

LogLogic LX Product Family

Better, Faster, Smarter Log Analysis for Security, Availability and Compliance

Smooth business operations in today's increasingly digital world hinges on reliable, secure and highly available networks. Industry regulation organizations and best practices experts agree that log data holds the key to any organization's IT risk management strategy by enhancing security, enabling regulatory compliance and improving network availability in enterprise networks.

Unfiltered log data collected from firewalls, VPN concentrators, servers and other network devices provide the necessary information for activity monitoring, policy validation and problem resolution. However, until recently there were no solutions for high-performance, reliable log management. Event management solutions merely summarize and prioritize events, ignoring most log messages and providing slow response times for ad-hoc queries. Homegrown syslog servers can also take hours or days to search, a clear drawback when time is of the essence.

The LogLogic™ LX family of products makes log data immediately accessible and actionable. After a simple drop-in-installation, LogLogic appliances provide high-performance, reliable and automated log data aggregation, real-time analysis and historical archives for enterprise IT departments, helping IT departments isolate network risks in minutes for accelerated remediation and improved network visibility.

LogLogic Log Management Appliances

The LogLogic LX family of products provides network administrators:

- **Aggregation:** Reliably collects unfiltered log data from local and remote devices at high speeds and parses a copy of the log data in real time.
- **Analysis and alerting:** Provides early warning of unusual and suspicious behavior and provides decision support to accelerate problem resolution and security policy validation.
- **Archives:** Forwards a complete record of access and activity, as well as configuration changes to an ST appliance for long-term archives.
- **Automation:** Improves ROI through a high-performance, distributed appliance-based architecture with no maintenance requirements.

Key Benefits

Better

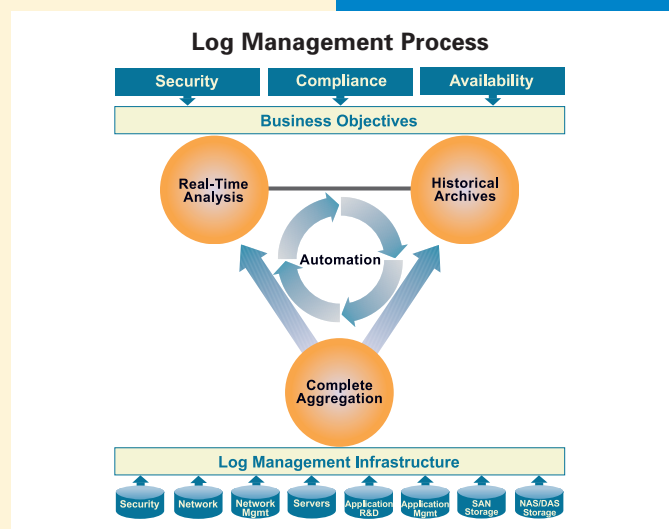
- **End-to-end:** Standardizes enterprise-wide log management
- **TCO:** Reduces maintenance and support costs through automation

Faster

- **High performance:** Accelerates problem resolution
- **Reliability:** Minimizes dropped log messages to ensure data integrity

Smarter

- **More useful:** Improves security, compliance and availability
- **Easier:** Logs become instantly insightful and actionable



Features

Reliable aggregation

The LX appliance features a distributed, appliance-based architecture that combines high-performance, redundant hardware, a Linux-based OS and patent-pending software. Auto-discovery technology detects local and remote devices and the LX appliance begins collecting and aggregating all log data. It parses and summarizes a copy in real time, then forwards the raw data to the LogLogic ST appliance-the aggregation head-end. The data can be secured and compressed for TCP transport over the WAN to the ST appliance. Proprietary auto-sensing technology detects WAN failures if they occur, and buffers log data for safe re-transmission after the outage.

Real-time analysis, alerting and reporting

LogLogic's high-performance appliance architecture enables unique alerting algorithms and can process all log messages in real time. Device-specific alerts warn administrators of rate-based, policy-based or message-code anomalies. Both behavioral modeling and rules-based alerts are available.

The LX appliance also makes valuable log data instantly searchable and insightful with real-time reporting and targeted queries. Drill-down fields and unique root-cause correlation technology help to

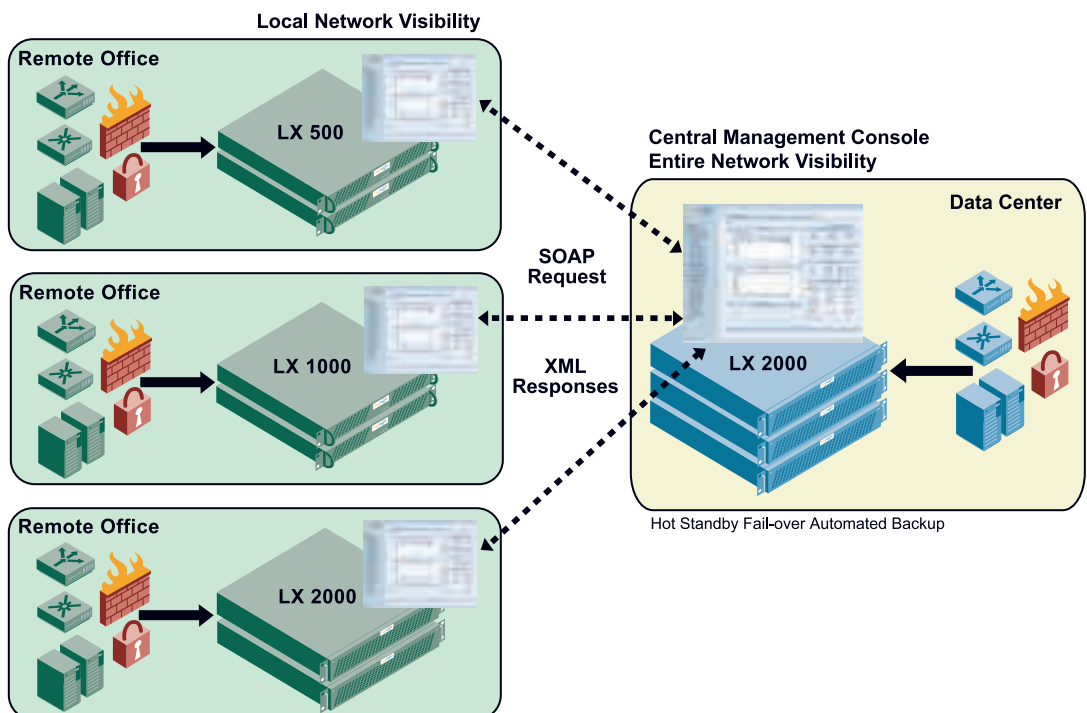
isolate problems and speed remediation. The data is easily searchable from any web browser, and a live viewer helps users analyze log data messages in real time. Ad-hoc, customizable graphical management reports organize the results of access and change control audits, security policy audits, and more general-use analyses.

Secure data archives

The LogLogic solution features central, secure log data archives, which are physically separate from the metalogs used for real-time analysis. The LX appliance stores a parsed and summarized metalog copy of the data for up to 90 days for instant retrieval.

Automated solution

The LX appliance requires no training, and the self-maintaining database eliminates the need for additional staff. The LX appliance auto-discovers new network log sources, further reducing maintenance and labor costs. It is interoperable with network management through SNMP traps and integrates easily with other applications through SOAP and XML. The LX appliance also features unique domain virtualization technology, so administrators can scale by simply adding appliances, while performing analysis on any log source or group of sources, regardless of physical location.



Applications

Timely information wards off security intrusions

When monitored effectively, log data provides early warning of worm or virus attacks—for instance, day zero attacks. Abnormal log data patterns can point to infected machines and allow a swift, targeted remediation effort. For more malicious intrusions, log data delivers timely information to accelerate remediation.

According to the American Chamber of Commerce, enterprises lose an average of \$1,250,000 annually due to Intellectual Property (IP) theft. Monitoring log data on an ongoing basis helps to deter IP theft. The LX appliance has saved LogLogic customers over one million dollars annually by thwarting attempted IP theft and reducing the negative impact of virus attacks.

Simplified regulatory compliance saves on resources

Increasingly strict requirements put forth by regulatory legislation and best practices frameworks require enterprises to separate tasks associated with policy configuration from the tasks of network monitoring and policy validation. While security software enables authentication, identification and

configuration management, log data provides an independent third-party audit trail of user activity and system configurations. According to Financial Executives International, an average corporation spends more than three million dollars on achieving Sarbanes-Oxley compliance. The LX appliance can pay for itself quickly by reducing the amount of manual data mining necessary to complete regulatory audits and provide policy validation.

High availability ensures smooth network operation

Event management solutions can help identify potential threats, but 80 percent of Global 2000 organizations rely on unfiltered log data to provide decision support when resolving problems. According to Gartner, Inc., the average Global 2000 organization experiences 87 hours of downtime per year, which results in a loss of four million dollars, assuming downtime costs of \$42,000 per hour. Manually monitoring and analyzing log data slows response times, affecting IT productivity and prolonging downtime unnecessarily. The LX appliance's auto-alerting capabilities warn administrators of potential performance or security threats, before they disrupt network operation. Furthermore, analyzing trends helps with planning for more reliable operation. Meanwhile, searches and real-time reports let administrators drill down to find specific data to isolate and resolve problems.

Features and Benefits

Better End-to-end <ul style="list-style-type: none">■ Robust log management for entire data center■ Distributed analysis with central management■ Flexible domain virtualization technology	Faster High performance <ul style="list-style-type: none">■ Appliance-based high-speed architecture■ Real-time processing of raw data and metadata■ Ad-hoc reporting and searches in seconds	Smarter More useful <ul style="list-style-type: none">■ Rate-based anomaly detection■ Fast search and root-cause correlation■ Built-in graphical trend and policy reports
TCO <ul style="list-style-type: none">■ Dedicated, plug-and-play appliance■ No installation or training required■ Self-maintaining database technology	Reliability <ul style="list-style-type: none">■ Automated fail-over, fail-back and backup■ Protected, TCP transport over WANs■ Intelligent protection from WAN failures	Easier <ul style="list-style-type: none">■ Flexible search interface for any syslog source■ Browser-based, supports SOAP, XML, SNMP■ Automated discovery of new log sources

Product Specifications



System Management

- Command Line Interface
- Web-based GUI (Internet Explorer, Netscape, Mozilla, Firefox)
- Built-in central management station
- SNMP support

High Availability

- External backup capabilities
- Hot standby and fail-over for log message capture
- Hot swappable redundant power supplies (LX 2000)
- Redundant fans (LX 2000)
- RAID-5 storage (LX 2000)

Operating Environment

- Linux hardened and optimized kernel

Device Support

- All syslog protocol compliant devices including firewalls, VPNs, routers, switches, servers and other devices.
- OPSEC LEA including firewalls and VPN systems.

Safety and Emissions Certification

- **Safety:** UL-Safety, CB to IEC 60950: 1999, 3rd edition; TUV GS mark to EN60950: 2000; TUV C-US to UL60950: 2000; CAN/CSA-C22.2 No 60950: 2000
- **Emissions:** FCC Class B, VCCI Class B, CE class B, C-Tick, ICS, EN 60.950/IEC



Appliance Specifications	LX 500	LX 1000	LX 2000
Sustained message per second (mps) rate*	200 mps	1,500 mps	3,000 mps
Data storage lifetime	up to 90 days (metalog)	up to 90 days (metalog)	up to 90 days (metalog)
Summarization ratio	up to 20:1	up to 20:1	up to 20:1
Management station	not available	available	available

*Peak message rate up to 5x sustained rate

Hardware Specifications	LX 500	LX 1000	LX 2000
CPU	1.7 GHz AMD	2.8 GHz P4	2x 2.8 GHz Xeon
Memory	512 MB	1 GB	4 GB
Hard drive	40 GB IDE	160 GB IDE	4x 160GB SATA RAID
Power	180 W	180 W	2x 350 W
Chassis	1u	1u	2u
Ethernet	1x 10/1000	2x 10/100	1x 10/1000 1x 10/100/1000
Console port	9-pin serial	9-pin serial	9-pin serial

LogLogic, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Product Specifications are subject to change without notice.



LogLogic, Inc.
1154 E. Arques Ave.
Sunnyvale, CA 94085
www.loglogic.com

US Toll Free: 888 347 3883
Tel: +1 408 215 5900
Fax: +1 408 774 1752
info@loglogic.com