RAZ-LEE

iSecurity Anti-Ransomware

Cyber Security

RAZ-LEE iSecurity

About Raz-Lee

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).

- ✓Corporate offices in: Israel, USA & Germany
- ✓Partnerships with major global SIEM & DAM solution providers

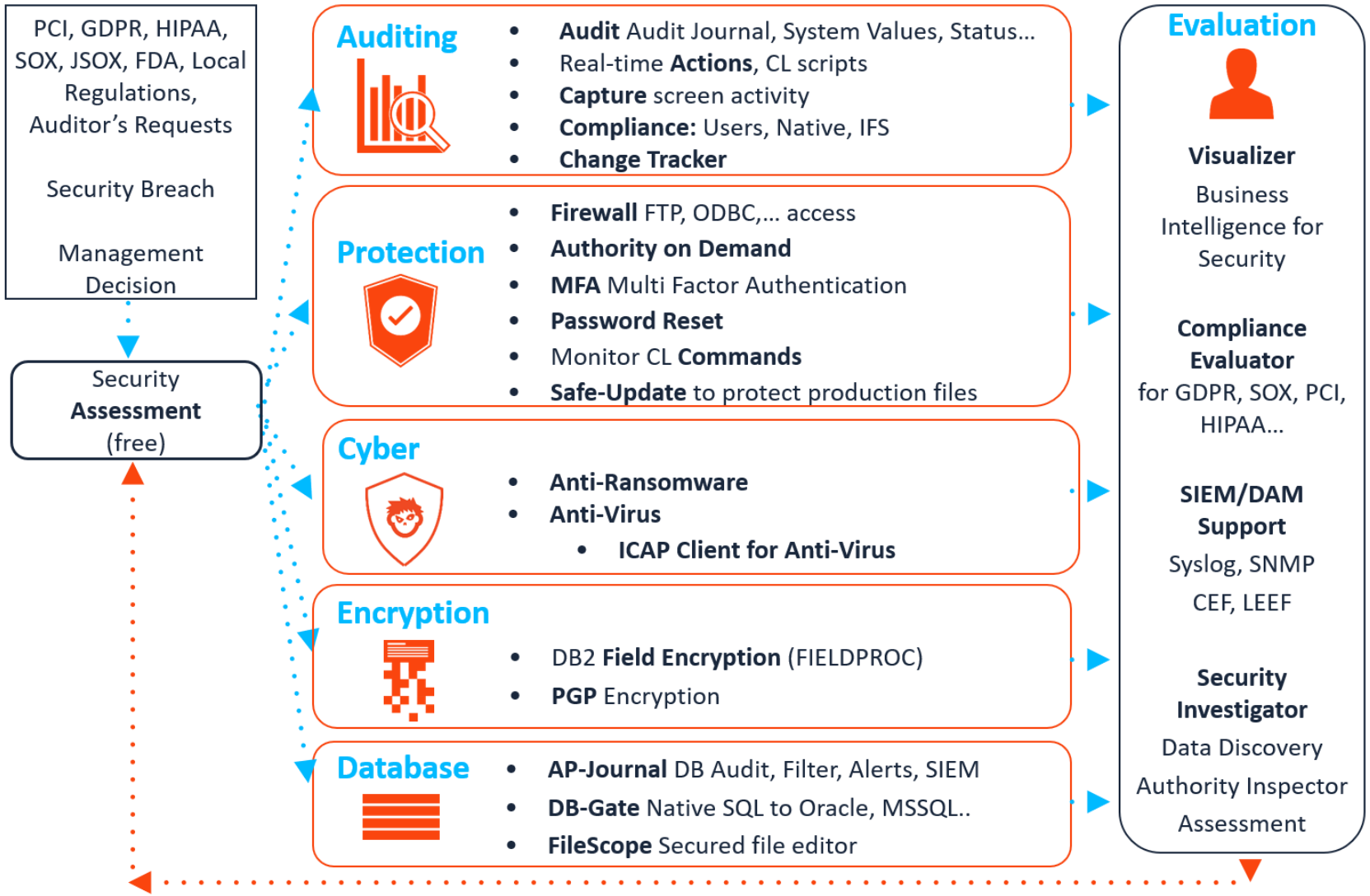
Technology Business Partners

imperva Akamai SEA™ SOFTWARE ENGINEERING OF AMERICA

McAfee™ IBM

RAZ-LEE iSecurity

iSecurity Suite



RAZ-LEE iSecurity

What's Ransomware?

Ransomware is a cyber-attack that blocks access to a computer system or files until a determined amount of money is paid for a decryption key.

- Ransomware attacks any file it can access including connected devices, mapped network drivers, shared local networks, and cloud storage services that are mapped to the infected computer.
- Ransomware doesn't discriminate. It encrypts every data file that it has access to, including the IFS files.
- Every 11 seconds a ransomware attack on businesses networks is expected

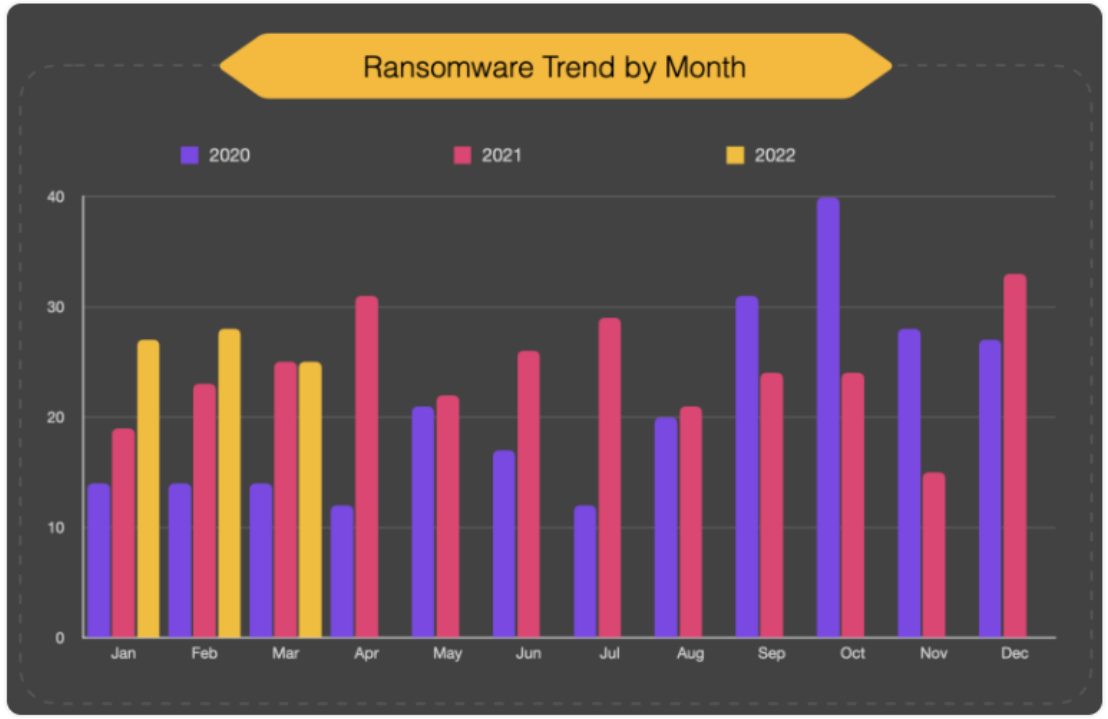
RAZ-LEE iSecurity

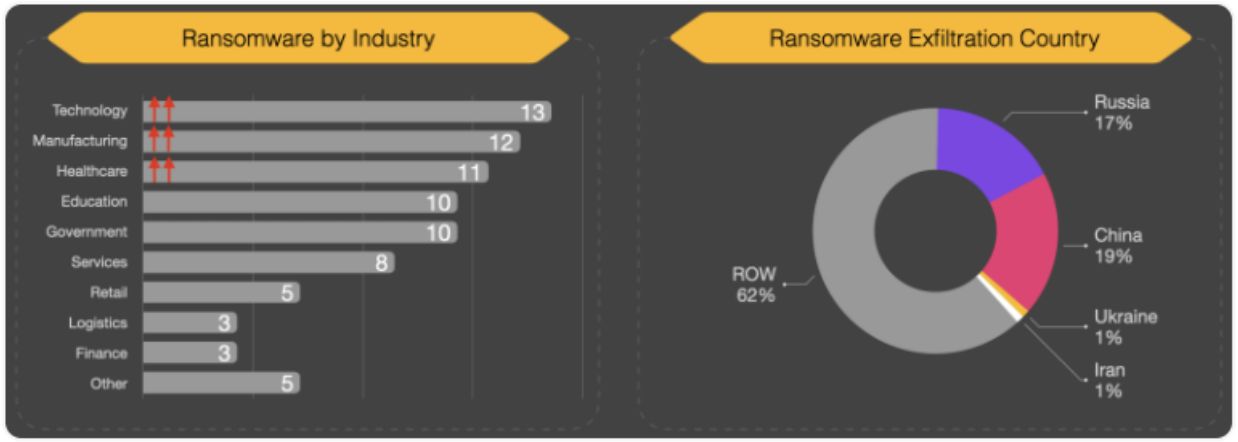
Actual Situation

Ransomware started strong in 2022 with a significant attack on Bernalillo County in New Mexico making headlines.

The incident closed most government buildings and impacted education in the area.

The cyberattack also had a knock on effect at a county jail when the security camera and automatic doors were knocked offline leaving the inmates in lockdown.





RAZ-LEE iSecurity

Latest Reports

This major ransomware attack was foiled at the last minute. Here's how they spotted it
https://www.zdnet.com/article/this-ransomware-attack-was-foiled-at-the-last-minute-heres-how-they-spotted-it/

Over 65,000 ransomware attacks expected in 2021: former Cisco CEO
https://finance.yahoo.com/news/over-65000-ransomware-attacks-expected-in-2021-former-cisco-ceo-125100793.html

Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices
https://threatpost.com/linux-variant-ransomware-vmwares-nas/167511/

IBM i /AS/400 Viruses, Malware, Spyware, Ransomware, the IBM i Operating System, and the Integrated File System 2020
https://www.ibm.com/support/pages/viruses-malware-spyware-ransomware-ibm-i-operating-system-and-integrated-file-system

RAZ-LEE iSecurity

How to protect our systems?

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

- 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

RAZ-LEE iSecurity

iSecurity Anti-Ransomware at a Glance

View Video

RAZ-LEE iSecurity

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.

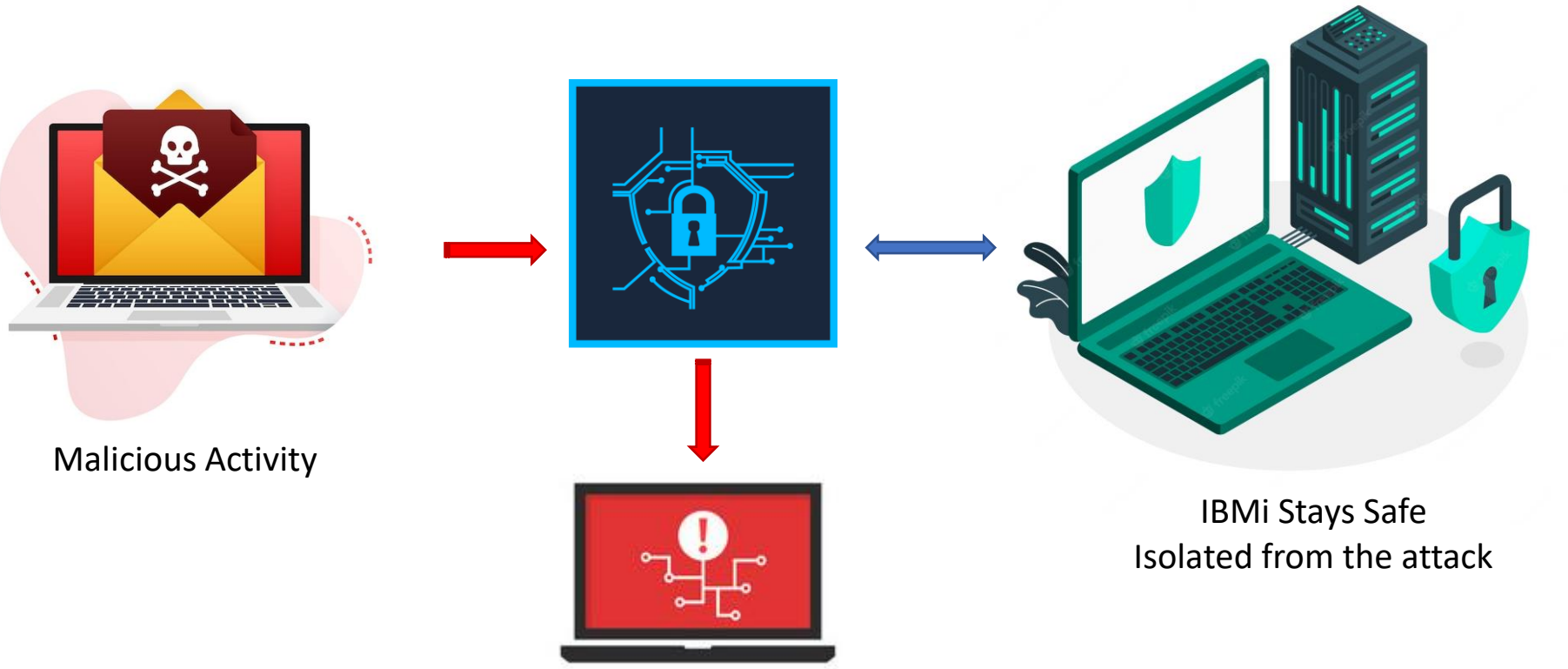
Our Solution:

- 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

RAZ-LEE iSecurity

How Anti-Ransomware Works?

As malicious activity is diagnosed, the anti-ransomware stops the attack, disconnects the intruder, and raises an alert.



Malicious Activity

Administrator
Alert

IBMi Stays Safe
Isolated from the attack

RAZ-LEE iSecurity

Results speaks for their own

iSecurity Anti Ransomware was tested in a completely isolated lab which included:

- 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!

RAZ-LEE iSecurity

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.

*******************************************************************************
```

RAZ-LEE iSecurity

Key Features

- 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

RAZ-LEE iSecurity

RAZ-LEE

Thank you

Please get further information at **www.razlee.com**

RAZ-LEE iSecurity