



## THE SMARTEST WAY TO MANAGE LOGS

### The Need for Effective Log Management

Log Management is a necessity for regulatory compliance and essential to maintaining a positive security posture in your environment. As your IT organisation evolves to comply with today's regulations and defend against new network security threats, you should choose a solution that avoids expensive maintenance and operating costs, reduces the number of resources needed to maintain and support your solution, and most importantly provides the most effective log management solution on the market today.

As the first cloud-powered log management solution, Alert Logic's Log Manager is designed to remove the resource and financial burden of on-premise solutions. Our SaaS offering collects log data via an agentless collection device and provides log storage, reporting, correlation and monitoring leveraging our grid computing and storage architecture in our highly secure redundant datacentres.

Alert Logic's cloud-powered Log Manager solution is the smartest choice for overregulated businesses with underfunded IT departments.

1. Reduce costs: No hardware, software or maintenance to purchase greatly reduces your cost of ownership. All storage, monitoring, maintenance, upgrades, and support are handled by Alert Logic, removing the need for staff resources to manage the solution.
2. Effective Log Management: Log Manager collects, stores, reports and correlates log data in our highly secure and redundant datacentres, helping you avoid the maintenance and operating costs of on-premise solutions.
3. LogReview Service: Extends the value of Log Manager and frees up your resources by transferring the burden of daily log review and maintaining a PCI DSS compliant audit trail to our team of certified security analysts.

The screenshot displays the Alert Logic web interface. The top navigation bar includes 'Summary', 'Dashboard', 'Threats', 'Vulnerabilities', 'Logs', 'Cases', 'Management', and 'Reports'. The 'Logs' section is active, showing a 'Log Incidents' and 'Log Messages' view. A bar chart displays 'Archived Messages' and 'Analyzed Messages' for the range 'Dec 26 2009 - Jan 26 2010', with a total of 910,240 messages. The chart shows a steady flow of messages with a significant spike on Jan 25. Below the chart, a 'Recent Messages' section provides a table of the latest incidents.

Latest Incidents	ID	Summary	Date
Sources Not Logging	493783	New Domain Admin Detected	Today 07:16:31
Busiest Sources	493141	New Domain Admin Detected	Jan 25 2010 14:48:50
Appliance Performance	492391	New Domain Admin Detected	Jan 24 2010 21:05:19
Appliance Transport	492268	New Domain Admin Detected	Jan 24 2010 15:34:09
Appliance Queue	491547	New Domain Admin Detected	Jan 23 2010 20:40:15
Top Message Types			
Disk Usage History			

Home | My Account | Help | Contact  
Version 4.6.0 © 2001-2009 AlertLogic, Inc. U.S. and International Patents Pending.

Quickly view log data in the user interface

# How We Do It

## Collect

Our collection appliance automates syslog and windows log collection in your environment without agents.

## Store

Our proprietary flat-file architecture allows for log data to be stored for as long as you need based on either compliance mandates or network security policy. All of the log data is stored uncompressed and is fully searchable to enable you to easily access your data.

## Search

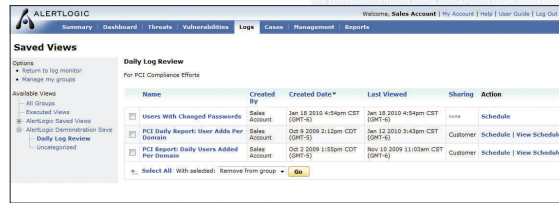
Full text searching allows you to easily search for specific log data from both parsed and unparsed log sources. "One-Click-Filtering" gives you the ability to quickly drill down into log data by selecting parsed messages via hypertext links, which results in automatically creating and applying filters to log data.

## Report

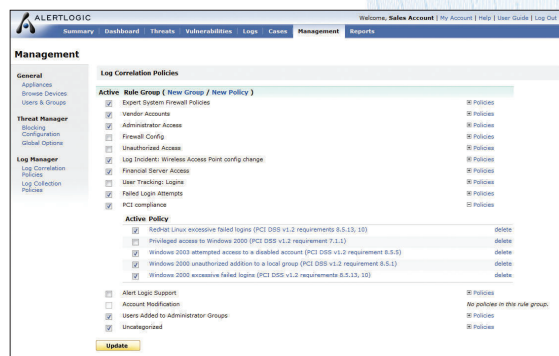
Create a scheduled report from any view and distribute to the necessary staff for review. Custom reports allow you to be in control of the log data you need to review.

## Correlate and Alert

Custom and out-of-the-box correlation rules are designed to identify suspicious activity in your log data and alert you to possible security threats. Correlation rules automatically review message types for specific properties and fields. If a rule is triggered, you will be notified via email.



One-Click-Filtering allows you to drill down into log data



Custom and out-of-the-box correlation rules alert you on suspicious activity



### Virtuous Networking Ltd

4th Floor, Bush House, 72 Prince Street, Bristol, BS1 4QD, United Kingdom  
+44 (0)7500 660649 | info@virtuousnetworking.com | www.virtuousnetworking.com

### Alert Logic, Inc.

1776 Yorktown, 7th Floor, Houston, TX 77056  
877.484.8383 (toll free) | 713.484.8383 (main) | 713.660.7988 (fax) | www.alertlogic.com

Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or service marks of Alert Logic Inc. All other trademarks listed in this document are the property of their respective owners.

© 2010 Alert Logic, Inc. All rights reserved.

