ALERT LOGIC®

OFFERING BRIEF:

CONTINUOUS LOG MANAGEMENT & MONITORING

ALERT LOGIC® LOG MANAGER™ AND ALERT LOGIC ACTIVEWATCH FOR LOG MANAGER

Virtually every system you use to manage and run your business creates log data. This data is your system of record, detailing material changes to your networks, applications, and systems on a daily basis. For years, businesses have looked for better ways to harvest this rich data for operational, compliance, and security uses. Unfortunately, the traditional method of deploying hardware and software on-premises to collect, manage, and analyze log data involves a significant investment of time and money.

The complexity of this approach is compounded by the trend toward "cloud first" hybrid data centers where an organization's most sensitive data is now dispersed across public clouds, private clouds, and hosting providers as well as on-premises. 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.

ALERT LOGIC® LOG MANAGER™

TAKES THE COMPLEXITY AND COST OUT MANAGING LOGS. WITH ALERT LOGIC LOG MANAGER YOU CAN COLLECT, AGGREGATE, AND NORMALIZE LOG DATA FROM ANY OPERATING SYSTEM, NETWORK DEVICE, AND APPLICATION IN YOUR ENVIRONMENT AUTOMATICALLY.

ACTIVEWATCH FOR LOG MANAGER

PROVIDES 24X7 REAL-TIME SECURITY MONITORING THAT IDENTIFIES POTENTIAL COMPLIANCE AND SECURITY ISSUES THAT COULD COMPROMISE YOUR ORGANIZATION'S SECURITY POSTURE.

Alert Logic Log Manager with Alert Logic ActiveWatch delivers on the promises made by traditional log management products without the cost and complexity. Alert Logic Log Manager is a cloud-based log management solution that enables easy, scalable collection of log data from across your datacenter environments, whether they be on-premises, in the cloud, or a combination of both. With lightweight deployment options, you can collect logs from operating systems, applications, network devices, and more in a matter of hours. Powered by a massive processing grid, Alert Logic Log Manager allows you to search logs in a consistent, reliable manner without creating complex queries or custom reports. This powerful technology, coupled with an intuitive web interface, will allow your IT resources to spend more time uncovering valuable information and less time sorting through mountains of meaningless logs.

THE KEY TO MEETING YOUR SECURITY AND COMPLIANCE GOALS

Collecting, parsing, and, storing logs are the first of your security and compliance goals, but without continuous expert monitoring, meeting your goals is unlikely, if not impossible. To truly maintain your desired compliance and security posture, you need a team of experts working for you around the clock, identifying compliance issues and indicators of compromise from your log data. This is what Alert Logic ActiveWatch for Log Manager delivers: continuous expert monitoring.

SECURITY & COMPLIANCE ACROSS ALL YOUR IT ASSETS

- Uncovers compliance and security issues from your log data: automate log collection, aggregation, and normalization of logs across your entire environment, saving time, money and reducing complexity
- Scalable real-time log collection with 90-day and 1-year data retention to accommodate your growing and changing environment
- Delivered as-a-Service so you don't have to focus on managing the storage, computing and software required for 24 x 7 availability

Alert Logic ActiveWatch for Log Manager is a managed service that delivers 24x7 security monitoring of your log data and identifies potential security and compliance issues that could impact your organization. Alert Logic security and compliance experts use advanced technology, up-to-date threat intelligence, and correlation rules to help you gain deep insight and visibility into the security posture of your IT environment. Unlike other costly and incomplete managed security services, Alert Logic ActiveWatch for Log Manager not only identifies security issues, but also provides the recommended steps you need to resolve the issue. With ActiveWatch for Log Manager, you can also meet the log review mandates required by many regulations, such as PCI DSS 3.1. By eliminating the burden of daily log review and delivering an easy to use search capability, you can focus your efforts on other important, business critical projects.

This simple, easy approach to log management and analysis increases your ability to maintain compliance and increase your security posture without being an expert.

"WE'RE HAPPY TO PUT IT SECURITY IN THE HANDS OF ALERT LOGIC SO WE CAN FOCUS ON BUILDING GREAT PRODUCTS FOR OUR CLIENTS."

GAUTAM LULLA, CHIEF OPERATING OFFICER

travel tripper

ALERT LOGIC LOG MANAGEMENT: THE COMPONENTS

Unlike other log management approaches that require you to purchase software, hardware, hire and/or train staff, and maintain the solution, Alert Logic's approach to log management is all-inclusive, providing everything you need to meet your log management goals.

ALERT LOGIC® LOG MANAGER™	Log management and analysis solution that collects, parses, and analyzes logs from operating systems, applications, and network devices.
ALERT LOGIC® ACTIVEANALYTICS	Security analytics platform that processes, parses, and analyzes data to identify security incidents
ALERT LOGIC® ACTIVEINTELLIGENCE	New threat intelligence sources and security content to support additional security use cases
ALERT LOGIC® ACTIVEWATCH™	24x7 security monitoring and investigation managed service staffed by security experts who understand threats and know how to respond to them

FEATURES AND CAPABILITIES

TECHNOLOGY	• Easy to use web interface with intuitive search interface • Over 4,000 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 • Automatic alerts sent when rule is triggered • 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 3.1, HIPAA, SOX, GLBA, cobit, etc.
SECURITY-AS-A-SERVICE DELIVERY	• Rapidly deploy across your environment and scale as needed • Pay-as-you-go model with minimal capital expenditure • No hidden costs – Subscription Includes: • Software and Hardware Upgrades, Maintenance and Patches

SPECIFICATIONS

WINDOWS AGENTS SPECIFICATIONS	
CPU Utilization	1-10%, depending on log volume
RAM	15 MB minimum
Disk	30 MB minimum
Internet connection	Port 443 - required for log transport and agent maintenance updates
Supported OS	Windows Server (2012, 2008, 2003, 2000) Windows (8, 7,Vista, XP) Platform: 32-bit / 64-bit
Log collection support	Agent-only deployments and with virtual and physical appliances, Virtual Private Cloud (VPC) and Public Cloud
Encryption	TLS Standard (SSL): 2048bit key encryption, 256bit AES bulk encryption
Log collection frequency	Every 5 minutes (logs collected and sent back to Alert Logic Cloud)
Host permissions	Local System account has all the requisite permissions by default

SPECIFICATIONS (CONT.)

SYSLOG AGENTS SPECIFICATIONS	
CPU Utilization	1-10%, depending on log volume
RAM	10 MB minimum
Disk	Up to 500 MB minimum
Internet connection	Port 443 - required for log transport and agent maintenance updates
Supported OS	Debian (Squeeze, Lenny), Ubuntu 7.x-12.x, CentOS 5.x -6.x RedHat 5.x -6.x), Platform: 32-bit / 64-bit
Log collection support	Agent-only deployments and with virtual and physical appliances, VPC and Public Clouds
Encryption	TLS Standard (SSL): 2048bit key encryption, 256bit AES bulk encryption
Log collection frequency	Every 5 minutes (logs collected and sent back to Alert Logic Cloud)
Host permissions	No special permissions are required

PHYSICAL APPLIANCE SPECIFICATIONS	
CPU	Intel 4, 8, or 16 core
RAM	4GB, 16GB, 32GB, or 64GB
Disk	2x 1TB, RAID 1
Internet connection	Port 443 - required for log transport and appliance maintenance updates
Log collection support	Both agent-based and agent-less Windows, Syslog, Flat File log collection
Encryption	TLS Standard (SSL): 2048bit key encryption, 256bit AES bulk encryption

VIRTUAL APPLIANCE SPECIFICATIONS	
CPU	2 cores minimum
RAM	2GB minimum
Disk	1GB – 50GB
Internet connection	Port 443 - required for log transport and appliance maintenance updates
Supported virtual environment	VMware only
Log collection support	Syslog via agent or agent-less, Windows and Flat File via Agent only
Encryption	TLS Standard (SSL): 2048bit key encryption, 256bit AES bulk encryption
Note	Not designed to run in a public cloud environment
Host permissions	Use agent-only deployments instead

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,300 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24x7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

© 2015 Alert Logic, Inc. All rights reserved. Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or servicemarks of Alert Logic, Inc. All other trademarks listed in this document are the property of their respective owners.

ALERT LOGIC®