

RAZ-LEE

iSecurity Antivirus

Advanced threat protection solution for defending AIX 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) and now to AIX.

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

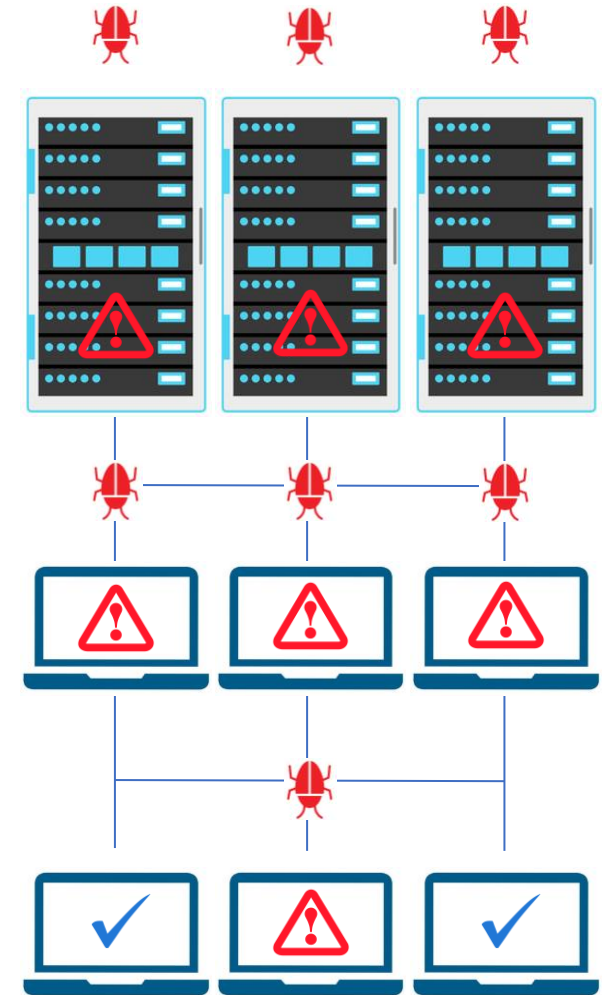
- Audit Journal, System Values, Status...
- Proactive re-**Action** in real time
- Capture screen activity
- Compliance of Users, Objects, IFS
- Change Tracker watch Production Libraries

iSecurity Antivirus

Advanced threat protection solution for defending AIx against malware

Is AIX affected by Viruses?

- The threat of malware, ransomware, and malicious code is nothing new. However, the makeup of the systems they target has changed. The days of believing it's "just a Windows thing" are over – and if your AIX servers aren't properly secured, your organization is at serious risk.
- Although the AIX 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.
- Windows clients connect to servers and become infected, interrupting business operations until they are cleaned – but the cycle repeats because the Servers are infected and hosting malware.



Why to choose iSecurity Antivirus?

ClamAV engine implementation brings

- A database of over eight million virus signatures
- Signatures are continually updated
- 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 implementation brings

- On-Access Scanning
- On-Demand Scanning
- **Only-New Scanning. Marking files as scanned so no need to scan them again unless they have changed**
- Cannot be disabled by any known virus keeping the server protected without interruption
- Runs Local and natively at the AIX

What is Only-New Scanning?

Scan for viruses is by definition CPU intensive. There are 8,600,000+ signatures that must be compared to the contents of the object. Beyond this there is the heuristic scan which search for zero-day viruses. iSecurity Antivirus marks internally object that were scanned. This happens on both On-Access and On-Demand scans.

When a file is opened, the On-Access scan is automatically called to scan the object. This WILL NOT happen if the file has not changed since it was last scanned. Huge performance advantage!

When the ON-Demand scan is used, a parameter can be set to scan Only-New or the file has changed since then. So much more efficient. So much faster.

Based on ClamAV



- iSecurity Antivirus uses ClamAV for scanning malware
- ClamAV is owned by Cisco
- Open-source, Cross-platform
- Considered as One of the Five best antiviruses

Antivirus in Action (Native Interface)

```
OpenSSH SSH client
bash-5.2# /avmenu

Menu Antivirus (AV)

1) Start AV on-access          9) Refresh signature DB Internet 17) Test AV on access
2) End AV on-access           10) Refresh signature DB Lan      18) Freshclam log
3) AV on access Status        11) Refresh signature DB Dir     19) Wget log
4) AV log                     12) Signature DB Directory       20) Scanav logs
5) AV on access debug         13) New log                     21) All logs & debug files
6) AV Configuration          14) New debug                   22) Q/q Quit
7) Freshclam Configuration    15) Remove old log/debug files
8) Refresh signature DB Razlee 16) Create virus file for test

Please enter your choice: _
```

Retrieving Signatures (Native Interface)

```
OpenSSH SSH client
bash-5.2# /avmenu

Menu Antivirus (AV)

1) Start AV on-access          9) Refresh signature DB Internet 17) Test AV on access
2) End AV on-access           10) Refresh signature DB Lan      18) Freshclam log
3) AV on access Status        11) Refresh signature DB Dir     19) Wget log
4) AV log                     12) Signature DB Directory       20) Scanav logs
5) AV on access debug         13) New log                     21) All logs & debug files
6) AV Configuration          14) New debug                   22) Q/q Quit
7) Freshclam Configuration    15) Remove old log/debug files
8) Refresh signature DB Razlee 16) Create virus file for test

Please enter your choice: 10
/SMZV/home/SMZVDTA/script/refresh.sh: line 346: ${freshLog}: ambiguous redirect
Start refreshing signatures for AV
Retrieve signature files from url: http://1.1.1.129
daily.cvd                      13%[=====>] 7.94M 465KB/s eta 1m 47s
```

On-Access in Action (Native Interface)

```
OpenSSH SSH client
24.04.01-13:48:47 : strrtav.sh : Starting Antivirus on access...
24.04.01-13:48:47 : strrtav.sh : View debug by: tail -50 -f /SMZV/home/SMZVDTA/log/on_access_debug.txt
24.04.01-13:48:47 : strrtav.sh : View log by: tail -50 -f /SMZV/home/SMZVDTA/log/av.log
24.04.01-13:48:48 : strmon.sh : Starting 1 avrt processes ...
24.04.01-13:48:48 : avrt 1 : start on-access
24.04.01-13:49:18 : avrt 1 : On-access finished signature loading
24.04.01-13:49:18 : avrt 1 : start on-access
24.04.01-13:49:20 : strmon.sh : 1 avrt processes started
24.04.01-13:49:20 : strmon.sh : Antivirus on access is active
24.04.01-13:52:14 : avrt 1 : Virus Win.Test.EICAR_HDB-1 detected in file: /home/AV/test/eicar.com
24.04.01-14:05:20 : endrtav.sh : De-Activating Antivirus on access...
24.04.01-14:05:22 : endrtav.sh : Antivirus on access De-Activated.
24.04.01-14:30:07 : strrtav.sh : Starting Antivirus on access...
24.04.01-14:30:07 : strrtav.sh : View debug by: tail -50 -f /SMZV/home/SMZVDTA/log/on_access_debug.txt
24.04.01-14:30:07 : strrtav.sh : View log by: tail -50 -f /SMZV/home/SMZVDTA/log/av.log
24.04.01-14:30:07 : strmon.sh : Starting 1 avrt processes ...
24.04.01-14:30:07 : avrt 1 : start on-access
24.04.01-14:30:41 : avrt 1 : On-access finished signature loading
24.04.01-14:30:41 : avrt 1 : start on-access
24.04.01-14:30:41 : strmon.sh : 1 avrt processes started
24.04.01-14:30:41 : strmon.sh : Antivirus on access is active
24.04.01-14:34:07 : avrt 1 : Virus Win.Test.EICAR_HDB-1 detected in file: /home/AV/test/eicar.com
24.04.01-14:38:28 : avrt 1 : Virus Win.Test.EICAR_HDB-1 detected in file: /home/AV/test/eicar.com
24.04.01-14:40:21 : avrt 1 : Virus Win.Test.EICAR_HDB-1 detected in file: /tmp/eicar.com
24.04.01-14:40:21 : avrt 1 : Virus Win.Test.EICAR_HDB-1 detected in file: /tmp/eicar.com
24.04.01-14:45:14 : sndEmail.sh : email --, sent to: oren.chemel@razlee.com cc:
24.04.01-14:45:14 : sndEmail.sh : help
24.04.01-15:03:33 : blockVirusFile.sh : *FYI*: Virus found in computer rlaix1
24.04.01-15:03:33 : blockVirusFile.sh : Path: /home/AV/test/eicar.com
24.04.01-15:03:33 : blockVirusFile.sh : Virus name: orentest
24.04.01-15:03:33 : sndEmail.sh : email *FYI*: Virus found in computer rlaix1, sent to: oren.chemel@razlee.com cc:
24.04.01-15:03:33 : sndEmail.sh : *FYI*: Virus found in computer rlaix1
av.log (55%)
```

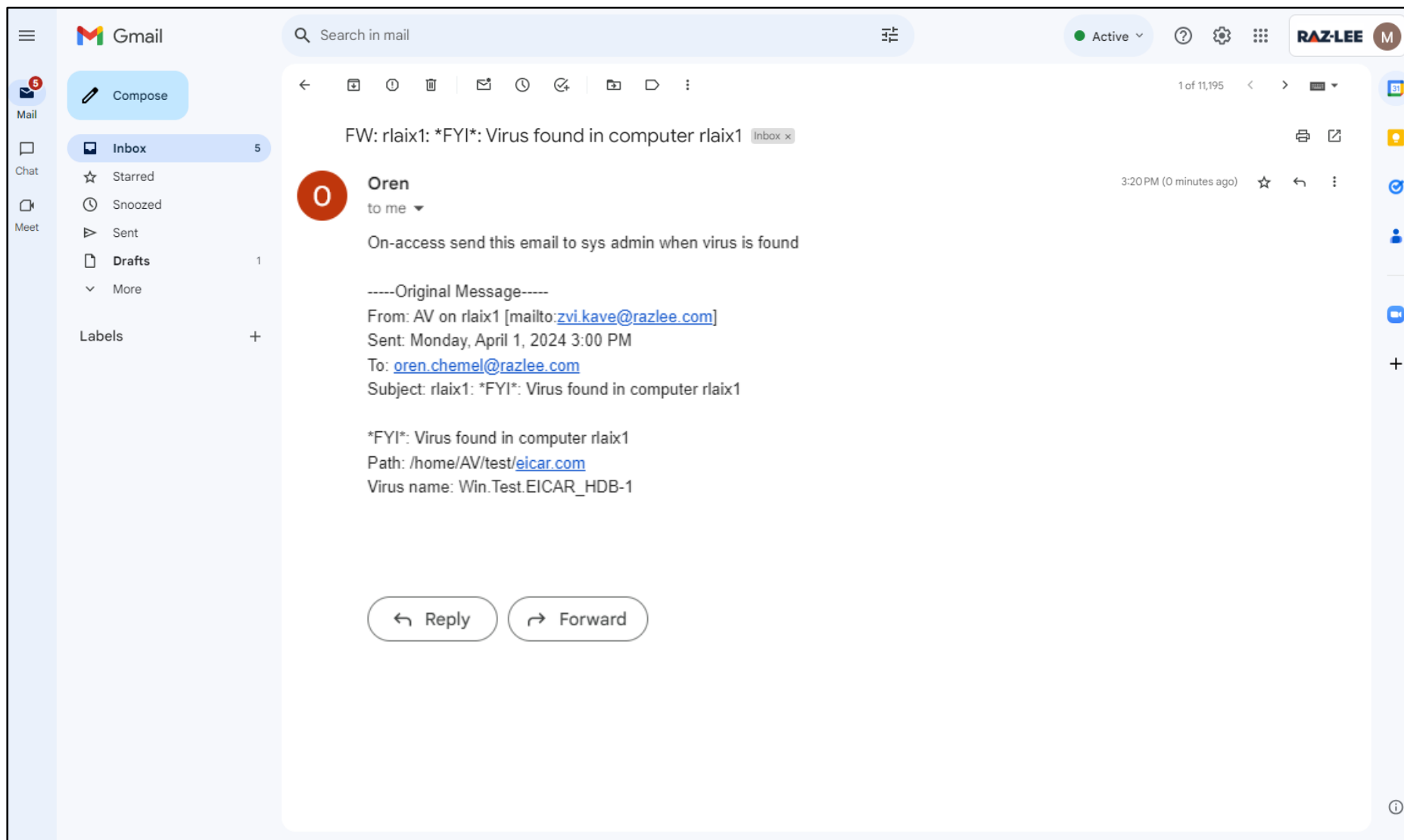
On-Demand in Action (Native Interface)

```
OpenSSH SSH client
bash-5.2# /scanav /home/orenc/test1/
LibClamAV Warning: *****
LibClamAV Warning: *** The virus database is older than 7 days! ***
LibClamAV Warning: *** Please update it as soon as possible. ***
LibClamAV Warning: *****
Loading: 28s, ETA: 0s [=====>] 8.68M/8.68M sigs
Compiling: 7s, ETA: 0s [=====>] 41/41 tasks

Scan request: /home/orenc/test1/
/home/orenc/test1/edemo.h: OK
/home/orenc/test1/edemo1.h: OK
/home/orenc/test1/edemo2.h: OK
/home/orenc/test1/edemo22.h: Empty file
/home/orenc/test1/edemo7777.h: OK
/home/orenc/test1/eicar.com: Win.Test.EICAR_HDB-1 FOUND
sh: /SMZV/home/SMZVDTA/scripts/snd_clamscan.sh: not found.
/home/orenc/test1/eicar.com: Win.Test.EICAR_HDB-1 PROBLEM TO SEND EMAIL WITH VIRUS INFORMATION
/home/orenc/test1/eicar2.com: Win.Test.EICAR_HDB-1 FOUND
sh: /SMZV/home/SMZVDTA/scripts/snd_clamscan.sh: not found.
/home/orenc/test1/eicar2.com: Win.Test.EICAR_HDB-1 PROBLEM TO SEND EMAIL WITH VIRUS INFORMATION


----- SCAN SUMMARY -----
Known viruses: 8683167
Engine version: 0.104.2
Scanned directories: 1
Scanned files: 6
Infected files: 2
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 40.005 sec (0 m 40 s)
Start Date: 2024:04:01 15:53:29
End Date: 2024:04:01 15:54:09
log: /SMZV/home/SMZVDTA/log/scanav_2024-04-01-15:53:29
```


Email Notification





Web Interface


Raz-Lee Security AV on AIX


perla


 Activation


 Configuration


 Logs


 Directories

 Refresh


 Functions

 Installation

 Help



<input type="checkbox"/>	IP	Description
<input type="checkbox"/>	1.1.1.97	AIX2 - second AIX server on our internal network
<input type="checkbox"/>	1.1.1.99	AIX1 - first AIX server on our internal network



<input type="checkbox"/>	Time	Task	Status
<input type="checkbox"/>	10/22/2024, 9:33:06 AM	wget Log	Completed
<input type="checkbox"/>	10/22/2024, 9:26:25 AM	Refresh signature DB Razlee	Completed
<input type="checkbox"/>	10/22/2024, 9:22:48 AM	Scan a directory	Completed
<input type="checkbox"/>	10/22/2024, 9:06:27 AM	AV on-access Status	Completed
<input type="checkbox"/>	10/22/2024, 9:06:19 AM	Infected Files In Quarantine	Completed
<input type="checkbox"/>	10/22/2024, 9:06:13 AM	All logs and debug files	Completed
<input type="checkbox"/>	10/22/2024, 9:06:06 AM	Scanav logs	Completed
<input type="checkbox"/>	10/22/2024, 9:05:58 AM	Signature DB	Completed

AV Configuration (Web Interface)

Raz-Lee Security AV on AIX

perla

Activation

Configuration

Create virus file for test

Check AV on-access

Test email settings

New log

New debug

Remove old log/debug files

Password of email

Freshclam

AV

Logs

Directories

Refresh

Functions

IP	Description	Time	Task	Status
<input checked="" type="checkbox"/>	1.1.1.97		wget Log	Completed
<input checked="" type="checkbox"/>	1.1.1.99		Refresh signature DB Razlee	Completed
<input type="checkbox"/>	1.1.1.99		Scan a directory	Completed
<input type="checkbox"/>	1.1.1.99		AV on-access Status	Completed
<input type="checkbox"/>	1.1.1.99		Infected Files In Quarantine	Completed
<input type="checkbox"/>	1.1.1.99		All logs and debug files	Completed
<input type="checkbox"/>	1.1.1.99		Scanav logs	Completed
<input type="checkbox"/>	1.1.1.99		Signature DB	Completed
<input type="checkbox"/>	1.1.1.99		wget Log	Completed
<input type="checkbox"/>	1.1.1.99		AV on-access debug	Completed
<input type="checkbox"/>	1.1.1.99		AV Log	Completed
<input type="checkbox"/>	1.1.1.99		Freshclam Log	Completed
<input type="checkbox"/>	1.1.1.99		AV version	Completed
<input type="checkbox"/>	1.1.1.99		Install AV	Completed
<input type="checkbox"/>	1.1.1.99		AV version	Completed
<input type="checkbox"/>	1.1.1.99		Uninstall AV	Completed
<input type="checkbox"/>	1.1.1.99		AV version	Completed

AV Configuration

```
# AIX Antivirus configuration file  
  
# includePrefix: Which path to be scanned On-Access.  
# Only the first (<Directory> must be full and exist, the rest of the path can  
# be prefix of the path  
#includePrefix /home/test  
#includePrefix /home1  
  
# Path that its prefix match excludePrefix is not scanned.  
#excludePrefix /home/test/abcd  
  
# onlyNew : scan only files that were modified since their last scan.  
# last scan can be done by On-Access or by On-Demand  
#onlyNew  
  
# scanRoot (Y) : Scan also files opened by root On-Access.  
#scanRoot Y  
  
#emailSMTP: SMTP server address of emailUser  
#emailSMTP smtp.gmail.com  
  
#emailPort: SMTP port number of emailUser  
#emailPort 587  
  
#emailUser: Email address sender from SMTP
```

Submit

iSecurity Antivirus Advantages

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

- Scan On-Access, On-Demand and Only-New
- Cannot be disabled by viruses
- Improved Memory and Processor usage, preventing unnecessary file's scanning if there is no change since last scan
- Command-line scanner
- Regularly updated database from ClamAV and Raz-Lee
- Database updater with support for digital signatures
- Built-in support for zip, gzip, jar, and tar files
- History Log for review and analysis
- User-friendly Web Interface & Native Interface



Thank You

For more information about our company and products please visit

www.razlee.com