EMA Radar™ for Enterprise Network Availability Monitoring System (ENAMS): Q3 2014

Report Summary & Infosim Profile

By Tracy Corbo and Jim Frey
ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Radar Report

July 2014

EMA Radar™ for Enterprise Network Availability Monitoring System (ENAMS): Q3 2014 – Report Summary

Table of Contents

EMA Radar™ for Enterprise Network Availability Monitoring System (ENAMS): Q3 2014 – Report Summary

Executive Summary

The practice of network availability monitoring can range from simple standalone up/down monitoring of individual devices to complex, highly customized and automated approaches that fully integrate into broader management systems architectures. ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts define the term "Enterprise Network Availability Monitoring System" (ENAMS) to include network-centric monitoring solutions that are used by enterprise network operations and engineering teams to discover, monitor, assess, troubleshoot, and manage medium to large enterprise network infrastructures. For this EMA Radar™ Report, specific focus has been placed on two areas: the core capabilities and features that address network operators' needs to ensure health and availability of the network; and the overall practitioner experience in procuring, deploying, administering, and using specific ENAMS products. In all, 17 products from 16 vendor suppliers are reviewed and compared in this study.

Enterprise Network Availability Monitoring

The purpose of this EMA Radar was to review and compare solutions that have been specifically designed for, and credibly deployed in, medium and large enterprise settings. Consequently, all ENAMS solutions were required to meet the following minimal criteria in order to be included in this report:

- Precious few enterprise networks are comprised solely of equipment from a single network equipment manufacturer (aka "mono-vendor"). Consequently, ENAMS solutions were required to support management of components and elements from multiple network equipment manufacturers.
- The products covered must be available for direct purchase by enterprise network management and operations teams and not purely designed to be used by Management Services Providers (MSPs) in order to deliver network management services.
- ENAMS solutions must manage large, fast-growing networks. To be considered, products must have been verifiably deployed and be successfully managing a network of at least 500 devices, not including systems and endpoints.

ENAMS products typically fall into one of two groups: those that are designed first and foremost for the scale and needs of small-medium enterprises, and those that are built for large or very large enterprises. This is not to say that products cannot span both groups, but typically a product tends to have a sweet spot on one side or the other. Truly large enterprise products can easily scale to support tens of thousands of network devices, but they tend to be less cost effective in smaller deployment environments. Those products initially designed for smaller environments tend to be much more cost competitive, but they will often struggle to scale gracefully to deliver management of very large networks.

A few quick words may be helpful here to clarify what EMA was *not* looking for, or rather what EMA specifically excluded from consideration for this particular study. First, many of the solutions EMA reviewed have also been deployed by communications service providers for monitoring revenue-generating network infrastructures; however, those examples (and the specific/unique requirements that come with them) were not part of this study. Further, while many multi-function/cross-domain products offer some aspects of network monitoring, EMA chose to focus primarily on those solutions that were intended to manage networks as a primary set of features and functionality rather than those that "also manage your network" in addition to managing, most typically, servers. Finally, tools that have

been designed to work with a single network equipment vendor's gear (a.k.a. element managers) have not been included, despite the fact that some of those solutions can be fairly broad and sophisticated.

In the development of this EMA Radar, EMA engaged 16 providers of ENAMS solutions in a detailed analysis of the scope and capabilities of their offerings. Across that group, we reviewed 17 ENAMS products. The solution providers represent a mix of vendors, ranging from small, privately held, pure-play vendors to very large public systems and software technology corporations.

The 17 ENAMS vendors/solutions covered in this study are:

- AccelOps/AccelOps 4
- AdRem/NetCrunch
- CA/CA Spectrum
- Centerity Systems/Centerity Monitor
- EMC/EMC Smarts
- Entuity/Entuity Network Management v14
- GroundWork/GroundWork Monitor Enterprise
- HelpSystems/InterMapper 5.7
- HP Software/HP Network Node Manager (NNMi)
- HP Networking/HP Intelligent Management Center (IMC)
- IBM/IBM Netcool Network Management
- Infosim/StableNet Enterprise
- Ipswitch/WhatsUp Gold
- Kratos Networks/NeuralStar
- ManageEngine/OpManager
- ScienceLogic/EM7
- SolarWinds/Network Performance Manager (NPM)

While there are other suppliers of such products, it is EMA's belief that this represents a significant majority of those that are actively and viably addressing the network infrastructure availability monitoring needs of medium and large enterprises today.

For this particular study, EMA made some additional changes to its approach. While EMA Radar reports always include direct product user/customer interviews to validate vendor claims and to gauge actual value and experiences, historically we have used those inputs only as a sanity check. Instead, this study has included direct scoring variables based solely on responses from the more than 40 real users of the ENAMS products reviewed here. It is our hope and belief that this modification improves and enriches the reality-based nature of our analysis and results.

The Role of Network Monitoring in the Enterprise

Despite the considerable maturity of the ENAMS market, these solutions continue to play a vital role in today's large enterprises, and not solely in older/mature IT shops. The long history and legacy of these products means that some large enterprise shops have heavily invested in and customized them, often to the point that removing them (and sometimes even upgrading them to the latest release) requires a major overhaul of the Network Operations Center (NOC) itself. At the same time, there are ENAMS products that are a good fit for younger organizations that have grown and matured to the point where the initial low-end (often open source or freeware) solutions they had been using exceed scale limitations and are too difficult to maintain. While ENAMS tools from the large IT vendors, such as CA, EMC, HP, and IBM, have venerable history supporting large enterprise NOC and datacenter operations, other vendors are finding opportunities to grow with the networks of smaller and mid-sized organizations and address the needs of network engineering/management/operations teams looking for more out-of-the-box alternatives.

Many factors, including the ongoing growth of server virtualization (and associated virtual networking), WiFi in the access layer, voice and video convergence over IP, endpoint mobility, and the Internet of Everything, are aligning to make networks ever more critical. Not only do networks need to expand to support all of the traffic, but they need to be rock solid (continuously available) and high performing. As the ENAMS solutions market continues to mature, new competitors continue to enter the sector, commonly focusing on faster deployment, ease of use, cross-domain functionality, new delivery models, and ever-lower price points. This has resulted in regular occurrences of co-deployment. EMA often encounters shops that are using more than one ENAMS product—often using one product in the NOC and another (or even more than one other) for regional or workgroup-specific purposes.

It is also worth noting here the relative role of ENAMS solutions. While this study looks primarily at availability monitoring of enterprise networks, such capabilities are often closely (and sometimes inextricably) integrated with other network and non-network management functionalities. For instance, it is common to have some degree of performance monitoring baked into an availability monitoring solution, and indeed this EMA study looks for such capabilities. A growing number of solutions also tie in configuration management and asset management features, expanding the total value of the solution. Others include the capability of monitoring non-networking equipment (most commonly network-attached servers, printers, or other endpoints) within the same system, allowing a more systemic approach to availability and performance monitoring. Finally, while some ENAMS products are most commonly deployed as standalone, many more—particularly those at the higher end of the market—are directly integrated with other management systems, such as event management, service management, help desk/trouble ticketing, and CMDB/CMS products.

The ENAMS Market and the Players

The ENAMS market is a mature but active global market. The majority of the vendors that are leading the market in terms of market share and existing installation are based in the U.S.; however, a growing number of active suppliers hail from other locations. ENAMS solutions constitute a very established sector with some products having been on the market for over twenty years. Even among the newer entrants, most have been in the market for at least six or seven years. Consequently, many of these solutions are in third or fourth, or even greater, generations and have survived because of clear and

continuous value delivered to enterprise network operations teams. But being mature does not mean that there are not ongoing new requirements, demands, and challenges. There is a relentless drumbeat of technological innovations that must be embraced, both in terms of managed elements and in terms of the techniques used to develop the ENAMS solutions themselves. For instance, the server virtualization tsunami has transformed datacenter architectures and brought new demands for managing mixed physical/virtual infrastructures. Growing adoption of cloud services has brought an increased sensitivity regarding network reliability, visibility, and efficiency for reaching externally-hosted systems, workloads, and storage. And evolving software development practices have moved UI/consoles from thick client to lightweight/Web-based and now mobile devices. Some solutions are even moving toward hybrid delivery models, with SaaS options and subscription licensing.

In the prior version of this study, *EMA Radar for Enterprise Network Management Systems (ENMS): Q4 2012*, EMA chose to segment solutions into two categories: solutions for large enterprise environments (requiring confirmed deployment managing 25,000 or more elements) and solutions for medium enterprise environments (requiring confirmed deployment managing at least 500 elements). While such segmentation was advantageous in some ways, allowing most-likely peers to be compared and relative scales to be tuned to each segment, it was a disadvantage in other ways. As most of the vendors covered here have tried to address both the large and medium enterprise segments, we were not providing comparisons that practitioners could use when making the transition themselves. Further, many solutions that have historical strength in small managed-environment deployments have been designed to support larger-scale deployments, and should rightly be compared to the high-end traditional players. Consequently, EMA chose to include all solutions in a single analysis for this study refresh. We still have a wide range of typical deployment centricities, with some products that are typically deployed in very large settings and others that are usually deployed in small-medium enterprises, but we can now review direct comparisons between the solutions on a true apples-to-apples basis, using the same scoring and rating scales for all solutions.

Most of the relatively new players have come into the ENAMS market by introducing solutions for small-medium enterprise—a sector that has been historically underserved by the bigger IT vendors. At the very lowest end of the network management tools market, small businesses and small enterprises have a plethora of open source and freeware/shareware point choices that can meet their needs, or they can turn to management services providers for network management. But medium-sized enterprises need something different, tending to favor tightly integrated or unified solutions that are on a single platform and are therefore easier to deploy and manage. While mid-market ENAMS solutions might lack the depth of features and ultra-high scalability of the largest platforms, they provide a good, solid solution for managing a wide range of devices. In a growing number of cases, including several based on EMA reference calls for this study, the buying decision for mid-market ENAMS solutions was made by an operations person in the datacenter rather than the NOC, largely because the traditional NOC is often small or doesn't even exist in a mid-market enterprise.

Focus of This Research

This EMA Radar report is intended to assemble a clear picture of the current range of ENAMS products in the marketplace, including how they differ in terms of product approach, core strengths, and weaknesses; the total cost of ownership and operations; and the relative strength/size of supplier vendors. The output is intended to guide IT practitioners engaged in research on this topic to identify a short list of solutions for their needs. In each of the key areas, we evaluated vendors and their respective ENAMS product and service offerings on a broad range of weighted factors and used the results to rate each relative to the others in the study. The report generated individual ratings charts (such as the one seen in Figure 1) for each solution as well as a final EMA Radar map showing how all of the vendor solutions scored relative to one another.

Criteria

In all EMA Radar reports, EMA evaluates solutions based on five key areas: *deployment and administration, architecture and integration, functionality, cost advantage,* and *vendor strength*. Figure 1 shows the ideal graphic for a perfect score, as well as the average scores resulting from this research. Each vendor has been evaluated by using the factors listed below to determine how close to an ideal score each ENAMS solution received. For a complete discussion of the EMA Radar Report process, please see Appendix A.

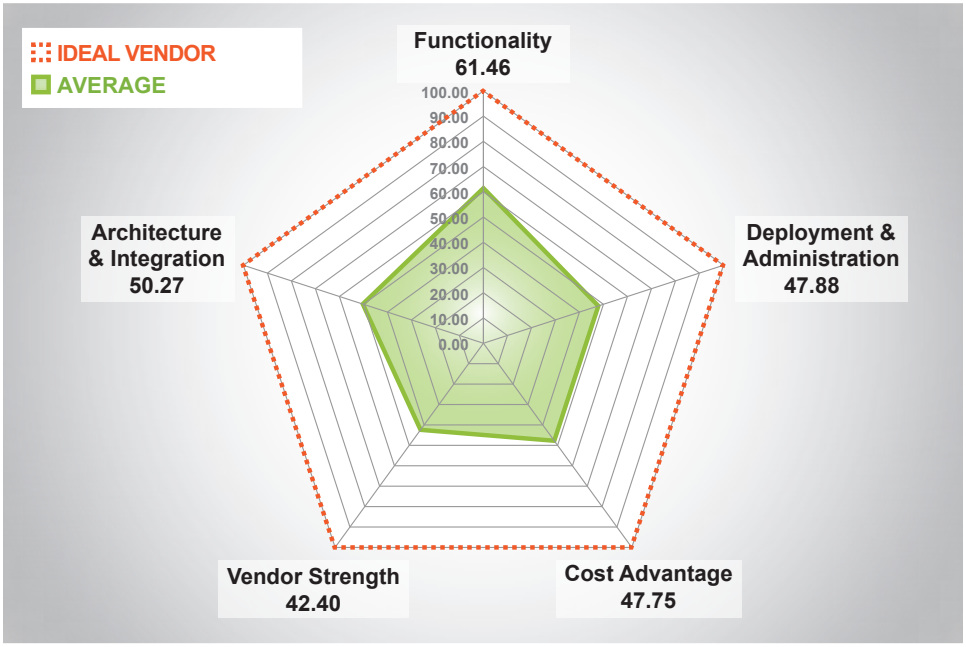


Figure 1. Ideal vendor-solution Radar chart with average scores

Deployment and Administration

Licensing Model and Manageability – These measures reviewed the range and type of licensing models for each ENAMS solution, as well as their complexity and the ongoing operational costs for associated maintenance and support charges. Models that were simple and easy to understand and allowed graceful scaling were rewarded in contrast to those that were complex or hard to sustain over time.

Deployment – This portion of the study examined how difficult it was to deploy a given ENAMS by factoring in items such as the configuration recommendations for a single instance of the product and whether or not separate installations are required for the database component or polling engines. Ratings reflected EMA's findings that for those ENAMS users seeking the greatest simplicity, an "all-in-one-box" solution may be the best fit, whereas a more component-oriented approach might make sense for very large deployments that will require maximum scalability and flexibility.

Ease of Use/Administration – The easier it is to maintain and manage an ENAMS once it is up and running, the "stickier" the solution becomes, fostering positive operator experience as well as improving the likelihood that the solution will be fully utilized. This part of the study looked at how cross-team–friendly each product is, whether it requires some degree of training to gain proficiency, and how easy it is to keep the product in sync with product releases.

Support and Services – The sophistication and completeness of maintenance support and services play an important role in overall ENAMS deployment success and operator satisfaction. This portion of the analysis considered the range and types of service and support programs offered in conjunction with each ENAMS solution, as well as the degree of non-vendor community support.

Cost Advantage

One of the most significant challenges for those seeking to procure an ENAMS solution lies in trying to untangle the various pricing models used by the vendors. There are no standard pricing methodologies, and some vendors' models are flatter and easier to understand than others. Some are so complex that it requires a Ph.D. just to understand the language, and EMA has documented cases where networking pros said they could not find a single salesperson who could provide a clear explanation. Making things even more complex, each vendor has a different discounting model. EMA attempted to level the playing field as much as possible by looking at the list price and using a perpetual licensing model. While EMA tried to make comparisons as fair as possible, it's important to understand that our comparative analysis provides only a rough guideline, and that actual end licensing costs can vary widely based on size of deal and sales channel. One of the more important lessons we learned was that it is imperative from a best practices standpoint for ENAMS users to focus on how any given licensing model will change/grow as their network grows.

For this study, ENAMS vendors were asked to consider two deployment scenarios—one for small-medium enterprise (SME) and one for large enterprise—and to provide product and support pricing for one year and for three years. The SME model assumed 500 network switches, each configured with 24 fully/continuously monitored ports, polled every 10 minutes. The large deployment environment assumed 5000 network switches, each with a configuration of 48 continuously monitored ports, polled every 10 minutes. Scoring was based on relative cost of licensing as well as how pricing scaled from one to three years.

Architecture and Integration

Platform Design – This portion of the analysis examined a number of factors that make up the underlying design of an ENAMS solution, including which capabilities and feature sets were part of the core product versus which were separate add-ons. Also considered were the scope and range of data collection techniques, availability for consumption as SaaS, support for high/continuous availability, and extensibility to support new/emerging technologies such as Software Defined Networking (SDN).

Scalability – Enterprise deployments can grow very large, sometimes in relatively short order, making it critical that solutions are capable of supporting expansion. This part of the study looked at just how large of a managed environment each ENAMS could truly support, with practice valued over theory. Customer references were sought to support deployment-size claims, and additional credit was given to vendors who supplied references that validated high-end scalability.

Integration/Interoperability – The growing demand for collaboration between IT departments is making integration an important component of ENAMS solutions. This section considered vendor-certified integrations between ENAMS and related IT management systems and disciplines, including event management, service desk, cloud/orchestration, and CMDB/CMS.

Functionality

Discovery – One of the most critical aspects of any ENAMS system is its ability to discover elements to be brought under management. This part of the study looked at the different methods of discovery available within an ENAMS, the types of elements that could be discovered on both network and non-networking sides, and the types of information that could be captured from those devices.

Alarm/Reporting – The primary outputs of most ENAMS products are alarms (for operational monitoring) and reports. Too many alarms create alarm fatigue, which makes it possible to miss critical events when they do occur. This element of the study examined each solution's ability to provide adequate alarm management, suppression, and customization, and also reviewed the scope and flexibility of the overall reporting features.

Fault Isolation/Troubleshooting – When failures do occur, the top priority is a fast response and an absolute minimum MTTR. This part of the study examined how each ENAMS solution delivers and facilitates isolation and root-cause analysis. Once a problem is isolated, the next step is to zero-in and understand the true underlying source of the issue so that mitigations can be applied. There are a number of methods for handling troubleshooting with an ENAMS, and this section looked at the breadth and depth of options available.

Inventory/Asset Management – In many cases, it can be useful to leverage the discovery and tracking capabilities of an ENAMS product as an inventory repository or as a primary or secondary asset management system. This section evaluated the degree to which each ENAMS solution offered features and functionality of this type.

Cloud – We are still in the early days for cloud in the enterprise, and while practitioner conversations continue to reveal only limited direct demand, EMA believes it is important that ENAMS solutions support cloud deployments so as not to impede this fast-growing functional area. This part of the study examined functional capabilities within ENAMS solutions to address integrated management of hybrid cloud environments.

Vendor Strength

When considering an ENAMS product, it is always important to understand the strength and viability of the vendor standing behind the product. EMA's analysis of vendor strength included the following:

Financial Strength – Vendors that are public companies provide a greater degree of financial transparency while the financial position of private vendors is more difficult to determine. Vendors of either type may be strong or weak. EMA examined the stability of each ENAMS vendor by considering longevity, profitability, growth of ENAMS-specific revenue, and other related factors.

Technology Partners – EMA believes that strong technology partnerships are critical, especially for smaller players who do not have the global and financial footprint of larger IT vendors. EMA rates these partnerships in terms of their relevance to supporting the network monitoring aspects of each vendor's product offerings.

Customer Satisfaction – EMA asked customers of each ENAMS vendor for direct feedback across a number of factors, such as quality of technical support, documentation, ability to contribute new features to future products, etc. We compiled these to develop a customer satisfaction component to the vendor strength measure.

General Findings

In the course of this study, EMA analysis and dialogues uncovered a number of noteworthy trends:

- **Discovery has its ups and downs.** While autodiscovery is considered a powerful capability, we found mixed use in practice. Some practitioners continue to rely on manual discovery/population methods. The primary concern with automated approaches is that they have the potential to add new management elements and "junk" into the system that must subsequently be deleted or otherwise dealt with. This may indeed be a case of discovery tools not behaving as preferred/expected, or it may be a case of the tools working well and revealing the unclean nature of the true managed environment. Regardless, EMA considers some aspect of automated discovery to be essential when moving into the realm of highly virtualized/programmable infrastructures so that device deployments or configuration changes can automatically trigger an update to availability monitoring.
- **Alarm management has many layers.** Network alarms are often forwarded up into higher-level event management platforms, but network managers really want to have a direct view into and control over how many alarms/alerts are active at any time as well. And while suppression, correlation, and root-cause analysis are considered beneficial, one of the more common and basic needs is simply to be able to easily ensure that the ENAMS will alarm on the things you want alarmed. In other words, is it easy to configure and create specific new alarms, or does it require digging deeply and creating custom scripts?
- **Customization can be good, bad, or just plain ugly.** The story is pretty much the same for all the vendors we analyzed. If you embark upon significant customizations (meaning coding, not just configurations) you are left holding the bag to make sure they continue to work. Upgrades can break custom code, and consequently, the more customization you find necessary, the harder it will be to deploy patches and upgrades. For this very reason, some ENAMS vendors strongly recommend that users do NOT customize their product deployments but instead stick within

the existing scope of configurability and work with the vendor to extend capabilities via product enhancements. EMA recognizes that specific management objectives and managed environment characteristics often require customizations—particularly for connecting an ENAMS with third-party management systems as part of an integrated management architecture. Consequently, EMA recommends that ENAMS administrators plan to treat such customizations as coding projects—subject to the same lifecycle dev-test/DevOps procedures as any development project.

- **Clouds are still largely on the horizon.** During the course of this study, EMA talked with more than 40 ENAMS product users and did not find a single case where the product was being used to monitor external cloud resources. Does this mean external cloud services are not being used? In many shops it did mean just that, but in others it simply meant that the networking teams had no access to or ability to monitor external cloud services. EMA research outside of this study conclusively shows that operating teams are converging, bringing together network, server, storage, application, and security monitoring needs in support of hybrid environments, but at least for the moment, ENAMS systems are not directly in the mix for cloud.
- **Just say yes to training.** EMA's initial assumption was that if a product required training or customers purchased training for a product, it was because the product was difficult to use. However, we found that across the board, regardless of which vendor's customers we spoke with, practitioners always seek to obtain training from the vendor as a simple matter of best practices—especially when it comes to using advanced feature sets. Virtually every ENAMS user and administrator we interviewed agreed on the value of training, noting that the training ensured that they got the best possible performance from the tool and that they would recommend training regardless of the product they were using. Furthermore, it's important to make sure the training selected matches the needs and skill sets of the population of ENAMS users; cross-domain operations teams will have different needs than level 3 network support engineers.
- **Reporting is a must-have for only a few.** While almost all of the practitioners we interviewed were aware of reporting features within their ENAMS, few used them on a regular basis. For the most part, folks preferred to export data from their ENAMS to external reporting tools.

EMA Radar Map for ENAMS

The ENAMS Radar map shown in Figure 2 demonstrates how the 17 ENAMS solutions reviewed in this study rank in relation to one another in terms of *resource efficiency* (*x* axis) and *solution impact* (*y* axis). The size of the bubble indicates relative measures of *vendor strength*.

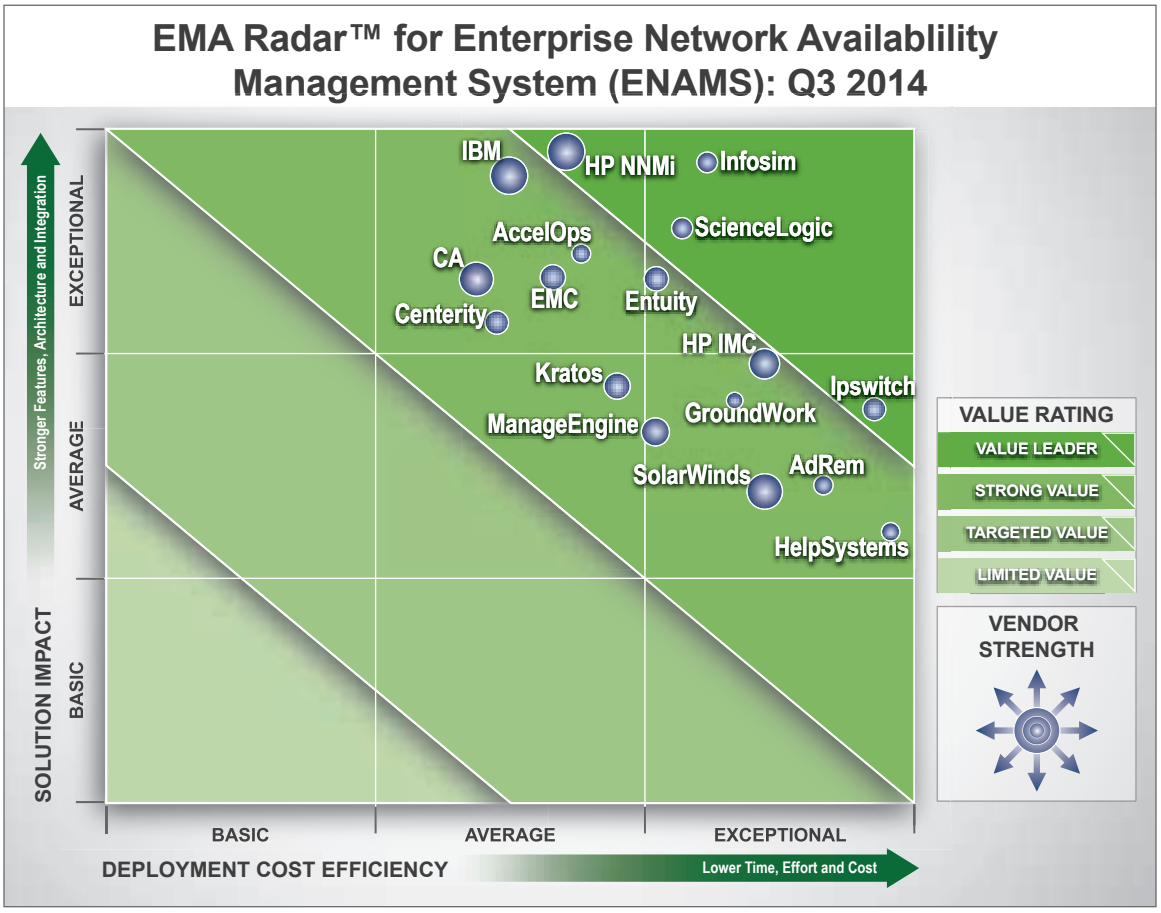


Figure 2. EMA Radar Map for ENAMS: Q3 2014

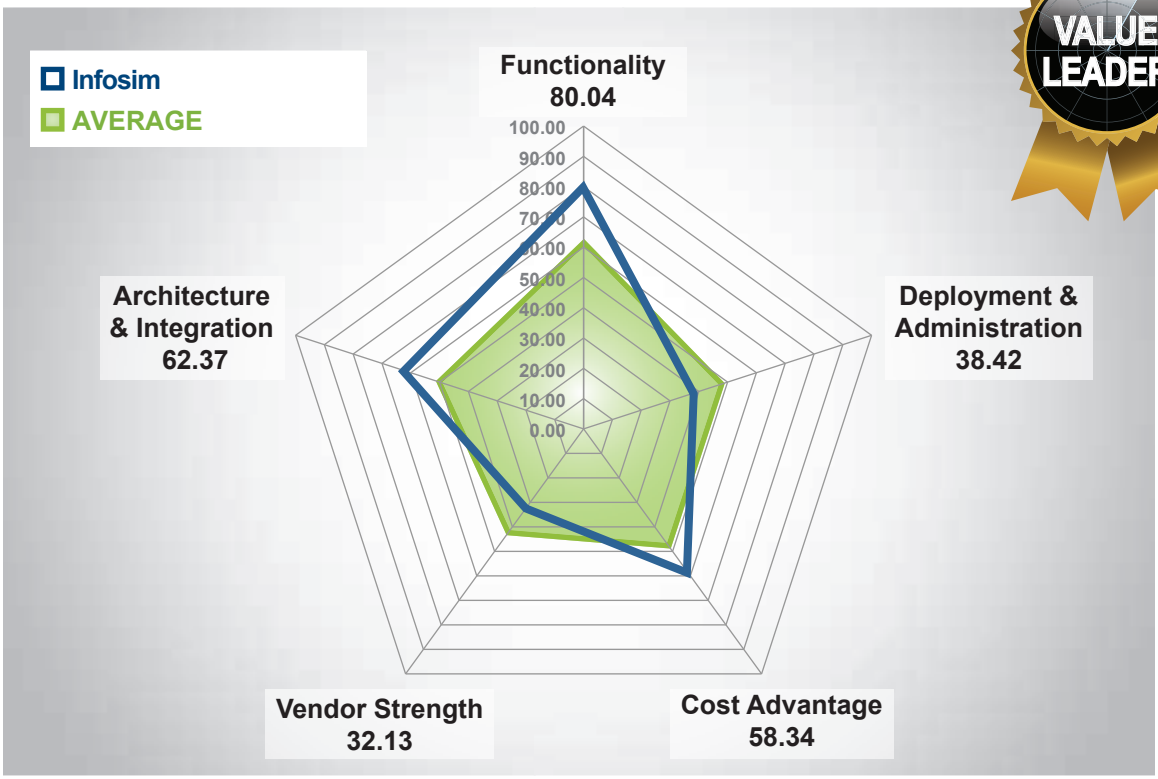
Distribution of Results

As would be expected within a mature and competitive market, results of this analysis reveal a large number of highly functional solutions that deliver substantial value. In fact, almost all solutions achieved "exceptional" status on one axis or the other, and a few—Infosim, ScienceLogic, and Entuity—achieved exceptional status on both. The general distribution reflects a very good range of choices that tend to offer trade-offs between greater functionality and greater resource efficiency.

As noted earlier, this chart merges two categories—products designed for small-medium enterprises and products designed for large enterprises—that were presented separately in the previous version of this study. In this chart, solutions that are not designed or intended to scale to the high end are presented alongside those that will probably never be deployed within a medium- or small-sized shop. However, as all solutions reviewed here are being scored/rated on exactly the same scale, relative differences should hold regardless.

Infosim

StableNet Enterprise 6.7



Introduction

Infosim, a company that operates globally, is based in Germany with regional headquarters in Singapore and Austin, Texas. Infosim produces StableNet, a multi-function ENAMS product based around advanced network availability management. The core technology of StableNet has been architected to support both large enterprise and service provider environments. (Infosim offers a Telco edition separately.) This allowed StableNet to earn very high scores on EMA's architectural measures while also achieving the highest score in our study in terms of total breadth of features. With an above-average rating for resource efficiency as well, this solution finished as the most definitive *Value Leader*. EMA reviewed StableNet Enterprise version 6.7 for this study.

Deployment and Administration

Infosim StableNet received above-average scores in our assessment of overall resource efficiency. Rather than employing the more common device-based licensing model, StableNet uses a licensing model that is based on measurements per device. More complex devices require more measurements, so while this model allows for greater flexibility, it also requires customers to pick and choose up front what they want to pay to monitor. The StableNet database and polling engines are embedded, but customers have the option of using their own database or installing polling engines on a separate server if they choose. From a deployment standpoint, Infosim had one of the best scores for supporting a large

number of network devices with a single server, simplifying the deployment and ongoing management of the product, especially in large deployments. Conversations with practitioners confirmed that while StableNet leans most heavily toward network monitoring usage, customers often use the tool for monitoring non-networking equipment, such as servers, as well.

Cost Advantage

Infosim StableNet finished in the top four overall in EMA's assessment of cost advantage. While scoring above average in the medium deployment scenario, the solution's clear edge is in larger deployment environments where its licensing model provides a measurable cost advantage over primary competitors.

Architecture and Integration

Infosim StableNet scored extremely well in overall architecture and integration. With the third-highest overall rank in our measures of architecture, StableNet includes a broad set of capabilities as part of the core product. The product has better-than-average data collection methods and is one of the most SaaS-ready ENAMS solutions. Infosim provided a number of large network monitoring deployments that fully demonstrated the ability of the product to scale up.

The solution also scored very high on our assessment of integrations, ranking second overall. StableNet provides integrations for multiple third-party systems in each of EMA's categories: event management platforms, service desk solutions, cloud and virtual systems orchestration, and CMDB/CMS platforms.

Functionality

Infosim StableNet led the entire ENAMS field in scoring for features/functionality. Key strengths were found in the areas of discovery features, range of non-networking devices that can be discovered/managed, and alarm management/correlation. Reports are highly customizable, though EMA's checks with StableNet users did not find this feature to be heavily utilized. The solution is one of the few ENAMS reviewed that provides a full set of inventory/asset management capabilities, including the ability to create asset tags and generate asset reports. StableNet can be run on the VMware hypervisor for cloud deployments, and the product is one of only four that are actively being used to monitor cloud-based resources above/beyond traditional network infrastructures.

Vendor Strength

Infosim is a privately held firm, so its exact financial position is unknown; however, the company does claim profitability over the last five fiscal years with continuous growth in both the company and its ENAMS product revenues for at least twice that long. The company has a few solid technology partners, including Cisco, Oracle, Ixia, and VMware, though its list is still a bit shorter than other ENAMS.

Strengths and Limitations

Infosim's ENAMS strengths are:

- **Feature/function scope** – The StableNet solution achieved EMA's highest score for ENAMS features and functions. Both basic and advanced capabilities were included, as well as support for emerging requirements, such as managing hybrid cloud environments.
- **Scalability** – Infosim provided valid large deployment use cases to support its network device monitoring scaling claims. Importantly, the solution scales not only from a management capabilities perspective, but also from a licensing/cost perspective. In EMA's assessment, Infosim scaled more gracefully than most other ENAMS in terms of licensing costs.

Infosim's ENAMS limitations are:

- **Emerging U.S. market presence** – While Infosim clearly offers a very capable solution that should compete favorably with the best ENAMS, the company itself is not yet well known in the U.S. Mitigating this the fact that the company is both stable and growing and the quality of local account and technical support raised no concerns within our findings.
- **Thin stable of technology partners** – Infosim has yet to build out a technology alliances portfolio that compares favorably with other ENAMS vendors. More network equipment vendors should be added, and perhaps some popular security or network optimization vendors as well.

Appendix A: EMA Radar Report Methodology

EMA has produced a report specially targeted at presenting and explaining EMA Radar Reports in general: *How to Use the EMA Radar Report*, EMA, April 2010. The goal is to use a combined approach for quantitatively and qualitatively evaluating providers of solutions in a particular IT management functional area and presenting their relative differences in a clear, graphical format. Also included is a detailed discussion of individual criteria and how each participating solution provider rated versus those criteria.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2932-Infosim_SUMMARY.080414