splunk> listen to your data™

CASE STUDY

Splunk at AZL

Increased Visibility Improves Security at Pension Fund Management Firm

AZL
Advies en management pensioenfondser
(an ING company)

"Splunk is a 'find' engine because it allows us to find the information we're looking for."

Wessel Landzaat
Information Security Manager

OVERVIEW

INDUSTRY
- Pension fund management

SPLUNK USE CASES
- Compliance reporting
- Financial transaction monitoring
- Proactive incident investigation

BUSINESS IMPACT
- Slash compliance report time from 24 hours per month to 4 hours per month
- Ensure safe and accurate transfer of funds
- Identify security issues proactively, before they become a problem

DATA SOURCES
- OS data
- Router/switch/firewall logs
- Application event data

The Business

AZL, founded in 1967, is a large pension fund management firm in the Netherlands, servicing more than 60 funds with a total of 550,000 participants. AZL is a subsidiary of Nationale Nederlanden, the large Dutch insurance company, which in turn is a subsidiary of global banking firm ING, also headquartered in the Netherlands.

Challenges

Security and compliance are a very high priority for AZL, which handles privacy data of pensioners and routinely processes large financial transactions. The firm's small security team is continually looking for new ways to increase visibility across their systems and infrastructure. Their goal is to efficiently provide AZL with a higher level of security and compliance.

One task in need of improvement was the mandatory SAS70 compliance report prepared monthly by Wessel Landzaat, AZL's information security manager. The largely manual process was error-prone and took Landzaat many hours a month to complete.

AZL also needed to improve the visibility into their funds transfer process. The company frequently transfers money directly to pension fund accounts or to AZL's own reserve accounts. Transaction reports were mailed daily to the internal department responsible for those transactions. But the information was at least 24 hours old by the time it was received. AZL needed a way to make status information available on a real-time basis.

One of the key functions of Landzaat's team is security incident investigations. Accessing the information needed to perform investigations, such as password misuse or abuse, was often labor-intensive and time-consuming, stretching the small team to its limits. AZL needed a more efficient and productive way of finding the right data to investigate and mitigate security issues.

Enter Splunk

AZL deployed Splunk Enterprise to streamline its compliance reporting, enable real-time financial transaction monitoring and provide proactive incident investigation capabilities. Splunk collects a full range of machine-generated IT data giving the security team a level of visibility and accessibility they never had before. "Splunk is a 'find' engine because it allows us to find the information we're looking for," says Landzaat.

The first challenge addressed by Splunk was the SAS70 report. Landzaat had deployed a product that collected event log data and pushed it to a syslog server. Custom PERL scripts then filtered out relevant information. "I had to manipulate a lot of the data by hand, which took a lot of time and was prone to errors. With Splunk all the data was there and it was possible to create reports with just the information we really needed," says Landzaat. This saved at least a day of labor per month.

Landzaat next turned to tracking fund transfers. They used an application to create a daily transaction report, which was mailed to the group responsible for the transfers. If there was a problem with a transfer, however, a day or more could go by before anyone became aware of it. Splunk enabled Landzaat to easily build a dashboard for the transfer managing group. They can now view the full status of payment transfers—from their approval to acceptance by the bank.

Landzaat quickly recognized the power of Splunk to monitor and respond to security issues faster and more efficiently. Drawing from event logs, application logs, and syslog output for systems Landzaat can identify, for example, when someone tries to access servers without permission, fails to change their password at the end of the month or uses an incorrect password and the job they scheduled fails to run. Splunk information is also shared with AZL engineers and application managers, helping them, for example, to correct authorization issues much faster than searching through IT data on their own.

Breakthroughs

Prior to Splunk, Landzaat spent many tedious hours each month compiling data for the SAS70 compliance report. “I needed 20 to 24 hours to produce and interpret the report,” says Landzaat. “With Splunk, that has been cut down to four hours. The report comes nearly automatically, and the quality of the information is much higher with less manual inspection needed.”

The group responsible for fund transfers no longer has to wait a day or more for a report to verify the status or accuracy of a transaction. An easy-to-use Splunk dashboard enables the supervisor and four subordinates to view the status and details of transfers at anytime in real time without assistance from the IT department. “It saves time and provides the peace of mind that transactions are being executed accurately,” says Landzaat.

Splunk has also streamlined the security investigation process. “I can log into Splunk at any time and see the information I want. I don’t have to run a PERL script,” says Landzaat, who stresses the importance of real-time data. “If someone tried to hack into one of our database servers three weeks ago, it’s rather late now to take action and prevent damage. With Splunk, if things are happening now, I can see them now. Furthermore, the productivity savings from Splunk have enabled us to do more innovative things for the business, like building out the payment tracking application.”