ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® LOG MANAGER™ & LOG REVIEW

CLOUD-POWERED LOG MANAGEMENT AS A SERVICE

Simplify Security and Compliance Across All Your IT Assets. Log management is an essential infrastructure management best practice, and is essential in achieving compliance. Log management is becoming more complex as companies transition from on premises data centers to public 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 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.

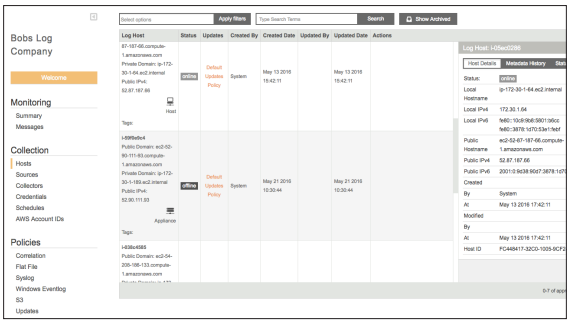
Meanwhile, strategic projects compete for limited IT resources. How will your organization meet these challenges?

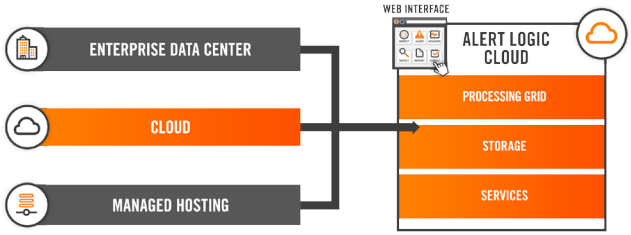
The Alert Logic® Security-as-a-Service approach to log management solves these challenges by making log management simple to implement, easy to afford and almost effortless to manage.

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.

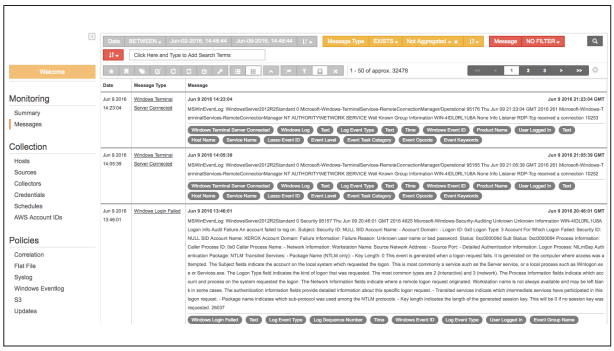
- Alert Logic® Log Manager™ collects, aggregates and normalizes log data whether it originates in your own data center, a hosted environment or the cloud.
- A powerful web interface gives you a unified view into all of your data, with tools to rapidly uncover the insight and alerts you need to remain 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.

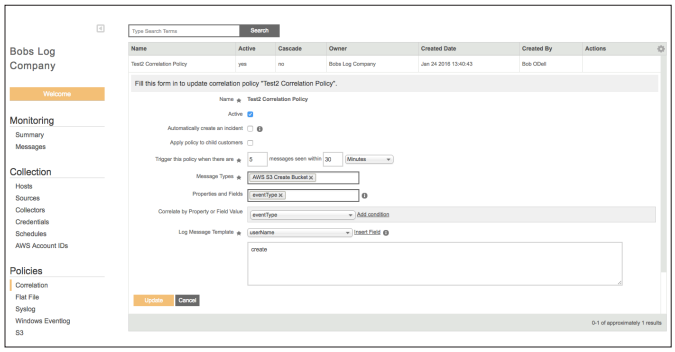




GET INSIGHT FAST WITH AN INTUITIVE WEB INTERFACE FEATURING SUPER-RESPONSIVE SEARCH.

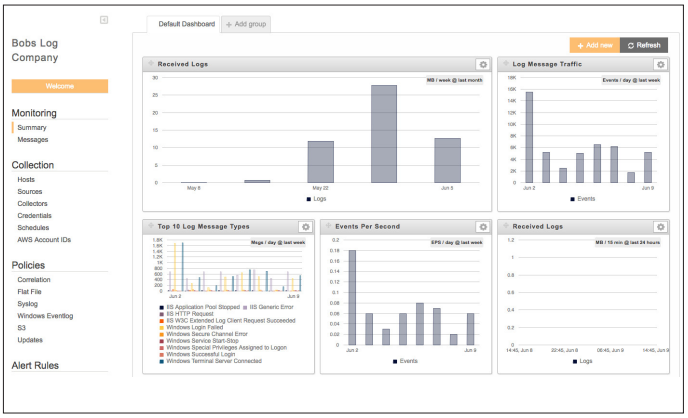
- Log Manager provides hundreds of pre-built reports, saved views, and dashboards to meet many of your security and compliance requirements on day one.
- Searching takes flight with an interface that predicts and suggests queries and makes it easy to change and refine queries mid-stream.
- Turn data into action: It's easy to correlate events and set automatic alerts and reporting to enable rapid response to security events.





GET RESULTS, NOT IMPLEMENTATION AND MANAGEMENT HEADACHES. SECURITY-AS-A-SERVICE DELIVERY MEANS THAT YOU'RE UP AND RUNNING FAST.

- Onboarding and provisioning in minutes.
- Access virtual appliances and agents quickly through the Log Manager interface.
- Subscription pricing model means no upfront costs or capital expenditures, and flexibility to scale with your growth.
- Rich APIs for deep integration into management systems, simplifying ongoing ordering, provisioning, billing and support.



UNDER THE HOOD, YOU'VE GOT THE POWER TO HANDLE YOUR BIGGEST DATA REQUIREMENTS.

With multiple petabytes of log data under management, Alert Logic has built the systems that support the massive volumes of log data that your systems and devices generate.

- The Alert Logic back-end grid processes log data rapidly to give you rapid access to data.
- Log data is stored securely for a full year to protect against unauthorized loss, access or modification in our SSAE 16 Type II verified data centers. (Longer storage periods are available.)

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.

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.

FEATURES AND CAPABILITIES

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 DELIVERY	• Rapidly deploy across your environment and scale as needed • Subscription model with minimal capital expenditure • No hidden costs – Subscription is all-inclusive

ENVIRONMENTS WE PROTECT

Alert Logic delivers Security-as-a-Service, protecting your critical data across public cloud, private cloud, on-premises, managed hosting/co-lo and hybrid environments.

Alert Logic has built deep integrations into the leading public cloud platforms including Amazon Web Services and Microsoft Azure.

amazon web services

Microsoft Azure

PRIVATE CLOUD

HOSTED

PUBLIC CLOUD

ON-PREMISES

ALERT LOGIC®