

Reinventing SIEM and Log Management at Amarillo National Bank

Across the high plains of the Texas panhandle along historic Route 66 and Interstate 40 lies Amarillo, a bustling town of 190,000 people. One of the businesses servicing this community is Amarillo National Bank (ANB). ANB was established in 1892, and has grown to become the largest family-owned bank in the nation, reaching \$2.7 billion in assets in 2010.

Amarillo National Bank's focus has remained a constant, as it places its customers and its community's best interests first. This is exemplified by all the bank does. ANB donates \$1M dollars each year to local charities and its employees donate over ten thousand hours annually to community service. Amarillo National Bank's dedication to the community has earned it an "Outstanding" in its Community Reinvestment Act (CRA) performance evaluations.

ANB's focus can also be witnessed in how it protects its customers from fraud, identity theft, and all the various threats that can occur when a company's data is connected to the Internet. To improve its overall IT security, ANB decided to implement a new SIEM and log management solution to protect their infrastructure of 150 servers, 600 workstations, platforms, network devices, applications, databases, physical security devices, card readers, doorway entry devices, HVAC units, UPS systems, biometric scanners, video recording systems, money counters, and intranets across 18 locations. "Security for our customers is first and foremost," said Bill Davis, head of data security for Amarillo National Bank, "take care of that and everything else, including meeting compliance requirements will be resolved."

Implementing a new solution was not Amarillo National Bank's first foray into SIEM and log management. ANB originally implemented another well-recognized solution, but the experience left the bank dissatisfied. "This solution collected logs, but didn't provide enhanced security in a user-friendly way. It was rarely updated, it was slow, it was difficult to use and it did not capture information in real time." When the support contract

"Service for customers is first and foremost..."

expired, ANB set out to find a quality solution to replace it.

Several well-known vendors responded to the request for proposal and were carefully vetted in their attempts to provide the final solution. Amarillo National Bank was looking for a solution that was easily recognized, extensible and proven. An idea that guided the search was the notion that ANB was looking for a vendor to partner with them, recognize and understand their needs, and replace its existing solution with one that would extend the scope of protection and monitoring. ANB's search ended with the decision to go with EventTracker from Prism Microsystems.

There were several primary goals that Mr. Davis had in implementing the new SIEM solution: detect and prevent unauthorized access while monitoring internal user activity, improve forensic analysis and event correlation, and ensure regulatory compliance - although the third was a byproduct of the other two. Each of these goals has been efficiently met through the implementation of EventTracker. "The rapid installation and functionality of EventTracker allowed us to do our jobs and focus on the customer," said Davis. "It inherited the unsolved challenges left over from our previous solution and lessened the learning curve so we could be up and running quickly, utilizing it to the fullest extent."

Data loss prevention was of key importance. But the focus on insider threats was nothing new to Davis. Although the news around WikiLeaks brought it to the forefront of the mainstream media, it has been a challenge that has been prevalent for a long time for data security managers. "We were way ahead of stopping WikiLeaks," said Davis. "Anyone who wasn't thinking about internal security is behind and will most likely get caught. EventTracker's 360 degree view of our IT infrastructure is key in heading off these types of threats."

One requirement at Amarillo National Bank was to be able to provide access to the information to the different groups within the bank without showing information that was irrelevant or improper - and each group had different

*"Anyone who
wasn't
thinking about
internal
security is
behind..."*

needs. This is something that was lacking from the previous solution. By utilizing the customizable role-based dashboards, the bank was able to implement a solution that met the needs of all of the groups including those responsible for the platforms, network, applications, web development, disaster recovery, security, ATM and credit cards, the vault, internal compliance, and ultimately senior management. Senior Administrators are able to determine which information each user should be able to see through their own customized dashboard view so that the information is relevant and easy to understand.

Another item lacking from ANB's previous log management solution was the ability to efficiently generate reports from their MS Windows servers and workstations - and in some cases the system could not generate the reports they wanted at all. With EventTracker, ANB is able to select from the hundreds of standard reports included, or build a report to their own liking. This flexibility allows each of the groups to quickly pull the information they need.

ANB's IT security thought leadership is highly respected in the banking industry, and other financial institutions look to them as how things should be done. Their entire infrastructure has been designed to be completely redundant, including a separate disaster recovery site. However, an impediment to full redundancy was that their previous log management was not redundant and represented a single point of failure. Since it was an appliance-based solution, it required one for one sparing which proved to be extremely cost prohibitive. With the implementation of EventTracker, ANB has easily eliminated that deficiency and has a fail safe solution. Since EventTracker is a software only solution, sparing is easily accomplished both utilizing existing infrastructure as well as "in the cloud".

Additionally, the increasing growth of Amarillo National Bank's virtual business and the number of transactions being conducted "in the cloud" further reinforced the selection of EventTracker as it provides a single,

"...ANB has eliminated that deficiency and has a fail safe solution."

comprehensive ability to access, analyze and correlate IT data from thousands of log sources across the enterprise. EventTracker's flexibility and redundancy easily enables the bank to be more proactive than reactive to potential security issues and expands the use of logs to the help desk so those issues can be viewed as they occur.

"From an IT perspective, I appreciate the incremental scalability. The role-based dashboards get information where it needs to be. We've got a fully-functioning disaster recovery center with EventTracker," said Davis. "The information stream it provides is helping me be proactive. I know more about our network than I did a month ago!"

Planned expansion of EventTracker use for Amarillo National Bank includes increased use of logs and information extrapolation - so personnel know what events changed and when.

"There were several reasons Amarillo National Bank chose EventTracker for SIEM and log management. The functionality surpassed our previous solution and the value was compelling. When we bought EventTracker, we also bought into Prism's corporate culture. We appreciate the responsiveness and how Prism is so customer-focused," said Davis.

And finally, while EventTracker enables Amarillo National Bank to demonstrate GLBA, PCI-DSS, and FFIEC compliance for its auditors, Davis wanted more out of the initiative. "Focusing on meeting these compliance requirements led to improving our overall security across the entire IT infrastructure," said Davis.

About Prism Microsystems

Founded in 1999, Prism Microsystems was a pioneering force in the development of Log Management technology. Building on its reputation as an innovator, the company today delivers the most comprehensive Security Information and Event Management (SIEM) solution in the industry, powered

*"I know more
about our
network than I
did a month
ago!"*

by a unique combination of real-time Log Management and Correlation with Change and Configuration Management.

Prism's customer-centric approach and the award winning EventTracker enable more than 1,000 customers worldwide to mitigate internal and external threats, comply with a variety of regulatory requirements, and improve IT processes and service availability. Additionally, EventTracker maximizes investment, improves IT processes and achieve tangible, demonstrable cost savings.

EventTracker
Prism Microsystems
8815 Centre Park Drive
Columbia, Maryland 21045
Toll Free: 877.333.1433 Main: 410.953.6776 Fax: 410. 953.6780
www.eventtracker.com

EventTracker 
ENTERPRISE