iSecurity

End-to-End Security for IBM i

SEA™

Software Engineering of America
info@seasoft.com | www.seasoft.com | 516.328.7000

iSecurity Products

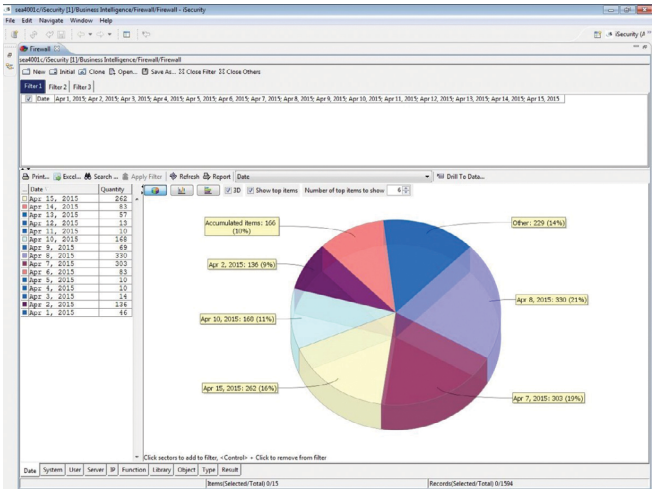
FIREWALL

Exit Point Monitoring and Management

iSecurity Firewall protects and secures remote access to and from the IBM i. It enhances native IBM i security by controlling access via known external sources and controlling precisely what users are permitted to do once access is granted. This robust, cost-effective security solution is by far the most intuitive and easy-to-use security software product on the market today.

Firewall Features Include:

- Monitoring and Management of remote activity
- Access rules can be generated and run in simulation mode for testing or in full intrusion prevention mode for active protection
- 100+ reports to meet your needs for GDPR, SOX, PCI DSS, HIPAA, and other laws, rules & regulations
- iSecurity's Visualizer business intelligence tool that provides a holistic view of your security logs for remote activity with full data mining capabilities
- Quickly reacts to security events by sending alerts, emails, executing corrective actions, MSGQ messaging, SIEM integration, texts & more



iSecurity Visualizer

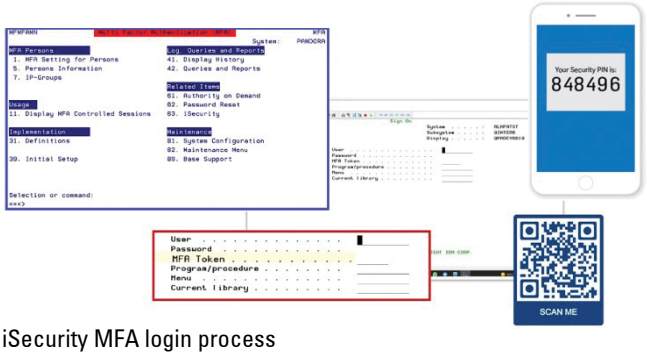
MULTI FACTOR AUTHENTICATION (MFA)

IBM i Multi Factor Authentication for Secure Access

iSecurity Multi Factor Authentication (MFA) provides increased security for users by adding another layer of identity verification to your IBM i resources. When activated, users are required to further identify themselves beyond using just a password, strengthening your systems against unauthorized access. iSecurity MFA helps you comply with governmental, regulatory and insurance carrier MFA requirements without imposing unnecessary workloads on your user base.

Multi Factor Authentication Features Include:

- Works with most leading Authentication apps available in the market.'
- Controls IBM i login activity by IP range, IP type, groups or rules
- Centralized IBM i-based controls provide MFA authentication for several IBM i servers
- Meets governmental, regulatory, industry and insurance industry requirements for MFA
- 100% Native IBM i installation, no external servers needed



iSecurity MFA login process

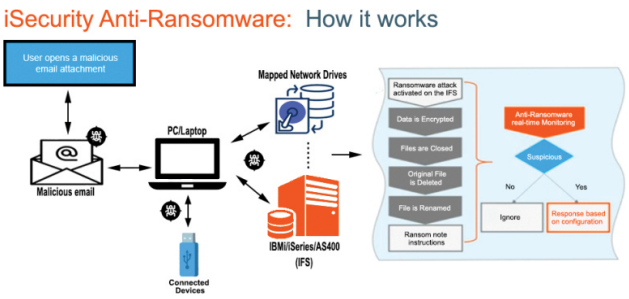
ANTI-RANSOMWARE

Protection from IFS Ransomware Attacks

iSecurity Anti-Ransomware protects against ransomware attacks that infect your Integrated File System (IFS) via mapped/shared drives. Ransomware duplicates, deletes and encrypts files on a computer system until a ransom is paid to the malicious actor. Anti-Ransomware is a proactive solution, designed to recognize and protect the system quickly and efficiently from known and unknown (zero-day) threats after malicious activity is diagnosed.

Anti-Ransomware Features Include:

- Identifies, stops, delays, and reports on ransomware attacks in real-time
- Suspends attacks by quarantining offending files/systems, while alerting administrators in real-time via QSYSOPR message queue, email or syslog
- Ransomware signature file automatically updated from the web using a proprietary signature file
- Provides a full audit trail, complete with logs and a robust query generator with the ability to export reports in spool file, PDF, HTML & Zip formats



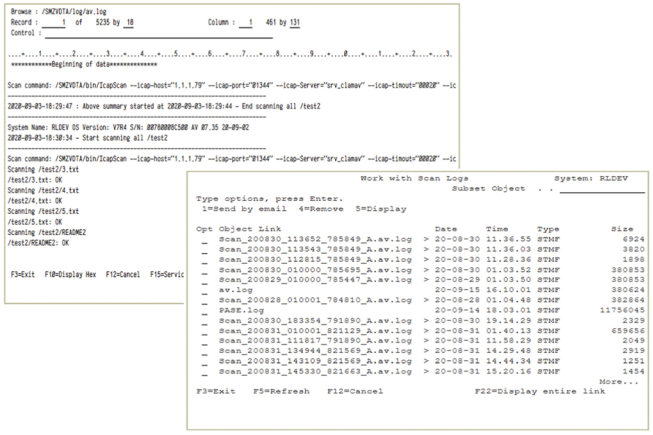
ANTIVIRUS

Virus Protection for IBM i Servers

iSecurity Antivirus offers total protection for the IBM i against viruses, trojan horses, malicious code, and other threats. Antivirus scans all accessed files, offers comprehensive virus detection by marking, quarantining and deleting infected files, preventing your IBM i from becoming an infection source. No effective security policy is complete without iSecurity Antivirus.

Antivirus Features Include:

- Provides full protection against standard PC types of viruses for files and programs used or stored on IBM i servers
- Real-time virus alerts sent as e-mail, message queues, Syslog and more
- Automatic, regularly updated virus signatures, using the Cisco ClamAV open-source engine



iSecurity Antivirus log files

SYSLOG

Enterprise SIEM Integration for IBM i

iSecurity Syslog provides real-time transmission of IBM i security event information to enterprise Security Information and Event Management (SIEM) solutions. iSecurity Syslog provides transmission of event information for standard IBM i audit types, as well as specific iSecurity Audit entry types to provide additional details beyond what QAUDJRN currently provides.

Syslog Features Include:

- Encryption of Syslog Messages sent using TLS over TCP and UDP transmission formats
- Supports use of up to 3 SIEM products in parallel
- Integrates seamlessly with other modules in the iSecurity suite to provide more extensive real-time security event transmission capabilities
- Supports "Super Fast" Transfer method—Enables sending extremely high volumes of information with virtually no performance impacts

CAPTURE

IBM i User Screen Capture, Recording and Playback

Capture is a 5250-screen tracking solution that allows you to automatically capture and save user activity as displayed on IBM i workstation screens. Capture works silently and invisibly in the background without adversely affecting system performance. Users may not even be aware that it is working.

Capture Features Include:

- Supports silent capturing, saving and playback of user (greenscreen) sessions on the IBM i
- Tracks and monitors suspicious users
- Runs a playback of all captured screens
- Includes powerful text search tools
- Real-time screen capture and storage

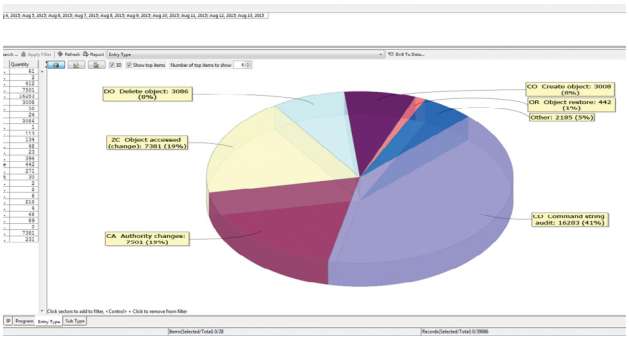
AUDIT

Compliance Monitoring and Reporting

iSecurity Audit provides real-time monitoring of system related activities and initiates responses to potential threats for the IBM i. Audit can respond to threats in real-time by generating alerts and taking immediate corrective action. iSecurity Audit gives organizations the flexibility to audit only their critical QAUDJRN events, eliminating the fear of DASD usage.

Audit Features Include:

- Integrates IBM's QAUDJRN providing a simplistic approach to IBM i auditing
- Over 200+ reports out of the box ready for SOX, PCI DSS, HIPAA and other auditing/regulatory reporting requirements
- iSecurity Visualizer business intelligence tool provides a holistic view of your security logs for local activity, with full data mining capabilities
- Actions; Ability to react to any activity by sending emails, SMS, SIEM, etc.



iSecurity Visualizer business intelligence tool

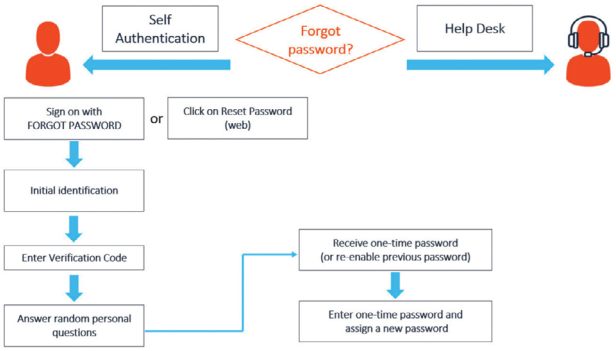
PASSWORD RESET

Self-Service Password Reset (SSPR) for IBM i

iSecurity Password Reset automates IBM i user password resets. Its self-service password reset (SSPR) capabilities allow users to securely reset locked, expired, and non-expired passwords from multiple interfaces without help desk or administrator involvement. User identities are correctly verified, password security is not compromised, and consistent efficient password reset procedures are enforced.

Password Reset Features Include:

- Allows a help desk to automatically assist users with self-authentication, without compromising security or efficiency of procedures
- Enables an enterprise to "introduce" first time use of a straightforward password control mechanism with minimum overhead
- Saves companies time, money and resources by allowing users to reset their password on their own
- Supports two-factor authentication (2FA) for user identity verification; 2FA can satisfy Multi Factor Authentication (MFA) requirements for most audit, legal, regulatory and government specifications



The iSecurity Password Reset process

REPLICATION

IBM i User Profile Synchronization

Companies are finding it mandatory to synchronize user profile definitions, user passwords and profile parameters between different IBM i systems, allowing for exceptions as needed in Production, Test or Development systems.

iSecurity Replication provides organizations with flexible user-defined IBM i replication rules for defining user profiles, passwords and parameters between systems.

Replication Features Include:

- Synchronizes user profile definitions, user passwords and system values between different IBM i systems
- Flexible user-defined replication rules for defining user profiles, passwords and parameters to be replicated
- Setting System Values to optimal value or site-defined baseline value

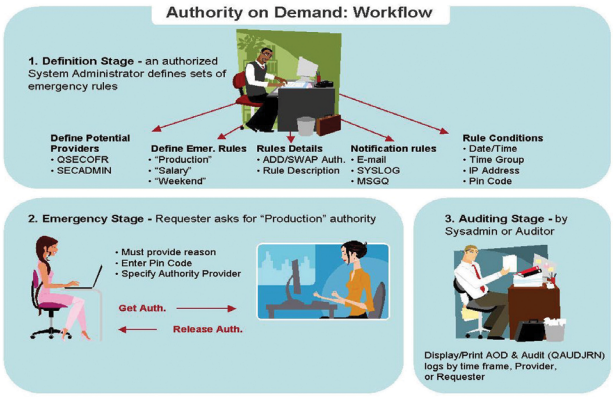
AUTHORITY ON DEMAND

IBM i User Authority Management

Authority on Demand (AOD) is a unique product for controlling user permissions while responding to the emergency security needs of an organization. AOD can provide users with temporary authorities, while fully monitoring individual user's activity when the higher authorities are active.

Authority on Demand Features Include:

- Automate granting of high-level privileges for system users
- Full audit trail of what users did while they had elevated authority
- Three levels of product usage- Full, Auditor (read-only) and Emergency
- Enables recovery from various emergency situations with minimum risk and/or error



ASSESSMENT

Free IBM i Security Assessment

With a free iSecurity Assessment, SEA provides a non-intrusive detailed report that identifies security vulnerabilities on your IBM i systems. The assessment is done from your PC without requiring command line access. After completion, you'll be able to view potential security risks in areas such as user class, user privileges, elevated authorities, password control, and more.

Assessment Features Include:

- Non-invasive assessment that installs on a PC—not your IBM i—to keep your private data private
- Identifies vulnerabilities and areas where security enhancements can be made in your organization's IBM i current environment
- Assessment is 100% free, runs in minutes, and is followed by a complimentary 30-minute consultation with an SEA Support Engineer
- Generates a detailed report on your system's security status covering numerous security categories, that can be forwarded to appropriate reviewers

COMPLIANCE EVALUATOR

Comprehensive Single-View Compliance Reporting

Compliance Evaluator easily determines the overall compliance status of your systems and, if necessary, asks IT Security personnel to investigate specific compliance related issues. iSecurity Compliance Evaluator provides managers, auditors and systems administrators a quick, yet comprehensive overview of their IBM i's level of compliance with PCI DSS, SOX, HIPAA and other government, industry or enterprise-related regulations.

Compliance Evaluator Features Include:

- Provides managers with the ability to view company-wide system compliance with industry and corporate policies
- Network-wide compliance status at a glance
- PCI DSS, SOX, etc. compliance checks
- Results in colorful Excel spreadsheet

ENCRYPTION

IBM i Field Level Encryption

iSecurity Encryption provides field-level (column) encryption for sensitive IBM i data. Encryption is the final layer of protection for business-critical data, making your data entirely meaningless to those who manage to bypass your other protection layers. Encryption also helps your IBM i stay in compliance with PCI DSS, HIPAA, GDPR, SOX, and other regulatory bodies, where sensitive parts of your data are required to be encrypted.

Encryption Features Include:

- Built-in security layers segregate keys into hierarchical systems, designed to secure your keys from hackers
- Multiple LPARs can be managed with a single key
- Sensitive fields or reference fields can be easily identified and slated for encryption
- Fundamental logs & reports provide a complete audit trail to satisfy audit and compliance requirements

COMMAND

Control & Monitor CL Commands

iSecurity Command monitors and filters commands and their parameters before they are run, enabling you to control each parameter, qualifier or element, in conjunction with the context in which it executes.

Monitoring, controlling and logging CL commands is essential for both the ongoing functions of a company as well as to comply with regulations such as SOX, HIPAA, PCI DSS and auditor-mandated policies.

Command Features Include:

- Total control over system and user defined CL commands, regardless of how the CL command was entered
- Provides the ability to control CL commands, their parameters, origin, context (i.e., the program which initiated the CL command) and the user
- Command execution options including Allow, Allow with Changes and Reject
- A comprehensive log, proactive alerting and integration with SIEM systems

AP-JOURNAL

Server Application Security & Business Analysis Solution

iSecurity AP-Journal is an Application Security and Business Analysis Solution for the IBM i. AP-Journal protects business-critical information from insider threats as well as external security breaches. It keeps managers closely informed of important changes in their business-critical data and streamlines journaling procedures.

AP-Journal Features Include:

- An application security tool that monitors field level, before & after, changes in data
- See who made changes, at what time, and from which application
- Get alerts and take action when specific fields are modified past certain thresholds
- Copy over critical business information from your journals, saving disk space by retaining the critical information necessary for compliance.

SAFE UPDATE

Enforces Authorized File Editor Usage for Data Updates

iSecurity Safe Update monitors and ensures that data updates are only made by authorized programs. It enforces federal and other regulatory requirements prohibiting users from data updates using unauthorized & unsecure programs, such as DFU, Start SQL (STRSQL) commands or third-party file editors. It can also restrict unauthorized file editor usage for *ALLOBJ users. When data updates must be updated using unauthorized file editors, Safe Update can provide workflow ticket authorization where temporary approved use of an unauthorized file editor can be assigned and documented.

Safe Update Features Include:

- Provides whitelists of approved programs or a blacklist of programs that are not allowed
- Monitors and protects data updates, according to the program used
- Ensures dangerous file editors such as DFU and STRSQL are not used, even when the user possesses *ALLOBJ authority
- Supports "Super-Fast" Transfer method—Enables sending extremely high volumes of information with virtually no performance impacts

CHANGE TRACKER

Automatic Program & Object Change Identification

iSecurity Change Tracker automatically monitors and logs object changes made to IBM i production libraries at both the source and object levels. Change Tracker relies solely on actual library updates.

Change Tracker Features Include:

- Based on the QAUDJRN system journal, provides a robust and comprehensive solution for IBM i systems that can't be bypassed
- Works in real-time to automatically record every revision and collect all information relevant to the modifications made, including object attributes, source code, changes to file structures and more
- Full tracking of all change details, including creation, deletion, modifications, etc., ensuring total accountability and transparency
- Built-in report generator and scheduler include a set of queries tailored to specific auditing needs
- iSecurity Change Tracker gives auditors access to all the data they require, such as who made changes, why, when and from which IP address

NATIVE OBJECT SECURITY

Object Security Management

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

Native Object Security Features Include:

- 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
- Set current security status to the planned definitions
- Plan security definitions using generic names, reducing the number of rules required to maintain

About SEA

Established in 1982, Software Engineering of America has built a worldwide reputation as a leading provider of data center software solutions. With products licensed at over 10,000 data centers worldwide, SEA's customers include 9 of the fortune 10 and over 90% of the Fortune 500.

For a Free Trial Contact SEA Today
Call: 516.328.7000
www.seasoft.com

SEA™

Software Engineering of America
info@seasoft.com | www.seasoft.com | 516.328.7000