

Meeting Securities Regulations with Automated Risk Management and Compliance

Challenges

- Increased risk of security threats and violations due to manual inspection of data
- High costs associated with labor-intensive review of event logs and audit information
- Time delays in threat identification due to manual review of multiple systems
- Numerous compliance audit violations due to incomplete distributed systems data

EMC Compliance Solution for Financial Services

- RSA enVision platform
- RSA enVision NAS3500 appliance (based on EMC Celerra)

Results

- Decrease in threats resulting from intelligent analysis of security events
- Avoided \$2.25 million dollars in additional annual staffing costs due to automated review of event logs
- Greater efficiencies with centralized log management to meet compliance and audit requirements
- Compression of time required to identify threats across multiple systems
- High confidence in identifying threats and vulnerabilities with defined correlation rules

Proactive security monitoring enables faster isolation and resolution of issues

As local economies worldwide become increasingly interdependent, global organizations responsible for processing heavy volumes of securities trades have a tremendous responsibility to ensure their operations are secure and reliable. A prime example of these institutions is one of the world's largest post-trade infrastructures, which provides clearing, settlement, and processing services for millions of transactions executed in U.S. and international financial markets and exchanges each day. Given the sensitive financial information processed via its network, the U.S.-based institution is closely regulated by the U.S. Securities and Exchange Commission and also has its own extensive internal policies to enforce information security.

In recent years as transaction volumes have grown and financial data security regulations have become more stringent, this organization's traditionally reactive approach to security monitoring created an unacceptable level of risk. The 28-person information security team would only take action when notified of a potential breach, creating a situation where financial losses and other damages could occur before issues were resolved. In addition to responding to security breaches, the financial institution also needed to respond to increasingly frequent and comprehensive government security audits and findings. It also faced a significant challenge to audit the unstructured data that was captured from disparate locations and devices.

Recognizing the potential risk, the organization's security team analyzed the security audit findings and evaluations it had received dating back several years. The team concluded a proactive approach to security monitoring would allow it to comply with regulations and internal security controls more quickly, effectively, and cost-efficiently.

EMC Compliance Solution for Financial Services

The security team spent several months defining their requirements for a new security solution. The goal was a security information event management system (SIEM) that supported the organization's mix of legacy and newer systems. It also needed to enable proactive monitoring and analysis of large volumes of disparate data across multiple layers, including perimeter devices, middleware device log data, application logs, and workstation log data.

In addition, the post-trade processor required robust monitoring of privileged user activity, multiple login failures, and other security-related events, as well as access to actionable, realtime alerts about potentially suspicious behaviors. Because the organization needs to retain at least 60 days of log data, sufficient storage was also an important consideration. After evaluating a range of vendor solutions, including Cisco Security MARS and LogLogic, the organization decided that the RSA® enVision® platform best met its selection criteria. It chose RSA enVision because it supported their multiple platforms and logging protocols, ranging from mainframe logs to Windows Active Directory to UNIX and web servers, providing easy and intuitive alerts, along with robust reporting.

The financial organization transformed their environment from a collection of unstructured disparate logs without any analysis or event capturing to one that generates and logs over 350 million events daily across 3,000-plus devices in a centralized, structured, and manageable environment. The organization also leveraged RSA enVision's strong analytic capabilities to define over a dozen correlation rules, identify security events, and issue alerts based on customized criteria. Not only are these events logged centrally and in a structured manner, but also now over 60 nightly reports are generated and distributed to infrastructure and security teams for review. The RSA enVision NAS3500 appliance, which is based on EMC® Celerra® network-attached storage, is the repository for more than two terabytes of logs.

Results

Since implementing enVision, the financial organization has significantly improved its ability to identify and respond to security infractions occurring on its network. In particular, enVision has provided the following benefits:

- **Comprehensive automation of event information.** The security staff receives realtime alerts and reports that quickly isolate anomalies and security events that require follow-up actions. The automatic, proactive alerts and reporting enable security staff to focus on analysis and risk assessment as opposed to log aggregation and manual review of log files.
- **Improved monitoring of privileged users and user authentication.** The security team can easily detect multiple unsuccessful logins.
- **Fast isolation of problems.** Each day, enVision captures over 350 million events through logs. The log data is normalized into just over 60 nightly reports, and critical events are flagged through automated alerts. Instead of reviewing all the events, security and infrastructure experts are notified in near real time about problems, enabling quick isolation of issues.
- **Simplified alert creation.** Proactive alerts are simple to create so that security staff spend minimal time configuring and maintaining the system.
- **Robust reporting.** RSA enVision provides several hundred “out-of-the-box” reports and the ability to easily customize these reports for internal and external compliance efforts.
- **Extensive platform and logging protocol support.** RSA enVision supports more than 70 percent of the organization's system platforms—far greater than any other solution evaluated—and nearly all of its logging protocols, including those of the older legacy systems.
- **Substantial cost avoidance.** If the organization had not deployed enVision, it would have needed to hire at least 15 full-time employees (FTEs) to manage increasingly frequent government security audits. With an estimated \$150,000 cost for each FTE, the additional expense would have been \$2.25 million annually for manual log review, provided log data did not increase in volume.

With improved security monitoring and intelligence, the post-trade processor can more easily and effectively comply with ongoing government audits and regulations and respond to any concerns. And by satisfying its own stringent policies for information security, the financial industry leader is contributing to more reliable and secure operation of global financial markets.



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