RAZ-LEE iSecurity

Solution Catalogue

2025

Download

Keep yourself always Up to Date with the latest from **Raz-Lee iSecurity** by Downloading the Newest version of our Solution Catalogue.

Table of Contents

About Us

Raz-Lee Security is a leader in security and compliance solutions that guard business-critical information on IBM i servers.

Inspired by the power of working together, Raz-Lee develops business solutions that make the IBM i the most secure place in your organization. We protect hundreds of clients from cyberattacks each day. We work hard to ensure that you are protected with the most state-of-the-art technology for your IBM i.

"We are committed to providing the best and most comprehensive IBM i compliance, auditing and security solutions."

Shmuel Zailer

iSecurity Suite

iSecurity suite comprises solutions that help your company safeguard and monitor valuable information assets against intrusions.

Our state-of-the-art products protect your files and databases from both theft and extortion attacks. Our technology provides visibility into how users access data and applications, and uses sophisticated user tracking and classification to detect and block cyberattacks, unauthorized users and malicious insiders.

With exclusive IBM i security focus, Raz-Lee has achieved outstanding development capabilities and expertise. We work hard to help your company achieve the highest security and regulatory compliance.

Anti-Ransomware

Advanced Ransomware Threat Protection for IFS

Detects high volume cyber threats deployed from an external source, isolates the threat, and prevents it from damaging valuable data.

- **iSecurity Anti-Ransomware** has the ability to work multithread as IBM recommends it. It results in having a single job for all the user-shares, rather than a job for each one – If you have 100 users and each has 3 shares = 300 jobs.
- Our **Sandbox** will reduce false alert to virtually zero. Files that are suspected to have been compromised, are passed to a sandbox which tries to run them. If they run in the sandbox, they are not compromised, and vice versa. The Sandbox runs in the IBM i. No additional hardware/software is needed.

Antivirus & ICAP

iSecurity Antivirus is a Total Protection Solution

ClamAV engine implementation brings

- A database of over eight million virus signatures
- Signatures are continually updated
- Recent, leading-edge technologies
- Improved scanning based on up-to-date algorithms
- Significantly faster scanning of PDF, ZIP and other file types
- Reduced load time of the signatures

iSecurity implementation brings

- On-Access Scanning, On-Demand Scanning and Only-New Scanning
- Cannot be disabled by any known virus keeping the server protected without interruption
- Runs Local and natively at the IBM i

What is Only-New Scanning?

Scan for viruses is, by definition, CPU intensive. There are 8,600,000+ signatures that must be compared to the contents of the object. Beyond this there is the heuristic scan which search for zero-day viruses. **iSecurity Antivirus** marks internally objects that were scanned. This happens on both On-Access and On-Demand scans.

ICAP Client Key Features

Raz-Lee Security has enhanced iSecurity Antivirus with the addition of the **ICAP Client**. Virus scans tend to be CPU-intensive because they scan millions of possible virus signatures. Using ICAP ensures that your IBM i is always protected without a performance drop. Scan time is faster – by twenty times in some tests. The portion of the IBM i CPU that would have been used for virus scanning becomes available for other purposes.

Antivirus for AIX

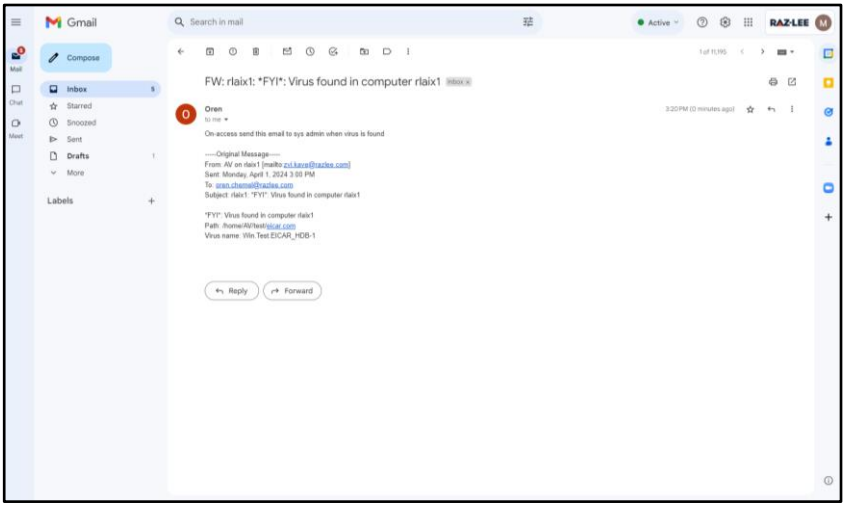
Is AIX affected by Viruses?

Although the **AIX** doesn't run .exe files, it can house infected files – where they can wait, silently and deadly, until someone on the network transfers and opens that file on their PC.

Main Advantages

- Scan On-Access, On-Demand and Only-New
- Cannot be disabled by viruses
- Improved Memory and Processor usage, preventing unnecessary file's scanning if there is no change since last scan
- Command-line scanner
- Regularly updated database from **ClamAV** and Raz-Lee
- Database updater with support for digital signatures
- Built-in support for zip, gzip, jar, and tar files
- History Log for review and analysis
- User-friendly Web Interface & Native Interface

Email Notifications

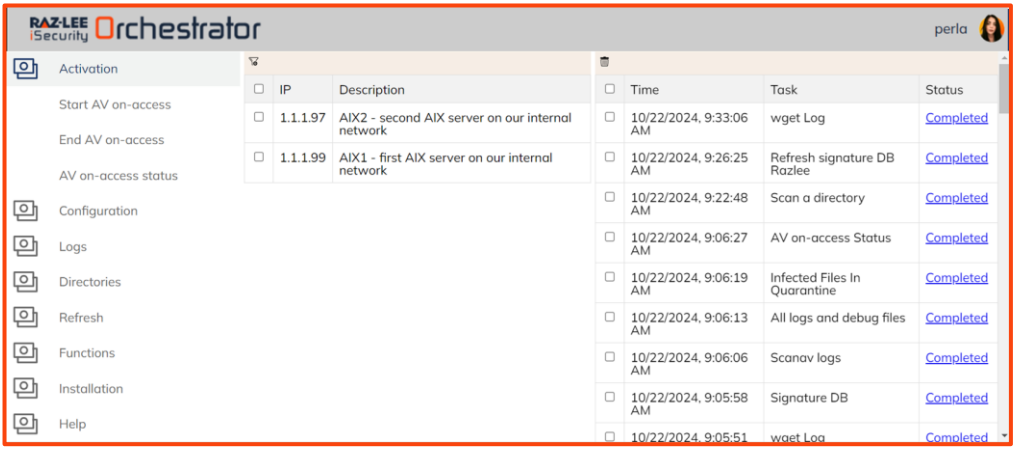


Orchestrator

Simplify Server Security Management

The New iSecurity Orchestrator makes automation and orchestration tasks easier for your iSecurity Products on the **AIX** Servers.

As a first step, it manages several AIX servers at once, and entirely the AV module for **AIX**, from a simple Web Interface.



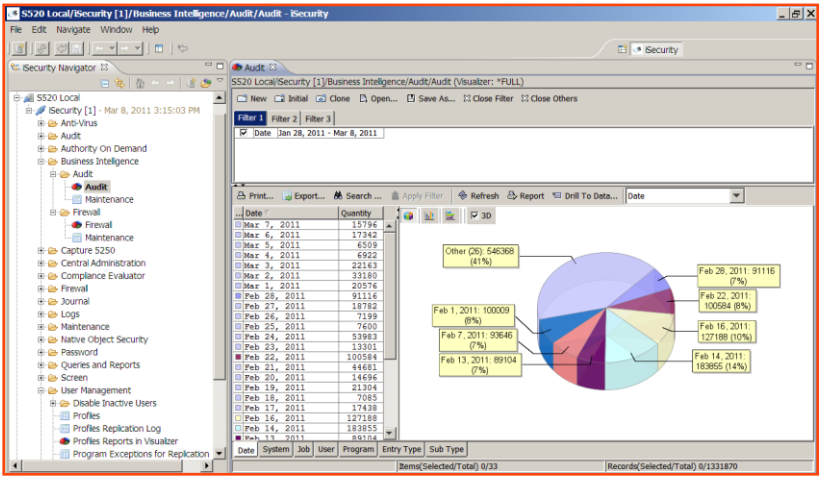
iSecurity Orchestrator helps you to:

- Install / Uninstall iSecurity Modules.
- Activate / Deactivate iSecurity Modules.
- Update AV Signature.
- Start/End On Access Scan.
- Scan Directories.
- Send Files to Admin.
- Configure Directories for DB, Logs, Etc.
- View Logs.

Audit

IT Audit at IBM i

Auditing determines whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals. Our **Audit** module examines events in real time triggering alerts and other responsive actions to potential threats. Our **Up-to-Date GUI** features a user-friendly interface for working with the large, often confusing number of system values and parameters.



iSecurity Audit's enhanced reporting possibilities

Audit offers the most powerful and flexible reporting features available today. It includes more than eighty ready-to-run queries and reports.

- **Query Wizard** allows users to create reports without programming.
  - Queries employ robust selection criteria such as AND/OR, equal/not equal, greater/less than, like/not like, included in list, etc.
  - Fully **Customizable Reports**.

Action

iSecurity Action Benefits

It is easy to define rules and actions with the Action Rule Wizard feature. Based on one or more parameters associated with a particular event, selection parameters include user, date, time, job, workstation, library, object name, IP address, command, job name, etc.

- Rule criteria use many different Boolean operators such as: equal/not equal, greater than /less than, like/not like, “contained in list”, “starts with”, even Group/Item. For example: “**NE ALLUSERS/MANAGER**” would filter events which were initiated by a non-manager!
- **Action** includes additional security features such as automatic disabling of inactive users, restricting user access during planned absences and control over creating and running programs that use adopted authority.

Real-Time Detection

Action real-time detection continuously monitors the system for a wide variety of security and other system events, including:

- Events detected by **Audit** real-time auditing
- Transactions detected by **Firewall** network security rules
- Viruses detected by **Antivirus**
- Suspicious data changes by **AP-Journal**
- Active job status and checking for jobs that are not active including current system and memory pool status

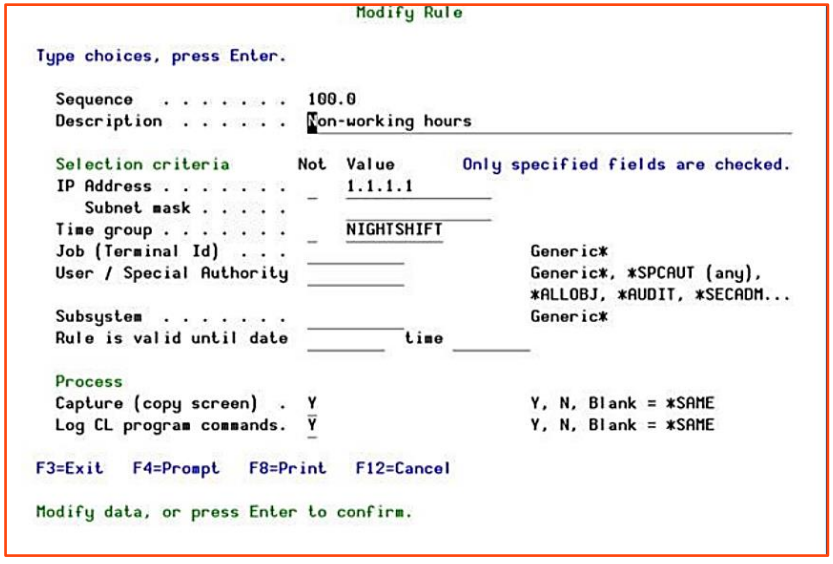
Any Way to have a Visual Track of User's activities?

iSecurity Capture solves this problem by complementing journals and reports with a visual audit trail of user activity. Capture shows exactly what users are doing and when they are doing it! Screen capture sessions are initiated as required and are retrievable using an intuitive process featuring flexible scrolling and a powerful free-text search engine for locating the captured data screens and logs.

iSecurity Capture Capabilities

The Capture Menu also provides commands for displaying the job log and the Audit log entries related to the particular screen and capture session.

You can even access the DSPJOB command and print the screen directly from the Capture Menu.



Capture works both as a stand-alone product and as a module fully integrated into the iSecurity Suite.

Change Tracker

Advantages of using Change Tracker

Our solution iSecurity Change Tracker is dedicated to automatically monitoring and logging object changes made to production libraries at both the source and object levels.

- Since **Change Tracker** relies solely on the actual updates within a library, no manual intervention is required.
- Auditors have access to all the data they require, such as who made changes, why, when, and from which IP
- Change Tracker is dedicated to **automatically monitoring and logging object changes** made to production libraries at both the source and object levels.
- Built-in Report generator and Scheduler includes a set of queries tailored to specific auditing needs

Comparison between Our Solution and standard CMS

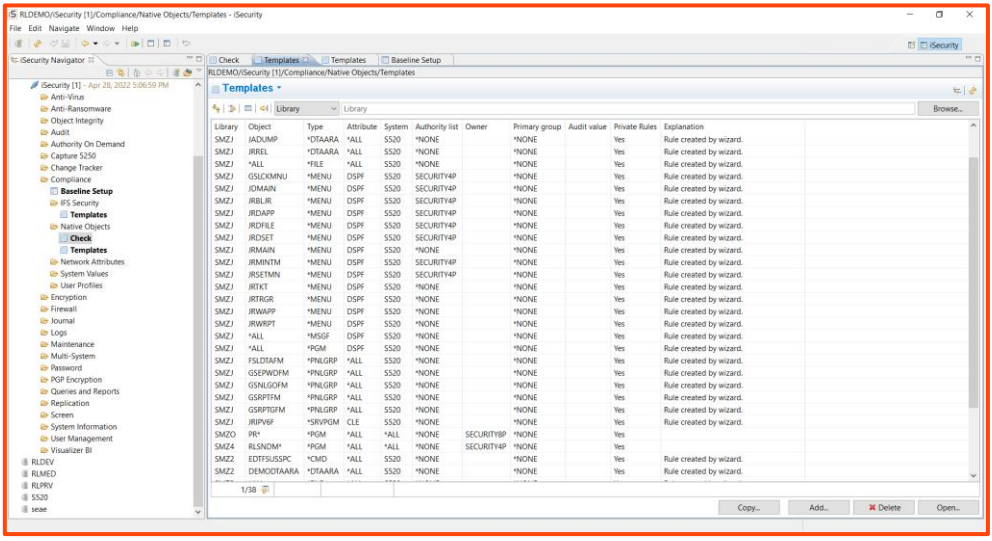
Activity	iSecurity Change Tracker	CMS
Track Activity	Automatic	Human Responsibility
Full Tracking	Yes	No
Implementation Time	Immediate	Minimum over a month
Auditor Interaction	By Email	None

Benefits of using **Change Tracker** are many, but the best is that your company will immediately see a noticeable difference in auditors' productivity.

Compliance Manager

Security levels per Object

The challenge of securing both Native and Integrated File System (IFS) OS/400 objects is the basis for all IBM i security due to the unique object-based architecture.



Helps to secure IFS and Native Object security

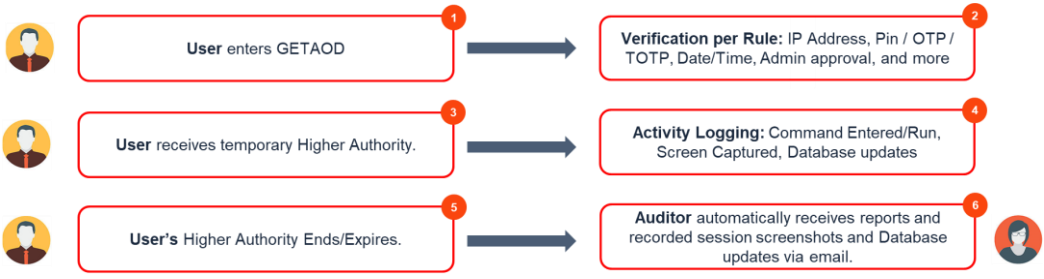
iSecurity Compliance Management solution helps system administrators to painlessly secure IFS and Native object security.

- Reduces non-compliance with company defined security policy settings
- Assures settings for object security are not changed and can be combined with iSecurity Audit
- Assures audit and compliance that the data is secure

Authority on Demand

Elevate Authorities at a Glance

iSecurity Authority on Demand saves valuable time and resources, enforces segregation of duties and enables relevant personnel to obtain access to approved information when needed. Its real-time audit of access rights protects sensitive corporate assets and significantly reduces the number of profiles with powerful special authorities.



iSecurity Authority on Demand simplifies the process of granting special authorities when necessary, and incorporates easy-to-use reporting and monitoring mechanisms to ensure that this extremely sensitive and potentially dangerous capability is not misused.

It also enables recovery from different types of emergency situations with minimum chances for human error.

Rule Definition to Elevate Authority

iSecurity Authority On Demand elevates authority based on predefined rules to help System administrators to make it easy and have total control of every authority given in special cases.

- Who can get an Elevated Authority?
- Which Level of Authority this User can get?
- For How Long this Level will stay before going back to his previous Authority Level?

Multi Factor in One Single Step

Multi Factor Authentication (MFA) helps organizations meet compliance standards and improve the existing security environment on IBM i. It requires a user to verify his or her identity with two or more credentials before gaining access to sensitive systems and data. Used for achieving and maintaining compliance with the leading industry regulations, such as PCI-DSS. Lately it has also become a necessity to qualify for cyber insurance.

MFA significantly reduces the risk of system penetration, up to a remarkable 99%

iSecurity Multi Factor Authentication does it simple inside the IBM I, and as a part of the initial program, prompting for MFA at sign-on. We do not need to use multiple login stages; One step is enough. iSecurity MFA is powerful solution to enable **Secure Sign On**.

Authentication Freedom

MFA works with every Authenticator App available in the Market.

We can use ANY Token generator, such as Google Authenticator or by any other compatible hardware device.

Controls more than Sign-On

One **MFA** is good enough for all of a Person's activities, from the same IP, for a specified time.

Including: **Secure Sign ON, FTP Server, REXEC, FTP Client, ODBC, File Server, Remote PGM/CMD, DDM/DRDA.**

Password Reset

iSecurity Password Reset makes it Safe and Simple

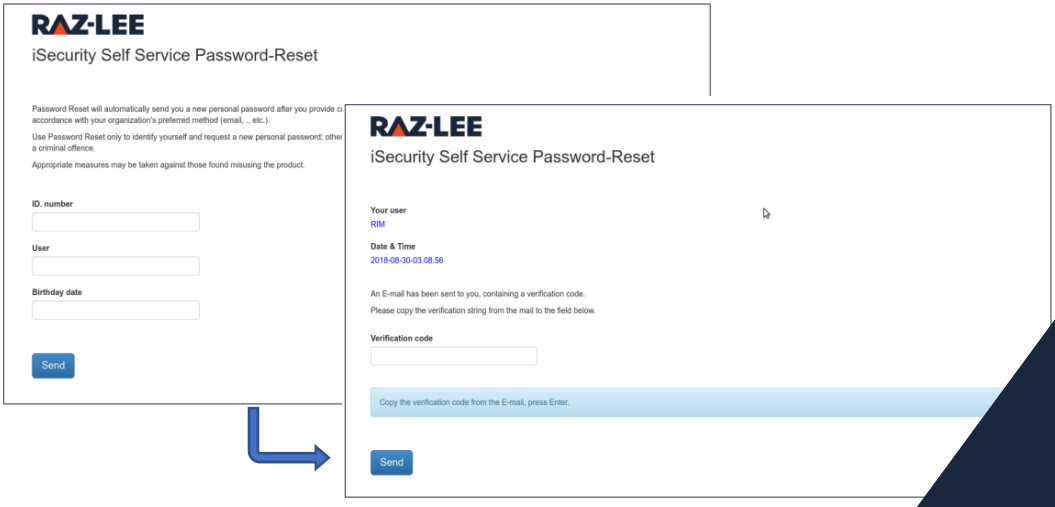
With all the personal information available on Facebook, LinkedIn, and unofficial web resources, private questions are not as safe as they once were.

- iSecurity Password Reset, part of the iSecurity suite, is a unique product, designed on the principle that restoring sensitive information such as passwords without disclosure of verification questions entered by the user is more secure than any other solution against hackers.

- Secured by three levels of authentication – personal identification, verification by intermediate one-time code, and only then personal questions

Web Interface

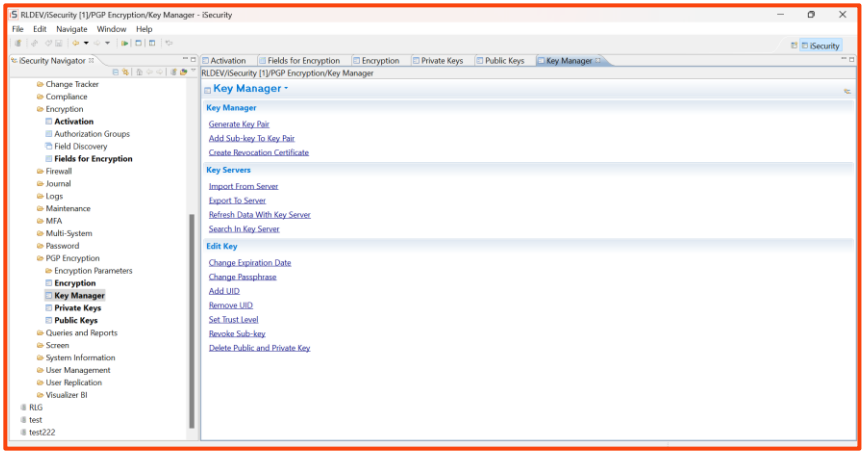
iSecurity Password Reset features a user-friendly, Web-based in addition to the traditional green-screen interface.



Open PGP Encryption

Using the Open PGP Standard

- **Open PGP Encryption** uses a combination of methodologies to keep data secure, multiple encryption algorithms, including AES and TDES
- Only users possessing the correct private key can decrypt and open the protected files.
- Also built to support multi-site, multi-LPAR organizations
- Key management capabilities, enabling users to create, import, and export the keys needed to encrypt and decrypt files



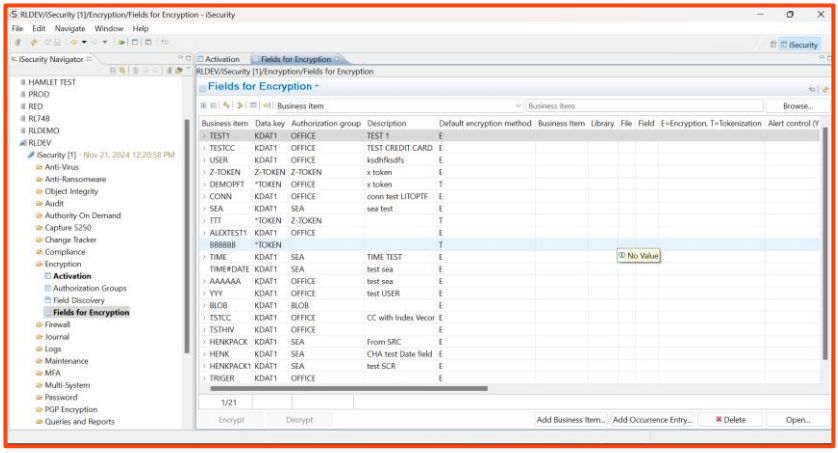
CLOUD Benefits

iSecurity Open PGP Encryption allows you to encrypt files that are transferred to the cloud or to encrypt files on the cloud that are to be transferred to on-premises. Files can be automatically encrypted and transmitted to recipients while received files can be automatically decrypted by user applications.

FIELD Encryption

Compliance and Encryption

Encryption is also the way to ensure that sensitive data is presented in the way that suits the user, and the circumstances. Those who are entitled to access your data will see the data in clear text, masked, scrambled, or not see it at all, as appropriate. **PCI-DSS, HIPAA, GDPR** and other regulatory bodies require encrypting sensitive parts of the data.



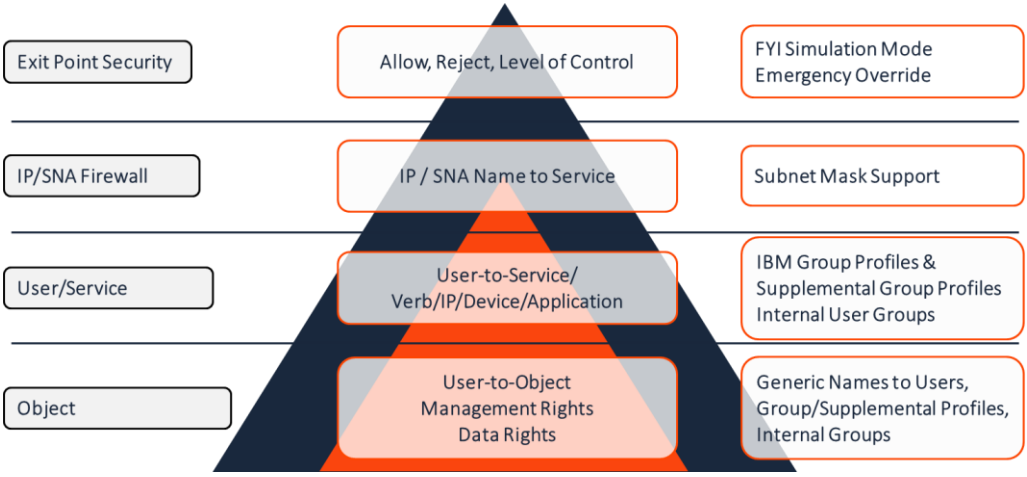
iSecurity Field Encryption Keys

Supports a single Key Manager / single Token Manager for multiple Data Managers.

- Built to support also multi-site, multi-LPAR organizations
- Local Master Key protects an Organization Key.
- Organization Key protects the Key Encrypting Keys (KEK).
- KEK is used to protect the Data Key.
- Data Keys encrypt data.
- Organization Key is entered once on each LPAR (including HA).
- Master, KEK and Data Keys can & should be periodically modified.
- There is no way to see or access any actual Key Value.

Firewall

Layered Security



Our Solution

iSecurity Firewall protects and secures all types of access to and from the iSeries, within or outside the organization, under all types of communication protocols (**TCP/IP**, **FTP**, **Telnet**, **WSG**, **Passthrough**, etc.).

iSecurity Firewall is a comprehensive, all-inclusive intrusion prevention system that secures every type of internal and external access to the IBM i server. It enables you to easily detect remote network accesses and, most importantly, implement real-time alerts.

Best-Fit Algorithm minimizes throughput delays by rapidly and efficiently applying security rules.

Rule Wizards dramatically simplify security rule definition
State-of-the-art intrusion detection guards against hacker attacks.

Command

Reacting to CL Commands

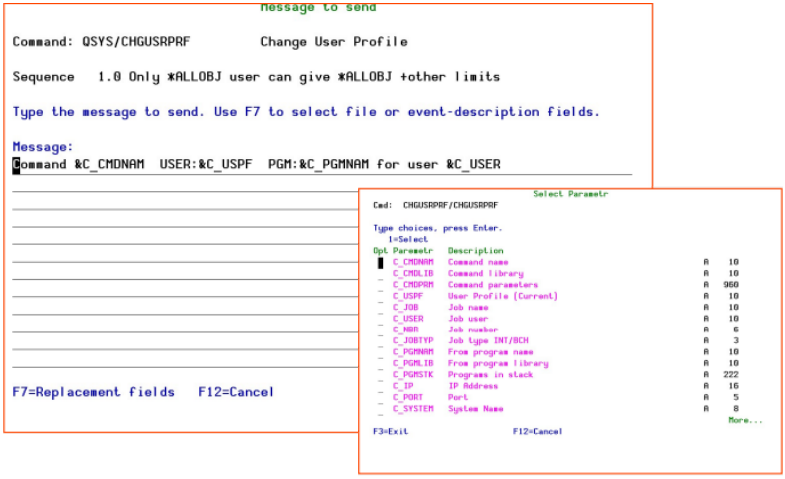
During CL command processing, iSecurity Command is able to:

- Allow normal CL command processing
- Allow CL command processing after modifying parameters or parts of parameters
- Execute a different CL command
- Reject the CL command

And, as iSecurity Command is totally integrated into the infrastructure of products in the iSecurity Suite, it can send real-time alerts as event-specific e-mails or SMS, Syslog and other forms of messages. Command can even trigger the execution of a CL script.

Real Time Alerts

Sends real-time alerts as event-specific e-mails or SMS, Syslog, MSGQ messages. iSecurity Command Can even execute CL script.



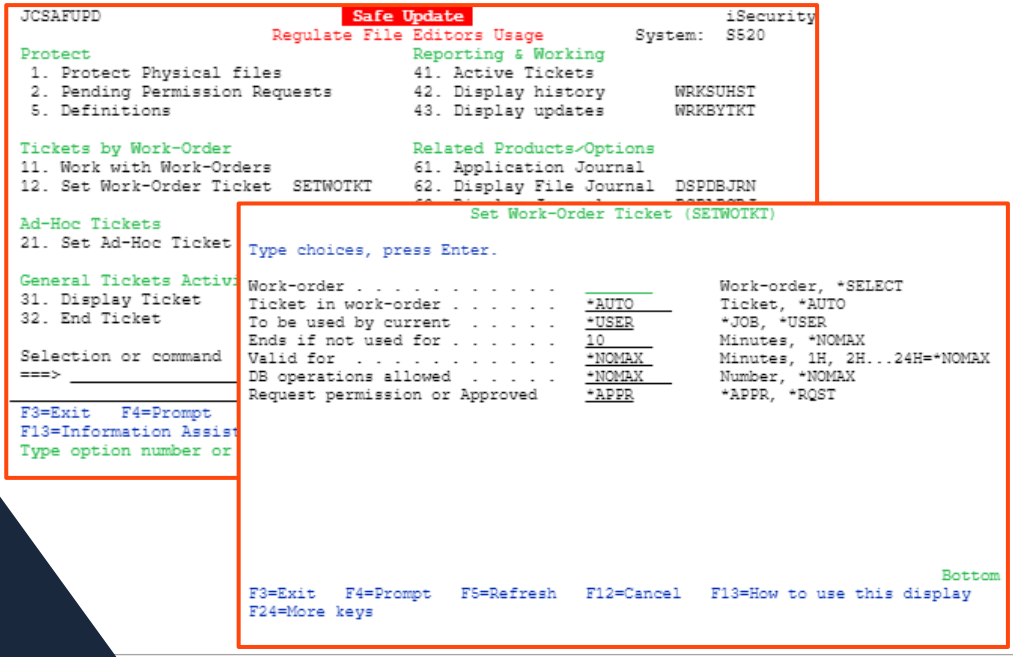
Safe Update

Adding a New Security Layer

iSecurity Safe-Update's new security layer ensures that only authorized programs are used to update business critical files. Implements a workflow that consists of work orders, created by management, that specify who can work with the data, the reason for the work, and the limited time during which the work order is valid.

Based on the work order, the specified user can then open a ticket and perform the requested updates interactively or in batch. All work under the tickets is logged, even if the data files themselves are not journaled.

If an unauthorized update is attempted, a window appears requesting the entry of a ticket.



Assessment

Get your Security Assessment in minutes!

iSecurity Assessment checks your systems' security-related definitions and values and reports – in minutes – the exact strengths and weaknesses of your computer's security policies.

iSecurity Assessment is a Windows-based program for in-depth analysis of the full scope of the IBM i (AS/400) security strengths and weaknesses, pinpointing the security risks which should be addressed. The output is a detailed report, grading each facet of IBM i security, with full explanations.

Security Scores and Recommendations Summary

Section	Score	Explanation
3.1 Sign-on Attributes	32	The computer's settings are invalid and pose immediate security threats.**iSecurity User Sign On functionality should be implemented.**
3.2 Use of Adopted Authority	0	Only the actual usage of adopted programs can be analyzed.**iSecurity Firewall can locate all programs using Adopted Authority and also allows for approving/disapproving Adopted Authority for such programs.**
3.3 Unattended terminals	0	Computer settings are faulty.**Avoid a possible security threat to the network by implementing iSecurity Screen.**
3.4 Miscellaneous Sign-on	66	Some miscellaneous sign-on values are in accordance with industry standards. However, the computer's scores are borderline and should be reviewed.
3.5 Password Control	13	Computer settings are faulty and open to password-related security threats.**iSecurity Password should be implemented.**
3.6 Activation of Network Protection	15	The computer is not protected and therefore may have a severe security threat.
3.7 Auditing System and User Activities	83	Most of the computer's auditing policies are in place and require only minimal revisions.**iSecurity Audit should be implemented.**
3.8 Users Class	50	This number is too high for proper security; review security policies and reduce the number of power users.**iSecurity Audit should be implemented.**

SIEM & DAM Support

Integration at its Fullest

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems. Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS virus detected, malicious network access, and more.

Main Advantages:

- Sends Syslog messages **in parallel to up to 3 SIEM** products.
- Transmission is supported via UDP, TCP or TLS (encrypted channel).
- Support in all iSecurity solutions enables infrastructure-related alerts and field-level application alerts on unauthorized data changes or access.

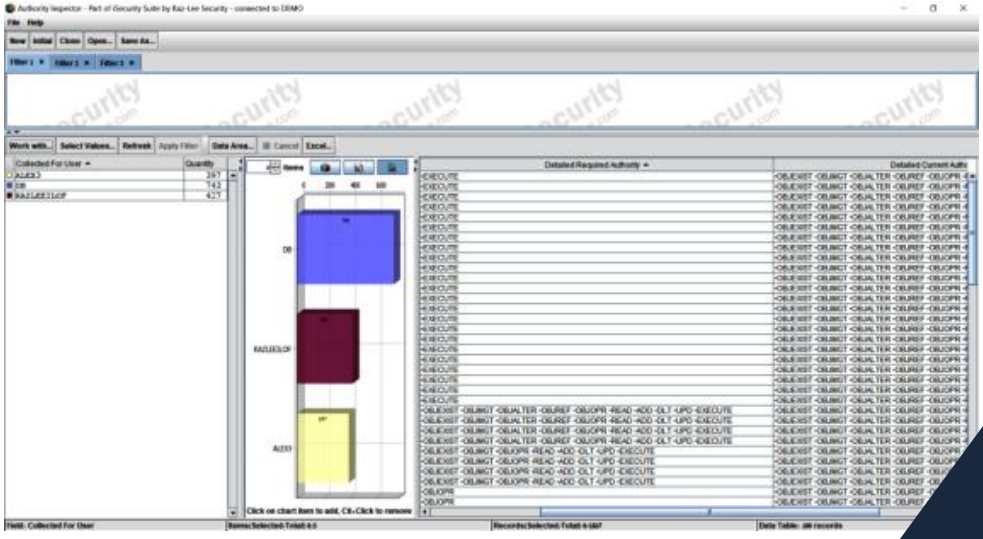
Authority Inspector

Identifying the Breach

The **iSecurity Authority Inspector** is installed on a PC while processing data pulled off the IBM i. And identifies this security breaches. There are various methods to confine authorities:

- Adopted authority
- Authorization lists
- Group Profiles

The **Authority Inspector** supports the user regardless of the specific method in use. It enables comparison of utilized authority versus the required ones, and supports selection of the method. Also provides information on the minimal authority to be given at each stage and the frequency of testing authorities.

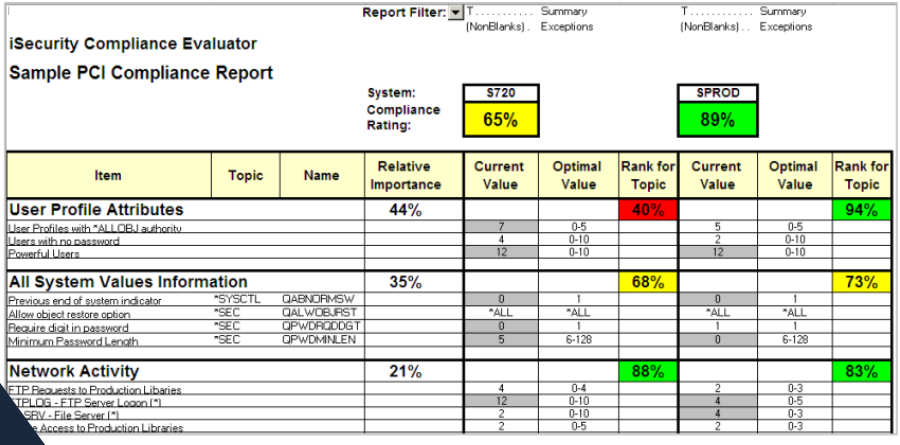


Compliance Evaluator

Single-View Overall Compliance Reports

Managers, auditors and administrators need a quick yet comprehensive view, analyzing the compliance of their systems with **DORA, NIS2, PCI, SOX, HIPAA** and other regulations.

With **iSecurity Compliance Evaluator**, managers can easily produce any number of compliance checklists, choose the contents and structure of the result, and attach different weights to each item. iSecurity Compliance Evaluator can be scheduled to run automatically, and its results can be emailed directly from Power i to the relevant person.



Report Filter: T..... Summary (NonBlanks) . Exceptions T..... Summary (NonBlanks) . . Exceptions

iSecurity Compliance Evaluator

Sample PCI Compliance Report

System:	S720	SPROD
Compliance Rating:	65%	89%

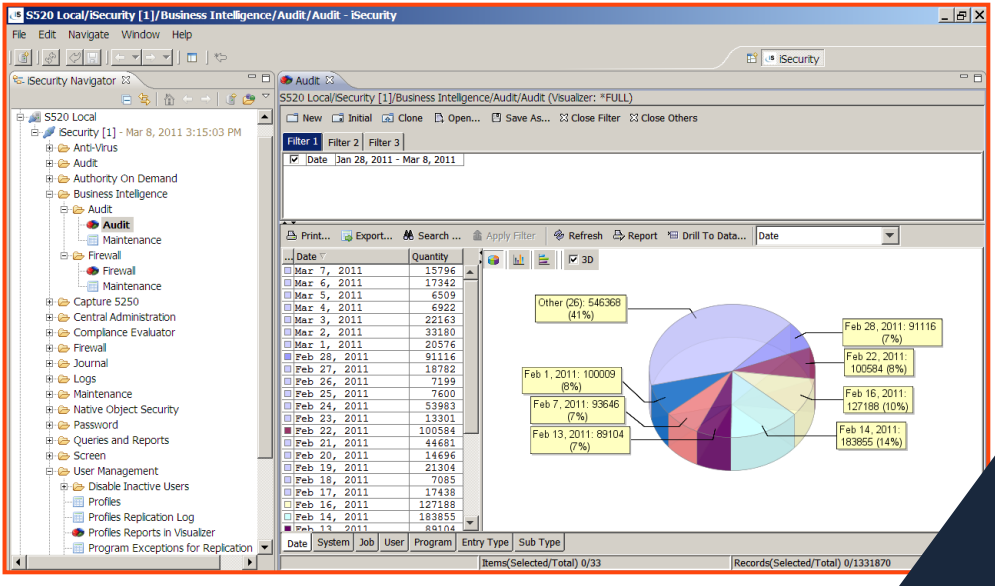
Item	Topic	Name	Relative Importance	Current Value	Optimal Value	Rank for Topic	Current Value	Optimal Value	Rank for Topic
User Profile Attributes			44%			40%			94%
User Profiles with *ALLOBJ authority				7	0-5		5	0-5	
Users with no password				4	0-10		2	0-10	
Powerful Users				12	0-10		12	0-10	
All System Values Information			35%			68%			73%
Previous end of system indicator	*SYSCTL	QABNORMSW		0	1		0	1	
Allow object restore option	*SEC	QALWOBJRST		*ALL	*ALL		*ALL	*ALL	
Require digit in password	*SEC	QPWDRQDDGT		0	1		1	1	
Minimum Password Length	*SEC	QPWDMINLEN		5	6-128		0	6-128	
Network Activity			21%			88%			83%
FTP Requests to Production Libaries				4	0-4		2	0-3	
TPLOG - FTP Server Logon (*)				12	0-10		4	0-5	
SRV - File Server (*)				2	0-10		4	0-3	
e Access to Production Libraries				2	0-5		2	0-3	

Visualizer

Advantages of Drill Down Data

iSecurity Visualizer is an Eclipse-based product which makes security investigation and analysis a snap. Simply clicks to select filters and a 3D pie chart, or similar graphics will show the exact breakdown by criteria.

- Exceptionally fast “slice and dice” technology to show graphics
- Report generator creates statistical reports with rich graphics
- Automatically associates all significant data elements
- Easily filter data to “drill down” into log files
- Set up multiple filter criteria and reuse as necessary
- Operates with other iSecurity products and with any SQL table



Business Intelligence Traceability

With its unique technology, iSecurity AP-Journal logs database access (READ operations) directly into the journal receivers.

- **iSecurity AP-Journal** report data can include key fields, description fields and modified fields (highlighted) being able to see before and after the value changed.

- By providing a timeline report of all changes relating to application data, **iSecurity AP-Journal** reduces unauthorized activity and enables users to meet regulatory requirements.

- **iSecurity Ap-Journal** issues real-time alerts to inform managers of any changes in application databases or unapproved access to critical data.

- **iSecurity AP-Journal** can answer complicated questions like:

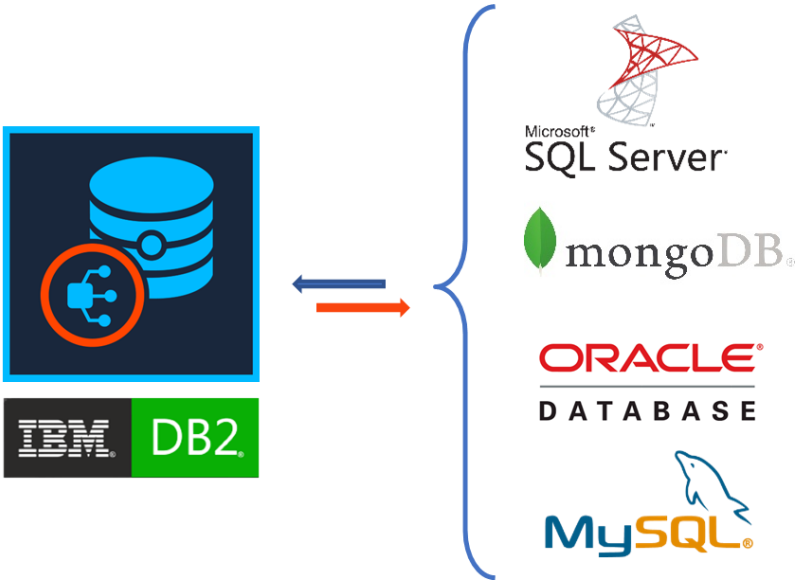
    - Who worked on the SALARY file during non-standard business hours, and accessed employees whose salaries exceed $5,000 monthly?
    - Provide John with a timeline report of all changes made to his MORTGAGE (covering the dozens of files in the MORTGAGE application), during the past 25 years.
    - Send an SMS message and e-mail to the Security Officer when the PRICE_OF_ITEM changes by more than 4%.
    - What changes to the hospital's PATIENTS file were made via utility application DFU?

And so on...

DB-Gate

Transparent Access to any Database

As your enterprise applications expand in database requirements and complexity, so does the need to access multiple databases from your main application server.



iSecurity DB-Gate empowers IBM i customers with exciting data access capabilities, based on Open Database Connectivity (ODBC), employing standard IBM i facilities to enable fully database-transparent access to remote systems.

- Using native SQL on the IBM i, users can connect to specific files on DB2 and non-DB2 remote databases without any special hardware or software on the remote DB
- From interactive STRSQL and from any standard program in RPG, COBOL, C, or other languages, access is now more natural.

Efficient and Secured File Editor

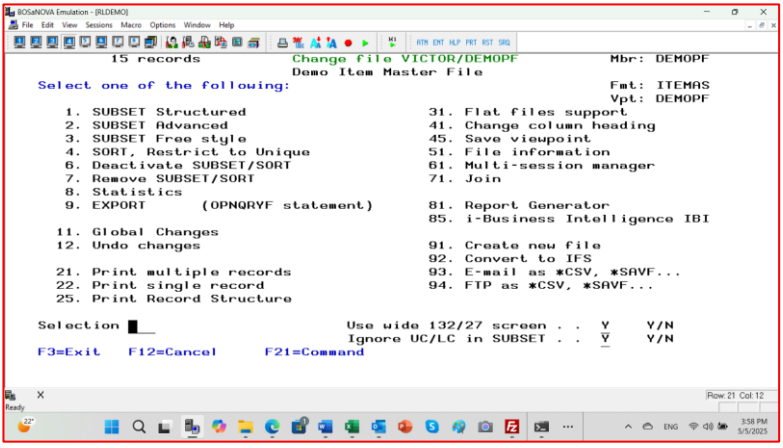
Information retrieval and manipulation methods such as DFU or QUERY, require compilation and definition steps. Unlike SQL**, iSecurity FileScope** enables modifying database requests on the fly, performs record updates under your visual control, holds complete control over printing of reports and supports UNDO for any change!

Edit files at IBM i

The primary focus of **iSecurity FileScope** is to enhance general user productivity and at the same time provide super user level tools to those who can benefit from them:

- System Administrators
- DBAs

Enabling thousands of iSeries users worldwide to quickly and easily perform file editing functions as well as advanced activities such as global and local record updates, data conversion and creation of test data.



iSecurity Suite Map

Cyber Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Client/Server
  - **Antivirus** for **AIX**
  - **Orchestrator AIX**

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Network Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- **Field Encryption**
- **Open PGP Encryption**

Database Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** QAUDJRN, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

RAZ-LEE
iSecurity

Visit our Website

www.razlee.com