



A Multifaceted Approach to System i Security

by John Ghrist

One of the most daunting aspects of keeping on top of System i security is the sheer number of directions from which trouble can come. Threats to system security are like the mythical hydra, a source of danger from many angles: outsider intrusion, viruses, internal tampering, and authorized users wielding too much power with unintended consequences, to name the most common. It's only logical for system managers to consider remedies that offer similarly versatile protections.

Raz-Lee Security, Inc.'s iSecurity is such a solution, a suite of 13 modules that provides control of all aspects of System i security and protection from a wide array of dangers. iSecurity is designed to take a top-down approach that offers protection at the exit-point, firewall, user, object, and logon levels.

Protection from the Outside

Damage caused by viruses, Trojan horses, and other malware is usually the first security danger that comes to mind. The Anti-Virus module of iSecurity helps here by scanning in realtime all accessed files and giving system managers tools with which to mark, quarantine, and delete infected System i and PC files. Anti-Virus offers a choice of green-screen and graphical interfaces in several national languages, is menu-driven, supports V5R3 scanning enablement, and incorporates a malware-definition database that's automatically updated. It also includes internal protections that keep the module itself from being disabled by viruses. In addition, it lets operators exclude up to 50 file extensions or directories during virus scans and provides tools for handling "suspicious native objects" that may be infected or show signs of tampering.

The Firewall module is an intrusion-prevention system that currently covers 53 security-related program exit points and provides protection for all communication protocols. In addition to securing access to and from the system, it includes a GUI (Figure 1) that helps managers control individual user accounts and their access privileges and profiles account activity by time. Managers can also direct server access at user, profile, group, and firewall-user group levels. A series of Rule Wizards simplify security rule definition for incoming and outgoing IP addresses, users, and native-object access. Rules control activity for individual or ranges of IP addresses using standard subnet mask notation. An "FYI Simulation Mode" lets security officers simulate the application of security rules without actually blocking any activity so users can research and test the effects of their proposed rules before implementing them.

Solution Spotlight is a feature of System iNEWS that provides more in-depth coverage of significant System i products. Offerings are selected for Solution Spotlight by System iNEWS editorial staff, based on staff perception of the product as either new or innovative, or because the product is the subject of extensive discussions in Internet forums on SystemiNetwork.com and elsewhere.

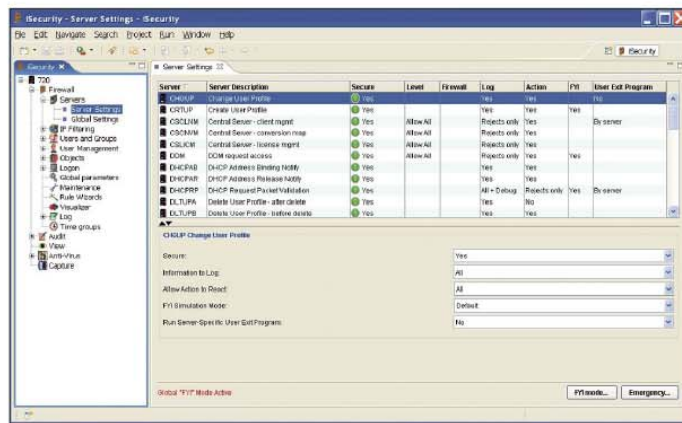


FIGURE 1 iSecurity's Firewall GUI helps system managers monitor user accounts and access privileges

tion to securing access to and from the system, it includes a GUI (Figure 1) that helps managers control individual user accounts and their access privileges and profiles account activity by time. Managers can also direct server access at user, profile, group, and firewall-user group levels. A series of Rule Wizards simplify security rule definition for incoming and outgoing IP addresses, users, and native-object access. Rules control activity for individual or ranges of IP addresses using standard subnet mask notation. An "FYI Simulation Mode" lets security officers simulate the application of security rules without actually blocking any activity so users can research and test the effects of their proposed rules before implementing them.

VENDOR CONTACT INFORMATION

Raz-Lee Security, Inc.
(888) 729-5334-3102
razlee.com
iSecurity

Protection from the Inside

Unfortunately, not all security threats come from outside the enterprise, so iSecurity provides tools for managing potential internal threats as well.

iSecurity's Password module integrates and expands on native i5/OS password features via several dictionaries that prevent users from choosing passwords that are too easy to guess or crack. Screen is a session time-out utility that locks screens and automatically logs users off if workstations are inactive for a preset period. It also lets managers restrict access from particular workstations based on date, time of day, or user profile.

The View module conceals sensitive record and field data from unauthorized users. Managers can implement it with few or no changes to existing applications. iSecurity provides multiple general-purpose security tools as well.

Assessment, which Raz-Lee currently distributes free of charge, performs automated analysis of a server's security strengths and weaknesses, including password controls, exit-point protection, system settings, excessive user privileges, and use of adopted authorities.

Audit examines and responds to security events in realtime and generates management reports via user-defined templates

or one of its more than 100 predesigned templates. Audit constantly monitors the system for a variety of events that range from approaching predefined thresholds for system activity and memory-pool status to unusual network transactions.

Action is an intrusion-detection "automatic operator" that Audit, Firewall, and other iSecurity modules can call to initiate corrective or preventive actions against potential security breaches. Managers can also use Action with Capture (see below) to monitor and disable unauthorized user actions.

Capture is a module that records and documents user screens, either for monitoring purposes or to aid help-desk troubleshooting activities. Capture features a playback mode and text-search capabilities, which can assist in, for example, searching archived user online activity for possible illicit behavior to meet SOX, HIPAA, and other mandated requirements.

Visualizer is a data warehouse and statistical tool that provides security-related analysis in graphical formats. It uses business-intelligence techniques to process system transactional data and scan system logs to provide a holistic view of system activities.


The Journal module automatically manages database changes by documenting and reporting exceptions made to the database journal. Its timeline reports of before-and-after changes made to, for example, mortgages and patient information include information such as who made database changes and when. This lets companies, auditors, and customers examine application changes made to information systems even over a period of years.

If taking a multifaceted approach to the many security threats your system faces makes sense to you, iSecurity is a software suite you may want to explore. ■

▶ **John Ghrist** is senior products editor for System iNEWS.

RPG TOOLBOX

RPG SOURCE MODERNIZER AND DEVELOPER TOOLS



- ▶ Convert RPG III and RPG/400 source code to modernized RPG IV syntax
- ▶ Convert RPG IV fixed-format C specifications to free-form syntax
- ▶ Over 70 new Source Entry Utility line commands
- ▶ Quickly find and insert pre-defined source code (Snippets) into your source
- ▶ Over 190 source code Snippets are shipped with the Toolbox
- ▶ Color your source code or convert its case to upper, lower or mixed
- ▶ FREE 30-day trial

LINOMA SOFTWARE

REVOLUTIONARY SOLUTIONS FOR YOUR WORLD

1409 Silver Street • Ashland, NE 68003 • Tel: (402) 944-4242 • Toll Free: (800) 949-4696
Web: www.linomasoftware.com • Email: sales@linomasoftware.com

Struggling with Microsoft Integration?

Welcome to "My i - .NET," a monthly e-mail newsletter and quarterly digital magazine that present articles and tips on how to effectively incorporate Microsoft .NET technologies and SQL Server 2005 with your System i. Sign up at SystemiNetwork.com; click on "My Profile."