

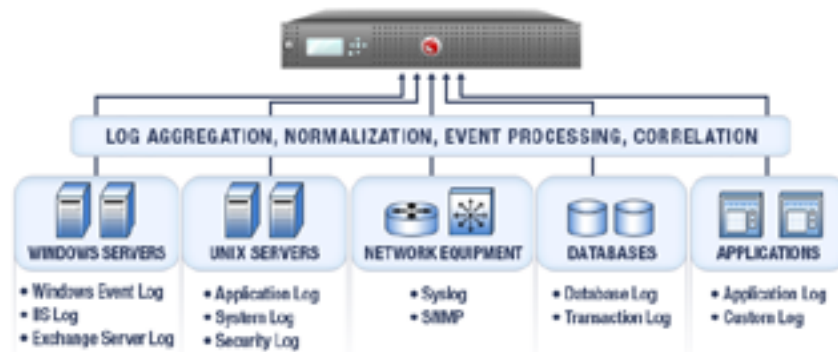
## FireScope Tech Brief : Log Consolidation

“FireScope is pushing the concept of mashups for IT management.”

- Jeff Vance, CIO Update

As server farms expand, the volume of syslog messages produced can become unmanageable. The sheer number of messages, as well as their points of origin can simply become too large to manage and control effectively. FireScope Dash provides a single point of management for all your syslog messages. You can consolidate as much or as little of your server log messages as needed to meet operations or retention requirements.

Easy to configure and operate, FireScope Dash provides three levels of log consolidation depending on your needs. You can consolidate all messages from all servers, collect messages from specific servers, and monitor specific messages. Messages can be filtered via common regular expressions, allowing you to monitor events from specific messages. Monitored messages can originate from either UNIX or Windows servers.



### Key Features

- Three levels of log management are provided.
- Consolidated log messages are prefixed with the arrival timestamp and originating ip address, while maintaining the original message contents.
- Utilizes standard UDP protocols for message forwarding.
- For off-site storage and security, consolidated logs are automatically encrypted and compressed, using techniques specified in RFC 2440.
- Syslog messages do not have to be RFC 3164/5424-compliant. FireScope BSM's parsing can handle virtually all log formats.

### Business Value

- Provides a single point of contact for managing log files.
- Meets privacy and security requirements of all compliance standards.
- Maintains integrity of original log records.
- Can be easily tailored to customer requirements.
- Designed and built with stability and availability as a primary goal.
- Proactive solution, allowing customers to more effectively use syslog messages to meet SLAs.

### Competitive Advantage

- Integrated with FireScope Dash, provides needed functionality without requiring a separate product.
- Syslog viewer with filtering and sorting of syslog data.
- No requirements for additional modules/features/programming.
- Customized event notifications based on specific contents of log messages.
- High performance solution tested at arrival rates in excess of 200 messages per second.
- Throttling and queuing capabilities to handle peaks in traffic.
- Normalization of data provides independence from message origins.