iSecurity

System i Security Solutions

End-to-End Security for IBM System i

ABOUT SEA

Established in 1982, Software Engineering of America has built a global reputation as a leader in the field of data center software solutions. SEA is one of the most successful companies in the Data Center software industry, with products used at thousands of installations worldwide. Over 10,000 data centers of all sizes and configurations are utilizing one or more of SEA's products, including 9 of the Fortune 10 as well as 85% of the Fortune 500 Companies. SEA believes strongly in the philosophy of user-driven development and complete availability of high-quality technical support, 24 hours a day 7 days a week.

SEA has flourished since its inception, enhancing and strategically expanding its entire product line to meet the dynamic needs of the automated workplace. Since 1986, SEA has consistently been ranked as one of the Top One Hundred independent software vendors by industry trade journals. A noted industry analyst for Hambrecht & Quist, quoted by COMPUTERWORLD, described SEA as a "high-quality and thoughtfully managed company."

ABOUT iSECURITY

The iSecurity solution is the most encompassing, insightful and user-friendly security solution for the System i market. The product's well thought-out and developed protective mechanisms are uniquely engineered for the System i server environment, greatly minimizing any interference with the server's on-going production needs.

All products are defined, developed and supported by System i experts which provide them with critical, intimate knowledge of the OS and its related technologies. iSecurity's development has been enhanced by the capture and integration of customers real world requirements during the design phase. iSecurity provides users with solutions meeting SOX (Sarbanes Oxley), PCI, HIPAA, GLBA and similar recognized standards and requirements. With iSecurity, SEA defines the standard for System i security!

iSecurity consists of distinct solutions to meet the full scope of System i security requirements and relate more effectively to the specific needs of various customer and application segments. The iSecurity solution is aimed at top-tier, corporate customers as well as small and medium sized enterprises. These solutions assure customer specific ROI; no other product fits these requirements within the System i market pyramid.

End-to-End Security for IBM System i

FIREWALL

Intrusion Detection and Prevention

iSecurity Firewall provides complete protection against all types of access related security risks on your System i Server. Firewall has the ability to monitor security related exit points for unauthorized access, block users from gaining access via poor password policies and strengthening an organizations management of user profiles. Firewall has the ability to control access by IP address, location, date and time, library and down to the object level. iSecurity's Firewall provides complete intrusion prevention including the ability to manage passwords, control screen sessions, manage sign on attributes and graphically analyze data.

Firewall Features Include:

• Protection of all System i exit points
  and communication protocols

• User Management capabilities containing comprehensive
  information and management of all user profiles, including
  password control

• Terminal screen security that protects unattended
  terminal screens, including PCs running terminal
  emulation software, from unauthorized use

• Built-in business intelligence tool that enables
  IT managers to graphically analyze system exit
  point access and functions quickly and easily
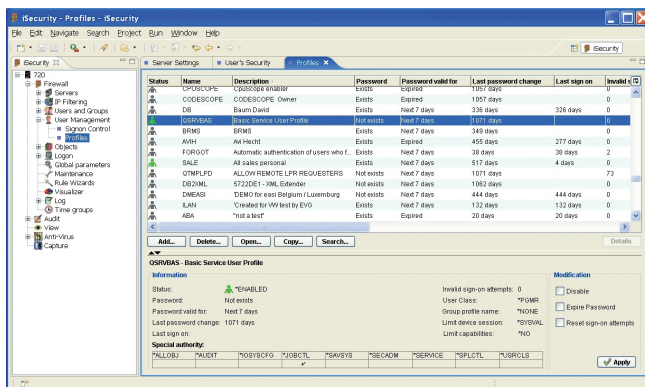
User management functionality

AUDIT

Compliance Monitoring

iSecurity Audit provides complete monitoring of system related activities and initiates responses to potential threats in real time. iSecurity Audit's real time response can trigger alerts and take immediate corrective actions. iSecurity Audit gives organizations the flexibility to audit and report on all critical events for internal security requirements or for compliance with Sarbanes-Oxley, PCI, HIPAA or GLBA.

Audit Features Include:

• Highly sophisticated CMS (Compliance Monitoring
  System) feature to provide real time alerts, warnings and
  provide corrective actions to threats in real-time

• Built-in business intelligence tool that enables
  IT managers to graphically analyze and/or export security
  related system activity quickly and easily

• Monitors user activities and object access in real-time

• View multiple audit types with one query

• Report Scheduler - automatically
  run reports at specified times

• Time groups apply rules and filters at predefined times
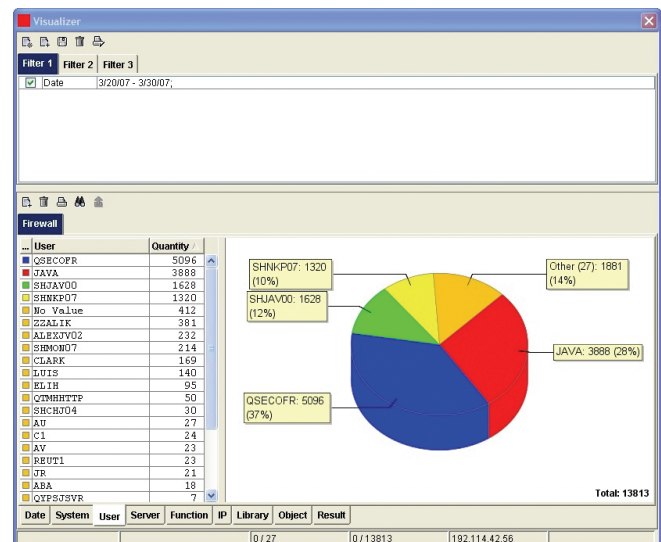
ADDITIONAL iSECURITY MODULES

Action

Action is powerful security solution that intercepts security breaches and other events in real time and immediately takes appropriate corrective action. Actions may include sending alert messages to key personnel and/or running command scripts or programs that take corrective steps.

Anti-Virus

iSecurity's Anti-Virus module offers total protection for the System i against viruses, Trojan horses, and malicious code. Anti-Virus scans all accessed files, offers comprehensive virus detection by marking, quarantining and deleting infected files, and prevents your System i from becoming an infection source. No effective security policy is complete without Anti-Virus.

AP-Journal

Automatically helps manage database changes by documenting and reporting exceptions made to the database journal. With iSecurity's AP-Journal module, every field is tracked and monitored so that a trigger may be initiated if for example, the amount of a bank loan has been modified by more than 20%. AP-Journal also provides tools and analysis capabilities to compare the changed data values and results with the previous data.

Assessment

Assessment enables you to test your System i security vulnerability within minutes, comparing a score of your current network security status, with the network if iSecurity were in place..

Authority On Demand

Authority on Demand (AOD) is a unique product for controlling user permissions while flexibly responding to the ever-changing security needs of an organization. Authority on Demand performs real-time audit of access rights in order to protect sensitive corporate assets. It reduces the number of profiles with high-level authorities, while enabling relevant personnel to easily obtain access to approved information upon demand, saving valuable time and resources. AOD also provides a Crisis ID with fire alarm-type "Break Glass" control.

Capture

Silently captures and documents user screens for tracking and surveillance, without affecting system performance. iSecurity's Capture module can run in playback mode and can be used to search within texts. Capture provides three solutions in one product - a powerful auditing solution, a regulation compliance solution, and a help-desk troubleshooting solution.

Compliance Evaluator

iSecurity Compliance Evaluator enables managers to quickly check the compliance of their systems with industry and corporate policies based on customizable user-friendly reports. It provides concise one-page reports featuring an overall compliance score, as well as specific ratings for any security-related component of System i, such as system values, network attributes and user profiles. A number of pre-defined spreadsheet plans relating to PCI, SOX and HIPAA security regulations are supplied with the product.

FileScope

iSecurity's FileScope module is recognized by System i professionals as the leading System i solution for data manipulation. FileScope provides unprecedented file editing capabilities, while adhering to the highest standards of quality, reliability and performance. File-Scope has enabled thousands of System i users to quickly and easily perform both basic file editing and advanced activities such as global and local record updates, data conversion and creation of test data.

Native Object Security

Native Object Security enables system administrators to easily define target security levels per object and object type, and to check for inconsistencies between actual and planned object security settings. The product also enables using generic object names, and includes full reporting features.

Replication

User Profile and System Value System i Replication synchronizes user profile definitions, user passwords and system values between different systems and LPARs, allowing for exceptions as needed in Production, Test or Development systems. The product also repli-cates system value definitions between systems, using "optimal" system values defined in Compliance Evaluator and "baseline" site-defined values.