

## Enhanced Security for iSeries



...is a unique product designed to enhance iSeries/ AS/400 security in the client server arena, providing additional security checks when remote requests are received.

These security checks are designed to stop **authorised** users from performing **"unauthorised"** functions.

By capturing incoming requests from clients attempting to access server functions, **Fortress/400** reacts and performs a series of checks based on defined rules, creating an audit trail of all remote requests received and rejected.

## The security risks

All computer server installations require security. It is important to protect sensitive data, and, where necessary, comply with all appropriate legal and business regulations. The AS/400, iSeries and i5 systems are no exception and Fortress/400 is the ideal security product for these computer systems.



Using a PC networked to an AS/400, iSeries or i5 system poses a security threat. Applications such as FTP, Telnet, NetBios, or ODBC/JDBC enabled applications can be used to gain access to OS/400 and i5/OS objects. If iSeries Access is installed on the PC then even greater threats exist. Many differing functions are available without the user needing to sign on to a green screen session. For example:

- One can issue AS/400 commands from a DOS session using the iSeries Access Remote Command feature (e.g.):
  - ♦ RMTCMD PWRDWN SYS (Power the system off)
  - ♦ RMTCMD CLRLIB xxxxxxxxxx (Clear a library)
  - ♦ RMTCMD CLRPFM xxxxxxxxx/yyyyy (Clear data out of a file)
- Download confidential or sensitive data to a PC file. Once on the PC, it is no longer under the control of OS/400 or i5/OS.
- Transfer data back to the AS/400, replacing any data that may have been in the target file with data from the PC. The resulting transfer may corrupt the target file.
- Use ODBC/JDBC to connect PC software to the AS/400, iSeries, or i5 database



All of the above functions are, of course, subject to OS/400 and i5/OS security, however, removing authority to a command, library, or file may prevent your users from doing their job. In addition, many applications use group profiles to provide users with read/write authority to the entire database. These applications rely on front-end menus to control application security.

## The solution

**Fortress/400** enhances AS/400, iSeries and i5 security ensuring that the system is as secure as possible in networked environments. By capturing and recording incoming requests from clients attempting to access server functions, Fortress/400 performs a series of security checks based on Security Officer defined rules and retains an audit trail of all transactions processed.

**Fortress/400** was developed to address the security issues involved in networking iSeries and i5 computers. It significantly improves remote access security.

**Fortress/400** operates in conjunction with OS/400 and i5/OS security. It checks each remote request for the required level of authority before the request is executed by the operating system. This security check is in addition to, but independent of, normal OS/400 and i5/OS authority checking. Users can be authorized to use or update OS/400 or i5/OS objects via application software, whilst, at the same time, being prevented from copying, modifying or deleting objects using a networked computer.

### **Fortress/400:**

- Facilitates regulatory compliance (e.g. Security auditing, and SOX)
- Utilizes the exit program facilities provided in the OS/400 and i5/OS operating systems.
- Can prevent fraud and malicious damage.
- Security database is set up and controlled by a system administrator.
- Operates in conjunction with standard OS/400 and i5/OS security.
- Protection from unwanted and unauthorized access via network connections.
- Allows authorized users do their work, whilst preventing unwanted network access.
- Locks OS/400 and i5/OS security exposures.
- Protects against unwanted network transactions.
- Recognizes Group and \*PUBLIC authorities.
- Easy to use and install.
- User friendly command driven interface.
- Context sensitive Help for every command and display screen.
- Retains an audit trail of all remote instructions showing the date and time of the request, the user ID, the remote instruction string and whether or not Fortress/400 rejected the request. A hard copy of this audit trail is readily available.