# SC Magazine 2009 Reader Trust Award

## BEST SIEM

### (Security Incident/Event Management)

**Winner: LogRhythm for LogRhythm 4.0**
**www.logrhythm.com**

SC MAGAZINE AWARDS 2009 WINNER
Honored in the U.S.

LogRhythm integrates real-time log management and analysis, event management and data-mining capabilities. This unique combination delivers a comprehensive solution for monitoring network security, meeting regulatory compliance requirements and audits, and performing forensic investigations. LogRhythm automatically gathers, normalizes and analyzes log information across the network and alerts IT departments to unauthorized and suspicious activity as well as to problems that require immediate attention. To reduce the cost of compliance with regulartory mandates, LogRhythm provides regulation-specific reporting and archiving, along with granular access controls for restricting user access to log data and auditing usage. Finally, LogRhythm features a strong log data warehouse, LogMart, which enables fast, online investigations and reporting across weeks, months or even a year's worth of log data.

Unlike SEM/SIM solutions, which only gather security events and discard log data, LogRhythm maintains a record of all log files. This allows users to drill down from security events into log data to identify the source of suspicious activities or a breach. LogRhythm can be deployed and begin collecting logs, without professional services, in hours not weeks for fast time to value. LogRhythm also provides unprecedented visibility into critical security information buried in the volumes of logs generated on the networrk. LogRhythm LogMart maintains a secure historical log data store that is equipped with powerful query, visualization and trending tools that make it easy to trace intrusions, audit events, discover trends and more.

LogRhythm recieved a five-star rating and Recommended designation in the Group Test conducted by SC Magazine. Gartner recognized LogRhythm as a Visionary in recent SIEM "Magic Quadrant" reports. From a business prespective, LogRhythm enables enterprises to protect their networks by detecting insider and ousider threats, meeting regulatory compliance requirements and conducting forensic investigatrions -- with fewer IT resources.

## Finalists in 2009

- Alert Logic for Alert Logic Log Manager
- ArcSight for ArcSight SIEM Platform
- LogRhythm for LogRhythm 4.0
- Symantec Corporation for Security Information Manager 4.6
- TriGeo Network Security for TriGeo SIM

LogRhythm®
COMPLY. SECURE. OPTIMIZE.