

LogLogic 4

Open Log Management and Intelligence

Driven by an urgency to find sustainable solutions for achieving regulatory compliance, simplifying operations and improving security, CIOs and IT departments rely on LogLogic® for Log Management and Intelligence (LMI)—a best practice and integral part of IT strategy.

Log Data—The Evolution

Initially used only for reporting on the health and status of IT infrastructure, log data is now a critical business asset, instrumental in fulfilling a variety of business initiatives. Everything from performance management and capacity planning to internal HR investigations to audits and security incidents requires extensive use and analysis of log data. Additionally, industry and governmental regulations mandate that businesses collect, monitor, analyze, report on and store log data from all applications, servers and endpoints. For businesses of all sizes in all industries, log management is now top of mind.

LogLogic unleashes the vast potential of log data from any device or source to protect information assets, mitigate risk and achieve operational excellence through Log Management and Intelligence (LMI). Easy-to-install log appliances automate compliance and allow administrators to capture a fingerprint of systems, user and services activity for audit and activity monitoring.

Key Benefits

First Open Log Services Platform:

Full Services Oriented Architecture (SOA) and Web Services let you create portals for compliance, risk and forensics and automate compliance and business processes.

Fully Integrated Log Data

Warehouse: Eliminates log silos in the enterprise with an open, distributed, efficient platform that is both scalable and easy to use.

Multidimensional Analytics:

Improves audit, investigations and troubleshooting productivity. Benefit from built-in compliance and services management policies. Instantly view and drill-down on normalized information. Easily perform “Google-like” searches on terabytes of indexed log data.

Business Applications

LogLogic for Compliance

LogLogic 4 helps to automate compliance activities and dramatically improve audit accuracy. Additionally, LogLogic 4 improves operations with automated, real-time reporting and alerting and the ability to map those reports and alerts to company policies. It accelerates time to risk mitigation, with the ability to search through terabytes of data in seconds.

An integral part of its comprehensive LMI platform, LogLogic Compliance & Control Suites™ automate and simplify the process of using log data to evidence and enforce business and IT policies—and can be installed in minutes, delivering results in seconds.

Regulations Require LMI	Mandates Demand It	Controls Require It
SOX FISMA GLBA JPA	PCI SLAS HIPAA	COBIT ITIL ISO
NIST 800-53 <ul style="list-style-type: none"> Capture audit records Regularly review audit records for unusual activity and violations Automatically process audit records Protect audit information from unauthorized deletion Retain audit logs 	PCI: Requirement 10 <ul style="list-style-type: none"> Logging and user activities tracking are critical Automate and secure audit trails for event reconstruction Review logs daily Retain audit trail history for at least one year 	COBIT 4.1 <ul style="list-style-type: none"> Provide audit trail root-cause analysis Use logging to detect unusual or abnormal activities ISO 17799 <ul style="list-style-type: none"> Maintain audit logs for system access and use, changes, faults, corrections, capacity demands Review the results of monitoring activities
Get fined, Go to jail	Get fined, Get sanctioned	Lose customers, reputation, revenue or job

Compliance Suites to Suit Your Business Needs

- COBIT 4.1 and SOX Compliance & Control Suite
- PCI Compliance & Control Suite
- HIPAA Compliance & Control Suite
- FISMA Compliance & Control Suite
- ISO 17799
- ITIL

LogLogic for Operations

Aside from security and compliance, logs help organizations address operational issues such as problem isolation, troubleshooting, service level and performance management, configuration and change management, capacity planning and business analysis.

Advanced features in LogLogic 4 and embedded ITIL IT Services Management best practices reports make log data available for operational applications.

“Implementing new processes and policies in support of compliance has become a significant burden for IT departments worldwide. A key element of any such activity is collecting, storing, analyzing and reporting on log data. LogLogic’s Compliance Suites promise to reduce the costs and improve the accuracy of these initiatives.”

—Jon Oltsik, Senior Analyst, Enterprise Strategy Group

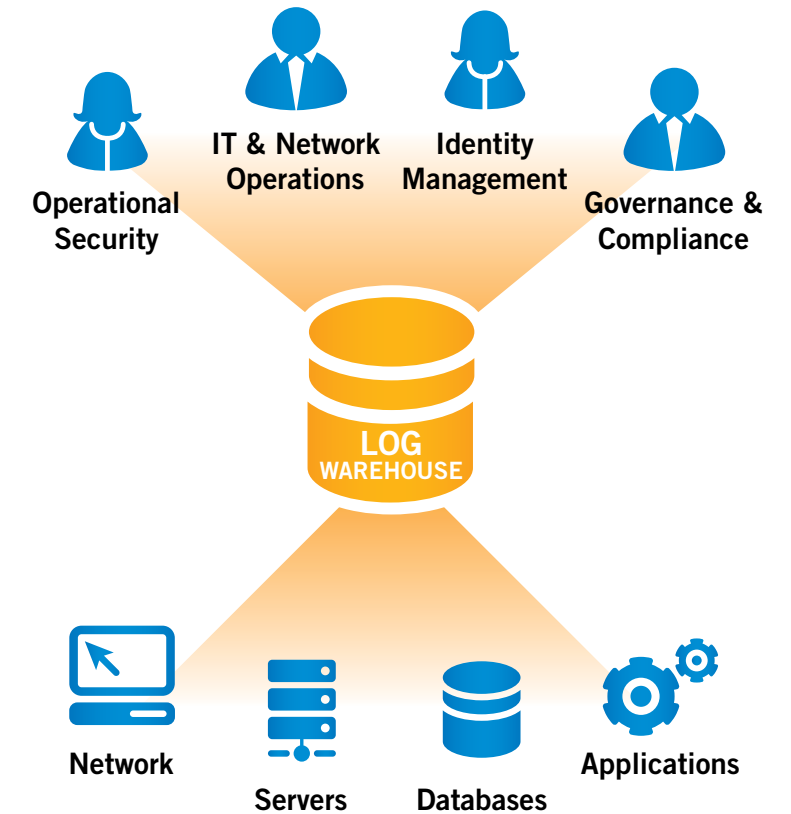
LogLogic for Security and Forensics

LogLogic reduces reporting and forensics requirements, typically associated with audit and investigations, from months to weeks, boosting IT productivity and streamlining the audit process. LogLogic also enables data to be stored in a tamper-proof environment for use in litigation and investigations.

The LogLogic Platform – A New Approach

To make data readily accessible from all network devices, applications and operating systems, a fundamentally new approach to log management is necessary. LogLogic 4 provides a standardized, automated drop-in solution that scales easily to meet business needs. It collects 100% of log data from all devices, applications and operating systems, providing agile reporting and fast search capabilities for rapid log data mining.

Security features protect data integrity, allowing for reliable long-term storage of unaltered data. Through LogLogic’s open architecture, critical information can be shared easily with other departments and applications. LogLogic archives can leverage on-board storage or be extended with a customer’s SAN, NAS or WORM infrastructure.



COLLECT

100% of log data, 100% of the time, from any device, including databases, servers and applications using a drop-in appliance and auto log source identification.

ANALYZE

Industry-first combination of indexing and search technology with deep parsing and normalization—with reports and machine learning alerts available for known and unknown log data, real-time data and historical information.

APPLY

Out-of-the-box search, reports and alerts, as well as deep compliance content in the form of Compliance & Control Suites. Customer and partner applications and mash-ups are available through the open web services API.

RETAIN

Store raw and normalized log data in separate data structures, and protect the chain of custody over the archives for immutability. Replay and re-analyze any segment, any time for forensics and root-cause analysis.

“... CIO’s goal should be to build a log management architecture ...”

“41% and growing consider integrated capabilities a higher priority than point solutions.”

—Jon Oltsik, Senior Analyst, Enterprise Strategy Group



Key Features & Benefits

Return on Investment for Businesses of All Sizes— in All Industries

- **Realize ROI in Six Months or Less:** Report and alert on custom applications and unique devices in just minutes, instead of days or weeks.
- **Boost IT Productivity:** Reduce reporting and forensics requirements typically associated with audit and investigations from weeks to minutes.
- **Reduce Infrastructure Costs:** Eliminate syslog servers and duplicated log storage, while standardizing reports and alerts.
- **Reduce compliance costs:** Save time and money on compliance audits by automating log data collection, retention and analysis. Generate reports in real time for proof of compliance.
- **Mitigate risk in seconds:** Drive business continuity by alerting in real time and allowing rapid risk mitigation. Reduce the time for an average investigation from 50 hours to two hours per incident.
- **Improve availability:** Get a complete view of IT performance issues and bottlenecks to minimize downtime and improve service delivery.
- **Integrate through open services:** Maximize your log management investment as well as existing software and hardware resources through an open architecture.

Open Log Services

LogLogic provides a fully integrated Log Data Warehouse that eliminates log silos with an open, distributed, efficient platform. Open Log Services™ provides the first integrated Services Oriented Architecture (SOA) to allow log data, reports and alerts to be easily integrated with existing security, network management, trouble ticketing and other solutions. Users can create web portals and custom dashboards to track compliance, risk mitigation and forensic activities and to automate various compliance and business processes. The LogLogic API also allows customers and partners to develop applications and mash-ups on top of our platform, permitting integration with existing portals and dashboards. A number of after-market applications are already available from LogLogic and its partners.

Integrated Log Data Warehouse

The LogLogic log data warehouse is scalable, reliable and easy to use. LogLogic 4 provides plug-and-play deployment and a maintenance-free database and operating system. At the same time, LogLogic 4 can scale up to serve telco-grade customers, including log management for central office deployments, and scale down to meet the needs and price-points of mid-market customers. Drop-in appliances

make it easy to expand the solution, when needed. LogLogic 4 collects logs from up to 4,000 devices and 75,000 messages per second per appliance for near infinite capacity.

Multidimensional Log Analysis

LogLogic 4 is the first solution to deliver both search and normalization in a single platform. Together, search and indexed reporting provide universal log processing coverage of all log sources out of the box, including homegrown and custom applications. Normalization provides in-depth analytics and business intelligence for the most frequently used data center applications.

LogLogic— The World's Leader in Enterprise-class LMI

LogLogic provides the world's leading enterprise-class platform for collecting, storing, reporting and alerting on 100 percent of IT log data from virtually any device, operating system or application.

LogLogic has established a position as the market visionary and leader, winning numerous industry awards.

For more information, visit www.loglogic.com and <http://blog.loglogic.com>.



LogLogic is a registered trademark in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders. LogLogic reserves the right to alter product offerings and specifications at any time without notice, and is not responsible for typographical or graphical errors that may appear in this document.

© 2008 LogLogic, Inc. All rights reserved.