Guardium®

Customer Success Story

McCarran International Airport

Organization: Clark County Dept. of Aviation

Headquarters: Las Vegas, Nevada, USA

URL: http://www.mccarran.com

Industries: Government, Transportation, Travel

Employees: Between 1,000 and 2,000

Annual Revenue (in USD): $250-$500 Million

"Prior to deploying SQL Guard, our DBAs spent three to five hours a week digging through logs and monitoring real time access to the databases. We now spend a few minutes each week reviewing SQL Guard reports."

"With SQL Guard, we are alerted immediately of any issues and we can handle them before they become problems. In this day and age, that is a vital advantage."

~ Phillip Murray, DBA OCP, McCarran Airport

Overview

McCarran needed to:

- Secure data and protect information
- Create independent audit trails
- Detect database attacks
- Increase visibility to see when users, authorized or not, gain access to sensitive data

Guardium provided:

- Instant alerts for any unauthorized activities
- Independent audit trails and vault safe auditing repositories
- Powerful protection for all private, confidential, and personal information
- Complete visibility into all database access activities
- Immediate time and cost savings

Multiple issues, a single solution

McCarran International Airport is part of the Clark County Airport System, which owns and operates six airports, including five general aviation facilities. The airport consists of 96 gates in two terminals.

Several issues combined to bring to light McCarran's need for a comprehensive layer of database security. McCarran's databases contained, among other things, sensitive data. Also, a number of databases were being consolidated into a single enterprise repository, and the access control application was being moved from a stand-alone network to the corporate network, thus leaving the databases more vulnerable. Finally, McCarran wanted to increase database access visibility.

Security staff at McCarran needed a tool that would empower them to prevent inside and outside attacks, provide alerts when unauthorized access or restricted data manipulation occurred, and create independent audit trails.

"I read an online news story about Guardium's SQL Guard and it sounded like the product had the potential to address the problems we had identified," said Phillip Murray, DBA OCP and Departmental System Administrator.

"When placed on the network, SQL Guard can be used to efficiently monitor, report, and manage database access activities. SQL Guard delivers non-intrusive data access monitoring and control. So I discussed [SQL Guard] with our Assistant Director of Aviation, Information Systems, and the Airport Security Administrator, who both agreed that it was worth investigating."

"It was that simple"

McCarran invested in G2000 platforms to monitor SQL Server and Oracle databases. "After we received the SQL Guard appliances, we plugged them in and away we went – it was that simple," said Murray.

SQL Guard's Dynamic Policy Baseline Builder collected access information. This data enabled Murray's team to automatically create a baseline of normal database activity based on access pattern history and ongoing activities. This baseline became the foundation on which they could build additional enforceable rules, as well as utilize the rules automatically suggested by SQL Guard.

After analyzing the baseline, policies were created to reflect normal database usage. SQL Guard was then configured to alert DBA staff, in real time, to anything outside of normal activity.

Using SQL Guard, Murray and his team immediately found "database changes that would never have been detected before SQL Guard," said Murray. "Additionally, we discovered that a third party application was producing 130,000 database errors a day."

Instant ROI

Murray presented his SQL Guard trial period findings to the Deputy Director of Aviation.

"We weighed the cost of the system against the cost of any event that led to the failure of our access control system and it was an easy decision to make. Failure of the access control system would mean that, according to FAA regulations, the airport would have to be shut down until access control was restored.

"Every moment that a database attack is left unnoticed means loss of money, time, and reputation, and increases the time it can take to repair the resulting issues. With SQL Guard, we are alerted immediately of any issues and we can handle them before they become problems. In this day and age, that is a vital advantage."

SQL Guard also provided McCarran with immense time and cost savings.

"Prior to deploying SQL Guard, our DBAs spent three to five hours a week digging through logs and monitoring real time access to the databases. We now spend a few minutes each week reviewing SQL Guard reports," said Murray

"Without SQL Guard, due to workload and resource constraints, only random samplings of SQL code could be reviewed. With the SQL Guard appliance, ALL SQL is monitored automatically. Additionally, the time to discovery of any database access issues went from days or weeks to instantaneous.

He continued, "With real time alerts and easily-created reports provided by SQL Guard, we can now swiftly and instantly respond to any potential issues."

Future plans

To achieve enterprise-class manageability and scalability, McCarran is now planning to deploy a SQL Guard Aggregation Server. Using this powerful server, data from various SQL Guard units can be collected and managed by the single aggregation unit for central task management and enterprise views.

"The SQL Guard Aggregation server would allow us to use multiple systems to monitor large-scale database deployments and then manage all of the data collected and view all database activity using a central repository," said Murray.

"It [is] clear that, using SQL Guard, we [can] easily handle our database access concerns."

Guardium®
SAFEGUARDING DATABASES™

230 Third Avenue • Waltham, MA 02451 • T: 781 487 9400 • F: 781 487 7900 • www.guardium.com