

Alert Logic Threat Manager™ and ActiveWatch Features and Capabilities

Threat Signatures and Rules

45,000+ IDS Signature Database; Weekly Signature Updates
 Rule Set Consolidated from Multiple Sources
 Alert Logic Security Research Team
 Emerging Threats
 Open Source, Third-Party Collaboration
 Real-Time Signature Updates to Alert Logic Expert System
 Custom Rule Creation and Editing

Vulnerability Assessment

Unlimited Internal and External Scans
 PCI DSS 2.0 Compliant External Scanning
 Broad Scanning Capabilities
 Network Infrastructure
 Server Infrastructure
 Business Critical Applications

Intrusion Detection

Advanced Network Traffic and Payload Visibility
 Web Technologies (IPv6, Ajax, SQL Injection, etc.)
 Detect SSL-Based Intrusion Traffic
 Signature and Activity-Based Correlation
 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
 Common Vulnerability Scoring System (CVSS) to Assess Risks
 Audit-Ready Reports
 Single Web-Based Console for Entire Environment
 User Management and Administration
 Dashboards and Drill-Down Analysis
 Report Scheduling, Creation and Review
 Scan Scheduling and Results Review

Compliance Support

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




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 Cloud Environments



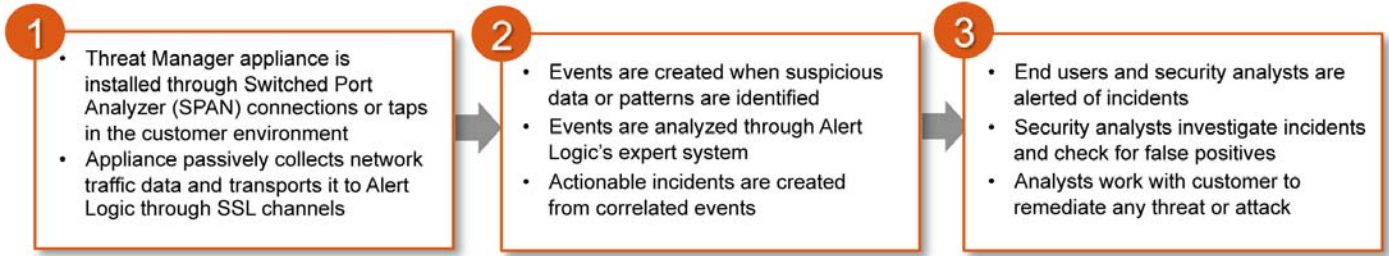
Appliance Specifications

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	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)	Up to 10Gbit	
					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 Threat Manager is a cloud-powered vulnerability assessment and intrusion detection solution that is delivered using a Software-as-a-Service (SaaS) model. Integrated with Threat Manager, ActiveWatch provides 24x7 monitoring and expert guidance 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

- IDS and vulnerability signatures
- 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