ANTIVIRUS ICAP CLIENT

Offload Resources

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 ICAP CLIENT

Offload Resources

RAZ-LEE iSecurity

Virus Scan Load

We all know that scan of AV consumes high amount of CPU. AV has to compare each position of the file to see if it starts with one of the millions signatures.

This takes time...

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.

Reduce CPU usage

- The ICAP Client provides a consistent solution that frees your IBM i CPU from the burden of virus scanning, so you can protect your systems effectively and efficiently.

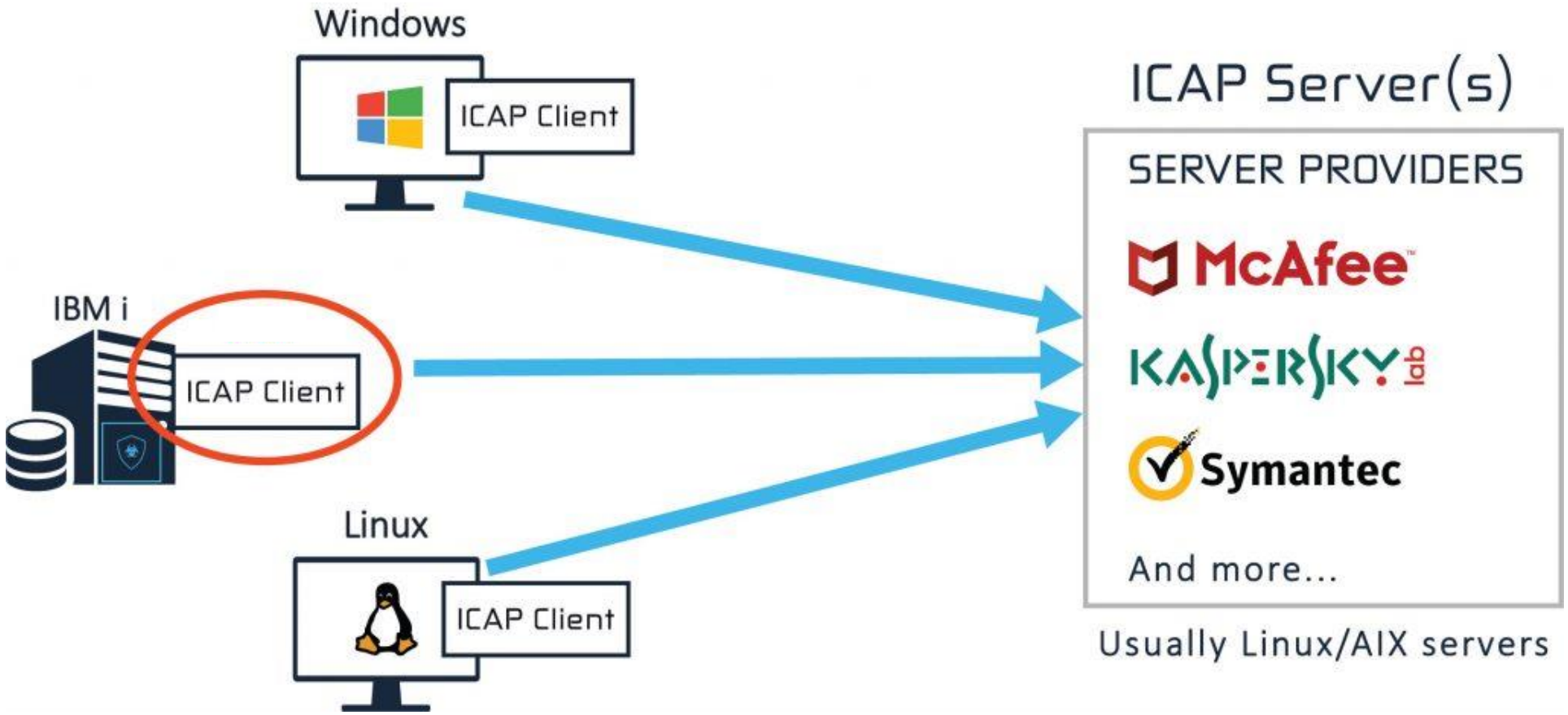
- Using ICAP ensures that your IBM i is always protected without a performance drop. Scan time is faster – by twenty times in some tests. The portion of the IBM i CPU that would have been used for virus scanning becomes available for other purposes.

- ICAP was explicitly created as a way to extend proxy servers on the Web, primarily in the context of virus scanning and content filters, thereby freeing up resources on the main servers they support.

- In this manner, Raz-Lee uses the ICAP client to offload virus scanning from the IBM i server to other servers connected to it.

iSecurity Antivirus ICAP Client

The portion of the IBM i CPU that would have been used for virus scanning becomes available for other purposes.

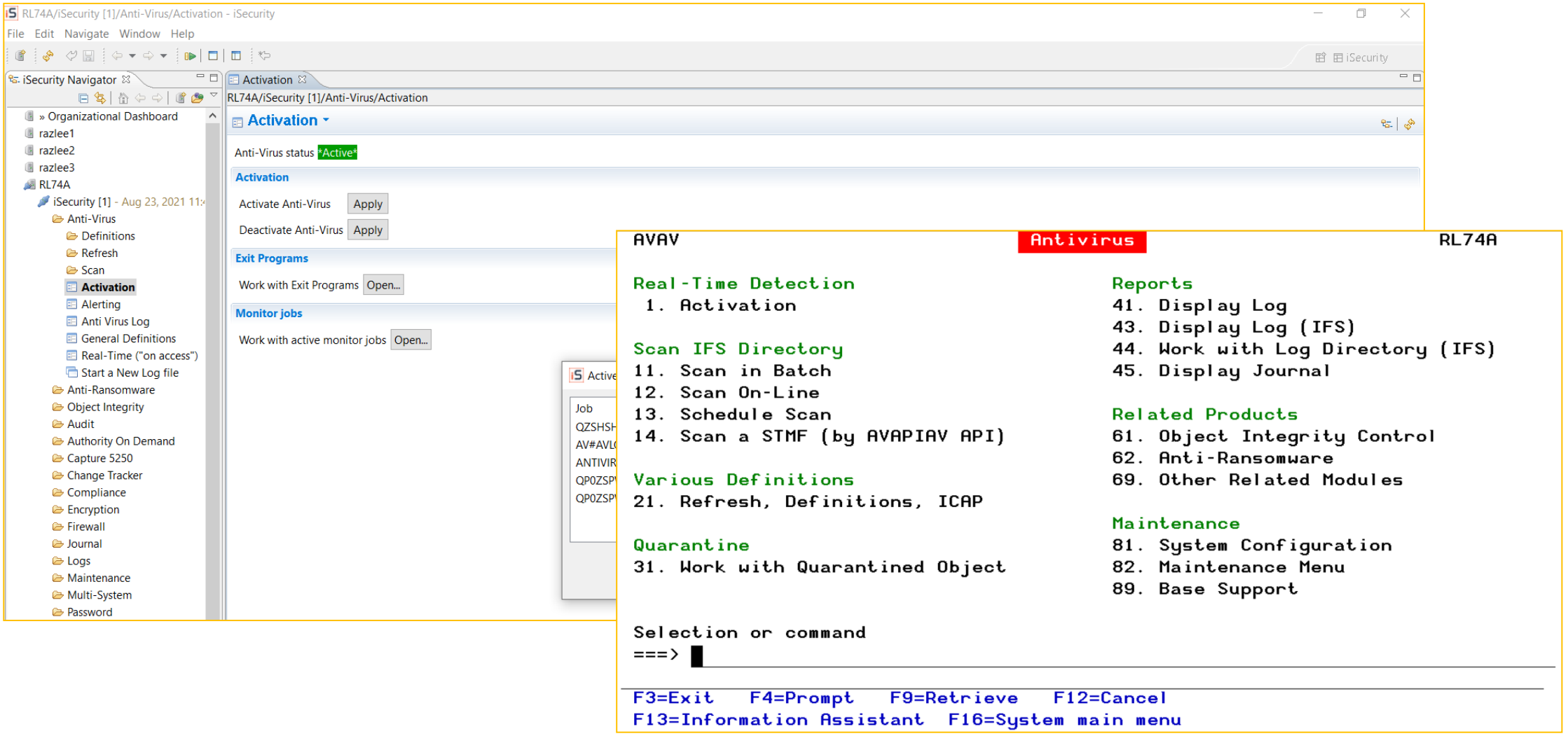


Why to choose Antivirus with ICAP Client?

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.

- When the ICAP Client for iSecurity Anti-Virus is enabled, iSecurity Anti-Virus can hand off virus scanning to an inexpensive external server.
- ICAP client reduces CPU usage and CPU peaks while enabling an organization to use the virus scanning solution of its choice.
- The organizational anti-virus server can run virtually any anti-virus that exists in the market, including Symantec, McAfee, Kaspersky, and Sophos.

Antivirus in Action



RAZ-LEE iSecurity

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

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 Advantages

- ICAP outsources CPU-intensive tasks to external servers.
- As a result the performance impact on the IBM i is lessened.
- With ICAP – Any antivirus can be used.
- Most suitable for Multiple LPAR Organizations

Advantages when being evaluated against competition

- ICAP Client. Organizations that have multiple LPARs especially if those have little core slices, can use this to offload the scan performance burden (5-8 million signatures) to an external ICAP server.

- ICAP enables to organization to use many other antivirus products, including Symantec (Broadcom), Mcafee, Trend Micro, Cisco, F5 .

IBM support https://www.ibm.com/docs/en/secure-proxy/6.1.0?topic=scenarios-icap-anti-virus-scanning

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