SEA™ SOFTWARE ENGINEERING OF AMERICA®
User Driven Software Solutions Since 1982
Phone: 516.328.7000 • Fax: 516.354.4015 • www.seasoft.com

# Case Study

## GERDAU MACSTEEL Relies on iSecurity for AS400 Security and Auditing

*GERDAU* MACSTEEL is an engineered steel bar producer headquartered in Jackson, Michigan with world-class steel manufacturing plants in Jackson, Michigan, Monroe, Michigan, and Fort Smith, Arkansas. *GERDAU* MACSTEEL is the second largest long specialty steel producer in North America, with an annual production capacity of 1.2 million metric tons of steel and 1.1 million metric tons of rolled products.

*GERDAU* MACSTEEL utilizes electric arc furnaces, ladle furnace refining, vacuum arc degassing, advanced rotary continuous casting, continuous casting and direct twist-free precision rolling to produce engineered SBQ carbon and alloy hot rolled and bright cold finished MACPLUS® steel bar products to direct end applications.

Janet Gentry, Business Systems Manager at *GERDAU* MACSTEEL, explains the major role that iSecurity from SEA plays. "We have been using the iSecurity Firewall and Audit products to identify who is accessing our AS/400's especially with FTP and ODBC. Prior to this, we had absolutely no way to identify, let alone control, who was accessing our systems remotely. These products have also helped us meet our SOX auditing compliance requirements. We currently have database journals over many of our critical files and use a query to access those journal receivers as part of our SOX compliance. Prior to using iSecurity, these queries were not easy to read and interpret. We have been replacing our current queries with these new queries supplied with iSecurity! We expect an increase in the productivity of our dba's as more and more rules are implemented and queries added to our job scheduler. These applications have been very helpful and productive tools for our Business Systems Managers and dba staff."

*GERDAU* MACSTEEL relies heavily on iSecurity's AP - Journal in their High Availability environment. As Janet explains, " iSecurity's AP - Journal application has been found to be a helpful and useful tool. The first time we used this product was during the re-synchronize of our High Availability system. We use the iTera (VISION) product for our HA solution which has 5 journals that must be interrogated to determine what has happened prior to the restart of our HA environment. Prior to implementing iSecurity AP - Journal, working with any IBM journal was not a task anyone looked forward to but now we can very quickly and easily query the information in any of our journal receivers and have that information presented in a very easy to understand format. We also have used iSecurity AP-Journal over our journals where we keep our critical data files. By using the filters provided by iSecurity's AP - Journal, we can monitor our journal receivers for database changes that are out of a normal range. For example, we have caught several changes to the customer price field and were able to quickly and easily identify who made the erroneous change, when and with what application. We are also able to correct the error before creating any embarrassing invoices. The iSecurity AP - Journal application is quickly becoming a valuable tool for our dba's."

Janet continues to implement additional features included within iSecurity, such as the alerting available in all three applications. "To be notified in real time about events being logged by iSecurity Firewall, Auditing and AP-Journal applications will be so much better then the delayed by days notice we get now. No more waiting to find our about a problem. We can react much sooner now. Prior to these iSecurity applications, we had implemented journaling over our critical files and had assigned our dba's the task of running queries over the journal receivers and trying to identify any issues. Now we can automate most of this task and utilize our dba's in a more productive way."

When it comes to meeting our SOX audit requirements, iSecurity has been a real asset, explains Janet. "One of our SOX auditing requirements is to minimize the number of user profiles being used to access our system, but up until now we had no way of knowing which remote server application was still using one of these "old profiles". Now with iSecurity we are able to identify the correct server and application that is remotely logging on to our system and we can notify that administrator to change the process to use the correct user profile!"

"Our staff is very creative and innovative and have needed very little support from Software Engineering of America. The online tutoring they provided along with the manuals has gotten us off to a great start!"

Disk utilization has not increased much after implementing iSecurity, explained Janet. "We currently keep the iSecurity Audit and Firewall logs on our system for 5 days. I do expect a savings in disk utilization when we stop using some of our 88 journals we had to create over our database files strictly for the purpose of our SOX compliance reporting. iSecurity will allow us to filter and keep what is required for auditing purposes and internal staff requirements."