

Logging In Depth

EventTracker is a Security Information and Event Management (SIEM) solution designed to enhance the security of critical systems, ensure confident compliance and improve overall performance and availability



DarbyBank

Drivers

- **Enable compliance with GLBA and SOX**
- **Maintain quality of service**

Overview

Darby Bank & Trust Company, headquartered in Vidalia, Georgia, is a full-service bank focusing on relationships with small to medium sized businesses. As a publicly traded company, Darby Bank is required to comply with the Sarbanes-Oxley (SOX) Act of 2002 which mandates the presence of IT controls to ensure the integrity of financial data and reports. Section 404 of the act specifically calls out for the collection, retention and review of audit trail events from all sources that touch company financial data. In addition, as a financial institution, the bank is also expected to comply with the Gramm-Leach-Bliley Act (GLBA) that requires the implementation and maintenance of an information security program that protects the privacy of customer records.

Darby has experienced unprecedented growth, increasing total assets by 18.8%, and has entered new markets in Lyons and Savannah. This extraordinary growth has put increasing demands on the Information Technology organization to manage a complex infrastructure that is widely distributed across multiple locations. As expected, the bank cannot tolerate any disruptions of service to key servers in the organization, especially those handling transaction processing for both brick-and-mortar and on-line customers.

The challenges, therefore, faced by Darby's IT staff were 2 fold

- ◆ Protect the privacy and integrity of information systems while enabling compliance with GLBA and SOX
- ◆ Maintain Quality of Service (QOS) for the bank by reducing downtime and optimizing network performance

Selecting a log management solution

Shan Venable came to Darby Bank and Trust Company as Vice President in charge of IT. His mission was to transform Darby Bank's operations to enable effective compliance and also maximize IT performance with limited personnel and budget. After doing a complete requirements analysis, he realized that he needed a solution that would automatically collect, consolidate, correlate and report on event log data generated by servers and alert him in real-time on server performance issues, external/internal intrusions and unauthorized access.

After a thorough evaluation of the Log Management market, Venable chose EventTracker as the critical enabling software for addressing the 2 challenges above. "I downloaded a trial version of EventTracker, and it was up and running within 15 minutes," Venable said, "Also, it had many of the features I was looking for, such as intrusion alerts, real-time notification, application monitoring, and customizable event log filters."

One key factor that drove the decision to implement EventTracker was Prism's knowledgebase, a repository of cause-resolution information on over 19,000 events, integrated with the EventTracker software. Using this functionality Venables's staff does not need device specific expertise to make sense of log data and can quickly look-up definitions and other useful information on unknown event types. The KnowledgeBase is also available free of charge to the public at <http://kb.prismmicrosys.com>

Confident compliance and proactive security

The EventTracker solution automates the time consuming tasks associated with compliance by monitoring millions of events from disparate sources across distributed areas, and by providing audit-ready reports that prove to auditors that Darby Bank is in compliance with SOX and GLBA. The solution allows the Bank to quickly isolate and remediate any dangers that might compromise compliance efforts and provides comprehensive audit trails and detailed historical reports that document access and authentication activities, review procedures, and due diligence efforts.

Most importantly, thanks to EventTracker's correlation and advanced analytic capabilities, Darby Bank is able to better protect itself against a variety of security threats and is instantly notified on unauthorized access, data modification and intrusion attempts. For example, if an employee tries to access a system or modify data he or she does not have permission to, or if a network connection is made on any port by a blacklisted or unauthorized source, or if a machine gets infected by a new worm or virus – In all these cases EventTracker instantly pinpoints the vulnerability and alerts the appropriate personnel in real-time. Another security feature, which also must be addressed for regulatory compliance, is data encryption of the log data.

EventTracker archives and stores all event logs in a tamper-proof vault for future analysis. Venable claims, "There are hundreds of attacks against our internet connection everyday, but with EventTracker I feel safer knowing that I have alerts and a secure audit trail in the event there is an incident."

Optimizing network performance with minimal resources

EventTracker has driven dramatic efficiency and performance gains at Darby Bank. Venable's team is now able to centrally monitor, manage and make sense of millions of cryptic events generated by distributed systems at one location for a clear overview of the Bank's IT infrastructure at all times. By monitoring and alerting on disk space trends, CPU usage trends, runaway processes, service downtime and dropped sessions Venable's team has been able to significantly improve availability and reduce unplanned outages.

When the unavoidable outage does occur, Venable's team uses EventTracker's analytics engine to quickly search and troubleshoot the cause of the incident. Since event data can be stored for multiple years by EventTracker, Venable can actually go back and look at data from systems to diagnose performance and availability issues thereby significantly reducing the time to resolution – For a bank that depends on its IT infrastructure for financial transactions, quick resolution of network issues is imperative for maintaining quality of service to customers.

Since the log review process is completely automated, little or no staff interference is required to monitor system health, freeing personnel to tackle other pressing IT projects. Additionally, as a software solution that comes with its own event repository, EventTracker does not require database licensing, administrators or lengthy service agreements and returns a positive return on investment within 9 months.

"There are hundreds of attacks against our internet connection everyday, but with EventTracker I feel safer knowing that I have alerts and a secure audit trail in the event there is an incident."

-Shan Venable
Darby Bank