

The logo features the text "RAZ-LEE" in a bold, dark blue, sans-serif font. A small orange triangle is positioned at the base of the letter "A".

RAZ-LEE

ANTI-RANSOMWARE

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

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



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

ANTI-RANSOMWARE

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

Is IBM i affected by Ransomware?

- Since the IBM i is no longer an isolated platform, there is a real risk of malware & ransomware spreading to it and other devices and systems via networked drives and cloud storage services.
- IFS directory files can easily become ransomware victims and unintentional ransomware propagators, through infected mapped drives.
- Ransomware encrypts every file that it has access to, including IFS files, leaving organizations feeling paralyzed, exposed and without many options.

Real-time Protection

Anti-Ransomware quickly detects high volume cyber threats deployed from an external source, isolates the threat, and prevents it from damaging valuable data.

iSecurity Anti-Ransomware STOPS Ransomware attacks immediately as they starts. Even if it is a Zero-Day Attack.

- Raz-Lee's Anti-Ransomware software is the first component of iSecurity ATP.
- A comprehensive advanced threat protection solution for defending IBM i IFS files against ransomware and other kinds of malware.

Why to choose iSecurity Anti-Ransomware?

Protects against ransomware attacks and other kinds of malware that may access and change IBM i data on the IFS. It prevents ransomware from damaging valuable data while preserving performance.

Our Solution:

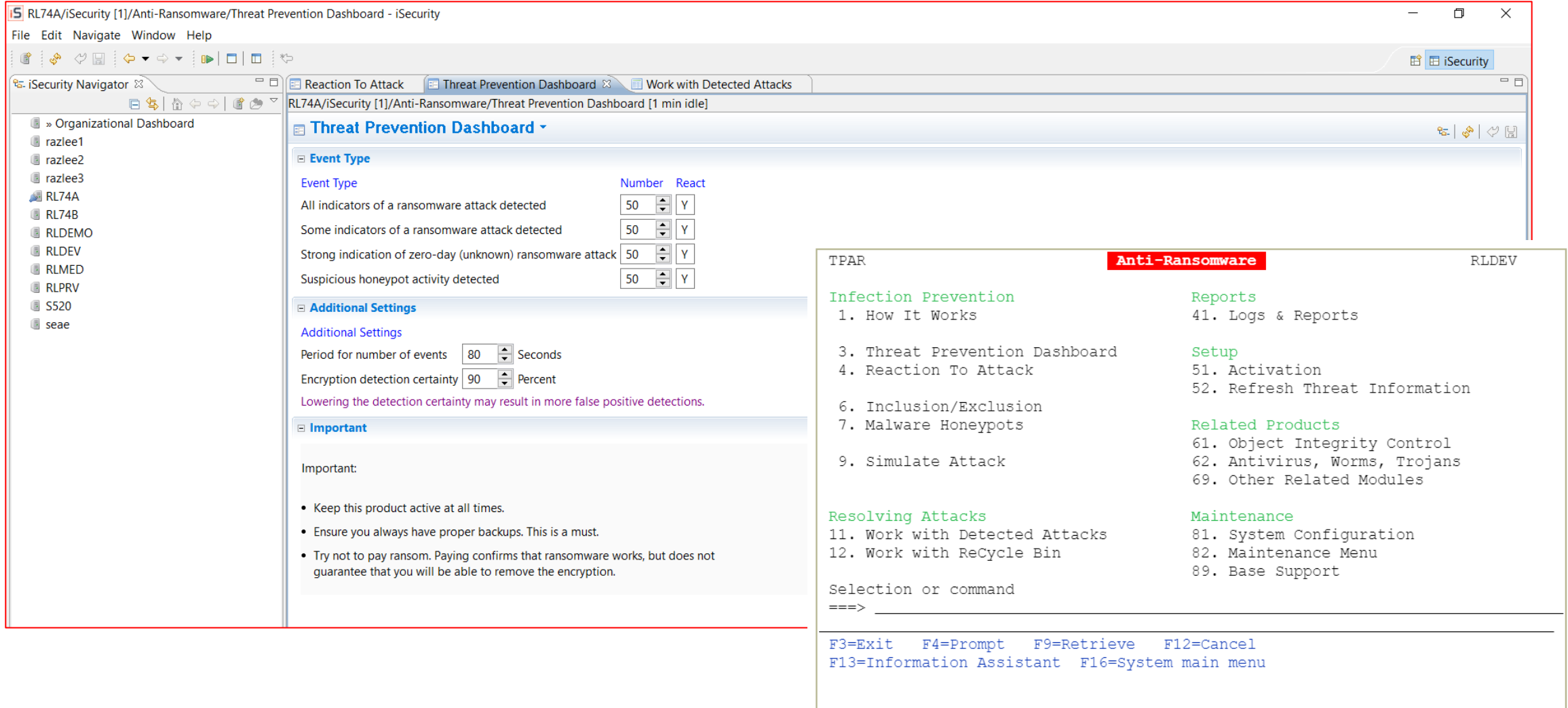
- Identifies, stops, delays, and reports attacks in real-time
- Suspends the attack and alerts the offending computer in real-time
- Disconnects the intruder and sends email, messages and Syslog messages to up to 3 SIEMS in CEF/LEEF formats
- Gets ransomware definitions updates every two hours

How to stop the attack immediatly?



**BUILDING
INTRUSION DETECTION
HONEYPOTS**

Anti-Ransomware in Action



The screenshot displays the iSecurity Threat Prevention Dashboard. The left sidebar shows the iSecurity Navigator with a tree view including Organizational Dashboard, razlee1, razlee2, razlee3, RL74A, RL74B, RLDEMO, RLDEV, RLMED, RLPRV, S520, and seae. The main panel is titled 'Threat Prevention Dashboard' and contains three sections: Event Type, Additional Settings, and Important.

Event Type

Event Type	Number	React
All indicators of a ransomware attack detected	50	Y
Some indicators of a ransomware attack detected	50	Y
Strong indication of zero-day (unknown) ransomware attack	50	Y
Suspicious honeypot activity detected	50	Y

Additional Settings

Additional Settings

Period for number of events: 80 Seconds

Encryption detection certainty: 90 Percent

Lowering the detection certainty may result in more false positive detections.

Important

Important:

- Keep this product active at all times.
- Ensure you always have proper backups. This is a must.
- Try not to pay ransom. Paying confirms that ransomware works, but does not guarantee that you will be able to remove the encryption.

Anti-Ransomware

TPAR RLDEV

Infection Prevention

- How It Works
-
- Threat Prevention Dashboard
- Reaction To Attack
-
- Inclusion/Exclusion
- Malware Honeypots
-
-
- Simulate Attack

Reports

- Logs & Reports

Setup

- Activation
- Refresh Threat Information

Related Products

- Object Integrity Control
- Antivirus, Worms, Trojans
- Other Related Modules

Resolving Attacks

- Work with Detected Attacks
- Work with ReCycle Bin

Maintenance

- System Configuration
- Maintenance Menu
- Base Support

Selection or command
====>

F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=System main menu

Results speaks for their own

iSecurity Anti Ransomware was tested in a completely isolated lab.

TEST ELEMENTS

- IBM i
- Windows based PC with mapped IBM i folder
- Set of 10+ real ransomwares (not emulators)

TEST OUTCOME

- PC data files are encrypted (as expected)
- When IFS file was attacked, the Anti-Ransomware stopped the attack before even the first file was compromised
- Alert was raised
- IBM i was disconnected from the attacking PC
- IBM i survived the attack!

Report after the Attack

Without protection

```
*****
* iSecurity/Anti-Ransomware Attack Simulator Time: 2020-07-09-16.43.31
* Simulating attack on drive A: mapped to IFS folder /atptest.
* User description for the attack . . . . . : Known ransomware without
  protection
* Simulation of ransomware with extension: WNCRY
*****
Now attacking A:\2016.xlsx
Attack completed. File "A:\2016.xlsx.WNCRY" COMPROMISED.
Now attacking A:\Balance.xlsx
Attack completed. File "A:\Balance.xlsx.WNCRY" COMPROMISED.
Now attacking A:\Business.xlsx
Attack completed. File "A:\Business.xlsx.WNCRY" COMPROMISED.

Now attacking A:\PLossSt.xlsx
Attack completed. File "A:\PLossSt.xlsx.WNCRY" COMPROMISED.
Now attacking A:\SInvoice.xlsx
Attack completed. File "A:\SInvoice.xlsx.WNCRY" COMPROMISED.
Now attacking A:\SOrd.docx
Attack completed. File "A:\SOrd.docx.WNCRY" COMPROMISED.
Now attacking A:\SOrder1.docx
Attack completed. File "A:\SOrder1.docx.WNCRY" COMPROMISED.
Now attacking A:\WH_inv.xlsx
Attack completed. File "A:\WH_inv.xlsx.WNCRY" COMPROMISED.
End of Ransomware attack in A:

*****
* iSecurity/Anti-Ransomware
* User description for the attack . . . . . : Known ransomware without
  protection
* Simulation of ransomware with extension . : WNCRY
* Attack completed on drive A: mapped to IFS folder /atptest.
* ALL 2217 FILES CORRUPTED.
* Activate iSecurity/Anti-Ransomware, and run the Simulator again.
*****
```

With protection

```
*****
* iSecurity/Anti-Ransomware Attack Simulator Time: 2020-07-09-16.45.47
* Simulating attack on drive A: mapped to IFS folder /atptest.
* User description for the attack . . . . . : Known ransomware with protection
* Simulation of ransomware with extension: WNCRY
*****
Now attacking A:\2016.xlsx
Attack completed. File "A:\2016.xlsx.WNCRY" COMPROMISED.
Now attacking A:\Balance.xlsx
Attack completed. File "A:\Balance.xlsx.WNCRY" COMPROMISED.
Now attacking A:\Business.xlsx
Connection to IFS is disabled. Attack failed. File A:\Business.xlsx SURVIVED.

*****
* iSecurity/Anti-Ransomware *STOPPED* the attack.
* User description for the attack . . . . . : Known ransomware out protection
* Simulation of ransomware with extension: WNCRY
* 2 Files compromised before the attack was detected and stopped
* Alerts were sent to the Administrator.
* Future connections to the mapped drive are rejected.
* To clear the attack use GUI or STRAR, 11.

*****
```

Advantages when being evaluated against competition

- Ability to work asynchronous achieving a huge performance impact.
- 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.
- Sandbox, Remember the Wolf, Wolf story? This 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.
- Attack simulator
- Ability to shutdown (or put in sleep mode) the attacker, before disconnecting him from IBM i.
- Recycle Bin.

iSecurity Anti-Ransomware Advantages

- Automatic, regularly updated database
- Command-line scanner
- Database updater with support for digital signatures
- Cannot 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