

Global Bank Adopts Comprehensive Information Security Platform

Challenges

- Increased risk exposure and costs due to growing volumes of logs examined through error-prone manual review processes
- Growing volumes of log files to be archived to meet compliance regulations
- Increased costs due to the growing volumes of logs requiring manual review
- New regulations driving increased requirements for additional monitoring and documentation

EMC Compliance Solution for Financial Services

- RSA® enVision®
- RSA enVision NS 3500 integrated storage based on EMC Celerra®

Results

- Payback of initial investment in six months and savings of \$7.4 million over four years
- Increased visibility into potential security threats to the bank's network
- Greater IT operational efficiencies with automated log collection, monitoring, analysis, and management
- Greater risk mitigation and line of sight to potential vulnerabilities and fraud
- Faster response to security issues, allowing for immediate corrective action

Automated log management generates savings of over \$7 million in four years

Challenge

Financial firms around the world are keenly aware that information security and compliance solutions are critical to their profitability and competitive advantage. As further evidence of this trend, the security software market in financial services is estimated at \$963 million based on IDC estimates and EMC® analysis. These solutions will become more vital as the industry braces for a wave of new compliance requirements in response to recent crises in the credit and banking markets.

The U.S. banking unit of one of the world's largest financial services companies has pursued a strategy of automating the monitoring, management, and analysis of information security. With hundreds of branches and several million customers, this bank oversees processing of tens of millions of dollars and sensitive financial information daily. In 2001, the bank, one of the ten largest in the U.S., found that manual monitoring and reporting on security and information logs were draining resources and increasing its risk exposure. As the bank grew, manual log review costs were rising and it would have to significantly increase its compliance and security staff. Additionally, they would have to continuously train them to keep up with new regulations, not to mention that manual log review was prone to errors causing significant quality concerns.

These issues only intensified when the U.S. government enacted the Sarbanes-Oxley Act of 2002 and other regulations governing financial reporting, disclosure, and data security. Not only did the bank have to monitor activity on its global computer network, but it also had to provide supporting documentation, including archived logs, or risk its ability to operate in the U.S., which would adversely impact their global position.

These circumstances, combined with the difficulty of collecting, monitoring, analyzing, and storing millions of security and event logs, drove the bank to find a new solution.

EMC Compliance Solution for Financial Services

The bank decided an automated security information event management system (SIEM) would be the most effective, cost-efficient solution. After carefully reviewing alternatives, the bank was impressed with the ability of RSA enVision to scale and collect all data generated by the IP devices on the network without filtering or agents, unlike other solutions that only take snapshots of the enterprise.

Today, the bank uses RSA enVision to capture and store up to 95,000 data events per second—providing a comprehensive picture of activity from 5,000 sources, including perimeter and network devices, operating systems, and even proprietary applications. By intelligently storing and analyzing the complete data set, the bank can respond quickly to any issues before they threaten compliance or data security.

RSA enVision was implemented in 2002 to automate the review of logs generated by the bank's growing firewall environment. The bank also began using enVision to monitor critical corporate security tools and automate audit and compliance requirements. Additionally, IT organizations outside of the bank's IT security department purchased RSA enVision to review auditing of 900 databases and to support a logging project covering 6,000 devices.

In 2005, the architecture review committee and IT management selected RSA enVision as a “Green Global Standard,” paving the way for deployments outside of the U.S. The bank now has 18 RSA enVision appliances installed across the U.S., Mexico, and Argentina and is expanding its deployment in the UK and Europe.

Results

Although cost reduction was a major goal, the bank was surprised to learn how quickly savings overtook the investment in RSA enVision in a return on investment (ROI) analysis. Based on a conservative estimate of an additional 15 full-time employees needed for manual log management and review at an estimated cost of \$150,000 each, the bank saved over \$7.4 million over a four-year period. Additionally, in this period, at a first-year enVision cost at just over \$1.1 million (70 percent cost of four-year enVision investment), they realized a payback of their initial investment in just six months.

RSA enVision has also greatly expanded management’s visibility into potential security threats. After numerous virus outbreaks on the Internet, IT security was asked how many viruses were blocked by firewalls. One manager estimated 80 viruses, but an RSA enVision report revealed that 1.3 million potential viruses were prevented in a single month.

Increased visibility combined with RSA enVision’s sophisticated analytic capabilities enable the bank to respond quickly and fully to threats. Correlated threat detection capabilities allow security personnel to analyze information from diverse network devices, correlate threats across domains and platforms, and eliminate false positives to pinpoint potential threats and proactively prevent them. In addition, material events are rapidly reported to the bank’s management so they can take corrective action and ensure customer confidence and regulatory compliance.

What started as a firewall logging project has become an enterprise security initiative extending to the bank’s U.S. and global operations. With this ongoing expansion, the bank will be able to adapt to new, unforeseen security threats and comply with expanding regulatory requirements for security and documentation.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com