



## Client Case Study

Leading Online Trading Company



## Leading Online Trading Company

Provides financial services including online brokerage and related banking products and services to retail investors

### Requirements:

The Trading Company Initially needed a compliance tool to capture log data from firewalls and support reporting requirements around Sarbanes-Oxley (SOX) and the Office of Thrift Supervision (OTS). Project has evolved to become part of a broad-based initiative around compliance and security monitoring for all business units where a key driver is ensuring a highly available customer Web site.

### Challenge:

The original solution chosen from RSA (Envision) did not support database access using standards-based tools – which prohibited the trading company from innovating with their security log information.

The solution also did not support load balancing, and the trading company wanted a solution that could be installed on commodity hardware (Envision is an appliance) in order to address operational and security policies.

### Environment:

Monitoring firewalls, Unix/WinOS, all network devices (switches, routers), all authentication devices, LDAP, RSA SecureID (wireless access, customer access, login to network devices).

Integrated Rapid7 asset identification & vulnerability management.

Global implementation across Americas, Europe and Asia.

### LogMatrix:

The Trading Company Is very happy about their relationship with LogMatrix and expect to continue to expand use of their products. They have seen quick turnaround on bug fixes and requested product enhancements.

### About:

The Trading Company provides financial services including online brokerage and related banking products and services to retail investors.

### About LogMatrix:

LogMatrix supports your regulatory compliance initiatives, detects security threats, and improves service availability and performance -- faster and at a much lower total cost than our competitors.

## Background

- Purchased LogCenter, EventCenter, and CommandCenter
- Implemented May 2009
- 6000 nodes
- Handling 250m events/day

*“Not only can we now check things that we could never examine before, but our internal security monitoring has improved because of our confidence that any alerts are in fact actionable.”*

*Principal, Security Engineering*

## Observations

- Easy platform to manage
- Very stable environment
- Scalable – well designed architecture
- Very few false positives
- Algorithms work “out of the box” – everything identified is “actionable”
- Columnar DBMS works well – query speeds very good

## Client Case Study

[www.logmatrix.com](http://www.logmatrix.com)

67 Forest Street,  
Marlborough, MA 01752  
+1 (800) 892-3646  
(t) +1 (508) 597-5300  
(f) +1 (508) 597-5399