Cautela Labs **Log Manager**

Cut compliance costs with log collection, storage and management

Cautela Labs **Log Manager** is a cloud based log management solution that provides collection, archiving and monitoring of logs, thus reducing the cost of compliance with a clear audit trail of activity that can't be repudiated. Log Manager efficiently collects, compresses, and retains all log files. Integration with Cautela Labs Enterprise Security Manager provides advanced searching, analytics, correlation, alerting, and reporting. All events and alerts provide easy, one-click access to the original source log record, so your forensics efforts will benefit too. Integrated with Log Manager, is Log Analysis which provides daily review and expert analysis services from certified analysts and security experts.

Key Advantages

- Universal log collection and retention to meet compliance requirements
- Flexible storage and retention appropriate to each log source
- Supports chain of custody and forensics
- Log analysis and search
- Stores logs locally or via a managed storage area network
- Fully integrated with Cautela Labs Enterprise Security Manager
- Flexible, hybrid delivery options include physical CL100 and/or virtual appliances
- Robust Dashboard

CL100

Front

Back

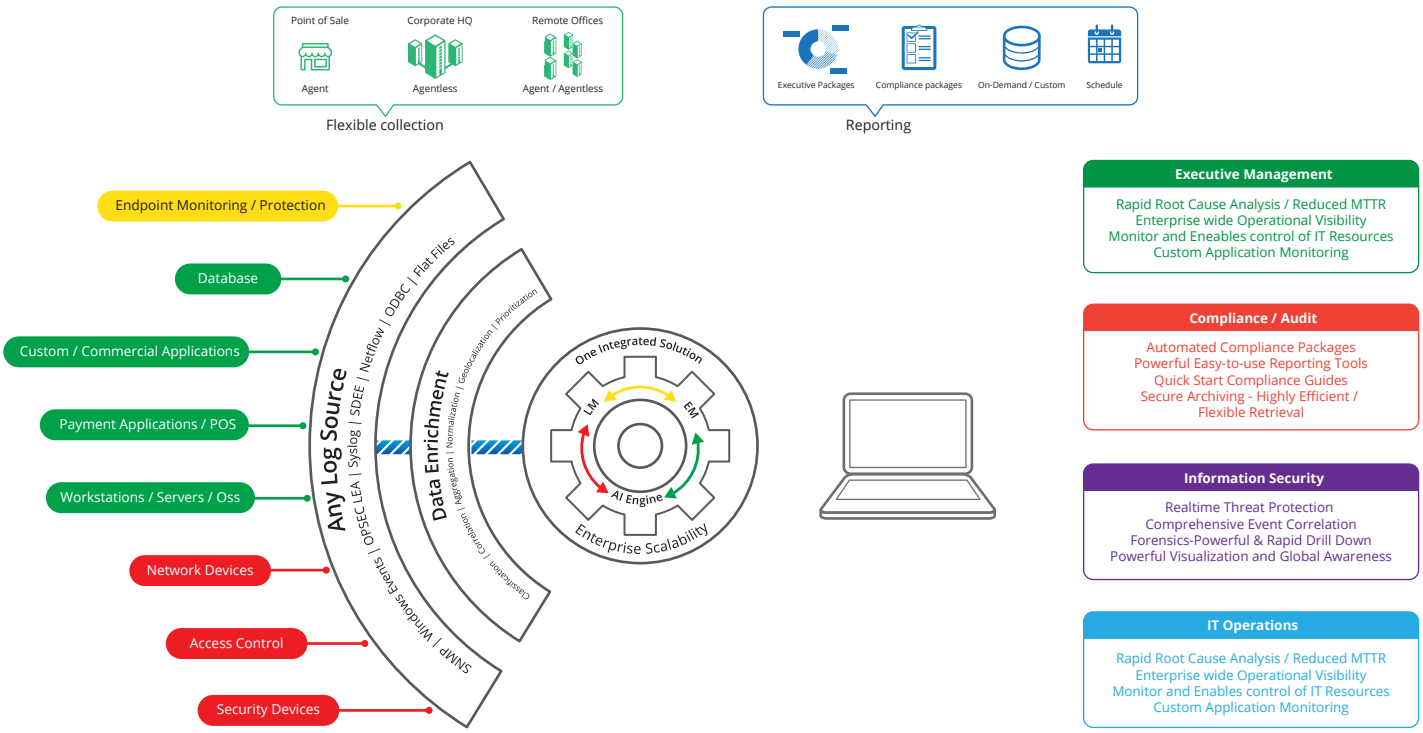
Features & Capabilities

- **Enterprise Wide Log Collection**. Secure and forensically sound collection of logs from almost any system into a central compliant cloud store.
- **Log Management**. Enterprise wide automated log collection, retention and management.
- **Forensic Readiness**. Logs are collected in a secure and forensically sound manner, retaining their original form, complete with relevant meta data, thus allowing repeated examination and re-analysis and use of the logs by other applications and processes.
- **Automated Analysis.** Collected logs are processed by a rules-driven analysis and anomaly detection engine. Flexible and extensible analysis rules allow 'interesting' events to be tagged and written to a database for further analysis and reporting.
- **Reporting.** Flexible analysis, correlation, aggregation and reporting in HTML, PDF, XLS, XML and CSV.
- **Agent Based Log Management.** Ensures the security, continuity and integrity of all collected logs and alerting at source.
- **Digitally Signed.** An RSA/SHA256 digital signature is calculated and the log digitally signed before transfer. Transfer is authenticated and encrypted using TLS.
- **Secure Storage.** Log cataloguing, 'chain of custody' records, archive creation and management. Archive to secure long term storage, complete with a digitally-signed manifest.
- **Scalable and Modular Architecture.** Designed to support almost any sized IT environment up to thousands of log sources. Supports multiple collection points, with load balancing and resilience built-in.
- Powerful Active Response technology enables you to quickly and automatically take action against threats.
- Quickly generates compliance reports for PCI DSS, GLBA, SOX, NERC CIP, and HIPAA.
- Out-of-the-box correlation rules, reports, and responses enable speedy deployment in an hour or less.

Cautela Labs **Log Manager**

Deployment:

- Log Manager Appliance (physical CL100 or virtual) is installed in the customer environment.
- Appliance collects logs from different set of host sources via an agent or agentless depending on the system and the amount of logs generated by the system.
- Log information is compressed and sent to Cautela Labs Cloud via a secure SSL channel.
- The information is presented to the security analyst in real time on the analyst console including correlation of events.
- Based on client escalation procedures the response from the security operations center are directed accordingly.
- Daily review and analysis of log activity including reports as requested by the client are sent over to the email and posted on the secure client portal.



Appliance Configuration

Hardware	Configuration	Description
CPU	Intel Xeon	All Intel Xeon processors and above
Memory	4GB / 8GB DDR3	Minimum 4GB RAM and above
Hard Drive	250GB	Minimum 250GB and above with RAID 1
OS	Linux	Hardened Linux
Network	INTEL Pro/1000	Dual Port NIC, other options available
Power	Single Power	Dual Power option available
Chassis	1U	1U Chassis with 2/4 Post Rails included

Virtual Appliance

A virtual appliance can be installed on VMware or XEN Server or a KVM virtualized environment. Recommended configuration per instance: 4GB RAM, 2 Cores, 100-200GB Disk Space with 2 NIC dedicated to the environment.

www.cautelalabs.com

sales@cautelalabs.com | 5080 N. 40th Street, Suite 300 | Phoenix, AZ 85018 | 800-997-8132