Addressing Complex Security Requirements at European Ministry of Interior

The Challenge

The Ministry of the Interior of a European country manages a diverse portfolio of critical tasks from fighting crime, terrorism, and corruption to addressing immigration, asylum, civil protection and airport security. Because of its broad mandate and the sensitive nature of the data it handles, the Ministry is required by federal and European Union (EU) security and compliance laws to monitor and maintain detailed records of every query associated with this sensitive data. This was no small task considering that there are over 50 classifications of sensitive data which the Ministry maintains in their complex mix of UNIX and mainframe database environments.

The detailed audit information required for each database transaction included the name and ID of the person who was accessing sensitive database tables and rows, what business intelligence (BI) or other application was used, the application report names, the semantic layer (Cognos Project or Business Objects Universe) and the SQL query which generated the report and, importantly, the actual information the query returned to the user.

The Ministry's security and compliance challenge was further complicated by the fact that the required audit information was either not available in current systems or captured by a variety of monitoring utilities across authentication tools, databases and server operating systems.

They also determined that there was no way to correlate each SQL database query with the actual user because the applications employed database connection pooling and generic proxy database ID's that masked the actual user identity. In addition the compliance audit information needed to be kept for seven years in a highly secure database that Ministry security and compliance staff could independently analyze quickly and easily with minimal training.

Finally, due to limited staff resources, and the immediate security requirements, the Ministry could not afford a complex and lengthy implementation and training cycle.

BENEFITS DELIVERED

Met demanding federal and EU security and compliance requirements

Integrated across complex database and system environments

Seamlessly integrated with authorization tools and applications to provide user-focused auditing and reporting

Enabled a quick implementation without costly customizations

Empowered staff to analyze activity across all 50 sensitive data classifications

The Solution

The Ministry selected Teleran's Data Security and Compliance software solution to fulfill their sophisticated security and compliance mandates. Teleran's solution enabled the Ministry to quickly and cost effectively address challenging EU and federally mandated regulations.

Teleran's solution not only enabled the Ministry to capture, audit and securely store highly sensitive data usage information, but also enabled Ministry staff to independently analyze and report on usage with minimal training and technical support.

The Benefits Delivered

Teleran's Data Security and Compliance solution provided the following benefits and advantages over competitive products.

- Captured 100% of the needed compliance audit information, combining actual user ID, with application and data usage, and the complete results sets
- Seamlessly integrated into complex Unix and mainframe database environments
- Integrated with authorization tools and applications to provide comprehensive auditing and reporting
- Enabled a quick implementation process without costly customizations
- Delivered a compliance analysis application enabling Ministry staff to flexibly analyze activity across all 50 sensitive data classifications
- Provided audit reports that documented the Ministry is meeting all mandated compliance regulations

For more information on Teleran's Data Security and Compliance Solution visit www.teleran.com or call +1.973.439.1820.