

Alert Logic Log Manager™ and LogReview

Growing Need to Turn Logs into Intelligence

On initial inspection, log management appears to be a straightforward and basic feature of infrastructure management. It has long been used as an operational best practice and security measure required for troubleshooting, performance management and security incident response. However, in the last five years, both governmental and industry-specific regulations have included log management as a required control within an infrastructure. These regulations have also expanded the scope of what log management is by specifying a higher frequency of manual log review, not just "spot use" of the information on an as-needed basis. Ultimately, the challenge for enterprises is to take millions of event logs generated each day and turn that sea of information into intelligence in order to identify perimeter security, and insider threat and compliance issues.

Advanced Log Management, Delivered as a Service

Alert Logic's Log Manager is log management solution that is delivered using a Software-as-a-Service (SaaS) model. Effective log management is imperative in maintaining compliance but is also a powerful security tool that can mitigate intrusion and security breaches.

Automating the log collection, aggregation and normalization process, Log Manager simplifies log searches, forensic analysis and report creation through real-time or scheduled analysis. Once logs are transferred to Alert Logic's secure cloud, Log Manager protects and stores the data to preserve against unauthorized loss, access or modification.

LogReview is a service enhancement to Log Manager and provides daily event log monitoring by Alert Logic's dedicated team of security professionals. By leveraging automated log collection, normalization and analysis, LogReview relieves clients from the costly, time-consuming burden of complicated manual review processes.

Log Manager and LogReview also include integrated review and case management capabilities that allow you to track and report on incident trends across your entire enterprise, extending into the services hosted outside of your perimeter. Built-in workflow and case management tools provide an auditable trail of any suspicious findings and give a historical perspective of your entire security and compliance operations.

Meet PCI DSS Requirements

Log Manager and LogReview help meet PCI DSS requirements 10.2, 10.3, 10.5, 10.6 and 10.7. Specifically, these solutions:

- Analyze event log data for potential security incidents, such as account lockouts, failed logins, new user accounts and improper access attempts
- Identify incidents that warrant investigation and send notifications to you for review
- Create an incident audit trail for auditors and regulators
- Monitor log collection activities and alert you when logs are not being collected
- Provide daily reports mapped to the PCI DSS standard

Key Benefits

Collect & Store

- Collect logs across enterprises with no agents required
- Safely store event logs in our SAS 70 Type II audited, redundant data centers
- Store and archive data according to business and security data retention policies
- Ability to create, edit and delete groups

Correlate & Alert

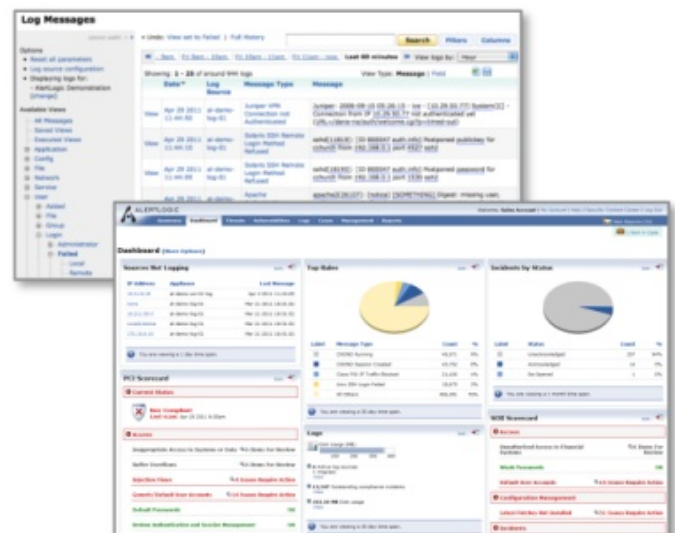
- Patented 7-Factor Threat Scenario Modeling accurately identifies and correlates events
- Automatic threat alerts sent directly to customer inboxes, mobile phones or ticketing systems
- Custom workflow and incident notification reports through case management system
- Collect, correlate and alert on text-based log files that are commonly used in third-party software applications, in-house business applications and Web servers

Report & Search

- Secure Web portal offers 24x7 access to dynamic reports and flexible search tools
- Cloud-powered infrastructure provides powerful search, analysis and forensic capabilities
- Dozens of out-of-the-box reports, scorecards and dashboards
- Saved views shareable within user's customer ID

Monitor & Comply

- Daily review, analysis and reporting services by certified security analysts
- Real-time response to security incidents following the customers' escalation procedures
- Easily maintained compliance with audit-ready reports
- Case alert rules available to notify a user when a case has been created or assigned, or when a due date has been exceeded



Log Manager & LogReview Features

Log Collection

Agentless Log Collection

Windows Event Logs

- Windows System Event Logs
- Windows Security Event Logs
- Windows Application Event Logs
- Microsoft Exchange Server Application Logs
- Microsoft SQL Server Application Logs
- Windows-Based ERP and CRM Systems Application Logs

Syslogs

- Unix, Linux Server Logs
- Most Network Device Logs (e.g., Routers, Switches, Firewalls)

Database Logs

Flat/Text Files

- Web Servers Logs (e.g., Apache, IIS)
- Windows ISA Server Logs
- DNS and DHCP Server Logs
- Homegrown Application Logs
- Exchange Message Tracking Logs

Log Parsing

New Parsers and Parsing Rules Updated Monthly

Parsing Set Consolidated from Multiple Sources

- Alert Logic Security Research Team
- Customer Requests
- Open Source, Third-Party Collaboration

Real-Time Parsing Updates to Log Management System

Custom Parsing Rule Creation and Editing

Event Correlation and Notification

Advanced Artificial Intelligence Correlation System

Custom and Out-of-the-Box Correlation Rules

- Designed to Detect Suspicious Activity
- Automatic Alerts Sent When Rule Is Triggered
- PCI Specific Rules to Comply with Requirement 10.6

Patented 7-Factor Threat Scenario Modeling

Monitor Suspicious Activity

Log Manager is able to produce a wide range of views and reports that turn reams of log data into relevant and actionable information. Below are examples of reports that help you monitor suspicious activity as well as be alerted at set thresholds.

With LogReview, security analysts review these reports on a daily basis to identify potential attacks and provide guidance and recommendations.

