

Choosing the Right Enterprise Network Management Solution

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for SolarWinds

November 2009



IT MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS AND CONSULTING

Table of Contents

Executive Summary	1
Introduction	1
Challenges	1
Solution Providers	2
Large System IT Vendors	2
ISV	3
Open Source	4
Appliance	5
EMA Perspective.....	6
About SolarWinds	7

Executive Summary

Enterprise networks are growing in complexity and size with globalization, outsourcing, and wireless expanding the reach of the network beyond its traditional design parameters. IT departments are tasked with ensuring that applications and services run well across both private and public networks. Add to that ongoing application and data center projects such as virtualization and cloud computing and the job of monitoring and troubleshooting all the components that make up that network becomes even more of a challenge. Virtualization decouples the hardware from the application and creates traffic that is more difficult to troubleshoot. Cloud computing abstracts the services away from and even off of the existing enterprise infrastructure and out over the public network. This makes it even more difficult to correctly identify and track down performance issues, as the process is now exasperated by the fact that ownership of the issue is now a shared responsibility between the enterprise IT staff and the service provider. It is therefore no surprise that enterprise IT network staff feel that things are spinning out of control as the job of resolving network related performance issues is getting harder and more complex. Meanwhile, IT departments are caught in the cross hairs of reducing costs, increasing operational efficiencies, and rolling out new applications and services to support the business. These new services must be delivered within acceptable levels of performance for all users regardless of their access points. This can only be accomplished with the right network management solutions.

Virtualization decouples the hardware from the application and creates traffic that is more difficult to troubleshoot.

Introduction

IT departments are charged with doing more with less. That means finding ways to work more efficiently and effectively. The right network management tools can do just that. They offer monitoring and management options that can extend the reach of a single operator and improve their effectiveness at monitoring and troubleshooting performance problems on the network. Most networking teams deploy several solutions to manage and monitor the health of the network. The challenge is finding the right mix of products that meet both monitoring and management needs as well as fitting with the personnel tasked with using them.

This ENTERPRISE MANAGEMENT ASSOCIATES[®] (EMA[™]) white paper is meant to serve as a guide to help decision makers purchasing or re-assessing their existing network management solutions. This paper discusses the challenges and the most widely available solution providers and how these tools can help achieve and deliver both reliability and performance on enterprise networks.

Challenges

In business, change is a constant. For IT that means keeping the network up and running despite all the moves, adds, and changes. One of the top concerns regarding the network is that IT managers feel they lack the appropriate visibility they need to understand what is running, where on the network, and how to effectively troubleshoot and resolve performance problems when they happen. Network management techniques and solutions were traditionally built around device management, but that is no longer sufficient. Modern networks are more complex and must contend with new types of traffic such as voice and streaming video which are very latency sensitive. The proliferation of high speed networks has made streaming video possible. The opening up of the private corporate network

to the public Internet has created new end-user generated traffic and security issues. Consequently, monitoring must now encompass everything from network traffic, end-user activities, applications, networking protocols, servers, and network hardware devices. This is necessary in order to obtain a complete end-to-end picture of what is happening and where on the network. Too often when there is performance degradation, the network is the first to be blamed, when in fact the problem could just as easily be caused by an application or by end-user activities. IT response has become reactive, and that is not acceptable if end users are experiencing performance problems before IT operations

is aware of it. A more proactive approach rather than reactive will help mitigate problems before they happen and reduce mean time between failures.

Leveraging the right enterprise network management solution removes the blind spots in the network and improves overall network stability and reliability.

Unfortunately, the current state of affairs in most enterprise IT network departments involves the use of many disparate tools in an attempt to improve visibility. The structuring of IT departments into distinct organizations compounds the problem as information remains siloed inside each group. It has become apparent that in order to gain greater visibility things must change, and IT groups must work to share information in order to be proactive. Network

management suites have expanded well beyond monitoring just devices to include applications, Virtual Machines (VMs), protocols, and end-user generated traffic. The new broader view helps networking engineers determine potential bottlenecks before they happen. Leveraging the right enterprise network management solution removes the blind spots in the network and improves overall network stability and reliability.

Solution Providers

There are several different types of network management solutions. They come from four different points of origin: large system IT vendors, ISVs, open source, and appliance-based solutions. Each solution has certain advantages. Each grew out of the need to fill a void in the network management landscape and most have evolved to encompass a much broader set of functionality than they might have originally been designed for. These solutions have been around for over ten years, so it is rare for an enterprise environment to implement only one of these solutions. It is even possible to find multiple versions of the same type of solution from different vendors in the same environment. In some cases, they compete with one another, and in others they are complimentary players in a shared working environment.

The purpose of this overview is not meant as a feature/function analysis of these various solution provider options, but rather a higher level view to determine if a solution is a good fit taking into account the following criteria: pricing, scalability, stability, ease of maintenance, customization, licensing, evaluation testing, functionality, and support options. Depending on how an organization prioritizes these criteria will determine which solutions align most closely with a given set of business requirements.

Large System IT Vendors

The most familiar network management solutions are those that come from the large system IT vendors such as CA (eHealth and Spectrum), IBM (Tivoli NetCool), HP (Network Node Manager), EMC (Ionix/Smarts), and Cisco (CiscoWorks). These solutions are widely available, and because of their

large portfolio of products and services are very successful in big, globally distributed corporations such as the Fortune 500 and the Global 500 companies.

The product pricing, discounting, and licensing models generally target the large corporate buyer. These solutions are stable and well established with a scalable architecture. They are feature rich with broad platform support which includes legacy systems. These environments are very extensible with almost an infinite number of plug-ins and add-ons. These vendors are large global entities that can provide 24x7 service and support options across all the continents. They have many partners programs for selling, technical development and support.

The complexity and scalability of these systems has a down side. These solutions are expensive. The pricing and licensing models are complex and confidential, making it difficult to understand the short and long term costs associated with these products. These solutions require significant investment of time to deploy and maintain. Extensive customization often involves assistance from third-party Systems Integrators (SIs) or consultants, which adds to deployment costs. Depending on how involved the customization is, it might require additional training for existing IT staff to properly operate and maintain. The size and complexity of these products also means that it takes longer for the vendors to roll out product updates and evaluation testing may or may not include the full feature set.

The strength of these solutions is their stability and scalability, their ability to run on multiple platforms, their prevalence in Fortune and Global 500 companies, and their global service and support offerings. These are good choices for large geographically dispersed companies with diverse IT environments that have legacy equipment and sizable IT budgets and staffing resources to support them.

ISV

The solutions from Independent Software Vendors (ISVs) went through some consolidation and rebirth over the last five years. The big system vendors gutted the market several years ago snapping up the mid-tier heavy hitters such as Concord and Micromuse. The acquisitions continue as CA recently snapped up NetQoS in order to expand its enterprise IT management portfolio. In their absence, other players such as Ipswitch, ManageEngine, and SolarWinds have been filling the void. These solutions benefited from initial success in the small to midsize markets which have traditionally been underserved by the large system IT players. These ISV solutions have resonated with users in organizations of all sizes. One of the most notable success stories in this area has been SolarWinds, who managed to launch a successful IPO in May 2009 despite one of the worst economic downturns and they continue to show solid growth. These ISVs have hit a nerve and are popular with IT organizations for several reasons. First, they are for the most part Windows-based and easy to use. Second, they have a lower cost of entry. Third, and probably the most important reason they have gained a solid foothold in the enterprise is that they play well with other vendors' solutions. These solutions do not require a rip and replace strategy. Often they can be added into the existing network management infrastructure for a much smaller cost than it might be to upgrade a license or add a new module from a larger system IT vendor or add a new appliance. Their licensing models are simple and often the software can be purchased over the Web starting under \$10k. These solutions began as point-based products, but over time they have added support for other capabilities. Because

ISV solutions do not require
a rip and replace strategy.

these products are Windows-based it makes them easier for users to maintain and operate and the code base tends to be smaller and more modular so software updates are more frequent than those from large system IT vendors. This enables ISVs to respond to customer needs and emerging technology trends more quickly.

The limitations in these solutions are in the area of legacy systems. For large production environments that have legacy equipment, ISVs can play a complimentary role, but cannot replace solutions from large system IT vendors. These ISVs are much smaller in size and do not have the global presence of large IT system vendors and appliance vendors. They are not designed to handle legacy equipment. Also, because ISVs tend to be smaller companies they are viable acquisition targets for larger IT vendors looking to refresh their product offerings.

Overall ISV-based solutions are a good fit in large enterprise organizations as a complimentary solution, because they work well with other solution providers. These solutions are continuing to mature and add new features that can even make them a viable alternative to other solutions, especially in organizations that do not have legacy equipment to support.

Open Source

Another option that has gained some footing has been in the area of open source. Some of the more popular projects for network management that have gained notoriety include: Cacti, GroundWorks, Nagios, OpenNMS, and Wireshark. Open source network management projects first found favor among those with limited budgets, those who don't mind doing the scripting to customize the application, and those with an open source bias. However, as the tools began to evolve from their earlier, first generation releases with improved user interfaces and some projects adding fee-based support services, it has helped these tools reach a wider audience. For example, support for the Nagios plug-in can be found on the IBM support pages. The software is free and users have access to the source code as well as the full-featured product for evaluation. Fee-based support services are available for purchase. For enterprise IT departments that need to highly customize their solution, access to the source code gives them a head start rather than building something in-house from scratch. The free support services have

been greatly expanded and include not just discussion groups, but Web-based training, user and developer documentation, and "how-to" videos. The community interaction which is part of any open source project enables users to report bugs and developers to push out new builds.

The strength of open source is its flexibility and openness, but it also creates some of the inherent challenges and limitations. An open source project is only as good as the team and community that is supporting it. While there may be many people contributing to the development, there is usually only a handful that work on the

project full time. The community has a voice in the ongoing development of a project, and this can be good and bad. For example, in the case of the Nagios project, a handful of developers decided things were not moving along quickly enough, so they started their own independent forked project. This can impact the stability of the project as users decide whether to continue with the original project or move over to the new project.

The strength of open source is its flexibility and openness, but it also creates some of the inherent challenges and limitations.

Open source network management projects were started by and targeted at network engineers. For the most part they are point solutions designed to perform a specific task such as Cacti, which is a network graphing solution, or Wireshark, which is a network protocol analyzer. OpenNMS is designed to be a more complete network management offering that they claim can compete with HP Network Node Manager. While the solutions are free to download and users are welcome to customize the product to meet their needs, open source solutions are not free to own. The hidden cost of open source is in the maintenance and upkeep. These tools are targeted at network engineers, so they assume a certain level of expertise to operate and implement effectively. The more customization that is done, the more unique the solution, and the more problematic if the resident experts leave the company. The pool of outside resources is much smaller than those for commercial solutions, and if it has been highly customized, smaller still. Most of the projects offer a subscription-based support model, but they vary between projects, so it is important to understand how the models are set up and what is and is not included.

Open source as a solution has proven itself as a viable alternative to commercial offerings. Open source network management projects have found their way into larger corporations, because they can coexist with those from other vendors. In smaller IT shops, they can comprise the entire network management toolset. This option works best in IT shops that have the in-house expertise to implement, configure, and maintain these solutions as well as work with the community to resolve technical issues.

Appliance

Appliance-based solutions have enjoyed a bit of a renaissance. These solutions are dedicated hardware devices with hardened operating systems and software that are optimized to collect and analyze very large volumes of data at a very granular level. These solutions have been on the market for twenty years, the most popular and well-known are in the area of packet flow analysis (NetScout and Opnet) and packet sniffers (i.e., Network General now owned by NetScout). This segment hit its stride in the mid-nineties when Ethernet and new forms of IP-based traffic began flooding networks and network managers needed more visibility into what was happening and where the bottlenecks were occurring. As WAN traffic began to increase in volume and impact network performance, new players entered the market including: Network Instruments, Fluke Networks, Niksun, and WildPackets. Therefore, it is no surprise since network visibility ranks at the top of the problem list for IT management that these types of solutions once again are enjoying newfound popularity in both enterprise and service provider environments.

Appliances are intended to be dropped into critical points on the network and were designed to be low touch and easy to maintain. Appliances provide many options for the types and amount of data to be collected and stored. Appliances are usually thought of as passive monitoring devices, because they were designed to do historical analysis of traffic patterns over specific periods of time and the information was then used for troubleshooting recurrent problems, figuring out where and why bottlenecks were happening, and for capacity planning. However, as access to this information has become more relevant for solving real-time performance issues, over time these tools have evolved to provide real-time analysis of traffic flows in addition to doing root cause analysis (troubleshooting). They run on dedicated hardware and usually have their own diagnostic software to monitor the boxes themselves, so set up does not require configuring, maintaining, and tuning a server. The strength of these products lies in their reporting and analytic capabilities and their low maintenance design.

The strength of these products lies in their reporting and analytic capabilities and their low maintenance design.

These solutions can be expensive for the physical devices as well as the probes. Major upgrades or scaling requires the addition of more boxes and/or probes. Solutions that pull the data across the network are not as optimal as those that do the analysis on the appliance. Detailed licensing and pricing information tends not to be readily available for comparisons on their Websites. Because these are appliances, it is not possible to download them for evaluation purposes.

These solutions appeal to both enterprise and service providers, who need to analyze large volumes of data. Volume pricing favors the larger IT buyer, but smaller vendors such as Niksun have starting points around \$10k. Appliances are a good low touch solution for gaining detailed visibility of what is happening on the network.

Table 1.0 Summary of Solutions Provider by Functional Category

The following table provides a quick summary of how each solution plays in some key functional categories.

Solution	Product Pricing	Licensing	Scalability	Ease of use	Maintenance Cost	Product Stability	Functionality	Support
Large IT Vendor	\$\$\$	Proprietary	Scalable	Complex	\$\$\$	Stable	Extensive	Extensive
ISVs	\$	Transparent	Varied	Easier	\$	Stable	Varied	Varied based on size of vendor
Open Source	Free	Transparent	Varied	Mixed	Varied	Varied	Limited	Limited
Appliance	\$\$	Proprietary	Scalable	Easier	\$	Stable	Limited	Varied based on size of vendor

EMA Perspective

EMA analysts believe that solutions which encompass monitoring and troubleshooting abilities across multiple components (server, VM, network, and application) are necessary to improve operational efficiencies. EMA believes that only through greater visibility and shared knowledge can IT departments hope to stay ahead of problems, before they become trouble tickets. Operators need tools that they can use and rely upon to provide both monitoring and troubleshooting information. If a tool is too difficult to use, it will often provide a limited view of the network, because it is underutilized, or worse, improperly configured. If a tool is too costly to expand or upgrade, then components might go unmonitored, leaving holes and gaps in coverage creating blind spots in the network. While gaps in coverage are sometimes filled with open source solutions as a quick fix, these are too maintenance intensive to keep up with. Also, support options can vary greatly between projects, and the more customized a solution the more difficult it can be to maintain and upgrade. While appliances can collect large volumes of data, they too can leave gaps in coverage depending on how they are deployed. For this reason ISV-based solutions such as those from SolarWinds provide a good alternative to those from system IT vendors and appliance vendors, because they combine a low cost of entry with ease of use while still providing enterprise-wide visibility and scalability. Other benefits include more frequent updates and revisions, because of their modular design, and most importantly, they work well with and alongside other vendors' products.

Adaptability is critical to survival as new technology translates into new operational problems for IT managers. Products from large system IT vendors are powerful, but they take time to update, and consequently the lag time between major product releases can be long. ISVs have the advantage of being modular in design, making them easier to revise. For example, on average, SolarWinds updates each of their products anywhere from two to three times per year. This enables them to adjust more rapidly to new products and technologies when they hit the market. Also unique to SolarWinds is their community Website, thwack.com. It provides a forum for SolarWinds to provide support and training as well as interaction between users and developers. Through the community, developers are alerted early to the problems a new technology may impose and are able to incorporate changes into the product roadmap to accommodate them.

Interoperability is necessary to share information. Because solutions from large system IT vendors are so prevalent, therefore it is critical that information from other vendors' products can be integrated. The nice thing about ISV-based solutions such as SolarWinds is that they work well within existing environments. They do not require a rip and replace scenario, but rather can work as a complimentary solution filling in the blind spots on the network.

Affordability is important as companies continue to cut back on budgets. Solutions from large system IT vendors are expensive to upgrade and expand. Appliance-based solutions can be expensive when upgrades involve adding new appliances and probes. Open source solutions provide the lowest point of entry from a cost perspective since they are free. However, they can be time consuming to maintain and upgrade, so their cost comes after the fact. ISV's can provide a lower point of entry with multiple support options both direct and indirect. Through the SolarWinds community Website, thwack, end users have access to a lot of free information ranging from webinars to shared templates.

Global economic conditions make it necessary for companies to remain flexible and adaptable, and the increasing mobility of the workforce creates new performance and security challenges. Companies need a management tools strategy which can grow and adjust to new situations and scenarios. EMA believes that IT organizations seeking to improve operational efficiency and network visibility should closely study their tool choices versus the requirements discussed in this paper, and consider vendors such as SolarWinds that offer broad capabilities coupled with flexibility, agility, and a strong supporting user community model.

About SolarWinds

SolarWinds is a publicly-traded company (NYSE: SWI) based in Austin, Texas. They currently have over 88,000 customers globally ranging from 425 of the Fortune 500 enterprises to small businesses. Their annual revenue in 2008 was \$93.1M which was a 50% growth over the previous year and look to be on track to break the \$100M mark in 2009. SolarWinds product offerings include enterprise network & application management solutions, tools for engineers, entry level fault monitoring solutions, and free tools. They also maintain a community website called thwack. They have strategic partnerships with Cisco and Microsoft. In addition, they have technology partnerships with Cisco, Dell, F5, Juniper, and Riverbed among others. They sell both direct and through a global network of resellers & VARs. All the products are available for download from the vendor's website.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT 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 its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow [EMA on Twitter](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2009 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com



1989.112409