USE CASE

Optimizing SIEM

syslog-ng™

syslog-ng™ Premium Edition

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

syslog-ng™ Store Box (SSB)

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

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTIONS FORM THE CORE OF MANY ENTERPRISES' IT SECURITY STRATEGY BUT THEY CAN BE EXPENSIVE TO DEPLOY AND MAINTAIN. OPTIMIZING YOUR SIEM SOLUTION CAN REDUCE COSTS AND IMPROVE PERFORMANCE.

Challenges

Log data collection - Companies struggle to make sense of log data received in varying formats, as generated by a broad spectrum of devices, including many legacy systems and applications.

Data Integrity - SIEM solutions focus on data analytics rather than reliable log collection, transfer and storage leading to missing log data.

Performance – Large networks produce massive amounts of logs from a wide variety of devices and applications. Many SIEMs become overloaded with data leading to searches that take hours.

Scalability issues – IT networks are continually growing both in terms of the amount of log sources and log data. Extending current solutions can be difficult and expensive.

High TCO – SIEM solutions are often very expensive to purchase, implement and maintain both in terms of money and internal resources.

Learn more

- Read more about syslog-ng™
- Request an evaluation
- Request a callback

Solution

Distributed pre-processing – The syslog-ng™ Premium Edition application can filter, parse, re-write and classify data on clients at unparalleled speeds to reduce the size and complexity of log data stored centrally. Filtering unimportant log messages that do not need to be analyzed also reduces the load on the SIEM, saving both processing power and license costs.

Reliable log transfer – syslog-ng™ Premium Edition and the syslog-ng™ Store Box can ensure zero message loss during transport from clients to the central logserver using TCP for transmission, the Reliable Log Transfer Protocol (RLTP™) for application acknowledgment, a client-side disk buffer, and client-side failover for network outages.

Centralized collection – The syslog-ng™ Premium Edition can be installed on over 50 platforms including a wide variety of Linux, UNIX, HP, IBM, Microsoft Windows, and Solaris variations.

Tamper-proof transfer and storage – syslog-ng™ Premium Edition and the syslog-ng™ Store Box use SSL/TLS encryption to transfer logs and the logstore, an encrypted, time-stamped and digitally signed logfile.

Straightforward, transparent licensing model – Licenses for syslog-ng™ Premium Edition and syslog-ng™ Store Box are based on the number of hosts sending logs, not the amount of data being processed so increases in the rate or the total amount of your log data will not increase your costs.

Benefits

Better SIEM performance – Reducing the size and complexity of log data can dramatically improve search times.

Higher quality data – Tamper-proof, secure logs in their raw format can be used in legal proceedings.

Increased confidence in SIEM analysis – Being certain that logs aren't missing or haven't been tampered with increases the confidence in the results of your investigation.

Cost-effective scalability – Expanding log management infrastructure is more easily planned with a predictable, host-based license model.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com