FOUR HUNDRED Stuff
Hardware, Software & Services

REPRINTED FROM VOLUME 10, NUMBER 20 – May 25, 2010

Security and Auditing Breakthrough Gives Cilasoft Compliance Advantage

by Dan Burger

Underestimating security issues and being unaware of the technology that makes systems more secure can be the dog you never thought would bite you until it did. The loss of sensitive data can hurt in many different ways. Regulatory compliance mandates have forced some IBM i-based companies to think about this, and software companies like Cilasoft are crafting new technology that can help. Cilasoft's database monitoring software is a good example.

The IBM i is not as secure as most people think. It's a bank vault compared to some well-known and more vulnerable systems, but the system and its operators have their weaknesses.

If you are familiar with the system, you understand it is possible to track and collect database modifications related to adds, changes, and deletes to a DB2 table. What it can't identify is who is looking at data, and that's a security breach that could be costly. Even though compliance standards have regulations in place for encryption of certain information (credit card numbers and Social Security numbers are two important pieces of info), much data remains to be seen by those who seek it.

"From a privacy law standpoint, this is huge," says Dan Riehl, the head of U.S. operations for the French company that's looking to make a name for itself in the United States. "Cilasoft's Database View Monitor for i is the only commercial product in the System i arena that does this. The PCI Data Security Standard, as one example, says you need to trace access to sensitive information, audit it, and report on it."

Riehl says there is a big hole in privacy and security of private information. As examples of compromised data that can affect a company, he notes that employees can access payroll information and production records.

Cilasoft's Database View Monitor identifies--by auditing the object--when files are accessed. It provides record-level information such as who was the user, what workstation was being used, what program was used to access the record, and the date and time the access occurred. It's the same type of information that's been available in logs that monitor add/change and delete events.

Riehl says he's been eagerly awaiting this product since hearing of the plans and design more than a year ago. He calls the tool "long overdue" for the IBM i market.

One of the common goals of most regulatory compliance standards is to make sure certain data is encrypted. Riehl says a lot of companies haven't gotten to that point yet.

"When they do," he says, "there will still be a need to see the access to sensitive data. Even if someone can't read the encrypted data, because they don't have the encryption key, there is other information with it--name, address, phone, and other private information."

Regardless of whether the data has been unencrypted, encrypted, or de-encrypted, companies will still want to identify records that have been accessed, Riehl says. And now that technology makes this available on the IBM i, he says auditors will ask that the technology be applied, as it is being done on other platforms.

"It's not a big technical challenge to build a tool to monitor database "view record" events on the i, but it is a huge challenge to build this tool in such an intelligent way that the performance metrics don't outweigh the great benefit of the tool," Riehl noted. "The development group at Cilasoft has tuned the performance of this software to the max."

Database View Monitor joins the newly upgraded Cilasoft Security Suite 5.0, which includes the products QJRN/400 and CONTROLER. The latest enhancements improve security, usability, and functionality, and the suite is compatible with the latest version of the IBM i/OS, which is 7.1.

QJRN/400 is used for auditing database changes and for monitoring and reporting on events from the security audit journal (QAUDJRN) and other system journals. It has customizable filtering capabilities and an array of reporting and alerting capabilities.

New reporting options include PDF output with customizable graphics, encryption, and password protection. It also has a colorized highlighter feature that allows selected fields within a report to be emphasized.

In terms of new reporting and alerting features, QJRN/400 now has a pop-up window alert and a more secure method of sending reports via FTP. Reporting on security-related and database events to the SYSLOG format also has been updated and enhanced to allow system monitoring through a stand-alone SYSLOG console or enterprise event console.

Cilasoft's CONTROLER product provides customizable auditing and granular control of network transactions through FTP, ODBC, file transfer, DDM, and remote command. The company says it goes beyond the capabilities of standard exit program software because it monitors and controls the use of all Control Language commands and enforces rules for all command parameter usage. CONTROLER can also monitor and control the use of all SQL database access using tools like STRSQL, RUNSQLSTM, RUNQRY, and ODBC.

Cilasoft also claims that CONTROLER is the only commercial exit point solution for the System i that can effectively audit and control Distributed Relational Database Access (DRDA) transactions across systems. According to Cilasoft, other exit point software packages only monitor the DRDA "Connect" function. CONTROLER audits and controls the entire DRDA session, including all SQL statements run during a DRDA connection.

Riehl says Cilasoft is unique because it makes auditing and controlling interfaces highly customizable, yet doesn't require a System i technical expert to configure them in order to get the monitoring and protection required in today's heavily regulated environments. He notes that the version 5 release has extended the number of exit points that are covered.

Database View Monitor for i, QJRN/400 version 5, and CONTROLER version 5 are all generally available. Each product is licensed separately, but is designed to work as an integrated environment. The product pricing is tier-based and begins at approximately $7,000 for use on a P05 box.

Cilasoft originally developed its products in response to policies and procedures dictated by the International Monetary Fund. They are certified as "IBM Server Proven" and Cilasoft is an Advanced IBM Business Partner. The company has a network of international sales partners and has customers in more than 45 countries.

For more information, visit www.cilasoft.com.