



CASE STUDY

Enhancing security with flexible, scalable log data management

Sterling National Bank automates log data management across the business, enhances security and scales to meet business growth

Key Facts

- **Company**
Sterling National Bank
- **Industry**
Financial Services
- **Country**
United States
- **Website**
www.snb.com

Challenges

- Inefficient log management system
- Needed flexibility and scalability

Results

- Improved data quality
- Better visibility into log data environment across the business
- Scalability to meet growth by acquisition

Solutions

- [syslog-ng Premium Edition](#)

Sterling National Bank wanted to find a more efficient, flexible and scalable log management solution. The company's existing solution lacked a central location for storing log data.

Sterling deployed One Identity syslog-ng Premium Edition, a flexible and customizable log management solution. The bank enhanced security by improving data quality, centralizing and gaining deeper visibility into its log data, and achieving the ability to scale the solution to keep pace with business growth.

Looking for a more flexible log management solution

Since 1888, Sterling National Bank has provided personal and commercial banking solutions and services to businesses and individuals across the New York City metro area. In recent years, Sterling has focused more than ever on security. "We have doubled in size every year for the past several years," says Thomas Blasi, assistant vice president, Cyber Product and Engineering Group. "At the same time, cybersecurity threats have increased, so we've had to ensure we have the right technology in place to prevent them."

As part of the focus on security, Blasi was tasked with evaluating the company's security information and event management (SIEM) platform. "When I started looking at that solution, I realized we had some challenges with log management," Blasi says. "It was not flexible enough and didn't provide the high availability we wanted. We needed a central repository for log data and the flexibility to send logs to the cloud or any third-party security tool."

"We needed something that was more stable, **powerful and cost-effective than our existing solution, and syslog-ng Premium Edition provided all those things."**

Thomas Blasi, Assistant Vice President,
Cyber Product and Engineering Group

Streamlining log management with One Identity syslog-ng Premium Edition

After deciding to replace its log management solution, Sterling chose to deploy One Identity syslog-ng Premium Edition. “We needed something that was more stable, powerful and cost-effective than our existing solution, and syslog-ng Premium Edition provided all those things,” says Blasi.

syslog-ng Premium Edition improves the quality of data feeding a company’s SIEM solution. The platform is designed with flexibility in mind, routing log data from multiple sources to different destinations. Sterling achieved redundancy by placing two syslog-ng servers behind load balancers.

Unifying log data collection and management

Using the One Identity solution, Sterling can unify its log data collection and management. “We needed a log management solution that consolidated everything into a redundant repository, and that’s what syslog-ng Premium Edition does for us,” says Blasi. “We can put our data logs into a central location where we can find them quickly or recover them in the event of an investigation. It gives us peace of mind that we’re housing all our logs in one place.”

Achieving full visibility into the environment

Sterling now has better visibility into its environment. “Being in a highly regulated industry, we need to have full visibility into the data across our entire environment. We get that visibility with our SIEM platform and syslog-ng,” Blasi says. “In addition, syslog-ng is very reliable, and it makes it easier to enhance security by encrypting our log flow.”

About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at [OneIdentity.com](https://www.oneidentity.com)



“Being in a highly regulated industry, we need to have full visibility into the data across our entire environment. We get that visibility with our SIEM platform and syslog-ng.”

**Thomas Blasi, Assistant Vice President,
Cyber Product and Engineering Group**

Gaining flexibility and scalability

By using syslog-ng Premium Edition, Sterling has the flexibility it requires in a log management solution. “We can be more agile, because syslog-ng Premium Edition gives us the flexibility to send logs to multiple tools, which we couldn’t do with our previous solution,” Blasi says. “In my role, I’m constantly looking for new tools to protect our environment. If I had to do three proof-of-concept projects requiring data logs, it would take me less than a minute to forward log flow to destinations because of the flexibility of syslog-ng.”

Sterling can also scale to meet its growth needs. “syslog-ng Premium Edition gives us nearly unlimited scalability,” says Blasi. “This solution is more than adequate for our needs, and it can scale to meet any future growth.”

The One Identity logo is a trademark of One Identity LLC and/or its affiliates. Other trademarks are property of their respective owners. Availability and terms of our solutions and services vary by region. This case study is for informational purposes only. One Identity LLC and/or its affiliates make no warranties—expressed or implied—in this case study. © 2019 Quest Software Inc. All Rights Reserved