datAvail
BI/Analytics • Applications • Databases

Case Study

Large International Aircraft & Charter Business Recovers from Large-scale Malicious Attack on its Datacenters

This case study covers how Datavail helped an aviation company recover from a massive datacenter attack by addressing Oracle database corruption issues and restoring the databases into a new environment.

The Challenge

The aviation company suffered from a malicious datacenter-level attack that corrupted its Oracle databases. The client could not connect to the databases to stop or start them, and the binaries and databases were all corrupted and encrypted, so they were unusable. The listener was also down, making it impossible to establish a remote connection to the databases. We already supported the company's SQL Server databases, so they reached out to us for assistance during this emergency.

The Solution

No working backups were available to restore the system. However, the client's infrastructure used Windows Servers. The data files, control files, and redo logs were safe because they were active during the attack. Since they were not encrypted or corrupted, they served as the starting point for restoring the Oracle databases.

We installed a fresh matching version of the database binaries but needed to associate the instance services with the new Oracle Home. We did this by editing the registry to point to the new home, which made it possible to associate the instance properly. At this point, we were able to start the database from the new home.

By deleting the listener services from the old home and creating new ones, we could make the database functional. All of the client's databases were migrated to the new servers with minimal downtime, and we moved to a UNIX-based cloud server over Windows Server.

Our recommendations also included:

- Implementing a robust backup policy
- Back up to a tape drive instead of the servers
- Putting a database monitoring tool in place, such as Oracle Enterprise Manager (OEM) for Oracle databases
- Limiting server access so only DBAs and UNIX admins can SSH with VPN
- Only the listener port should be listening from the database server

The Results

We were able to restore all their databases and hybrid connections from Oracle to SQL Server. Everything was functional in record time with a new server and environment. The aviation company was able to resume normal operations and avoid large-scale data loss.