

Improving Security with Estudias Enterprise

Putting Security Back in the Hands of IT

Improving Security with Estudias Enterprise

Putting Security Back in the Hands of IT

In the past ten years, security has certainly become one of the most important priorities for colleges and universities. With new viruses every day, hackers from around the world, legislation governing the release of student information, IT Administrators must be constantly aware of how information is being used. Schools have spent many thousands of dollars protecting their systems from hackers outside and even inside the school. Despite these precautions, group-specific requirements not possible to fulfill in Colleague have given rise to an entirely new class of security holes that undermine a school's security measures.

Problem: Group-Specific Requirements

Various groups on campus, from TRiO to Disability Services to Admissions, have to record information about their students. They need to be able to keep track of who their students are now, who their students were a year ago, when a student saw an advisor and for what reason. They need to be able to easily edit this list of reasons. They need to be able to select arbitrary groups of students and mail merge letters, create mailing labels and send emails.

As powerful as Colleague is, it was not designed to handle group-specific needs such as these. To compensate, groups resort to keeping their information on proprietary software programs, Excel spreadsheets or on sheets of loose paper. To "link" the information to Colleague information, they read information off one screen in Colleague and type it into their Excel spreadsheet or proprietary program. Not only is this incredibly inefficient and error-prone, it is a huge security risk. Each time someone does this, the information passes from a secure, centralized location (Colleague) where access could be closely regulated to insecure Excel files and proprietary programs with dubious security measures. Once this happens, is it impossible to know where that information is or who is looking at it. With viruses now

that can copy files off a person's hard drive and email them around the world, your control over this information is even more tenuous.

Problem: Proprietary Programs

Putting the information in proprietary programs represents a risk that's even bigger in some ways than in Excel files. The dozens of different proprietary programs is not only an IT nightmare in terms of maintenance, but support agreements that groups have with individual vendors makes it difficult to know who has access to your network. Most vendors do not pay adequate attention to laws governing sensitive information such as FERPA. As part of supporting their application, some vendors install software on client machines that gives them unlimited 24/7 control over client machines without clients' explicit permission. This of course undermines all of the thousands of dollars in security measures and makes the school's security only as secure as the vendor's security – which in many instances is not very secure at all.

This is not the fault of the individual groups – many may not have the computer knowledge to realize the security implications of such actions. Even if they do, they need these programs to do their job and vendors often will not support them without invasive support requirements. IT departments could create solutions for the groups, but few have the resources to learn and keep up-to-date on all of the intricate group-specific requirements mandated by the federal government and other agencies. For example, TRiO groups are required to submit a report to the government showing the status of every student ever served by the group. The description of the report is spread over dozens of pages of documentation. To develop our TRiO product, we have invested over 1000 man-hours to develop a program that would generate this report with a simple click. IT departments simply do not have the resources to invest this kind of time for each group.

The solution is to bring the information that each group records about a student to a central location that can be centrally monitored, allows security on fine-level of granularity, provides access to Colleague data via a user-friendly interface and empowers individual groups to customize the application logic themselves to match their group-specific requirements. This is where Estudias Enterprise comes in.

Solution: Estudios Enterprise

Estudios Enterprise is ostensibly a data warehouse with a very user-friendly front-end that allows generation of complex ad-hoc queries with a few clicks. However, it is the less visible “group tier” of Estudios Enterprise that helps drive down maintenance costs and puts security back in the hands of IT Administrators. It is this piece that allows groups to enter their contacts and other group-specific information about a student alongside the information automatically downloaded from Colleague. Information stays on the central server (SQL Server, Oracle, etc). Users do not have access to the actual database files and the server is separate from the web server, of course, so the data can be just as secure as Colleague. The data downloaded from Colleague is read-only, so this allows IT administrators to grant people access only to Estudios Enterprise and be confident that no student data can possibly be changed at the same time still allowing them to update group-specific information and run reports on Colleague data.

Perhaps most importantly, Estudios Enterprise comes with all of the source code so that a school can make changes and additions as it sees fit, rather than having to purchase proprietary programs. Of course, if it is necessary to purchase other programs, Estudios Enterprise make the integration task much easier because it is specifically designed to integrate well with programs by implementing open standards such as ODBC.

Estudios Enterprise is much more than a data warehouse. It allows users to easily access Colleague information and run powerful ad-hoc queries. It reduces IT costs and improves overall security by allowing all groups standardize on the same software. Instead of supporting insecure, proprietary programs for each group, groups will be able to access Colleague information through single program based on open standards.