

Log Analytics: Critical for Effective IT Operations



Seema Swamy, Ph.D.

The automated management and analysis of log data is rapidly becoming critical for an effective IT Operations strategy of virtual and cloud infrastructures. Organizations that have deployed Log Analytics solutions rate them as effective for Troubleshooting, Security and Compliance Management. This study uncovers the key drivers, value propositions, and requirements that IT organizations should consider when evaluating Log Analytics solutions.

*cmrinsights.com
408-455-4077
6/1/2013*

Table of Contents

Executive Summary	3
Audience	3
Methodology	4
Participants' Profile	4
Importance of Log Analytics for IT Operations	6
Overall Importance of Log Analytics	6
Reasons for Analyzing Log Data	7
Adoption of Log Analytics Tools	8
Effectiveness of Log Analytics Tools Currently Deployed	9
Requirements for Log Analytics Solution	10
CMR Insights' Perspective	11
About CMR Insights	12
About Seema Swamy	12



This White Paper was commissioned by VMware.

©2013 by CMR Insights, LLC. All Rights Reserved.

This publication may include the opinions of CMR Insights that may be subject to change periodically based on emerging Market Landscape.

Executive Summary

Log Analytics is quickly emerging as a critical component of an effective strategy for the management and operations of highly virtualized and cloud infrastructures. Existing tools are no longer adequate to analyze vast amounts of log data generated by the infrastructures and applications. Log management in a dynamic and complex IT environment has become a significant time sink for IT professionals.

This study underscores the need for a new category of Log Analytics tools designed for virtual and cloud infrastructures to enable better troubleshooting, security, and compliance management. Specialized Log Analytics tools are considered effective but the adoption is still relatively low. The key requirements for IT organizations considering a Log Analytics solution are ease of use, integration with existing virtualization management tools, and a predictable as well as cost effective pricing model. Additionally, IT personnel find it useful to collect, analyze, and correlate log data from all sources including the physical hardware, virtual infrastructure, operating systems, databases, and applications to increase visibility across all layers of the IT environment.

With vCenter Log Insight, VMware is extending its analytics-based IT Operations Management portfolio for virtual and cloud infrastructures to include log data and will potentially become a significant vendor in the Log Analytics market.

Audience

This paper targets individuals with the responsibility of determining or influencing their organizational IT strategies. These include the IT decision makers and IT influencers/professionals that seek information on key value propositions, management strategies, and business benefits. This paper addresses the perceptions and fundamental attributes of Log Analytics solutions in the context of IT Operations of virtual and cloud infrastructures.

Methodology

VMware commissioned CMR Insights to conduct a survey of 125 IT professionals including decision makers, influencers, and users with no influence on the purchase decisions. The main objective of the study was to understand customers' wants and needs as well as their requirements of an effective Log Analytics solution.

The sponsoring vendor was not identified and the survey was a *blind market research* study to garner unbiased responses.

Participants' Profile

The survey was deployed to IT personnel across a range of organization sizes as well as different levels of infrastructure virtualization. The participants were not pre-selected based on their functional responsibilities.

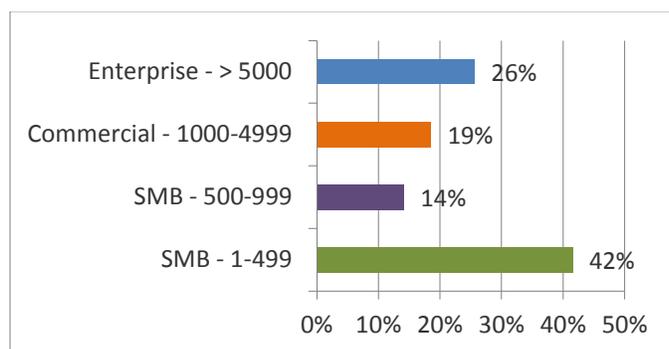


Figure 1: Distribution of Company Size

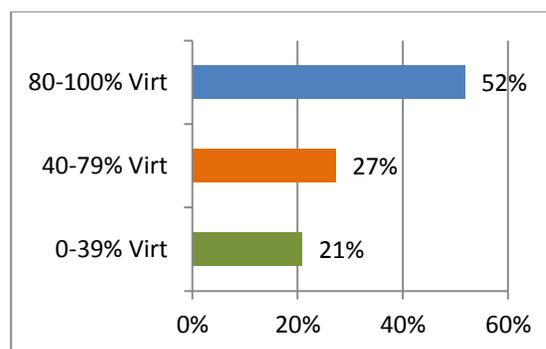


Figure 2: Rate of Virtualized Infrastructure

Over one-quarter of the respondents were from the Enterprise organizations with over 5000 employees. Almost one-fifth of the respondents worked for Commercial organizations with 1000-4999 employees.

Almost 15% of the respondents were from medium-sized SMB organizations (500-999 employees) and more than 40% of the respondents were from smaller-sized SMBs (1-499 employees).

More than half of the respondents' IT infrastructure was virtualized between 80-100%, while about one-fifth of the respondents' IT infrastructure was virtualized up to 39%.

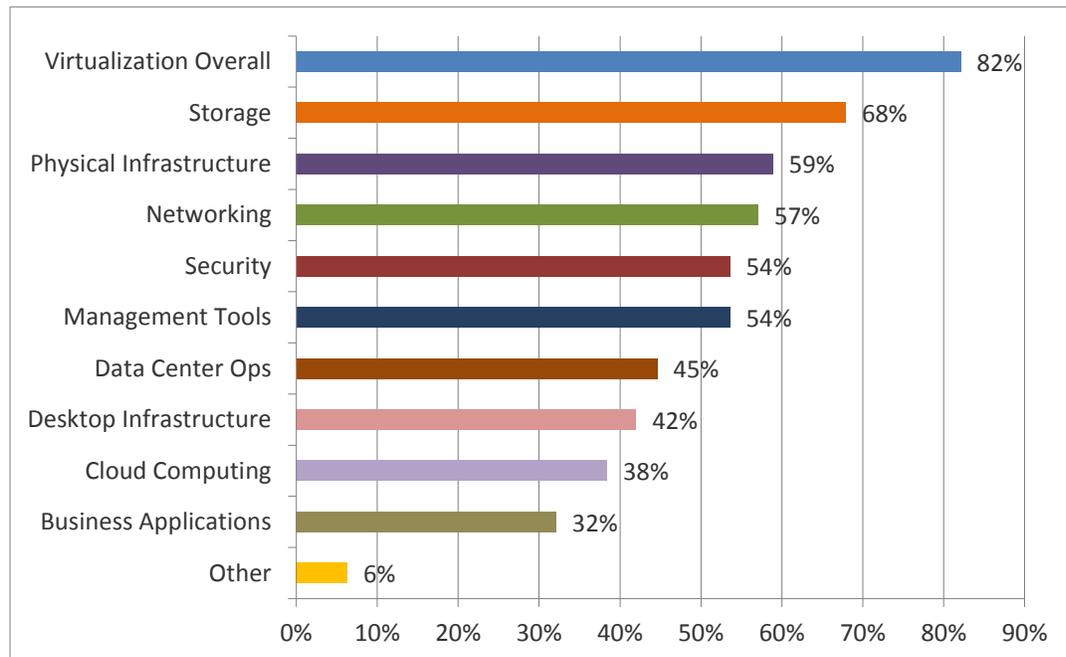


Figure 3: Functional Responsibilities of the Respondents

The functional responsibilities of the respondents ranged from Overall Virtualization to Storage, Physical Infrastructure, Networking, Security, Management Tools, Data Center Operations, Desktop Infrastructure, Cloud Computing, and Business Applications. Less than 40% of the respondents were responsible for Cloud Computing, but over 80% were responsible for the Overall Virtualization.

The functional responsibilities of the respondents tended to correlate with their self-reported knowledge levels in various domains. Over 80% of the respondents reported either expert level or significant knowledge of Overall Virtualization. Over 60% of the respondents reported high levels of knowledge about Storage, Networking, Desktop Infrastructure, and Virtual Management tools.

Importance of Log Analytics for IT Operations

Traditional management tools are geared towards IT professionals that need to monitor datacenter operations. However, these solutions rely on raw performance metrics and typically do not go beyond alerting administrators when performance thresholds are exceeded and do not provide additional insights from log files for troubleshooting and root cause analyses. This has created a blind spot and a need for a new category of tools that provide centralized log collection, analyses, and search capabilities that enable IT professionals to quickly ascertain the causes of problems when performing troubleshooting and other management functions.

Overall Importance of Log Analytics

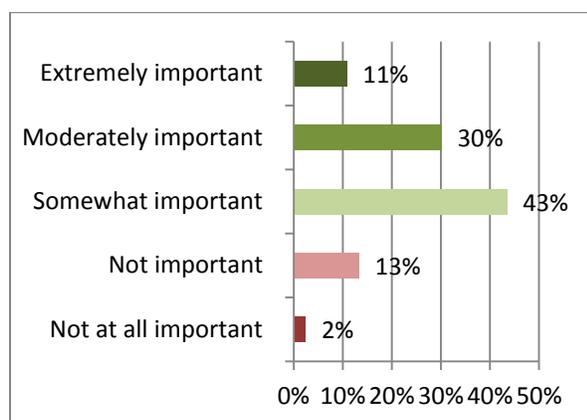


Figure 4: Importance of Log Management Tools to Organizations

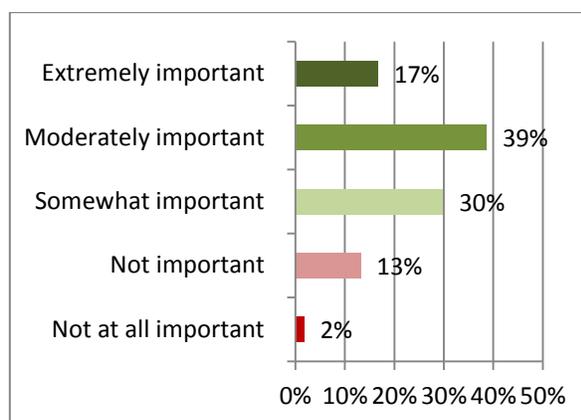


Figure 5: Importance of Log Correlation of Data across Storage, Networking, OS, Apps, etc.

We found that 84% of IT personnel consider Log Analytics tools to be *somewhat*, *moderately*, or *extremely important*. The importance of these tools is projected to increase slightly in the next 12 months with 3% raising their ratings of the importance of these tools from *somewhat important* to *moderately important*.

IT personnel working on troubleshooting issues, often have to evaluate the log files of various servers and applications before being able to provide resolution or chart the next course of action to address the issues. This is a time consuming activity. Not surprisingly, almost one-fifth of the respondents found the functionality of correlating data across the IT infrastructure as being *extremely important* and almost two-fifth of the respondents rated this functionality as being *moderately important*.

Respondents' Quotes:

"The most effective Log Analytics solutions would ideally have the ability to not only collect all data across every device and application, but would be able to put those pieces into groups that reflect the true nature of running a specific application."

"It is important for Log Analytics solution to correlate multiple entries into a single event, particularly in the areas of security and compromise."

Reasons for Analyzing Log Data

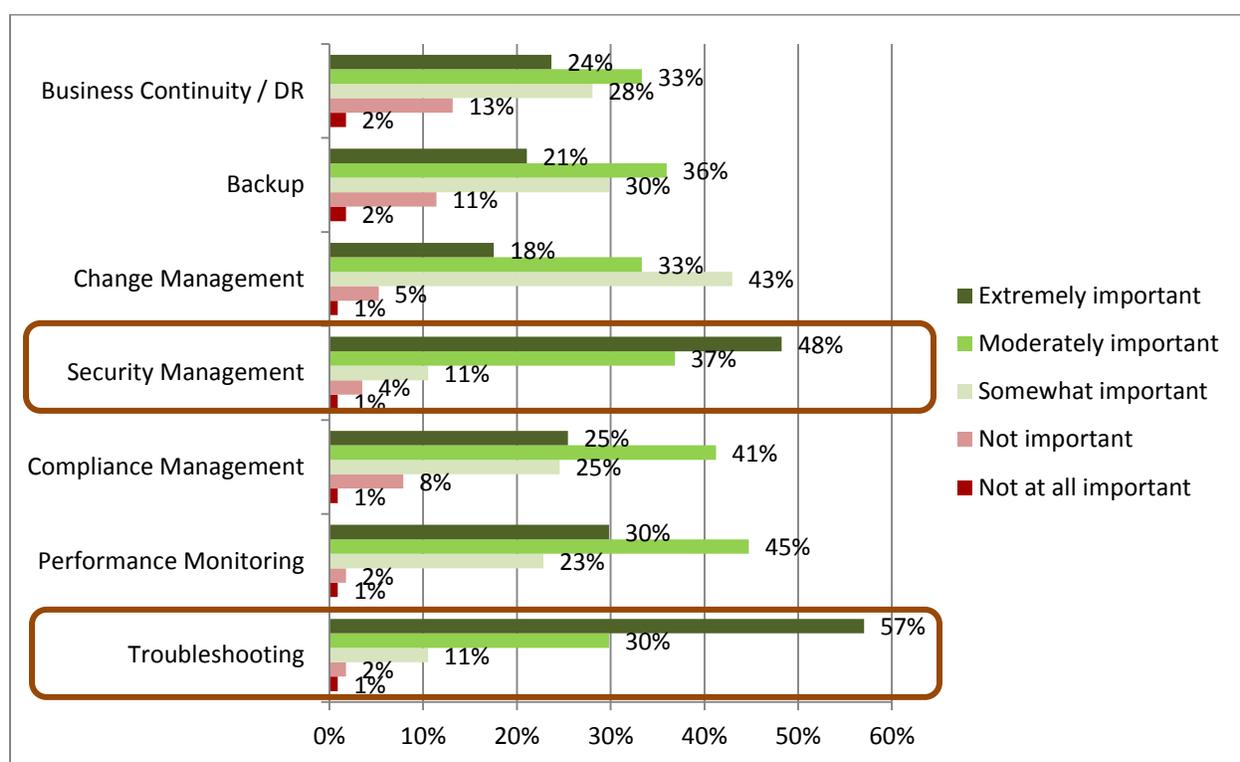


Figure 6: Importance of Log Analytics Tools for IT Management tasks

Almost 90% of those polled rated Troubleshooting and Security Management as the most important reasons for analyzing log files. Over 50% rated Log Analytics tools as *moderately* or *extremely important* for Performance Monitoring, Compliance Management, Backup, Business Continuity, and Change Management.

Adoption of Log Analytics Tools

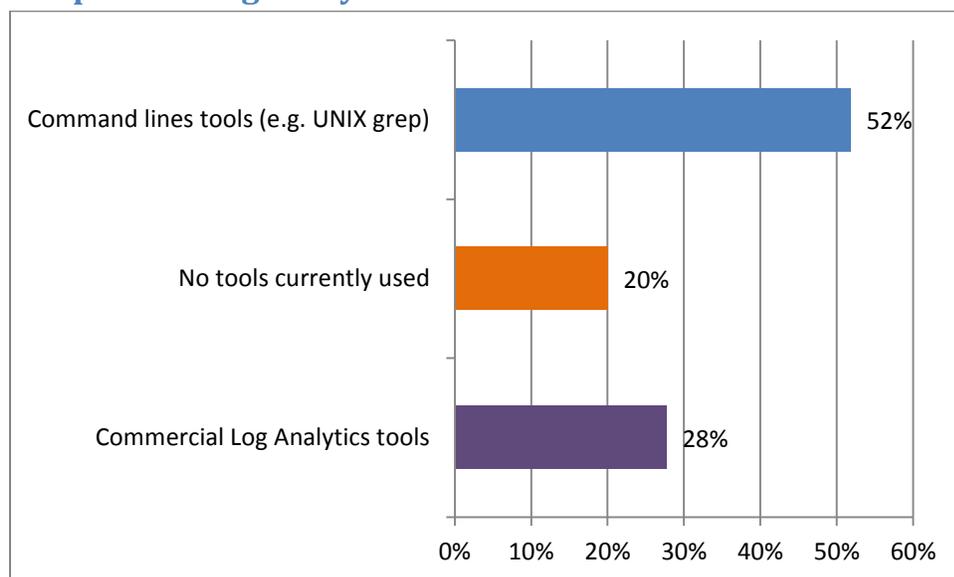


Figure 7: Use of Log Analytics Tools

More than half of the respondents reported using UNIX-style command line tools which were not rated as being *very effective*. About one-fifth reported that they don't use any tools at all. Close to 30% of the respondents reported using a commercial Log Analytics solution such as Splunk, Solarwinds, and ArcSight, among others.

The adoption of commercial tools is still fairly low but Log Analytics is a rapidly growing market, creating an opportunity for VMware and other new vendors to address growing customer demand by providing a comprehensive and differentiated solution.

Effectiveness of Log Analytics Tools Currently Deployed

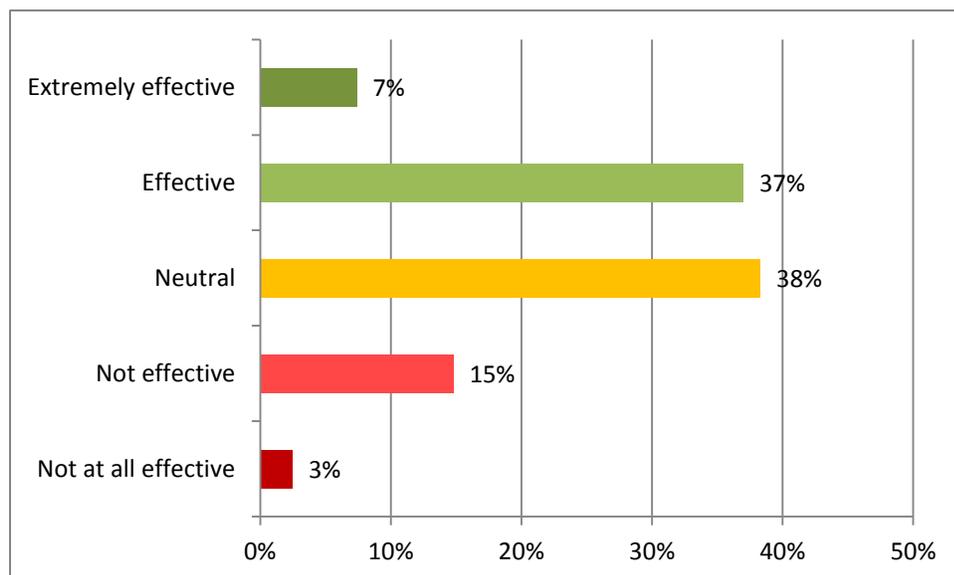


Figure 8: Effectiveness of Log Analytics tools Currently Deployed

About 45% of the polled IT personnel rated their currently deployed Log Analytics tools as being *effective* or *extremely effective*. While more than one-third rated the currently deployed solution as being *effective*, a slightly higher percentage of the IT personnel polled were ambivalent. Clearly, there is scope for a more optimized solution to move the perception gap from an ambivalent *neutral* to *effective* or *extremely effective*.

When the data in *Figure 7* are evaluated in conjunction with the bar graph in *Figure 8*, it is clear that there is scope for improving the ratings of Log Analytics solution by improving the user experience, optimizing license costs, and providing a seamless integration with the existing virtualization and enterprise management tools.

Requirements for Log Analytics Solution

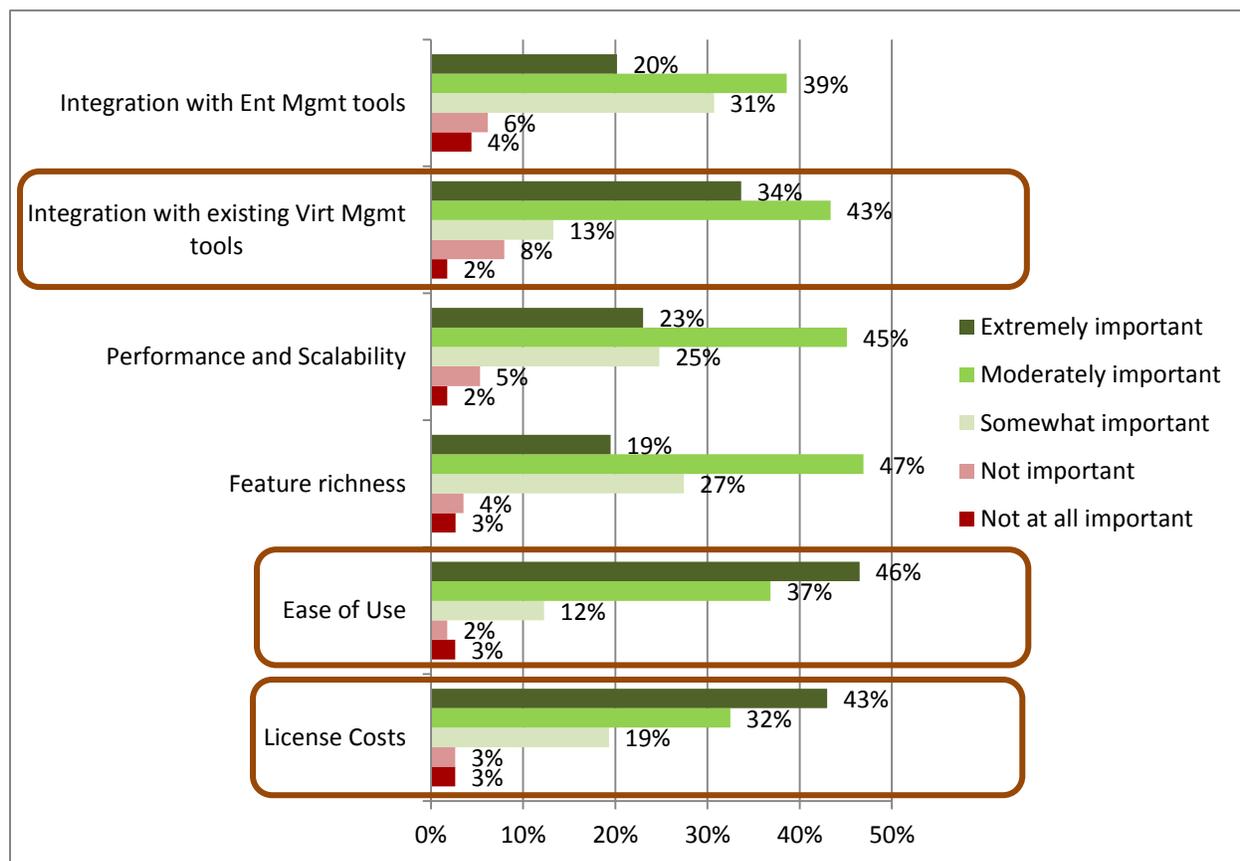


Figure 9: Requirements for Log Analytics Tools

Over 80% of the IT personnel surveyed rated *Ease of Use* as the most important attribute of Log Management tools. The *License Cost* of the Log Analytics solution was the second-most important attribute with over 40% rating it as *extremely important* and about one-third rating it as being *moderately important*. *Integration* of Log Analytics solution with existing virtualization management tools was highly valued with over one-third rating it as *extremely important* and over 40% rating it as *moderately important*.

Respondent's Quote:

"An effective solution should not require a team of dedicated resources to understand and use."

CMR Insights' Perspective

Log Analytics is an emerging but critical component of an effective strategy for managing virtualized and cloud infrastructures and operations. Applications, Operating Systems, Storage, and Network devices generate enormous amounts of log data that IT professionals need to analyze on a regular basis for Troubleshooting, Security, and Compliance Management. Today, most organizations that responded to this survey use traditional command line tools or no tools at all and the adoption of specialized Log Analytics solutions is still relatively low. However, IT organizations that have deployed such solutions rate them as *effective*.

With the introduction of vCenter Log Insight, VMware is poised to become a leader in Log Analytics. VMware's offering meets the key requirements for Log Analytics tools uncovered in this survey, offering a tightly integrated solution with vCenter Operations that is easy to use. In addition, its pricing model is based on the size of the environment, not the amount of log data analyzed which should help keep the costs predictable and affordable. Enterprise, Commercial, and SMB organizations should consider VMware when selecting an IT Operations solution for their virtualized and cloud infrastructure.

About CMR Insights

CMR Insights helps large and mid-sized organizations serve their customers better by providing actionable research insights and analyses. CMR Insights is focused on employing research expertise to evaluate the market landscape, assess the competitive environment, measure customer experience, and provide insights aimed at generating a delightful holistic user experience. CMR Insights' research is customized to the needs of the clients and informs marketing and business strategy.

About Seema Swamy, Ph.D.

Seema Swamy is a Principal Research Consultant at CMR Insights. She has over 10 years of industry experience having worked in several enterprise and end-customer based research throughout her career including VMware, eBay, and PeopleSoft.

She has a Ph.D. from Stanford University where her doctoral research examined the cross-cultural effects of collaborative workspaces. Seema Swamy has published several papers including *Cloud Computing Adoption within Organizations* and has participated in panel discussions at various professional conferences.



seemaswamy@cmrinsights.com

408-455-4077

©2013 by CMR Insights, LLC. All Rights Reserved.