

Alert Logic Log Manager™ and LogReview Features and Capabilities

Log Collection

- Agentless Log Collection
- Windows Event Logs
 - Windows System Event Log
 - Windows Security Event Log
 - Windows Application Event Log
 - 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, and 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

Integrated Managed Security Services

- GIAC-Certified Security Analysts and Researchers
- 24x7 State-of-the-Art Security Operations Center
- Trained Experts in Alert Logic Solutions
- Monitoring, Analysis and Expert Guidance Capabilities
- Customized Alerting and Escalation Procedures

Analysis and Reporting

- Dozens of Dashboards and Reports Available Out-of-the-Box
- Custom Reporting Capabilities
- Audit-Ready Reports
- Single Web-Based Console for Entire Environment
 - User Management and Administration
 - Dashboards and Drill-Down Analysis
 - Report Scheduling, Creation and Review

Compliance Support


- SAS 70 Type II Audited Data Centers
- PCI Level 2 Audited Vendor
- PCI Approved Scanning Vendor (ASV)
- Indefinite Storage and Archival of Incident Analysis and Cases
- Support for Multiple Compliance Mandates
 - PCI DSS 2.0, HIPAA, SOX, GLBA, CoBIT, etc.

Security-as-a-Service Delivery

- Rapidly Deploy and Scale as Needed
- Pay-as-You-Go; Minimal Capital Expenditure
- Always Utilize Latest Software and Signature Database
- No Hidden Costs – Subscription Includes:
 - Software and Hardware Upgrades, Maintenance and Patches
- Architected for Multi-Tenant Support
- Easily Deploy in On-Premise, Off-Premise or Hybrid Environments



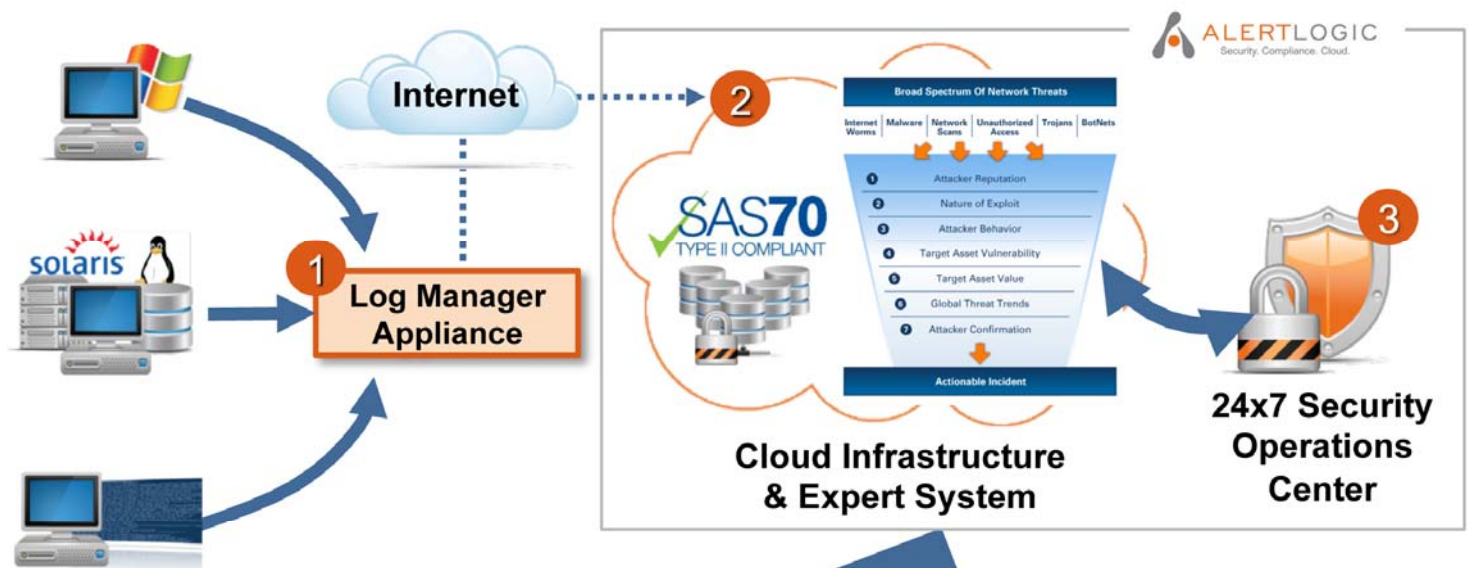
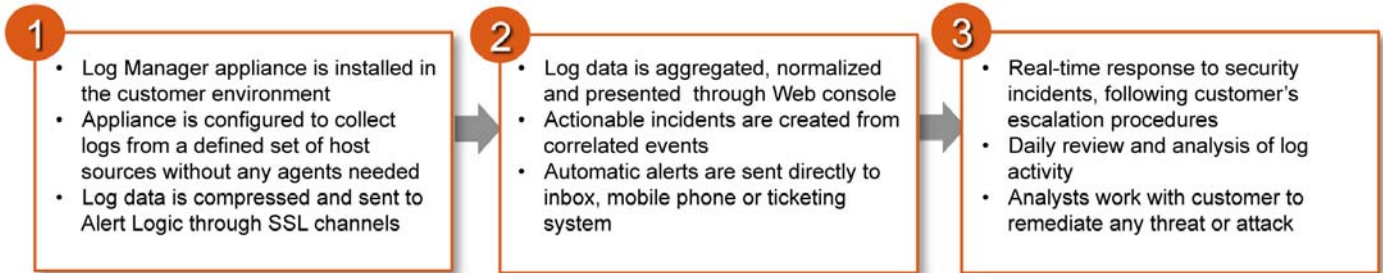
Appliance Specifications

Appliance	CPU	Memory	Storage	Chassis	Power	Rails	NIC Options	Bandwidth																		
Log Manager™ Appliance 	Intel Celeron / Intel Xeon	2GB / 4GB DDR3	250GB	1U Rack	250W Single Cabled AC			Static 2/4 Post Rails	Up to 10Gbit																	
					<table border="1"> <thead> <tr> <th>Details</th> <th>Min</th> <th>Typical</th> <th>Max</th> </tr> </thead> <tbody> <tr> <td>Measured Idle Power</td> <td>36.1</td> <td>41.5</td> <td>69.1</td> </tr> <tr> <td>Power at Full Load</td> <td>114.6</td> <td>114.8</td> <td>185.8</td> </tr> <tr> <td>Total Power Dissipation</td> <td>116.0</td> <td>149.0</td> <td>195.0</td> </tr> </tbody> </table>					Details	Min	Typical	Max	Measured Idle Power	36.1	41.5	69.1	Power at Full Load	114.6	114.8	185.8	Total Power Dissipation	116.0	149.0	195.0	Intel® PRO/1000 PT Single Port Server Adapter Intel® PRO/1000 PT Dual Port Server Adapter Intel® PRO/1000 PF Dual Port Server Adapter (Fiber) Intel® PRO/1000 PT Quad Port Server Adapter Intel® PRO/1000 PF Single Port Server Adapter (Fiber) Intel® PRO/1000 PF 1Gb Quad Port Server Adapter(Fiber)
					Details	Min	Typical			Max																
Measured Idle Power	36.1	41.5	69.1																							
Power at Full Load	114.6	114.8	185.8																							
Total Power Dissipation	116.0	149.0	195.0																							

Product Overview

Alert Logic Log Manager is a cloud-powered log management solution that provides on-demand log collection, storage, reporting and correlation capabilities across your entire environment. Integrated with Log Manager, LogReview provides daily review and expert analysis services from Alert Logic's state-of-the-art Security Operations Center (SOC), which is staffed by GIAC-certified analysts and security experts.

The Way It Works



Alert Logic Security Research Team

RESEARCH

- Real-time data from >1K global customer footprint
- Alert Logic security and emerging threat research team
- Third-Party security information sources and feeds

CONTENT DEVELOPMENT

- Correlation rules
- Remediation and resolution documentation
- Performance and accuracy tools

EXPERT SYSTEM

- Patented artificial intelligence system and correlation engine
- Continuously "learns" and correlates millions of data points into meaningful incidents