 50 (2012) list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Our R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com



Learn More

- [BalaBit syslog-ng products](#)
- [Request evaluation version](#)
- [Request a callback](#)