DATA SHEET

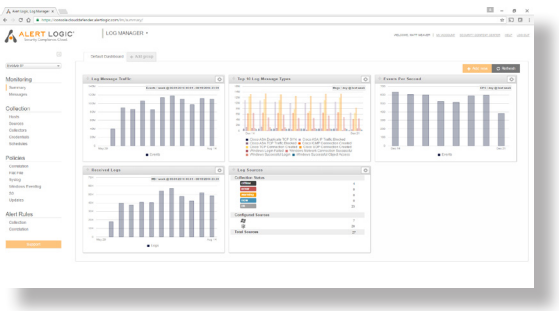
Alert Logic® Log Manager and Log Review

The Alert Logic® Security-as-a-Service approach to log management makes log management simple to implement, easy to afford and almost effortless to manage.

EVOLVE IP
THE CLOUD STRATEGY COMPANY™

ALERT LOGIC®
Security. Compliance. Cloud.

Addressing the challenges of Log Management with cloud-powered log management as-a-service.



Dozens of Pre-built Reports, Scorecards and Dashboards

GETTING INSIGHT FROM LOG MANAGER IS *EASY*

- Predictive search gets you to key data faster
- Intuitive query building – not SQL-like expressions
- Progressive search results for on-the-fly feedback and refinements
- 100+ Pre-built reports and dashboards

Log management is an essential infrastructure management best practice, and is necessary for achieving compliance. Log management is becoming more complex as organizations transition from on premises data centers to cloud environments. In today's "cloud first" environment, solving your log management needs with yesterday's technology is not viable. You need an approach to log management that delivers deep insight into your security and compliance posture without the headache of bringing yet another product in-house.

Log Managment Challenges:

- Log sources are more numerous and more varied.
- Infrastructure is moving from traditional hosted and on-premises deployments into the cloud, requiring new deployment models for virtual and elastic cloud environments.
- Compliance mandates such as PCI DSS, HIPAA and Sarbanes-Oxley have added new log management deliverables.

The Alert Logic® Security-as-a-Service approach to log management solves these challenges by making log management simple to implement, easy to afford and almost effortless to manage.

All Your Infrastructure - All Your Data - All Together

If your IT infrastructure is spread across in-house, hosted and cloud deployments, your log management needs to be there too.

- Alert Logic® Log Manager™ collects, aggregates and normalizes log data whether it originates in your own data center, a hosted environment or the cloud.
- A powerful web interface gives you a unified view into all of your data, with tools to rapidly uncover the insight and alerts you need to remain secure and compliant.
- Flexible data collection options – physical appliances, remote collectors with lightweight agents or agentless methodology, and cloud native APIs – provide low-impact deployment options for all of your infrastructure.

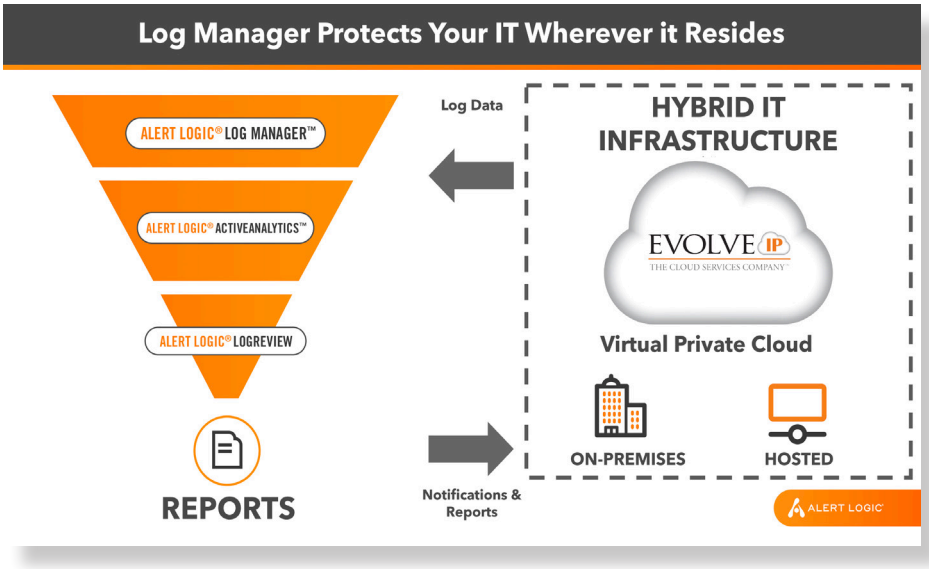
DATA SHEET

Alert Logic Log Manager & Log Review

EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Get a Virtual Team with Log Review

Log Review reporting provides daily event log monitoring by our dedicated team of security professionals. With Log Review, log analysis is never delayed or sidetracked by competing priorities. Log Review also includes integrated review and case management capabilities. Track and report on incident trends across your entire enterprise, including 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 operation.



Alert Logic Protects Your Data

Meet Your Key PCI DSS Compliance Requirements

Log Manager and Log Review help meet PCI DSS requirements 10.2, 10.3, 10.5 10.6 and 10.7:

- 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.
- Provide daily reports mapped to the PCI DSS standard.
- Create an incident audit trail for auditors and regulators.

PCI DSS COMPLIANT

Features and Benefits	
Technology	• Easy to use web interface with intuitive search interface • Thousands of parsers available with new log format support added frequently • Cloud storage with offsite replication for disaster recovery
Event Correlation and Notification	• Advanced correlation capabilities • Designed to detect suspicious activity • Rule based automatic alerts and notification • PCI-specific rules to comply with requirement 10.6
Integrated Managed Security Services	• Certified security analysts and researchers • 24x7 state-of-the-art Security Operations Center • Monitoring, analysis and expert guidance capabilities • Customized alerting and escalation procedures
Analysis and Reporting	• Dozens of dashboards and reports • Custom reporting capabilities • Audit-ready reports • Single web-based console for entire environment • Report scheduling, creation and review
Compliance Support	• SSAE 16 audited data centers • PCI Level 2 audited vendor • PCI Approved Scanning Vendor (ASV) • Storage and archival of incident analysis and cases • Support for multiple compliance mandates • PCI DSS, HIPAA, SOX, GLBA, cobit, etc.
Security-As-A-Service	• Rapidly deploy across your environment and scale as needed • Subscription model with minimal capital expenditure • No hidden costs – Subscription is all-inclusive

Visit www.evolveip.net/compliance for additional security and compliance solutions.