ANTIVIRUS

Advanced threat protection solution for defending IBM i IFS files against malware

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

ANTIVIRUS

Advanced threat protection solution for defending IBM i IFS files against malware

RAZ-LEE iSecurity

Is IBM i affected by Viruses?

- Until just a few years ago, the IBM i was used almost exclusively in a closed environment, and the OS/400 operating system provided the strongest data and system security in the world.

- Technological advances opened up the iSeries to the rest of the world, but in the process, brought with it many of the security risks inherent in distributed environments, leading to a shocking discovery.

- Although the IBM i (AS/400) 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.

Why to choose iSecurity Antivirus?

iSecurity Antivirus scans all accessed files, offers comprehensive virus detection by marking, quarantining, and deleting infected files, and prevents your IBM i from becoming an infection source.

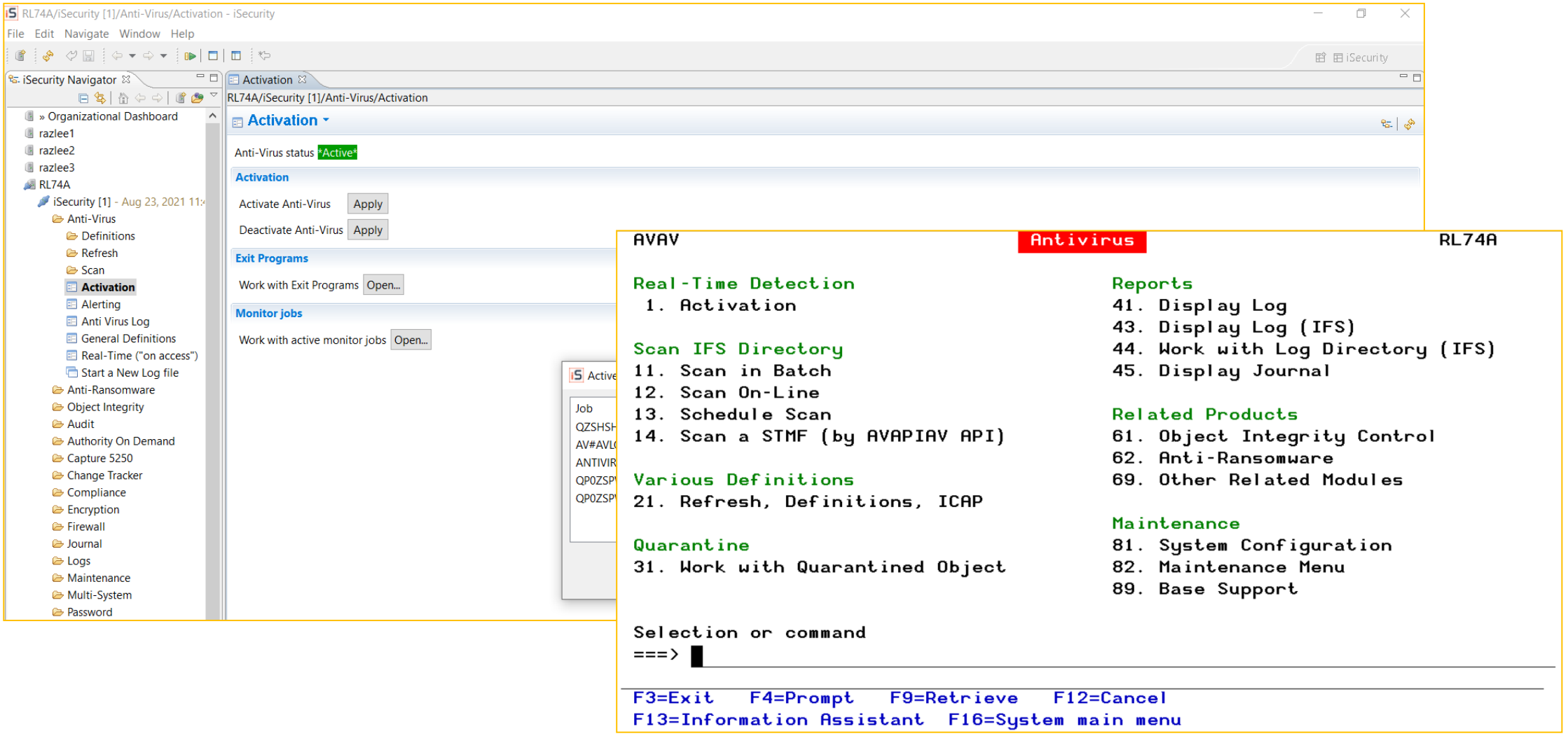
Our Solution:

- Raz-Lee's iSecurity Antivirus software cannot be disabled by any known virus.
- Runs Local at the IBM i server or on ICAP Client.
- Based on ClamAV Engine Developed by Cisco and Distributed as part of AIX package on IBM.

Based on ClamAV

- iSecurity Antivirus uses ClamAV for scanning malware
- ClamAV is owned by Cisco
- IBM Distributes it in the AIX Tool Kit
- Open-source, Cross-platform
- Considered as One of the Five best antiviruses

Antivirus in Action



RAZ-LEE iSecurity

ClamAV engine implementation brings

- A database of over five million virus signatures
- Signatures are continually updated by the community
- 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 Antivirus implementation brings

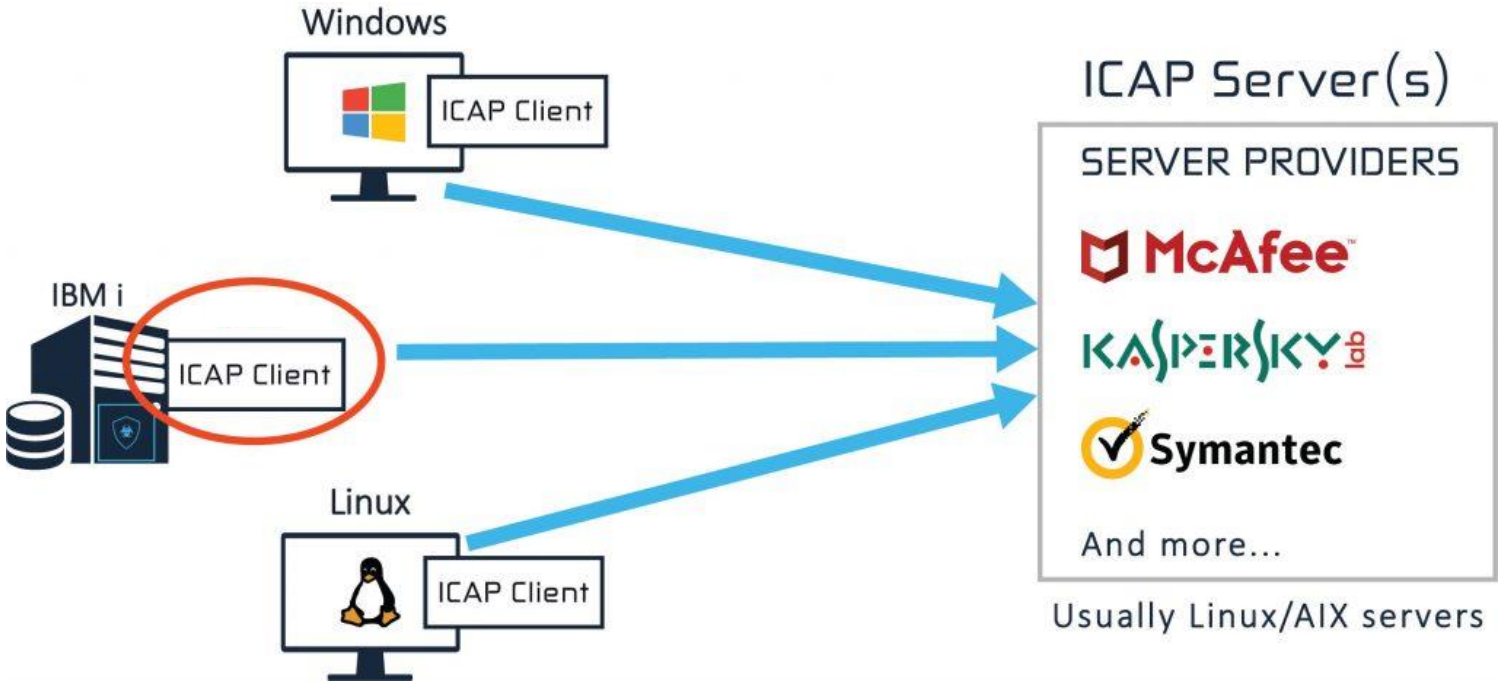
- Real-time Scanning
- On-demand Scanning
- Scheduled Scanning
- API that enables scanning at will of a single file

- ICAP – Client / Server Technology

iSecurity Antivirus ICAP Client

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.



RAZ-LEE iSecurity

Advantages when being evaluated against competition

- Real good native interface. User will never need to run DOS like command
- Command and API that provide the ability to scan a file in sub second (without any delay)
- Excludes are accepted, and can be used simultaneously as:
  - *generic* names (the IBM i native way, which all IBM I stuff members are used to)
  - Regular expression (the way that is the standard in Linux, and is completely strange to IBM i)
- Single “Work with Infected files”, to work with all infected files. Both those that were moved to quarantine (standard way), and those kept in place marked as unusable (IBM i way that is used in “On-Access”)

iSecurity Antivirus Advantages

- Automatic, regularly updated database
- Command-line scanner
- Scan On Demand
- Scan by Schedule
- Database updater with support for digital signatures
- Can not be disabled by viruses
- Built-in support for zip, gzip, jar, and tar files
- User-friendly, multilingual interface (green screen and GUI)
- Supports V5R3 Scanning Enablement
- Integration with OS/400 Scheduler
- History Log for review and analysis

iSecurity Antivirus & Anti-Ransomware Shared Advantages

- All detections are logged to a native WORM (Write Once, Read Many) native file, in addition to the standard IFS logs
- Report generator with scheduler
- Free SIEM support

Thank You

For more information about our company and products please visit

www.razlee.com