SEA™ SOFTWARE ENGINEERING OF AMERICA®

User Driven Software Solutions Since 1982

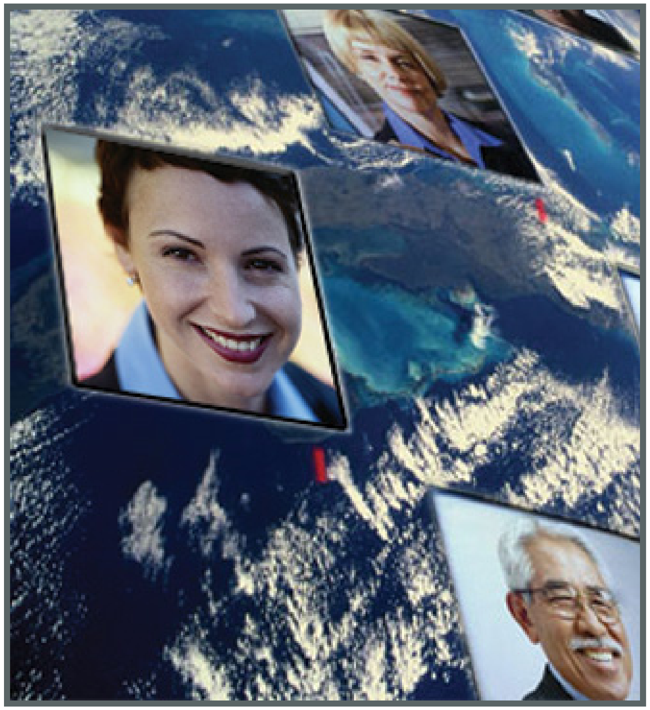
iSecurity

System i Security Solutions

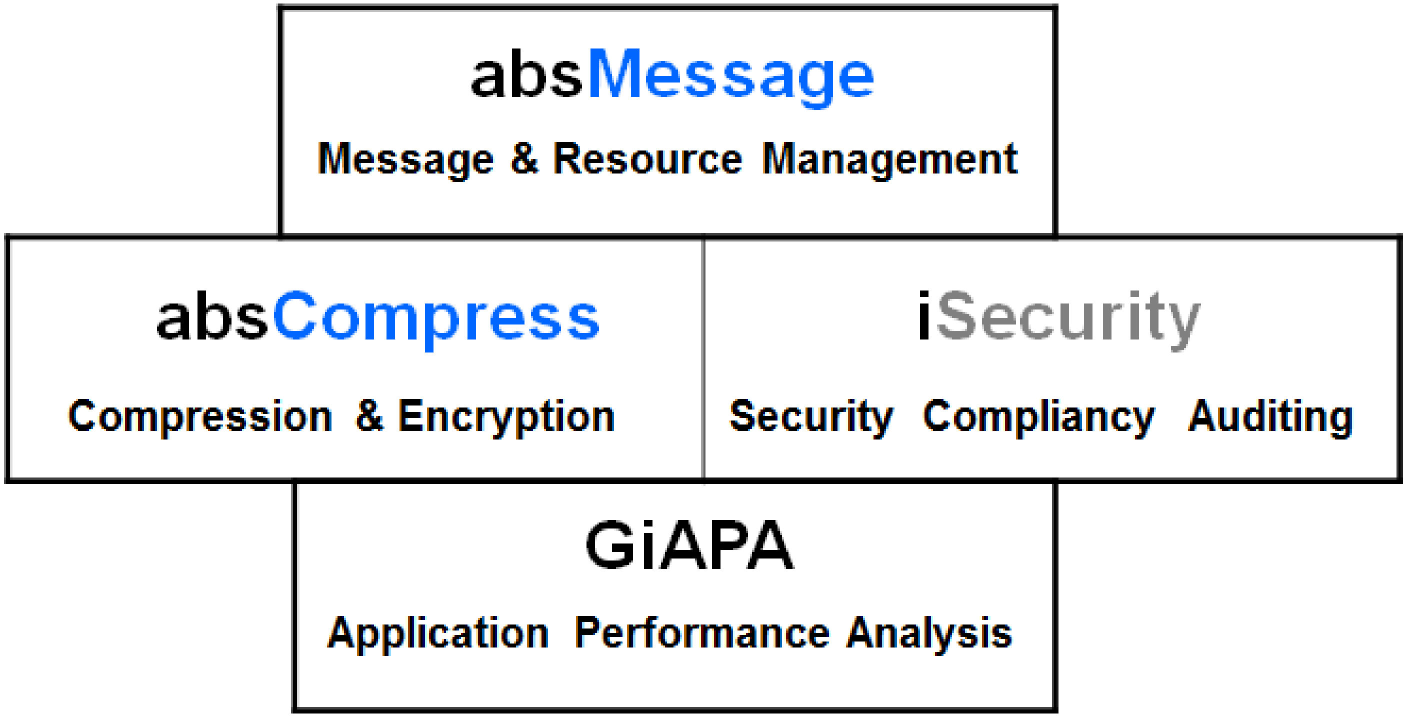
Company Overview

SEA™ SOFTWARE ENGINEERING OF AMERICA®
User Driven Software Solutions Since 1982

Company Overview



- 30 Years of Excellence
- 9 of the Fortune 10
- 85% of the Fortune 500
- Licenses in over 50 Countries



absMessage

Message & Resource Management

absCompress

Compression & Encryption

iSecurity

Security Compliancy Auditing

GiAPA

Application Performance Analysis

SEA™ SOFTWARE ENGINEERING OF AMERICA®
User Driven Software Solutions Since 1982

Company Overview

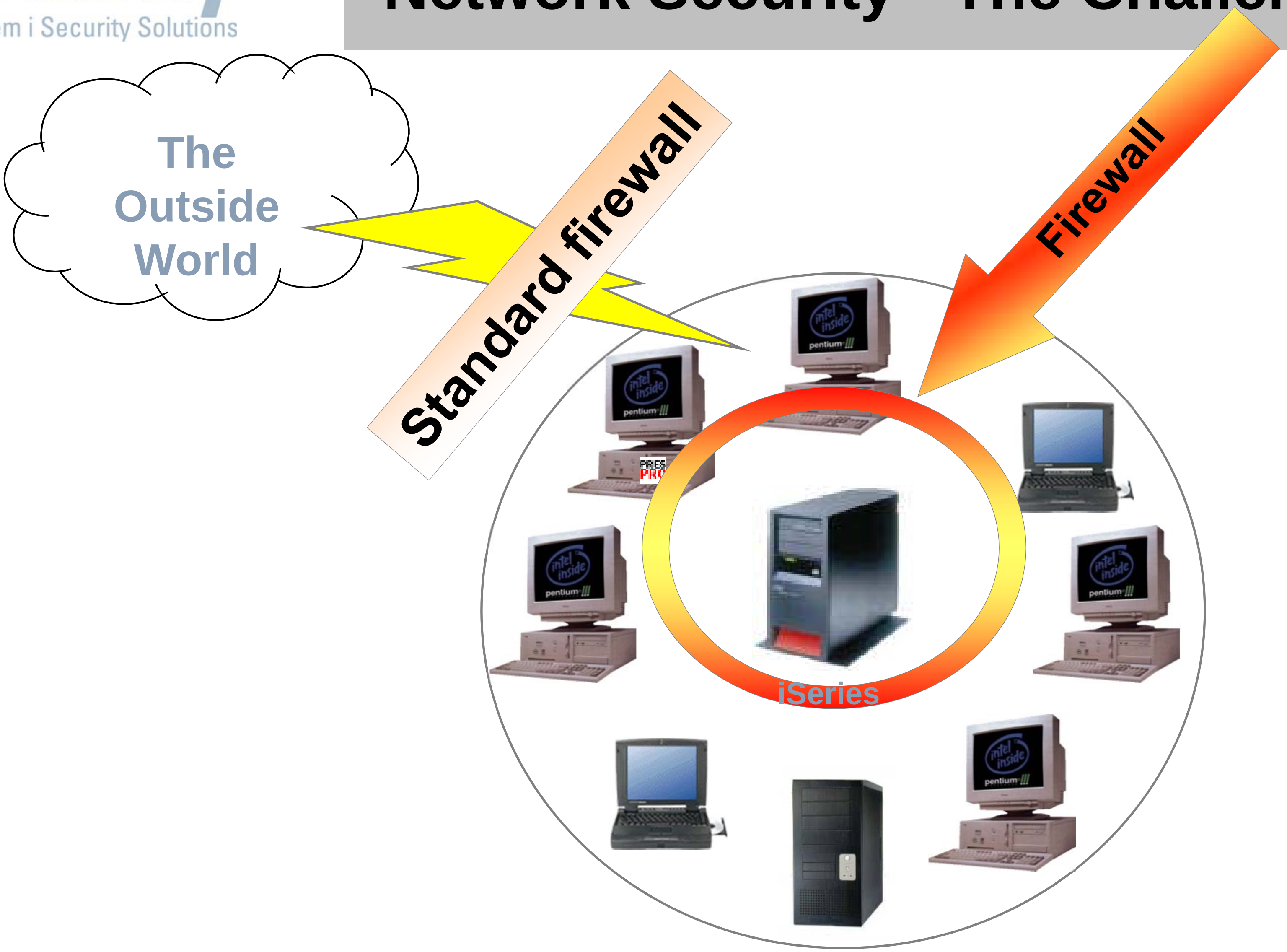
- Support - Live Operator 24x7x365
  - Always an SEA Employee
  - Never voicemail or VRU
- Training
- Conversions
- Consulting

iSecurity Solutions

iSecurity Firewall

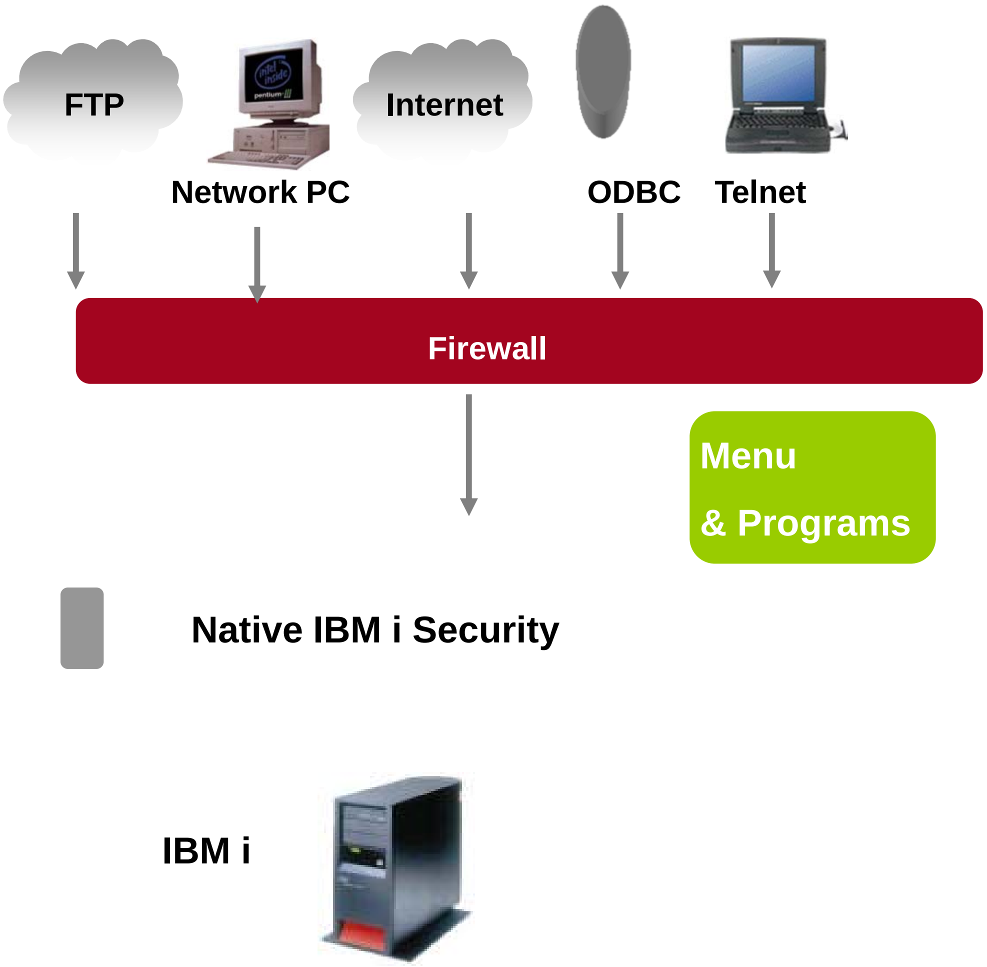
- Remote Activity on the I Series
- Compliance – Logging & Monitoring of Exit Points
  - •NOT logged by OS400
- Compliance – FULL Alerting, Action & Reporting Capabilities
- Intrusion Prevention
- User Management & Password Management
- Business Intelligence Tool
- Required Layer of Security
  - ➢ missing from OS400

Network Security - The Challenge



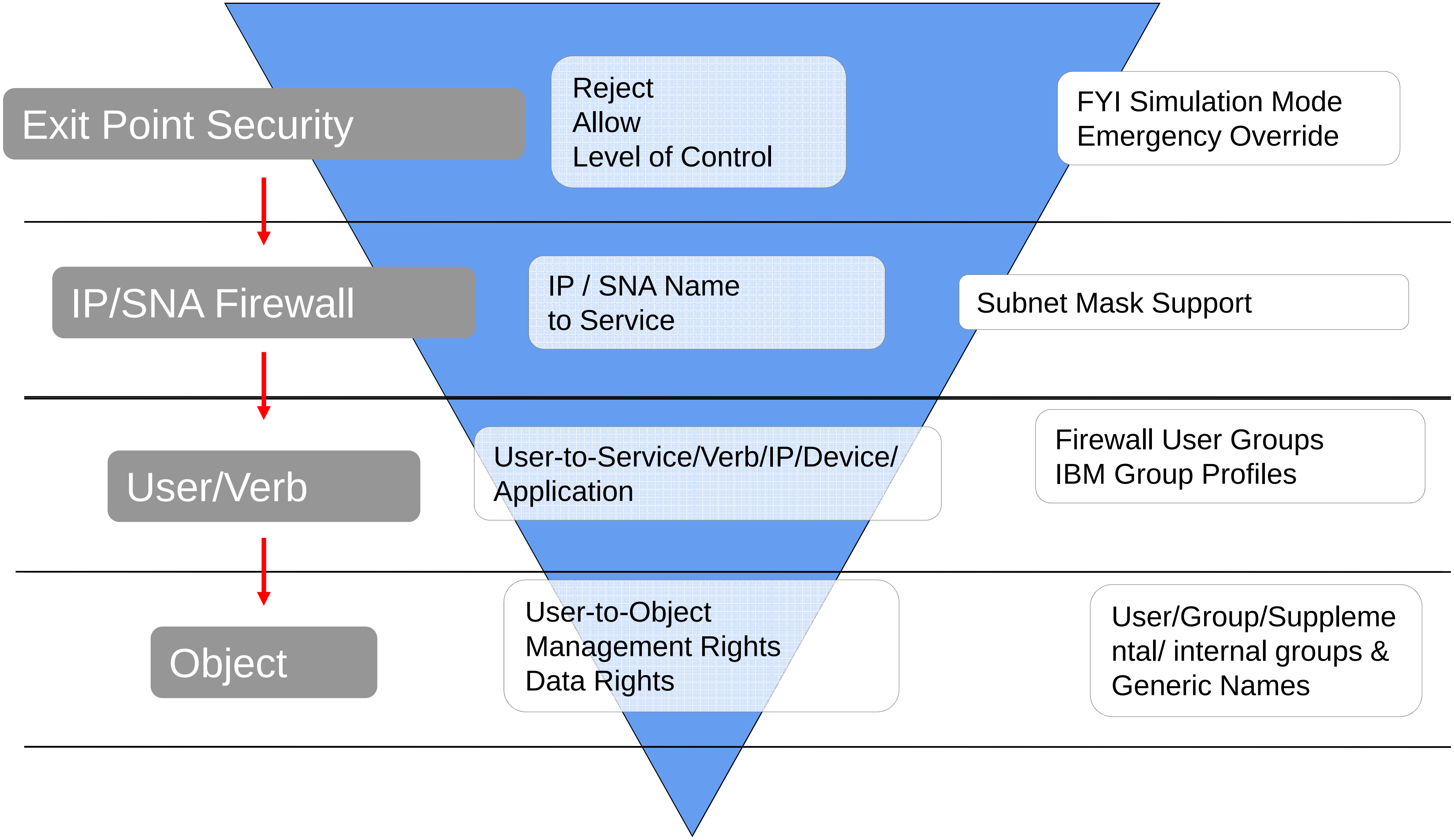
Firewall Adds Another Security Layer

- Native IBM i security: suitable for stand-alone systems
- External access bypasses IBM security
- The i is vulnerable in network environments



With Firewall

Firewall: Layered Security Design & Top - Bottom Implementation



Exit Point Security

Reject
Allow
Level of Control

FYI Simulation Mode
Emergency Override

IP/SNA Firewall

IP / SNA Name
to Service

Subnet Mask Support

User/Verb

User-to-Service/Verb/IP/Device/
Application

Firewall User Groups
IBM Group Profiles

Object

User-to-Object
Management Rights
Data Rights

User/Group/Supplemental/ internal groups &
Generic Names

AUDIT

iSecurity Audit

- Local Activity on the I Series
- Compliance – Real-time monitoring of system related activities
  - QAUDJRN
- Compliance – FULL Alerting, Action & Reporting Capabilities
- Business Intelligence Tool
- Ensure compliance of regulatory acts

Compliance Reports for Auditors and System Administrators

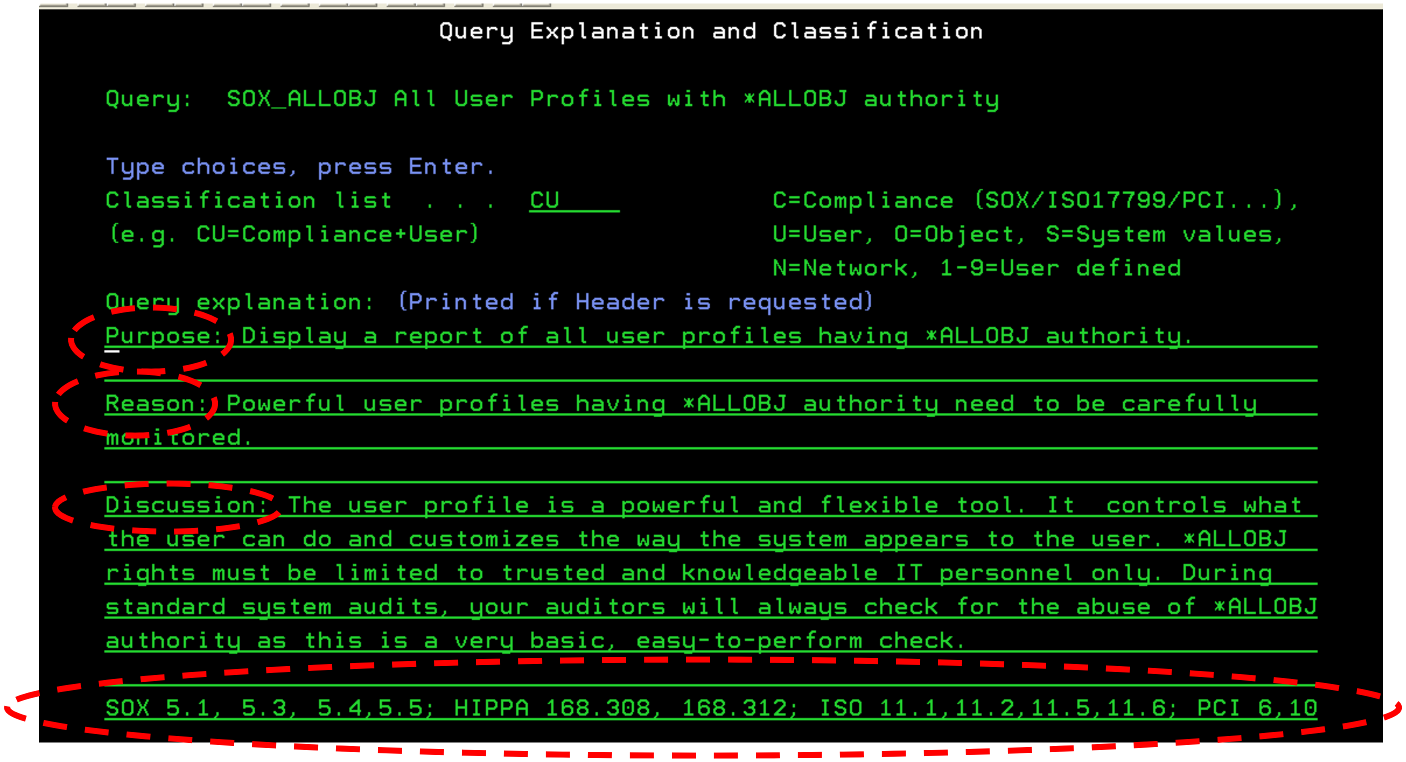
- $A User profile information
- $B Objects that are owned by a user
- $C Objects that a user is their primary group
- $D Objects for which a user has specific authority
- $E Job schedule entries
- $G Group profile and their users
- $I Object description
- $J Object authority
- $K Job descriptions with excess authority
- $L Libraries description
- $M User profile activation schedule
- $N User profile expiration schedule
- $P Users with default password
- $Q Programs that adopt authorities
- $S System values
- $T Network attributes
- $U Authorization Lists
- $V Native objects secured by authorization list
- $W IFS objects secured by authorization list
- A$ All types of QAUDJRN containing Library & Object
- A# All types of QAUDJRN
- AD Auditing changes
- AF Authority failure
- AP Obtaining adopted authority
- AU Attribute change
- C@ User profile changed (After & Before full images)
- CA Authority changes

Compliance Reports for Auditors and System Administrators

- Full Compliance Reporting
- View output as HTML, PDF, Excel in e-mail or GUI
- Support for Multi-Server environments
- All reports are site-tailorable and schedulable
- Report explanations include relevancy for compliance

Detailed Compliance Reports

- Compliance Explanations per report
- Specific references to regulatory sections

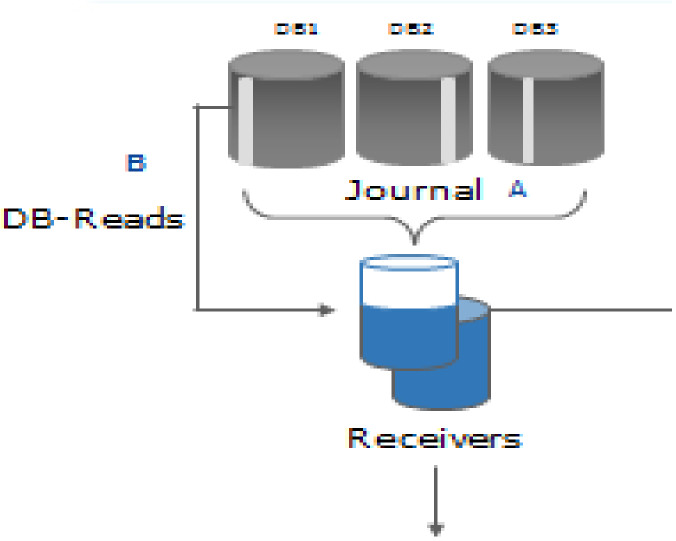


```
                      Query Explanation and Classification

  Query:  SOX_ALLOBJ All User Profiles with *ALLOBJ authority

  Type choices, press Enter.
  Classification list . . .  CU              C=Compliance (SOX/ISO17799/PCI...),
  (e.g. CU=Compliance+User)                  U=User, O=Object, S=System values,
                                             N=Network, 1-9=User defined
  Query explanation: (Printed if Header is requested)
  Purpose: Display a report of all user profiles having *ALLOBJ authority.

  Reason: Powerful user profiles having *ALLOBJ authority need to be carefully
  monitored.

  Discussion: The user profile is a powerful and flexible tool. It  controls what
  the user can do and customizes the way the system appears to the user. *ALLOBJ
  rights must be limited to trusted and knowledgeable IT personnel only. During
  standard system audits, your auditors will always check for the abuse of *ALLOBJ
  authority as this is a very basic, easy-to-perform check.

  SOX 5.1, 5.3, 5.4,5.5; HIPPA 168.308, 168.312; ISO 11.1,11.2,11.5,11.6; PCI 6,10
```

iSecurity

SYSTEM i SECURITY

AP-Journal



- **Send** E-Mail, SMS, SNMP, SYSLOG when the INTEREST RATE changes by more than 0.2%.

- **Who modified** PAYMENTS between 20:00 and 06:00 or over the weekend? What program?

- **When** did the Quantity on Hand fall below 125? Add alert for this

- **Which** users, who are not Managers, <u>viewed</u> the confidential PAYMENT TERMS table since the last business day?

Authority on Demand: Workflow

1. Definition Stage - an authorized System Administrator defines sets of emergency rules

Define Potential Providers
- QSECOFR
- SECADMIN

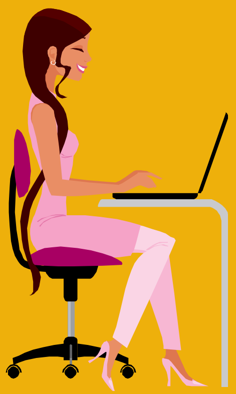
Define Emer. Rules
- “Production”
- “Salary”
- “Weekend”

Rules Details
- ADD/SWAP Auth.
- Rule Description

Notification rules
- E-mail
- SYSLOG
- MSGQ

Rule Conditions
- Date/Time
- Time Group
- IP Address
- Pin Code

2. Emergency Stage - Requester asks for “Production” authority



- Must provide reason
- Enter Pin Code (optional)
- Specify Authority Provider

Get Auth. →

← Release Auth.

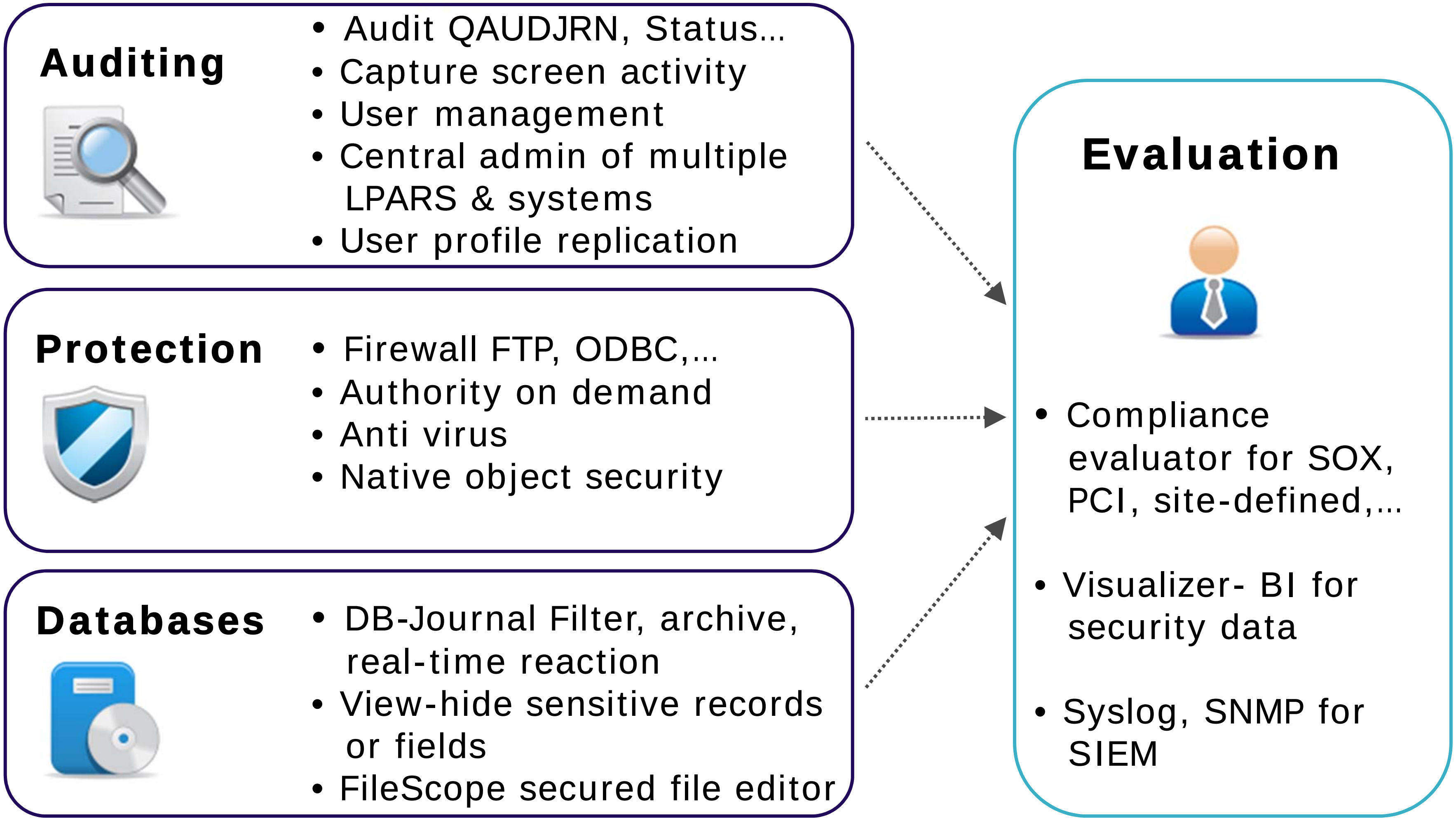
3. Auditing Stage - by Sysadmin or Auditor

Display/Print AOD & Audit (QAUDJRN) logs by time frame, Provider, or Requester

iSecurity

SYSTEM i SECURITY

iSecurity Solutions



Auditing

- Audit QAUDJRN, Status...
- Capture screen activity
- User management
- Central admin of multiple LPARS & systems
- User profile replication

Protection

- Firewall FTP, ODBC,...
- Authority on demand
- Anti virus
- Native object security

Databases

- DB-Journal Filter, archive, real-time reaction
- View-hide sensitive records or fields
- FileScope secured file editor

Evaluation

- Compliance evaluator for SOX, PCI, site-defined,...
- Visualizer- BI for security data
- Syslog, SNMP for SIEM

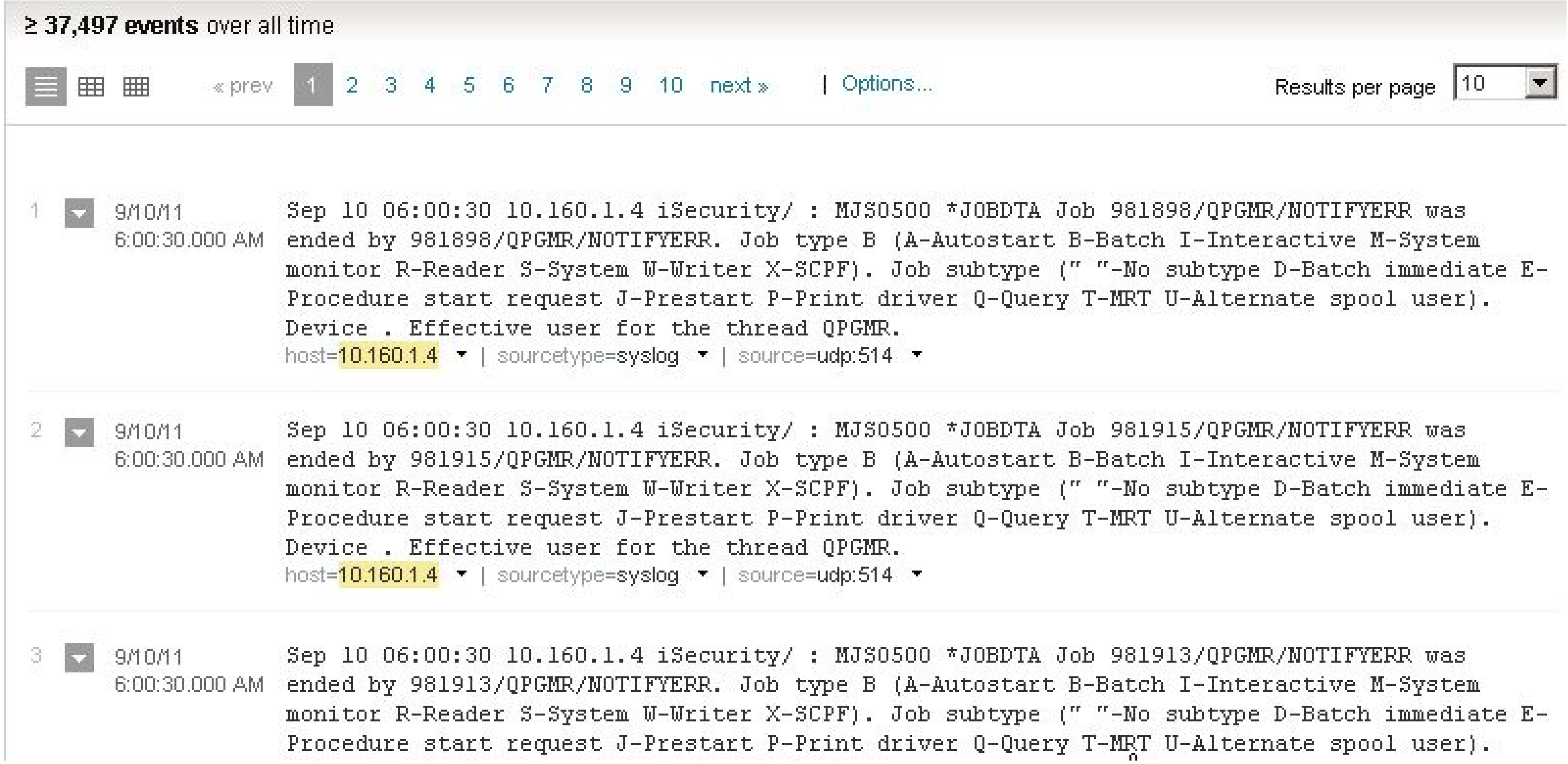
iSecurity
System i Security Solutions

SEA™ SOFTWARE ENGINEERING OF AMERICA®
User Driven Software Solutions Since 1982

End to End Security for the System i

Compliance Reports for Auditors and System Administrators

• Remote Syslog Support

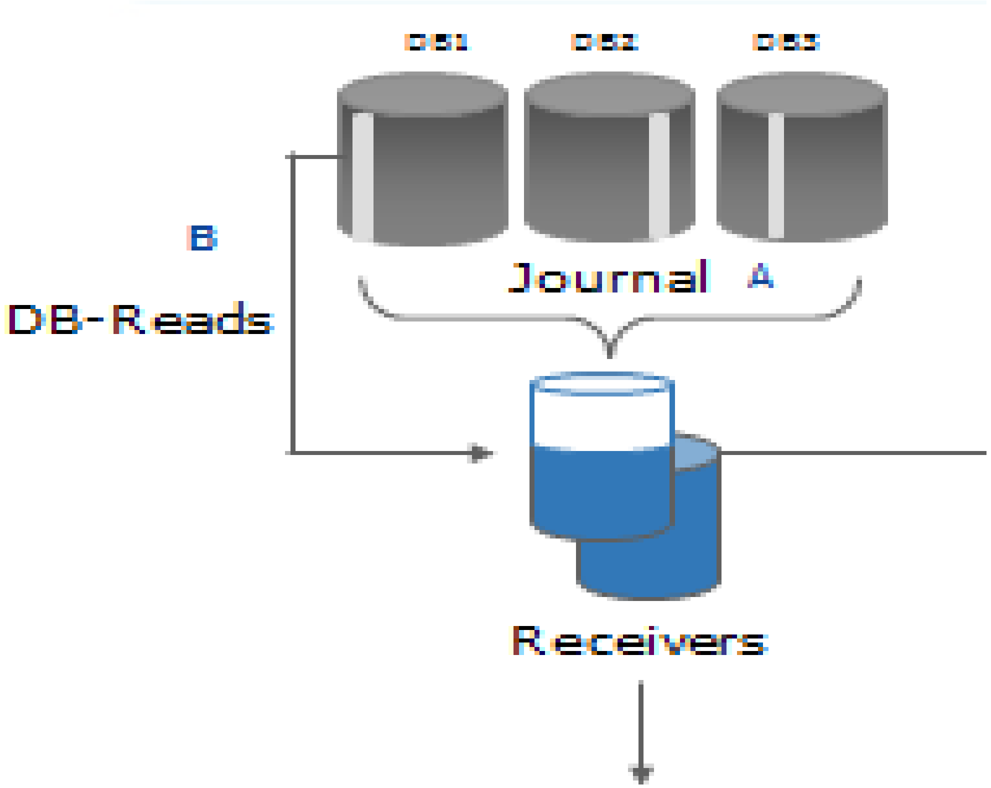


≥ 37,497 **events** over all time

```
1   9/10/11          Sep 10 06:00:30 10.160.1.4 iSecurity/ : MJS0500 *JOBDTA Job 981898/QPGMR/NOTIFYERR was
    6:00:30.000 AM   ended by 981898/QPGMR/NOTIFYERR. Job type B (A-Autostart B-Batch I-Interactive M-System
                     monitor R-Reader S-System W-Writer X-SCPF). Job subtype (" "-No subtype D-Batch immediate E-
                     Procedure start request J-Prestart P-Print driver Q-Query T-MRT U-Alternate spool user).
                     Device . Effective user for the thread QPGMR.
                     host=10.160.1.4 ▾ | sourcetype=syslog ▾ | source=udp:514 ▾

2   9/10/11          Sep 10 06:00:30 10.160.1.4 iSecurity/ : MJS0500 *JOBDTA Job 981915/QPGMR/NOTIFYERR was
    6:00:30.000 AM   ended by 981915/QPGMR/NOTIFYERR. Job type B (A-Autostart B-Batch I-Interactive M-System
                     monitor R-Reader S-System W-Writer X-SCPF). Job subtype (" "-No subtype D-Batch immediate E-
                     Procedure start request J-Prestart P-Print driver Q-Query T-MRT U-Alternate spool user).
                     Device . Effective user for the thread QPGMR.
                     host=10.160.1.4 ▾ | sourcetype=syslog ▾ | source=udp:514 ▾

3   9/10/11          Sep 10 06:00:30 10.160.1.4 iSecurity/ : MJS0500 *JOBDTA Job 981913/QPGMR/NOTIFYERR was
    6:00:30.000 AM   ended by 981913/QPGMR/NOTIFYERR. Job type B (A-Autostart B-Batch I-Interactive M-System
                     monitor R-Reader S-System W-Writer X-SCPF). Job subtype (" "-No subtype D-Batch immediate E-
                     Procedure start request J-Prestart P-Print driver Q-Query T-MRT U-Alternate spool user).
```

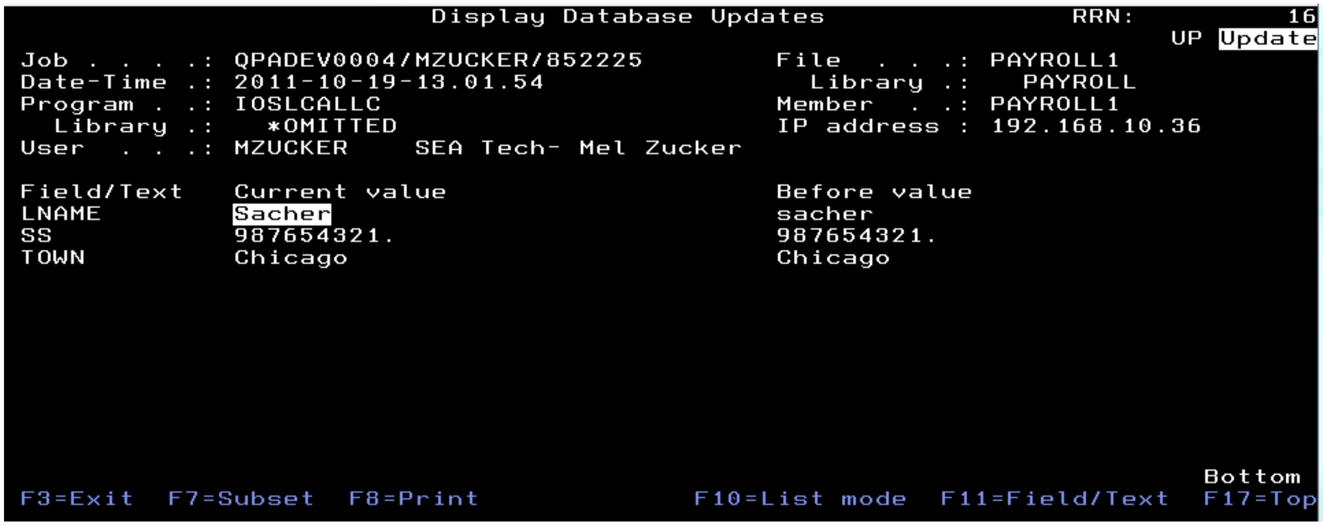
SYSTEM i SECURITY

AP - Journal

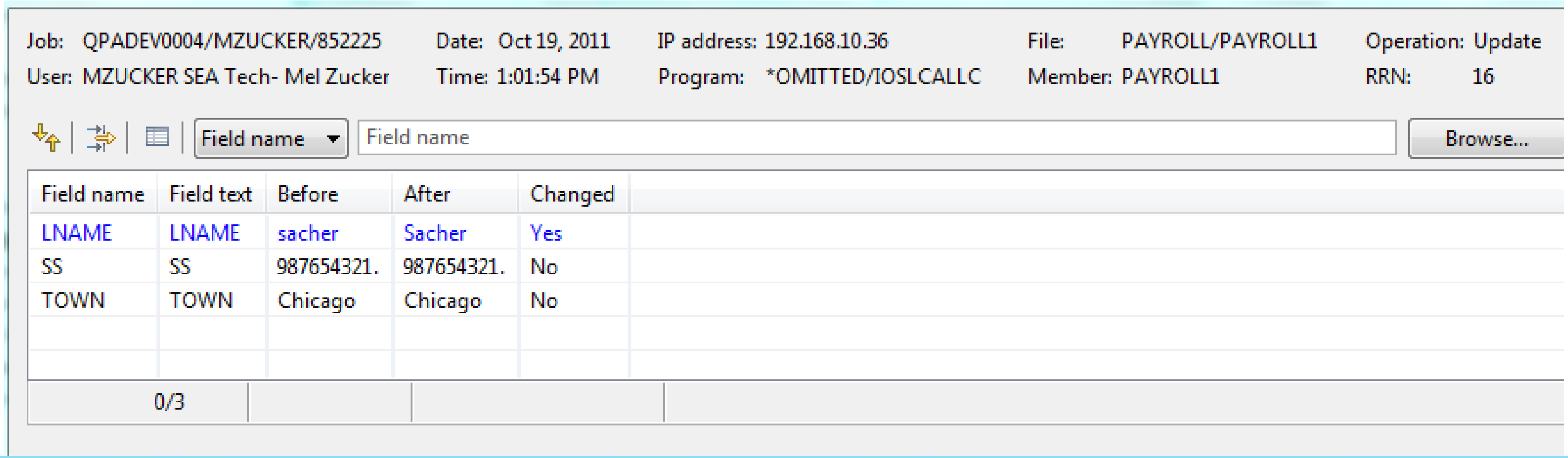


iSecurity ap-Journal

AP-Journal



```
                         Display Database Updates               RRN:          16
                                                                      UP Update
 Job . . . .: QPADEV0004/MZUCKER/852225          File   . . .: PAYROLL1
 Date-Time .: 2011-10-19-13.01.54                  Library .:   PAYROLL
 Program . .: IOSLCALLC                          Member   . .: PAYROLL1
   Library .:   *OMITTED                         IP address : 192.168.10.36
 User  . . .: MZUCKER     SEA Tech- Mel Zucker

 Field/Text    Current value                     Before value
 LNAME         Sacher                            sacher
 SS            987654321.                        987654321.
 TOWN          Chicago                           Chicago









                                                                        Bottom
 F3=Exit   F7=Subset   F8=Print          F10=List mode   F11=Field/Text   F17=Top
```



Job: QPADEV0004/MZUCKER/852225 Date: Oct 19, 2011 IP address: 192.168.10.36 File: PAYROLL/PAYROLL1 Operation: Update

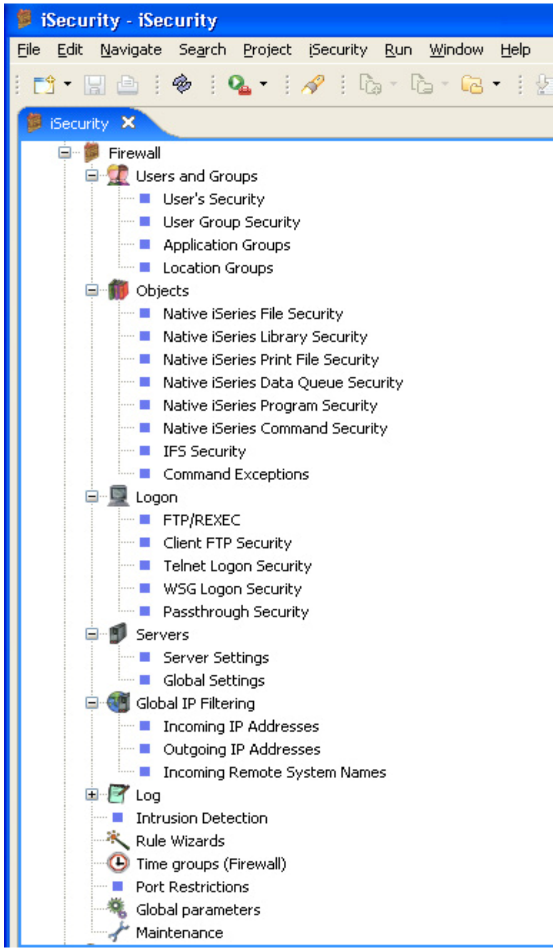
User: MZUCKER SEA Tech- Mel Zucker Time: 1:01:54 PM Program: *OMITTED/IOSLCALLC Member: PAYROLL1 RRN: 16

Field name	Field text	Before	After	Changed
LNAME	LNAME	sacher	Sacher	Yes
SS	SS	987654321.	987654321.	No
TOWN	TOWN	Chicago	Chicago	No

0/3

iSecurity
System i Security Solutions

The iSecurity Firewall Solution



- Firewall
  - Users and Groups
    - User's Security
    - User Group Security
    - Application Groups
    - Location Groups
  - Objects
    - Native iSeries File Security
    - Native iSeries Library Security
    - Native iSeries Print File Security
    - Native iSeries Data Queue Security
    - Native iSeries Program Security
    - Native iSeries Command Security
    - IFS Security
    - Command Exceptions
  - Logon
    - FTP/REXEC
    - Client FTP Security
    - Telnet Logon Security
    - WSG Logon Security
    - Passthrough Security
  - Servers
    - Server Settings
    - Global Settings
  - Global IP Filtering
    - Incoming IP Addresses
    - Outgoing IP Addresses
    - Incoming Remote System Names
  - Log
  - Intrusion Detection
  - Rule Wizards
  - Time groups (Firewall)
  - Port Restrictions
  - Global parameters
  - Maintenance

Protect <u>All</u> communication protocols

SNA TCP

Protect <u>All</u> security related Exit Points

- FTP
- ODBC
- TELNET
- REXEC
- DDM
- DRDA
- SQL