

Financial Services Company

Fortinet's FortiDB Protects Critical Databases

Situation

A financial services company with multiple locations throughout the Americas, the company sells financial packages including loans from their offices as well as via the internet. As a financial institution, the company processes sales transactions and financial transactions to a wide range of customers. Within the company, there are many custom built applications primarily for processing transactions and these systems are based on an SQL Server back-end and Oracle databases. Database security and meeting compliance mandates were key requirements for this company due to the nature of the business. Within the company, there are four critical systems that have average transaction volumes of approximately 500 per second and 720,000 per day.

There were multiple drivers and benefits for a database security and compliance product. The first driver was database security. There are a number of power users and database administrators (DBAs) who can directly access the production applications that host sensitive customer data. It was imperative that this data be safeguarded and monitored at all times. By implementing a database security solution these privileged users can be monitored continuously and when they access a critical database using a non-standard application such as SQL Server Management Studio, an alert is generated and an audit trail is created. Additionally, a database vulnerability scan had to be implemented on a monthly basis so the security team would understand the risks to each database and prioritize patching accordingly.

The second driver for the company was compliance. The company needs to provide COBIT-based reports to external auditors. Naturally the company had to go through an internal audit process followed by an external audit.

The company evaluated a number of database security and compliance products, but in the end they selected Fortinet's FortiDB™ solution for numerous reasons. FortiDB offers the most complete and accurate audit data due to the use of the databases' native audit functionality. None of the other vendors were able to provide this. FortiDB was the easiest solution to deploy because it did not require changes to the network infrastructure and there were no agents to install on the databases. Finally, the FortiDB solution offered the most functionality with the best model for the lowest total cost of ownership.

Solution

In order to provide the company with highest level of database protection, they selected Fortinet's FortiDB. FortiDB is the most comprehensive solution to secure databases and applications such as ERP, CRM, SCM and custom applications. The deployment of the appliance followed Fortinet's best practices methodology for securing databases.

During the configuration, the decision was made to use the native audit functions of the databases to collect security and audit data. The reason for this decision was that native audit provides the most complete and accurate security and audit data. FortiDB also supports other options for data collection such as network protocol agents and a network sniffer.

The first step of the deployment was to run the vulnerability assessment function, understand the risks and lock down the databases as much as possible. For the lockdown, FortiDB's standard reports for the remediation advice sections were used.

In addition to using the standard reports available in the FortiDB appliance, there was an account review whereby the "Privilege Summary" function was utilized to see which users had access to which schemas and also which privileges they have. This helped to further tune the privileges on each database.

Requirements

- 4 Systems need to be monitored (2 x Oracle 10gr2 and 2 X SQLServer 2005)
- Database Vulnerability Assessment – with periodic policy updates
- Database Activity Monitoring – alerts on users using applications such as SQL Server Studio and SQL Plus
- Database Compliance – CoBit framework based reports
- Number of transactions per database - approximately 500 per second

Deployment

- FortiDB-1000C appliance version 4.2
- Functions used with the FortiDB appliance:
 - Database vulnerability assessment
 - Database activity monitoring
 - Database compliance

Industry

Finance

The next step included identifying policies for all users and coinciding alert conditions were defined in case a user was accessing the database using the SQL Server Management studio on the SQL Server databases and Oracle SQL Plus on the Oracle databases. If users come through the standard applications there should not be any alerts generated. However, if users gain access via untraditional methods or applications, an alert would be generated.

Finally, the compliance policies were configured for the Oracle databases which run the financial systems. Configuration was made easy because of an existing compliance policy group integrated into FortiDB. The automated reports consist of the following:

- Verification of Audit Settings Control Code: DS3.5, DS5.5, DS13.3 (to track changes to configurable audit)
- History Of Privilege Changes Control Code: AI2.4, DS5.3, DS3.5, DS5.4 (to track changes to user access rights)
- End of Period Adjustments Control Code: AI2.3 (to track changes to the general ledger)
- Abnormal Use of Service Accounts Control Code: DS5.3 (to identify service accounts)
- Abnormal Termination of Database Activity Control Code: DS10.1 (to identify failed database processes)
- Abnormal or Unauthorized Changes to Data Control Code: AI2.3 (to track all changes made to data)

This process has allowed the definition of:

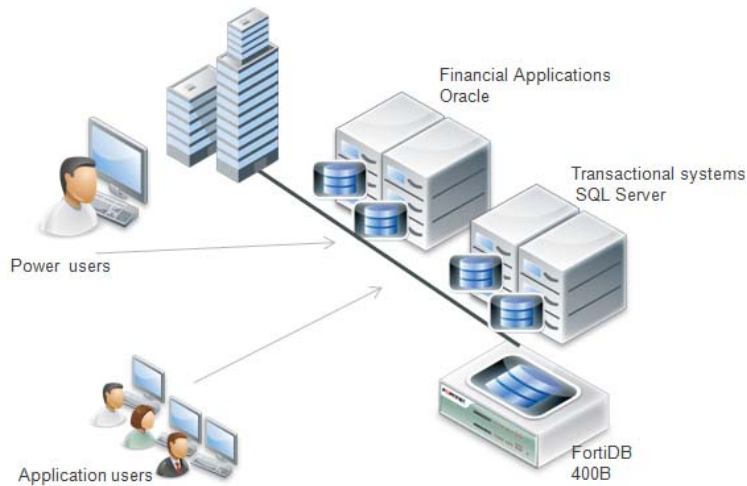
- Tight access control - If there are users accessing the database directly, without going through the applications
- Compliance automation, the data collected is used for reporting for the auditors

Success

The company has seen many benefits since installing Fortinet's FortiDB appliances. At the top of the list is the reduction in the amount of time needed for the database team to manage and maintain the security policies. Part of this simplification is the scheduled vulnerability assessment scans that run at the beginning of each month. These policies are automatically updated with Fortinet's FortiGuard® Network security services which automatically push new database vulnerabilities to FortiDB thereby reducing the amount of time and effort needed by the security team for database vulnerability research. Now the team only has to review access reports and remediate issues if necessary.

In addition, FortiDB monitors all users, so when new users are added they will be included in the appropriate user groups. Unusual activity will create an alert which will then be reviewed by the security team.

Finally, compliance reports are automatically generated and can be given to both internal and external auditors. These reports allow the security team to keep an eye on the verification of audit settings which can reveal if somebody tampered with the audit settings.



FORTINET®

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.