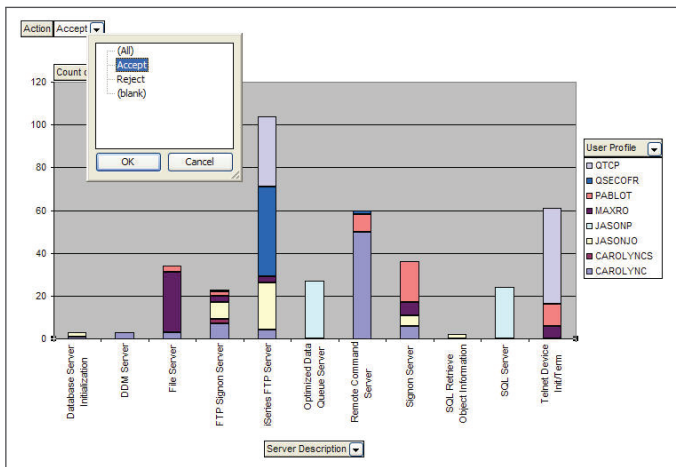




# Your greatest threat may come from within.



AS/400 server activity monitored by Network Security (displayed in MS Excel)

In the age of HIPAA, SOX, and PCI, every company needs a security policy that restricts data access to only those users who have a demonstrated need to use it for their job. In today's networked environment, there are hundreds of ways to access your iSeries data, making a security breach more likely than ever before. It doesn't take hackers or malicious intent to be at risk - the majority of security breaches happen by accident and by people within your company.

### Reduce Risk of Security Breaches

Protect your organization from the high cost and negative press associated with security breaches by tracking, monitoring, and controlling access to your data. Be sure that you know who is accessing what, when it was done, and how they got there. Network Security safeguards your iSeries by using OS/400 exit programs to allow only those people that you have authorized to upload and download data.

### Assure Secure Data Access

Access control is vitally important in protecting an organization, yet authorized data access is essential for day-to-day operations. Partial solutions such as shutting down specific servers can disable an organization's ability to compete in today's high tech business world.

Network Security delivers the best performance in the market. It has been designed to support high-volume transaction processing that is typical in today's Enterprise Resource Planning, Retail, and Financial applications.

```
me: 14:28:42      Work with Server User Authorities      Prog: LNSR031
                  NetworkSecurity Full License Version  User: BRENDAN

Server ID . . . : *FTPSERVER  iSeries FTP Server

Press Enter to continue.

Filter Rule Properties
-----
Action  User      Authority  Aud  Msg  Cap  Switch Profile
-----
LETEFILE ADMIN1  *REJECT   N   N   N   *NONE
LL      *PUBLIC  *OS400   Y   Y   Y   *NONE
NDFILE  HRCLERK  *SWITCH  N   N   N   USEONLY
```

Setting rules in Network Security

“The great draw to their products for us was features versus cost. PowerTech was light years ahead of the competition in that respect.”

— Don Stemberg,  
Charter Communications, IT Group

### Network Security at a glance:

FEATURE	BENEFIT
Monitor and control over 30 network access points (exit points), including: <ul style="list-style-type: none"> <li>• ftp</li> <li>• ODBC</li> <li>• Remote command</li> <li>• Fileserve (mapped drives to IFS)</li> </ul>	<p>Closes the “backdoors” not covered by traditional menu security schemes</p> <p>Implement policy to restrict access to those users who need it</p>
Records all transactions to a secure journal	Comply with COBIT and ISO controls that require logs of activity
Sends OS/400 messages for selected network transactions	Notification of security events in real-time
Rules by user or group	Grant access to only those individuals who have a demonstrated need
Rules by IP address for all exit points	Restrict access to only those locations approved by policy
Switch profile temporarily to assume authority of another profile	Allows greater (or lesser) access authority on a temporary basis for specific functions
Rules based on transaction detail	Limit access to specific libraries and objects
Report to spool file, database, or CSV file	Enables easy printing or graphical analysis of data in tools like Microsoft Excel
Support for High Availability environments	Avoids disruption to business when implementing disaster recovery plan or HA failovers
Dynamic rule configuration	Change rules quickly and know that they are being implemented immediately
Generic exit points	Network Security rule capability can be applied to proprietary and third party software
Central Administration available	With the Central Admin product, administrators can efficiently manage and set rules for multiple servers from a single console

### About the PowerTech Group, Inc.

PowerTech is your security expert in managing evolving compliance and data privacy threats with automated security solutions for IBM Midrange Servers. Our ServerProven security solutions are straightforward and save your valuable IT resources, giving you ongoing protection and peace of mind.

Because iSeries and AS400 servers are used to host particularly sensitive corporate data, it is imperative that you practice proactive compliance security. As an IBM Advanced Business Partner with over 800 customers worldwide, PowerTech understands corporate vulnerability and the risks associated with data privacy and access control.

Seattle, WA-based PowerTech Group was founded by security experts in 1996.

To learn more, please visit [www.powertech.com](http://www.powertech.com), to find white papers, case studies and detailed product specifications, or call 800-915-7700 to speak to a security solutions specialist.

