RAZ-LEE

AP-JOURNAL

Database Monitoring and Reporting

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world’s leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee’s flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

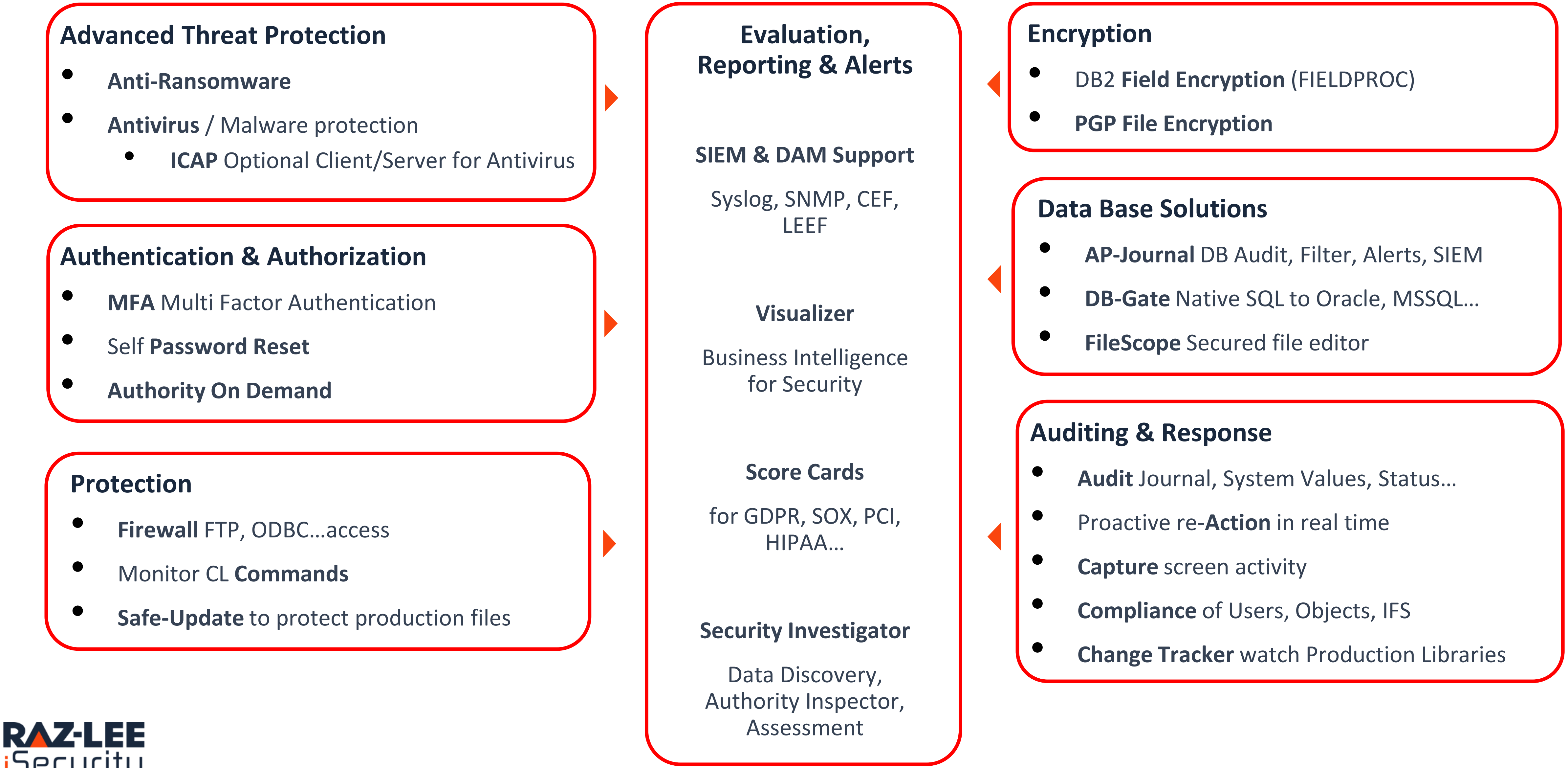
We build solutions that work with other companies’ technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva IBM McAfee™

Akamai RSA® SEA™ SOFTWARE ENGINEERING OF AMERICA

About iSecurity Suite



Advanced Threat Protection

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

Authentication & Authorization

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

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

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

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

Auditing & Response

- **Audit** Journal, 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

AP-Journal

Database Monitoring and Reporting

Business Intelligence Traceability

Due to have information from Multiple Sources, usually most systems bring the latest results, but most of the time we need to know all the changes done to the data before making a good Business decision.

- With its unique technology, AP-Journal logs database access (READ operations) directly into the journal receivers. This functionality, which OS/400 journaling does not provide, constitutes an important component of compliance.

- By providing a timeline report of all changes relating to application data, AP-Journal reduces unauthorized activity and enables users to meet regulatory requirements. It also issues real-time alerts to inform managers of any changes in application databases or unapproved access to critical data.

When could this be Useful?

When u need to answer complicated questions like:

- Who modified file PAYMENTS between 20:00 and 06:00 during vacation; among those, who reduced the PAYMENT_AMOUNT by more than 15%?
- Who worked on the SALARY file during non-standard business hours, and accessed employees whose salaries exceed $5,000 monthly?
- Provide 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 company's Chief Security Officer when the PRICE_OF_ITEM changes by more than 4%.
- Send a SYSLOG message and operator message when the PRICE_OF_ITEM for an ITEM shipped last month changes by more than $6.20.
- Send an e-mail when anyone accesses the record of an employee whose monthly SALARY is greater than $5000.
- What changes to the hospital's PATIENTS file were made via utility application DFU?
- And so on…

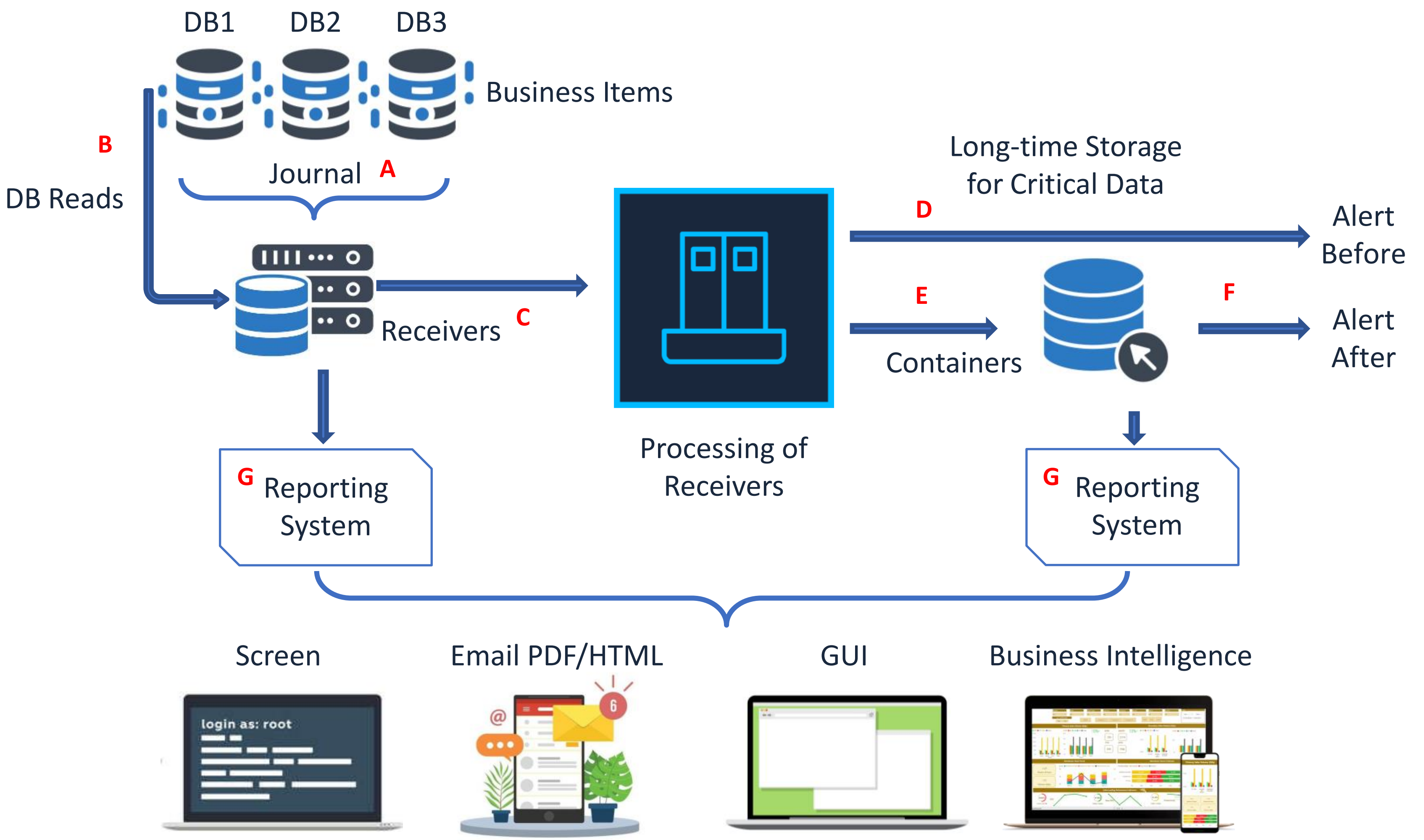
Getting the Data

AP-Journal Protects Business-critical information, and notifies managers of any changes to information assets and streamlines IBM i journaling procedures.

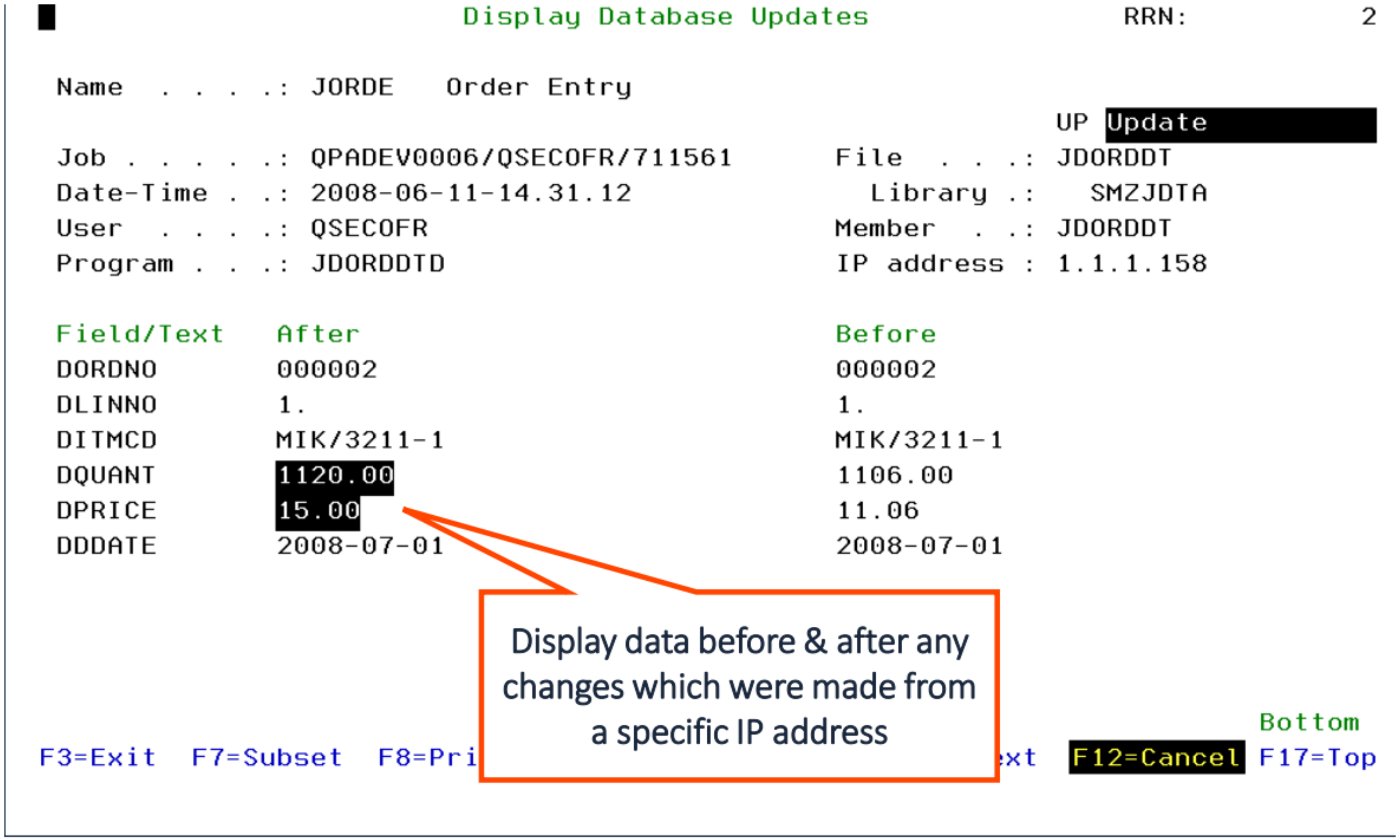
- Users can integrate information from various files and view all changes relating to a specified business item. In addition, AP-Journal helps enforce business rules by triggering external functions.

- AP-Journal logs the who, what, when and which of activities. It logs database access (READ operations) directly into the journal receivers, which is not provided by IBM i journaling and is an important component of compliance.

Workflow


DB1
DB2
DB3
Business Items
B
DB Reads
Journal
A
Receivers
C
Processing of Receivers
Long-time Storage for Critical Data
D
Alert Before
E
Containers
F
Alert After
G
Reporting System
G
Reporting System
Screen
Email PDF/HTML
GUI
Business Intelligence
login as: root
6

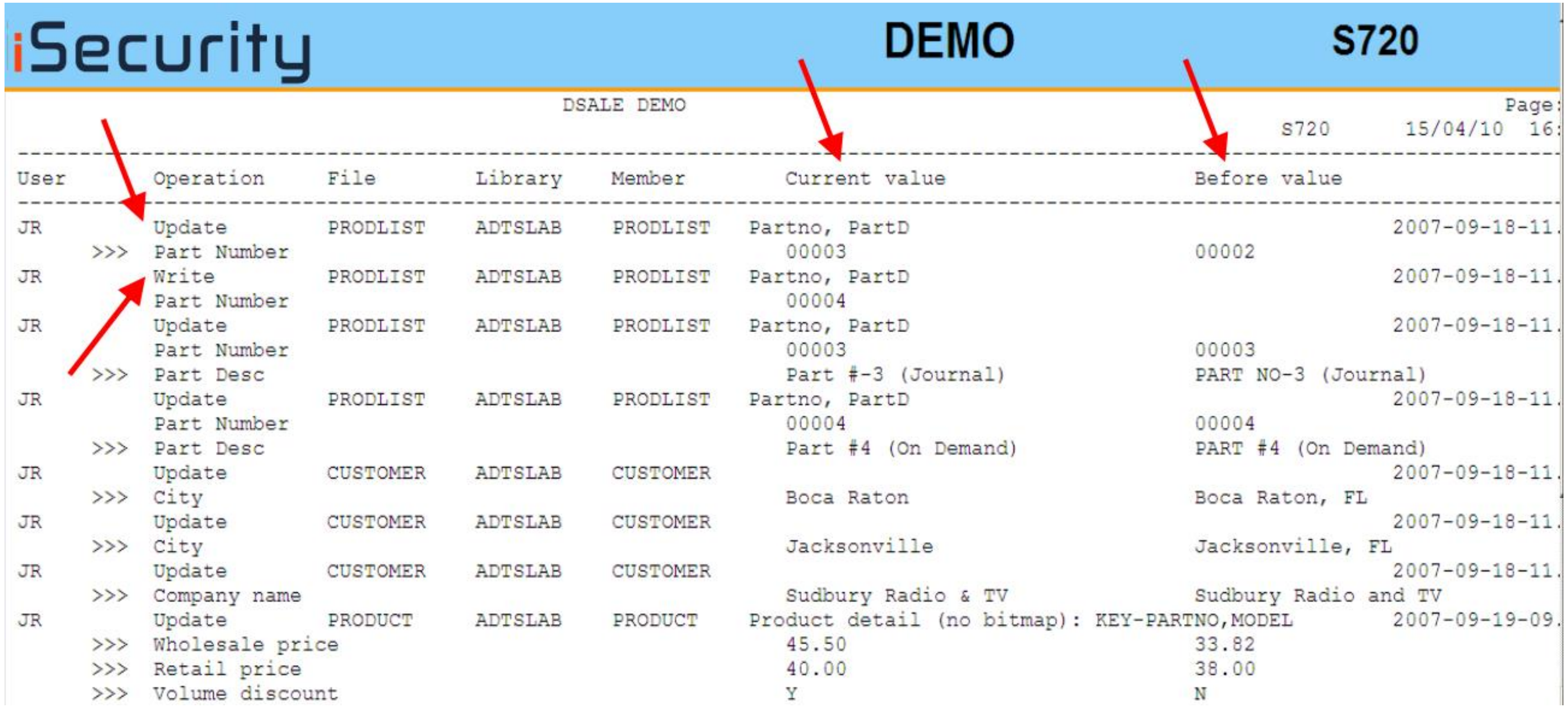
Screen Report



```
                         Display Database Updates                RRN:            2

 Name  . . . .: JORDE   Order Entry
                                                                  UP Update
 Job . . . . . .: QPADEV0006/QSECOFR/711561      File  . . .: JDORDDT
 Date-Time . .: 2008-06-11-14.31.12               Library .:   SMZJDTA
 User  . . . .: QSECOFR                          Member  . .: JDORDDT
 Program . . .: JDORDDTD                         IP address : 1.1.1.158

 Field/Text    After                             Before
 DORDNO        000002                            000002
 DLINNO        1.                                1.
 DITMCD        MIK/3211-1                        MIK/3211-1
 DQUANT        1120.00                           1106.00
 DPRICE        15.00                             11.06
 DDDATE        2008-07-01                        2008-07-01

                                                                            Bottom
F3=Exit   F7=Subset   F8=Pri                          xt   F12=Cancel  F17=Top
```

Display data before & after any changes which were made from a specific IP address

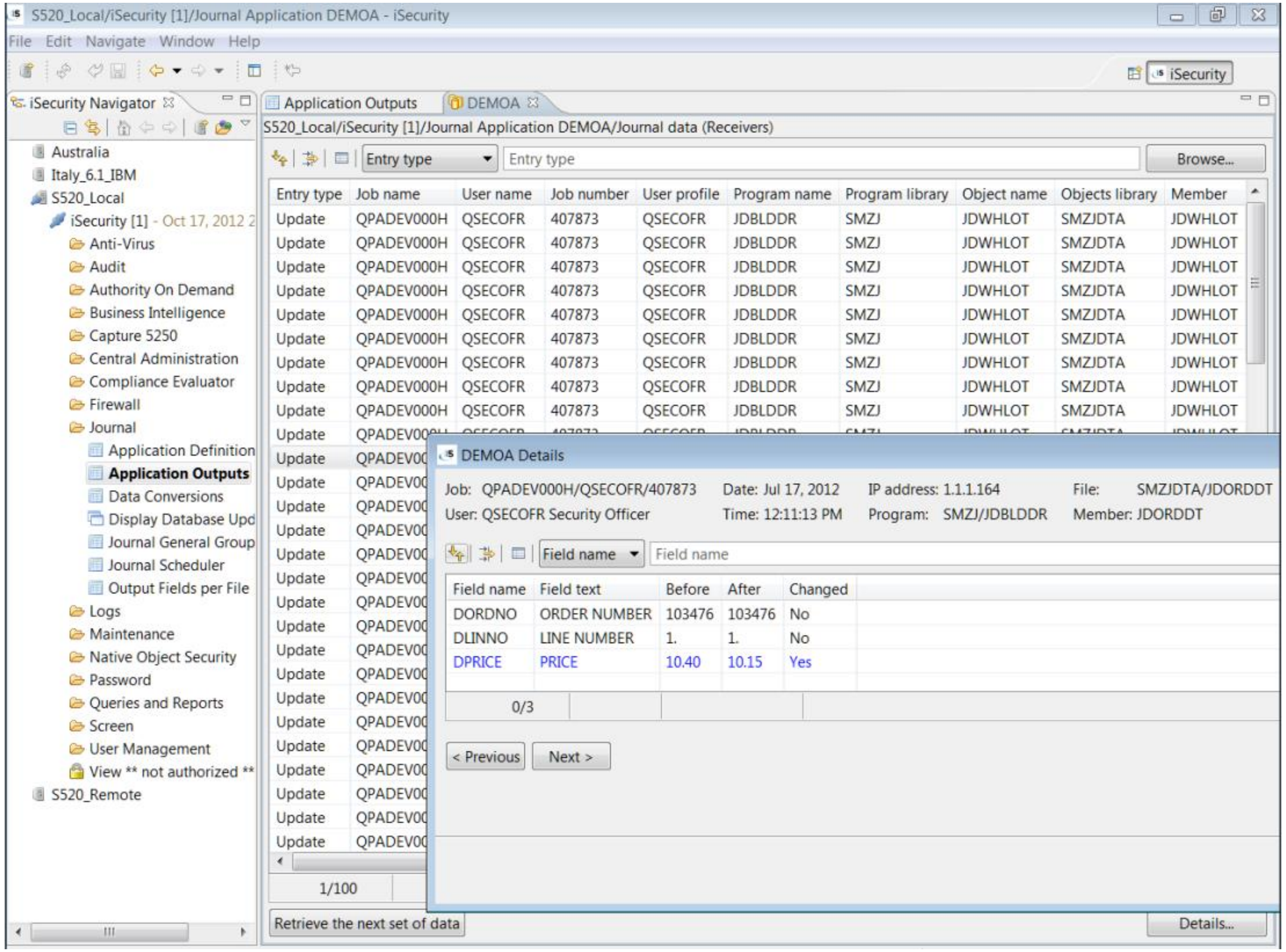
Html Report



DEMO S720

```
                                             DSALE DEMO                                                                    Page:
                                                                                                        S720      15/04/10   16:
--------------------------------------------------------------------------------------------------------------------------------
User       Operation      File        Library    Member        Current value                    Before value
--------------------------------------------------------------------------------------------------------------------------------
JR         Update         PRODLIST    ADTSLAB    PRODLIST   Partno, PartD                                          2007-09-18-11.
      >>>  Part Number                                         00003                            00002
JR         Write          PRODLIST    ADTSLAB    PRODLIST   Partno, PartD                                          2007-09-18-11.
           Part Number                                         00004
JR         Update         PRODLIST    ADTSLAB    PRODLIST   Partno, PartD                                          2007-09-18-11.
           Part Number                                         00003                            00003
      >>>  Part Desc                                           Part #-3 (Journal)               PART NO-3 (Journal)
JR         Update         PRODLIST    ADTSLAB    PRODLIST   Partno, PartD                                          2007-09-18-11.
           Part Number                                         00004                            00004
      >>>  Part Desc                                           Part #4 (On Demand)              PART #4 (On Demand)
JR         Update         CUSTOMER    ADTSLAB    CUSTOMER                                                          2007-09-18-11.
      >>>  City                                                Boca Raton                       Boca Raton, FL
JR         Update         CUSTOMER    ADTSLAB    CUSTOMER                                                          2007-09-18-11.
      >>>  City                                                Jacksonville                     Jacksonville, FL
JR         Update         CUSTOMER    ADTSLAB    CUSTOMER                                                          2007-09-18-11.
      >>>  Company name                                        Sudbury Radio & TV               Sudbury Radio and TV
JR         Update         PRODUCT     ADTSLAB    PRODUCT    Product detail (no bitmap): KEY-PARTNO,MODEL         2007-09-19-09.
      >>>  Wholesale price                                     45.50                            33.82
      >>>  Retail price                                        40.00                            38.00
      >>>  Volume discount                                     Y                                N
```

GUI Report



S520_Local/iSecurity [1]/Journal Application DEMOA/Journal data (Receivers)

Entry type: Entry type

Entry type	Job name	User name	Job number	User profile	Program name	Program library	Object name	Objects library	Member
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV000H	QSECOFR	407873	QSECOFR	JDBLDDR	SMZJ	JDWHLOT	SMZJDTA	JDWHLOT
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								
Update	QPADEV00								

1/100

DEMOA Details

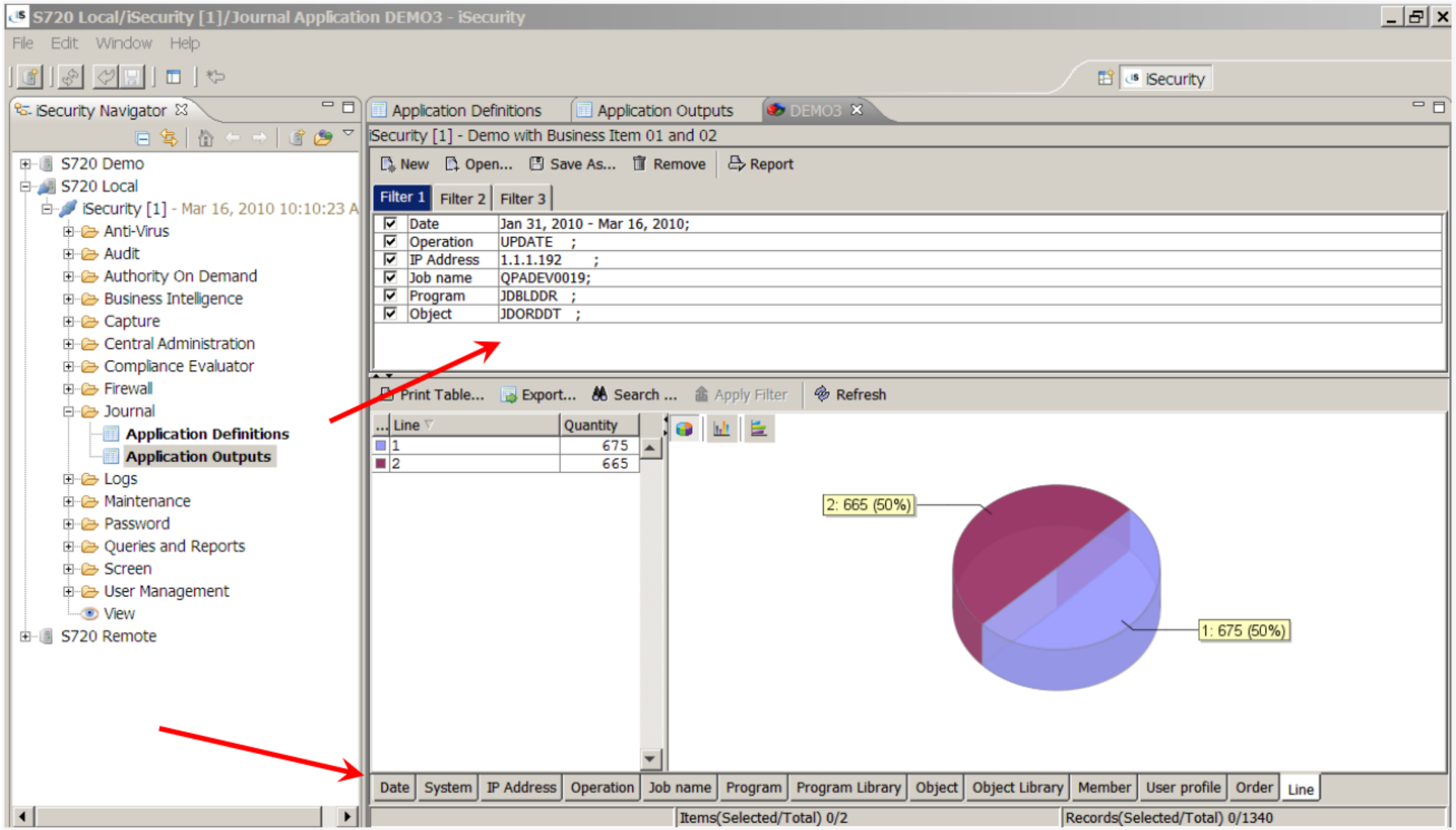
Job: QPADEV000H/QSECOFR/407873 Date: Jul 17, 2012 IP address: 1.1.1.164 File: SMZJDTA/JDORDDT
User: QSECOFR Security Officer Time: 12:11:13 PM Program: SMZJ/JDBLDDR Member: JDORDDT

Field name: Field name

Field name	Field text	Before	After	Changed
DORDNO	ORDER NUMBER	103476	103476	No
DLINNO	LINE NUMBER	1.	1.	No
DPRICE	PRICE	10.40	10.15	Yes

0/3

Business Intelligence Report



iSecurity [1] - Demo with Business Item 01 and 02

☑	Date	Jan 31, 2010 - Mar 16, 2010;
☑	Operation	UPDATE ;
☑	IP Address	1.1.1.192 ;
☑	Job name	QPADEV0019;
☑	Program	JDBLDDR ;
☑	Object	JDORDDT ;

...	Line	Quantity
■	1	675
■	2	665

Items(Selected/Total) 0/2

Records(Selected/Total) 0/1340

iSecurity AP-Journal Advantages

- Addresses PCI, SOX, HIPAA, etc. requirements
- Long-term storage of sensitive information, independent of journal receiver lifecycle
- Advanced filtering enables saving only important information, to suit storage limits
- READ operations selectively added to Journal, for compliance with PCI requirements
- Real-time alerts on changes in business-critical data & access, sent as operator messages, e-mail, SMS, SYSLOG; CL Scripts execution
- Timeline and cross-application reports based upon user-defined business items

iSecurity AP-Journal Advantages

- Report data can include key fields, description fields and modified fields (highlighted)
- Output as Online, Print, HTML, PDF, Outfile & Email
- Filter according to “before” or “after” values of each database field. Boolean And/Or, EQ, GT, LE… N/LIKE, N/LIST… conditions refer to percentage or absolute value changes
- Runs on a High Availability system, reducing performance impact on Production Systems
- Real-time or scheduled operation mode

RAZ-LEE

Thank You

For more information about our company and products please visit

www.razlee.com