# Optimizing SIEM Cost and Performance with syslog-NG and Splunk

## Why syslog-ng as plumbing for SIEM?

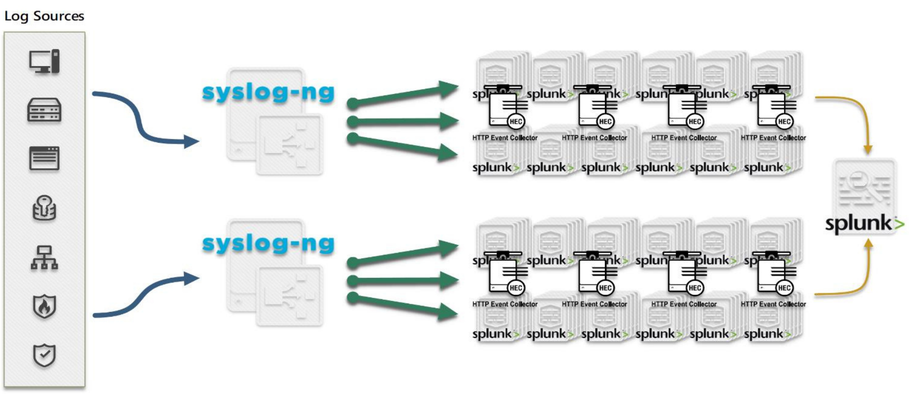
- syslog-ng filters and normalizes log data on clients at extremely high speed to reduce size and complexity of logs. Filtering unimportant log data reduces the load on SIEM and dramatically improves search time.
- syslog-ng customers save on average between 20-40% on SIEM costs by filtering unimportant logs.
- This integration will add a level of persistence to the syslog stream by writing events to disk, which can limit exposure to data loss for messages sent using the unreliable UDP as transport.
- syslog-ng can be installed on over 50 platforms including servers, networks, security devices, and applications. It can process hundreds of thousands of log messages per second from thousands of log sources.

### syslog-ng™ Store Box (SSB)

**Is a high-reliability log management appliance that builds on the strengths of syslog-ng™ Premium Edition.**

### syslog-ng™ Premium Edition

**enables enterprises to collect, filter, normalize, forward, and store log messages from across their IT environment.**



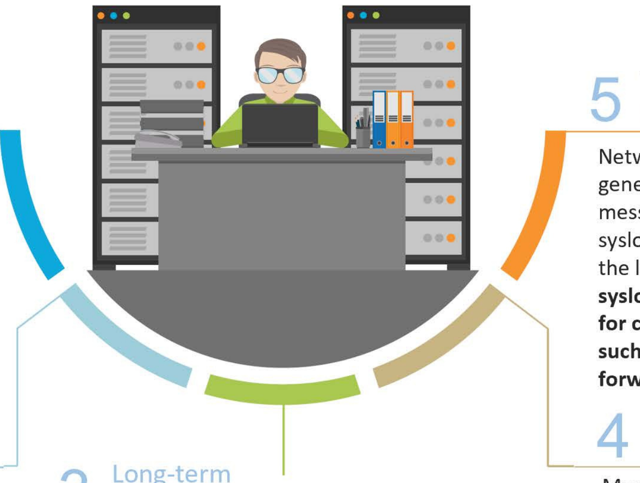
### Decrease complexity

- Reduce the number of syslog-ng aggregators
- Simplify the architecture and resolve scalability issues
- Eliminate or minimize Heavy Forwarders/Universal Forwarders
- Eliminate or minimize the HTTP load balancer
- Decrease HEC nodes to help the Splunk indexing process

### Dedicated log management

- Standard-based protocols and log routing
- Load balancing/distribution
- Long term retention, data management
- Small footprint agents
- Apply rules to the syslog stream that result in syslog events being written to dedicated files/directories for each source type (firewall events, OS syslog, network switches, IPS, etc.) to increase performance

## Top 5 Reasons Syslog-ng™ improves Splunk



1 Collecting log From network devices

Major router manufacturers transfer log messages using the syslog protocol, and syslog-ng™ natively supports both versions. RFC3164 and RFC5424. **Using syslog-ng™ can improve the reliability log data collection from network devices.**

2 Feeding multiple Analysis Tools

Feeding Multiple Analysis Tools - Organizations deploying Splunk usually have heterogeneous IT environments, often having different departments analyzing log data with different tools. **syslog-ng™ can collect and flexibly route logs to multiple analysis tools**.

3 Long-term Storage of Logs

Organizations are required to archive data for compliance purposes, often for months or even years. **syslog-ng™ reduces storage costs and secures log files.**

4 Advanced filter On clients

Many users use syslog-ng to filter Log messages on clients to reduce network loads. **syslog-ng™ can reduce the data load on Splunk improving performance and reducing license costs.**

5 Very high message Rate log sources

Network and security devices can generate large amounts of log messages. With its scalability, syslog-ng™ can meet the needs of the largest traffic environments. **syslog-ng™ eliminates the need for complex design workarounds such as load balancers or forwarder instances.**

## About Swish

Swish is a customer-centric, specialized integrator with an engineering first culture. Swish focuses on IT Modernization, Performance, and Cybersecurity solutions. Swish strives to bring value to clients through continuous improvement expertise; robust services, superior engineering, and creative solutions.

**To learn more, please visit: www.swishdata.com**

1420 Spring Hill Road Suite 320 McLean, VA 22102

**P** 703.635.3324 **/ F** 703.852.7904 **/ E** info@swishdata.com