NetIQ

Customer Success Story

Sentinel Log Manager

Faysal Bank

To improve security, Faysal Bank Ltd. wanted to improve its ability to supervise IT administrators' activities. The organisation needed to monitor critical systems supporting core banking, credit card processing and network infrastructure. NetIQ® Sentinel™ Log Manager consolidates logs from multiple systems in real time, providing a clear, central view of all activity, with the ability to create detailed reports and set up event-triggered alerts.

Overview

Faysal Bank Limited (Pakistan) offers corporate, commercial, retail and Islamic banking services in more than 260 branches in over 70 cities throughout Pakistan. The company is a wholly owned subsidiary of Ithmaar Bank B.S.C., listed on the Bahrain and Kuwait stock exchanges.

Challenge

Faysal Bank Ltd. employs approximately 4,000 people across more than 260 branches in Pakistan. The bank maintains dozens of large databases, many of which contain sensitive and business-critical data. Of the 100 people on the IT team, approximately 5 to 10 staff members work directly on database administration. Following internal best practices for security, the IT management team gives limited access rights to technical staff, providing temporary full administrative privileges only when necessary.

"We had introduced preventative controls for security reasons, but it was difficult to check that administrative privileges were being used appropriately," said Zahir Ali Quettawalla, Head ITSRM, Faysal Bank Ltd. "We needed a solution for monitoring logs from multiple systems that would present the information in a readable format. The ability to review and query the log data was vital: We did not wish to simply 'check the boxes' when it came to complying with audit standards."

Solution

Following a thorough analysis of security-monitoring solutions, Faysal Bank Ltd. selected Sentinel Log Manager and worked with NDS, a NetIQ partner, to deploy the solution. "The NetIQ solution met almost all of our log-monitoring requirements and was considerably less costly than the alternatives," said Zahir Ali Quettawalla.

Faysal Bank Ltd. is now monitoring logs for almost all of its critical systems and user IDs and is working to develop reports and alerts that will further improve visibility and simplify compliance.

"Sentinel Log Manager is a very comprehensive tool, but it's not humanly possible to read every line of every log," said Zahir Ali Quettawalla. "We are now working with NDS to create consolidated reports, and we are planning to flag up suspicious activity using alerts sent directly to BlackBerry devices."

Comprehensive reports enable IT management to see at a glance how and when users are using administrator IDs. The reports include the time and location of access and detailed information on what commands users are running with administrative privileges.

"With the NetIQ solution, we have a complete record of user-generated queries, which gives a very good idea of what users are actually doing

faysalbank
Bank on Ambition

At a Glance

- **Industry**
  Banking
- **Location**
  Pakistan
- **Challenge**
  The bank needed a solution for monitoring logs from multiple systems that would present the information in a readable format.
- **Solution**
  Use Sentinel Log Manager to monitor logs for critical systems and user IDs.
- **Results**
  + Provided the ability to capture logs in real time and with zero performance impact
  + Granted a clear view of administrator activity across the most important databases
  + Offered real-time alert capabilities for defined security events

> **"The business risk associated with administrative access to databases is now under control, thanks to Sentinel Log Manager."**
>
> **ZAHIR ALI QUETTAWALLA**
> Head IT Security Risk Management (ITSRM)
> Faysal Bank Limited (Pakistan)

www.netiq.com

on each database: which tables they have accessed, which fields they have changed, which values they have updated," said Zahir Ali Quettawalla.

With the log-monitoring solution in place, Faysal Bank is now embarking on a second phase.

"We have a system where users can request access rights," said Zahir Ali Quettawalla. "An automated workflow ensures approval by their line manager, but there's no easy way to check that the requested access really fits that person's role. We are planning to deploy Identity Manager…to provide full control over roles and access rights."

Results

Thanks to Sentinel Log Manager, Faysal Bank Ltd. now has a clear view of administrator activity across its most important databases. "Administrators understand that they are now being monitored…and that any out-of-the-ordinary activities, whether accidental or deliberate, will be permanently visible," said Zahir Ali Quettawalla.

Business managers previously had concerns about setting up logs on critical systems for fear of impacting performance. Sentinel Log Manager captures logs in real time and with zero performance impact. Likewise, the solution has minimal impact on the IT team's workload, enabling full monitoring and sophisticated reporting at the touch of a button.

The ability to monitor and report on comprehensive administrator-activity logs is of great value in demonstrating proper IT governance.

"The business risk associated with administrative access to databases is now under control, thanks to Sentinel Log Manager," said Zahir Ali Quettawalla. "We can set up real-time alerts for defined security events and we also have a full evidence trail for all historical activities."

Australia
+ 61 3 9825 2300

China
+ 86 10 6533 9000

Hong Kong
+852 2588 5288

India
+ 91 80 4002 2300

Japan
+ 81 3 5413 4800

Malaysia
+ 60 3761 00214

New Zealand
+ 61 2 9904 6111

Singapore
+ 65 6510 4200

South Korea
+ 822 2008 4690

Taiwan
+ 866 2 2376 0036

NetIQ
Worldwide Headquarters
Houston, Texas
713 548 1700
888 323 6768

www.netiq.com