Case Studies:
AV & AR

Rhenag Compliance for Cyber Security Regulations for EU Financial Entities

Protect IBM i Servers from Virus infection and Ransomware attacks.

As a large European trading company operating under strict regulatory frameworks, **Rhenag** must ensure continuous protection of its IBM i environment against modern cyber threats. With increasing exposure to **zero-day attacks, malware, and ransomware**, traditional perimeter defenses were no longer sufficient. The organization required the ability to **detect and respond to security events in real time**, ensuring business continuity and regulatory compliance.

To address this risk, Rhenag implemented a **Zero-Day Attack Prevention Solution** based on multiple modules of the **Raz-Lee iSecurity Suite**. The objective was to protect the IBM i system from malware that could already be present in the environment, preventing both system infection and the potential spread of ransomware across the network.

iSecurity Anti-Ransomware continuously monitors ransomware signatures and suspicious encryption behavior. When malicious activity is detected, the solution automatically blocks the attack. Even in cases where an authorized user initiates harmful activity, the software immediately disconnects the user session, stopping the attack before data can be encrypted or compromised.

In parallel, **iSecurity Antivirus** provides advanced protection for **native IFS files**, efficiently scanning content while preserving IBM i performance. The solution supports integration with an **ICAP server**, allowing **Rhenag** to select its preferred scanning engine and database for flexible and scalable malware protection.

Together, these capabilities deliver **real-time threat detection, immediate response, and strong protection against ransomware and virus infections**, enabling **Rhenag** to meet EU cybersecurity and compliance requirements while securing its IBM i infrastructure.

> “Being able to detect in real time is a great advantage, as every system in the company is secured and we have a global vision of our Cyber security.”
>
> **IT Security Manager, Rhenag**

Case Studies:
AV & AR

Protecting Municipal Data Against Modern Cyber Threats

Real-time ransomware detection and response for government IBM i environments

Bossier City Municipality manages and maintains vast amounts of sensitive data related to its infrastructure and residents, including property tax records, social security numbers, and voter information. At the same time, public sector organizations are legally required to operate with transparency. While open government initiatives improve access to public records, they also increase the attack surface for cybercriminals seeking to exploit systems that store sensitive information.

As a custodian of personally identifiable information, the municipality has a fiduciary responsibility to protect this data. With cyberattacks and ransomware incidents increasingly targeting local governments of all sizes, a reactive security approach was no longer sufficient. The IT team identified the need for a **proactive anti-ransomware solution** capable of operating natively within the IBM i server environment, with the ability to **scan activity, detect malicious behavior, and immediately disconnect intruders**.

The municipality implemented **iSecurity Anti-Ransomware**, gaining real-time protection against ransomware and unauthorized activity. The solution continuously monitors system behavior and automatically stops attacks before they can spread or encrypt data. Its **graphical user interface (GUI)** allows IT managers to define rules, generate reports, and manage security controls directly from a Windows workstation connected to the IBM i environment, simplifying both daily operations and security audits.

The implementation was completed across **multiple IBM i LPARs** without disruption, delivering centralized visibility and consistent protection across the municipal infrastructure. As a result, Bossier City Municipality now benefits from **real-time threat detection, immediate response, and simplified security management**, strengthening its overall cybersecurity posture.

> “Having a native IBM i anti-ransomware solution with real-time detection and a simple graphical interface has significantly improved our ability to protect sensitive municipal data without adding operational complexity.”
>
> **Cyber Security Consultant, Bossier City Municipality**

Case Studies:
AV & AR

Regulatory Compliance to protect MUFG IBM i from Virus infection.

Protect IBM i Servers from Virus infection and Ransomware attacks.

Banks and financial institutions, such as **MUFG**, operate in one of the most heavily targeted industries for cybercrime. The combination of high-value financial data, strict regulatory oversight, and mission-critical systems makes proactive cybersecurity not optional, but essential. Traditional, reactive security controls are no longer sufficient to defend against modern malware and ransomware threats.

To protect their IBM i environment, financial institutions require **proactive security technologies** capable of detecting, preventing, and responding to threats quickly and effectively—without disrupting core banking operations. Ensuring protection of native IFS files while maintaining system performance is a key requirement, as is meeting the expectations of internal compliance and audit teams.

Raz-Lee’s **iSecurity Antivirus** was implemented to address these challenges. The solution operates **natively on the IBM i server** or through an **ICAP client**, ensuring continuous protection without reliance on external processes. It is built on the **ClamAV engine**, developed by Cisco and distributed by IBM as part of the AIX package, providing trusted and proven malware detection.

iSecurity Antivirus cannot be disabled by any known virus and is specifically optimized to **protect native IFS files while efficiently using IBM i resources**. The flexibility to select the preferred **ICAP server and virus definition database** allows financial institutions to align the solution with their existing security architecture and operational requirements.

As a result, **regulatory compliance requirements are met and exceeded**, providing compliance departments with the controls, visibility, and assurance needed to satisfy internal policies and external regulations—while maintaining strong, real-time protection against virus infections and ransomware attacks.

> “Every financial institution needs an antivirus solution that is 100% reliable, native and always up to date...”
>
> **IT Senior Manager, MUFG Bank**