KEY RESOURCES
The Key to zSystems Integrity

CASE STUDY

Global Health Information and EHR Technologies Company converts to RACF

OUR CHALLENGE

- 16 months to convert from CA ACF2 to RACF in order to meet ROI Savings of $12M over 5 years
- Technically complex environment
- Heavy integration of CA ACF2 in applications and provisioning

CLIENT HIGHLIGHTS

- 29,000+ employees
- 27,000 facilities around the world
- 2020 revenue: $5.5 billion

REQUIREMENTS

- Convert 12 CA ACF2 databases to RACF
- Provide compliance services
- Convert native DB2 security to DB2 for RACF
- Provide RACF and zSecure training for 15+ remote admins and security engineers

Global companies collect millions of pieces of sensitive information from their clients, including names, addresses, social security numbers and employment data. This information is often stored within their mainframe enterprise because of its built in integrity.

After consolidating data centers this client decided they needed to power their security operations by modernizing their security with an open and connected security platform, but they also knew they needed to move to an integrated security model on the mainframe in order to take advantage of IBM's software integration and consolidation offerings.

Transforming their Mainframe Security in 16 Months

The goal was to consolidate security administration and audit reporting into a central security operations center that will help facilitate incident management.

We brought in our security conversion team to provide a mainframe security assessment that gave them the confidence the conversion could be done in 16 months with the appropriate resources. We supplied a Conversion Specialist to lead the project, a DB2 security conversion specialist, sophisticated tools to automate the conversion, and a dedicated Project Manager to keep everyone on track. Training was provided on RACF and zSecure.

As each security database was converted from CA ACF2 to RACF compliance assessment software was deployed to determine where compliance gaps were occurring based on their security policy. These gaps were then mitigated quickly and efficiently by the organizations security team.