



**Case Study** *Affordable IBM Midrange Software that makes you more productive*

**FDNY Fire Truck Builder Secures Their AS/400 with SafeNet/400**

New York City desperately needs new fire trucks. As a customer of FWD Corporation / Seagrave Fire Apparatus Company for almost a century, the FDNY is relying on the company to build 25 million dollars worth of new machines to replace those destroyed on September 11, 2001.

Founded in 1881, Seagrave Fire Apparatus Company originally made horse-drawn equipment for fire departments. The company now hand crafts some of the toughest fire trucks and emergency vehicles in the world. Because life and property hang in the balance, FWD/Seagrave is working day and night to deliver the new equipment.

At FWD/Seagrave there is no occasion for down time. Craftsmen at their Clintonville, Wisconsin facility are working continuously to get 54 new fire trucks out the door and into service for the FDNY. Under normal circumstances, production time for a single fire truck is 7 to 12 months. However, in response to New York's urgent need, Seagrave welders, painters,

plumbers, electrical technicians, and assemblers, through dedication and sweat, have cut that time to 120 days per vehicle.

**FWD/Seagrave Relies on Kisco's SafeNet/400**

FDW/Seagrave cannot afford to have problems with their ERP and financial software applications. To thwart unauthorized user's attempts to access applications and data through Client/Server tools on their model 730, FWD/Seagrave relies on SafeNet/400 from Kisco Information Systems ([www.kisco.com](http://www.kisco.com)). Problems caused by tampering with applications or data, could ripple through the whole manufacturing

process and delay delivery. "We don't need distractions right now. We use their product to protect our product, which is our data," states Jim Merdan, Information Systems Director at FWD/Seagrave.

Merdan joined the company 1988. His concern with system security began when he noticed that a few employees with access to the AS/400 through Client Access, were attempting to access information that was restricted based on their user profiles. Most violations were defined as illegal accesses to the system from Win 98/2000 desktops. Using Network Neighborhood, users can gain

**For more information on SafeNet/400 and other Kisco software solutions, log in at [www.kisco.com](http://www.kisco.com).**



**Kisco Communiqué**

**By Rich Loeber**

iSeries-AS/400s were once the benchmark by which other systems were measured in terms of invulnerability to intrusion. As IBM toiled to keep the platform viable by opening it up to the enterprise, it became more accessible to unwelcomed visitors. Since 1988 Kisco has been creating software solutions for IBMs midrange systems. Kisco has software installed on 6,000+ systems in 40 countries. SafeNet/400 was the first product in the industry to offer access controls, exit point blocking, FTP monitoring functions and other security features that reached far beyond those available in OS/400. Our goal is to continue to offer the best iSeries-AS/400 security and the best value. *Sincerely, Rich Loeber*

unlimited access to AS/400 data files that would otherwise be restricted. Merdan estimated that FWD/Seagrave had about 180 user sessions running on the AS/400 on any given workday. The majority of their workstations are Windows-based PC's, networked to the AS/400 and CAD servers with 802.2 and LANtastic's Net bios.



Merdan, an experienced AS/400 technician, felt that making changes to OS/400 security would not be beneficial. All users were already required to sign onto the menu driven system with a password and userid, and were individually limited, at the file level to what they could access.

### **An Invitation for Mischief**

After thorough investigation, Merdan learned that Client/Server programs like Client Access have created significant security challenges for midrange system security managers. Some client/server functions can bypass traditional OS/400 security checking unless users fully implement object-level security, which can make the system difficult to use. Seagrave's OS/400 security is set at Level 30, and Merdan notes that he doesn't want to make it any more difficult for authorized users to do their work. Without object-level

security, a PC-based database tool, such as Microsoft Access, users can easily access, update, or delete any data file on an AS/400.

In OS/400, exit points are instances in which users can register and insert programs, and override default application functions. Exit points can be used to call programs, block access to programs, and perform other functions. In early versions of OS/400, there were only about 30 exit points; now there are hundreds. Exit points can also be used to capture passwords.

To solve the problem, Merdan wrote his own exit point routines that successfully blocked this unwelcomed activity. Although his solution was satisfactory, Merdan found that maintaining these programs was a time consuming chore. Whenever a new operating system or application program release became available that included Client/Server functions, Merdan had to modify his exit point programs. "IBM said I could recompile my programs and they would go active, but I realized that I also had to bring down the whole subsystem, which involved a lot more off hours time. I wrote a couple CLs where you could just modify a data area, but as things got busier; it got unmanageable."

A more comprehensive solution was needed. Merdan knew of several third-party AS/400 audit/security software products that extend beyond the tools offered in OS/400 and help detect security holes. These products analyze systems to find all existing security faults and block all exit points. Security audit tools also

monitor activities and report violations. They notify operators of security issues through system messages or pager messages. Many tools have object and profile monitors that analyze the use of sensitive programs and commands, or produce a complete log of a specific profile's activities. Additionally, Merdan required a solution that would not change or impact any existing native OS/400 security settings, and it needed to be easy to implement and maintain.

### **A Closer Look**

After reviewing the literature and specifications of several offerings, Merdan chose to take a closer look at SafeNet/400 from Kisco Information Systems. Merdan states, "I decided to take a look at their product because they have developed a good name in the industry and their feature set fit my requirements."

*"We don't need distractions right now. We use their product to protect our product, which is our data."*

Jim Merdan, IS Director,  
FWD/Seagrave.

Merdan ordered the free trial offered by Kisco, to assess the software's ability to close the holes created by the non twin-ax desktops and open exit points.

Following a smooth installation during a regularly scheduled IPL, Merdan fired up the logging only feature. "I ran it for a week to get a picture of who was accessing

the system through network connections and what objects they were trying to gain access to. There seemed to be a lot of interest in system related files," states Merdan. "We also took a look at what exit points were being used."

He then proceeded to lock down server functions on their AS/400 using SafeNet/400 Access Controls. Each of the servers (there are more than 40 that SafeNet/400 controls) can be configured for no restrictions, just logging, restricted by user, restricted by user and object, or disabled. Each current user's access requirements were reviewed and rules were created for them within SafeNet/400. This was set up prior to locking down the servers. After the users were set up, server levels were set to maximum protection and SafeNet/400 was reactivated.

*"I decided to take a look at their product because they have developed a good name in the industry and their feature set fit my requirements."*

Jim Merdan, IS Director,  
FWD/Seagrave

After the second week, Merdan realized that the security problems that he had previously encountered were correctly identified by SafeNet/400 and resolved. Now, when SafeNet/400 detects an access violation, the illegal access attempt is rejected. The product automatically sends a message to the user stating that the operation has been blocked and notifies

security officer user profiles. If an access denial was made inadvertently, the rules can be updated immediately.

The only maintenance that is necessary with SafeNet/400 is when a new operating system or application program update is applied. "One time I put a new release of our Freidman Frontier ERP software on that had some client server applications which needed access to some exit points that we had blocked," notes Merdan.

Kisco's delivery of new SafeNet/400 releases and fixes is straightforward. New features introduced between release updates are available as PTF's that are delivered via e-mail along with bug fix PTF's. The Kisco website is kept current on changes to the product and provides information about the availability of new features and fixes.

FWD/Seagrave's AS/400 is not yet accessible by dealers or the public. However, he plans to implement TCP/IP to support internal Client Access sessions in the near future. Merdan notes that he is comfortable moving forward with this modification because SafeNet/400 has the ability to monitor and limit those activities.

Seagrave Fire Trucks cost between \$185,000 and up. Merdan would like to build an interactive fire truck configurator on the web so dealers and public safety agencies can design vehicles that fit their specific needs. "Right now we are engineered to order, but we would like to simplify the process," states Merdan. He would tie the

Web-based Fire Truck configurator to their ERP system so that once the machine

*"I ran it for a week to get a picture of who was accessing the system through network connections and what objects they were trying to gain access to. There seemed to be a lot of interest in system related files."*

Jim Merdan, IS Director,  
FWD/Seagrave

was certified as buildable and the order was confirmed, the ERP system would allocate resources for the order and schedule it into production. "SafeNet is going to play an important role here," states Merdan.

Merdan is pleased with what SafeNet/400 has added in terms of system security. The fires he originally had are now extinguished. SafeNet/400 will also enable FWD/Seagrave to comfortably execute future projects that involve ecommerce between distributors and end users.



**Kisco  
Information  
Systems**

7 Church St.  
Saranac Lake, NY 12982  
(518) 897-5002  
Fax: (518) 897-5003  
www.kisco.com  
sales@kisco.com