

# ALERT LOGIC<sup>®</sup> LOG MANAGER<sup>™</sup> & LOGREVIEW

### **CLOUD-POWERED LOG MANAGEMENT AS A SERVICE**

Simplify Security and Compliance Across All Your IT Assets. Log management is an infrastructure management best practice, supporting performance management, security incident response and compliance requirements. However, log management is becoming more complex all the time: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.

- 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 simple but 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 or remote collectors with agent-based or agentless methodology provide low-impact deployment options for all of your infrastructure.
- Collect syslog from firewalls, switches, routers, printers, Unix servers and many such devices.

_	Select Some Options		Apply filters Type Search Terms							
	Log Host	Created By	Created Date	Updated By	Updated Date	Actions			WEB INT	DEACE
	Fagsi	System	Jan 4 2010 14:20:06		never				••	
		i-abl	7ddda			showing 1 of 1 row		ENTERPRISE DATA CENTER	Q. 4	
			ladala History		1			ENTERPRISE DATA GENTER	<u></u>	CLOUD
			Jan 4 2	013 14 22 37	10.000					× ·
		Amil	D: ami.#540c29c		0.265					PROCESSING GRID
		Type	t1.micro		10000					
		Host	ec2:54-234-84-242.4 lp:10:114-49-251.ec	compute-1.amazonaws.com 2.internal			_)	CLOUD		
		Pré	54.234.84.242 10.114.49.251							STORAGE
		P/8	2001:0:9438:953c:14 fe80::1427:1134358		1333					
log			Jan 4 2	013 14 20 06	-					SERVICES
		Amil	D: emi-#540c29c				┋)	MANAGED HOSTING	-	JENTIOLO
		Tjpe	t1.micro							
		Host	names: ec2.54.234.84.242.0	compute-1.amazonaws.com						

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

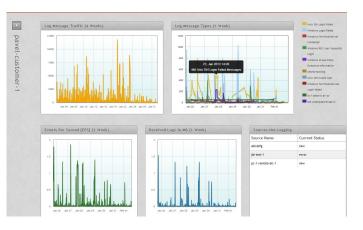
- Log Manager provides dozens of pre-built reports, scorecards and dashboards to meet many of your security and compliance requirements on day one.
- Searching takes flight with an interface that predicts and suggests queries, returns initial results in the blink of an eye, and makes it easy to change 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.

	_		4- 08-12-2012, 22:50 08-01-2013, 22:50 1/- Message Type x NO FILTER Not Apprepried - x 1/-	9		Type Search Terms 0						
emo	Ness	ege Text X	NO FILTER 11- Click Here and Type to Add Search Terms		Sales LM3 Demo	Name	Active	Cascade	Owner	Created Date	Created By	Actions
	Date	Message Type	Hessage Text	Actions 🔅		SQL Server Login Falled Policy	yes	no	Sales LH3 Demo	Jan 7 2013 10:53:35	Justin Criswell	
2	2013	Mindaws			Monitoring Summary Messages Collection Sources Hosts	Pill this form in to update correlation policy 1 Name + 5 Active Automatically create an incident Apply policy to child customers	Qi, Server Login Fa 2 2 <b>D</b>					
	2013 22:41:13	Windows Group Policy Execution Completed	delet-destage Westwerkene 2008/2004/armsen 0 Annuels Makane Grandelang Gerenstand 2004 West an 15 46-113 667 2013 BKD Marris Methods-destage Westwerkene 2008/2004/armsen 2008/2002/2014 BKD Marris 2004 BKD M		Appliances Credentials Schedules Policies	Trigger this policy when there are Hosoge Types Properties and Pielos Correlate by Property or Pield Value	SQL Server Login Fr	sie(X)	Minutes •			
	2013		skritekentagi Wein-Gerenzösskölatasener i Nicosati Hadan Graphicy/Gerstand 1987 Med an (9 Metri 10 07 201 1318 More International Antipolitik (Metri Metri Metri Metri 10 Metr	<i>u</i>	Correlation Flat File Systeg Windows Eventiog Alert Rules	Log Hessage Template 🔶 🤅	Host Name	enpt failed from %Clier	• Insert Field ()			
n	2013	Second Entiticy	Mitheliheading, Windowsferned/2008/Datacatere 0 Alconet Mindow Compilation/Operational 15565 Mito Jan 00 Autoriti Self 20213 3323 Marca Mindows Grauphille Mith/BRITTSSTERE User Information AMA2004/SGS24, None Info Service configuration update to atandation is not requir 6 and will be aligned. 3467		Collection Corrolation	Update Cancel						
		Execution Information	(nonshand) fan (retheling) fan finn fanlig (anlige (rethelingen)) fan helinen (lantweis) fanlige (rethelingen) fanligensk		Support							ste
				Ing 51 of 46848 rows								



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

- Cloud-speed provisioning in minutes.
- Access virtual appliances and agents quickly through the Log Manager interface.
- Pay-as-you-go 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 more than 2.8 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.

- Alert Logic's 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 LOGREVIEW

LogReview reporting provides daily event log monitoring by Alert Logic's dedicated team of security professionals. With LogReview, log analysis is never delayed or sidetracked by competing priorities. LogReview 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 LogReview 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	<ul> <li>Easy to use web interface with intuitive search interface</li> <li>Over 4,000 parsers available with new log format support added frequently</li> <li>Cloud storage with offsite replication for disaster recovery</li> </ul>
EVENT CORRELATION AND NOTIFICATION	<ul> <li>Advanced correlation capabilities</li> <li>Designed to detect suspicious activity</li> <li>Automatic alerts sent when rule is triggered</li> <li>PCI-specific rules to comply with requirement 10.6</li> </ul>
INTEGRATED MANAGED Security Services	<ul> <li>Certified security analysts and researchers</li> <li>24x7 state-of-the-art Security Operations Center</li> <li>Monitoring, analysis and expert guidance capabilities</li> <li>Customized alerting and escalation procedures</li> </ul>
ANALYSIS AND Reporting	<ul> <li>Dozens of dashboards and reports</li> <li>Custom reporting capabilities</li> <li>Audit-ready reports</li> <li>Single web-based console for entire environment</li> <li>Report scheduling, creation and review</li> </ul>
COMPLIANCE SUPPORT	<ul> <li>SSAE 16 audited data centers</li> <li>PCI Level 2 audited vendor</li> <li>PCI Approved Scanning Vendor (ASV)</li> <li>Storage and archival of incident analysis and cases</li> <li>Support for multiple compliance mandates</li> <li>PCI DSS 3.1, HIPAA, SOX, GLBA, cobit, etc.</li> </ul>



- Rapidly deploy across your environment and scale as needed
- Pay-as-you-go model with minimal capital expenditure

#### SECURITY-AS-A-SERVICE DELIVERY

- 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

#### 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



### **SPECIFICATIONS** (CONT.)

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 3,000 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 24×7 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.

