

# COMPARING NETWORK AND SERVER MONITORING TOOLS

---

Five data center managers speak out  
about LogicMonitor and Nagios

SaaS **vs.** Open Source

# Contents

**1.** Introduction

**2.** Quick Summary

**3.** Installation

**4.** Initial Configuration

**5.** Ongoing Configuration

**6.** Graphing

**7.** The User Interface

**8.** Customizing for Business Managers

**9.** Device Updates and Support

**10.** Costs and Pricing

# 1. Introduction

Server and network monitoring tools are essential for today's data centers. They help data center managers increase uptime, anticipate problems in system and application performance, troubleshoot outages, and track capacity needs. And the best products provide comprehensive data on nearly everything in the data center, including network equipment, web servers, file servers, hypervisors, storage devices, databases, and applications.

*When selecting a monitoring product, many operations managers and systems administrators find themselves comparing an open source tool like Nagios with a commercial solution like LogicMonitor.*

This paper summarizes the results of detailed interviews with five data center managers who have experience with both Nagios and LogicMonitor. All five have spent years "in the trenches" managing and monitoring complex environments and facing real-world business pressures.

**We will look at these findings in depth, based on specifics from the five data center managers.**

## 2. Quick Summary

The five data center managers agreed on a few main points:

### TIME COST

Nagios is a very flexible tool, but it takes a great deal of effort to configure it for a constantly changing set of devices and services. LogicMonitor, in contrast, uses auto-discovery to detect new devices and applications and to automatically set up monitoring of all services.

**As one manager put it:**

“Nagios is built around the idea that you have someone who’s willing to waste time every day in a constant tuning and changing mode. I’m not paying someone for that.”

### COMPLEXITY

Nagios requires more expertise in programming and in the devices and applications being monitored, so not only does it take more time, often it uses up the time of the most highly skilled systems administrator in the organization.

### GRAPHING

Graphing and trend analysis are essential to troubleshooting current problems and anticipating bottlenecks. Nagios needs to be integrated with a graphing program, and producing a new graph means writing scripts to connect the two programs, which can take hours. In LogicMonitor, graphing is an integrated feature that takes place automatically, without additional effort.

## BREADTH

Most organizations that use Nagios also use several other monitoring programs to collect data from different types of devices. LogicMonitor can track nearly all devices and applications in the data center, making it much easier to correlate data and find the underlying cause of problems.

## REPORTING

LogicMonitor provides dashboards to show business managers that the data center infrastructure is under control. Also, business executives are impressed by custom dashboard panels showing key business parameters like web site hits, transactions, and customer registrations. Nagios requires separate graphing tools, making correlation and display of information more convoluted, and therefore more difficult to report.

In short, Nagios is a good tool if you can dedicate a highly skilled systems administrator (or a team of them) to the software itself, but LogicMonitor is a far more cost-effective solution to monitor a complex environment.

***If the purpose of monitoring is to reduce the frequency and duration of service impacting events, then LogicMonitor presents a compelling argument for not only more monitoring, but deeper monitoring that leads to increased productivity and revenue.***

# 3. Installation

**Nagios** is an open source, premise-based software tool that can be installed in the data center on a variety of Linux distributions.

Our data center managers observed that installing Nagios was not particularly difficult, although it did require some expertise with Linux to set up the software and configure security, backup, and other administrative details.

They also observed, however, that Nagios should be installed on a “hefty” server, with a second server configured for redundancy, since monitoring is a mission-critical function that cannot be allowed to go offline because of hardware or network failures. For operations that ran multiple data centers, a separate Nagios infrastructure was required for each location. The cost of each of these servers was \$3-5k, and needed to be replaced every 3 years.

**LogicMonitor** installation consists of downloading a lightweight data collector and installing it on any server within the customer’s network. Being SaaS-based, LogicMonitor is responsible for the monitoring infrastructure cost, ongoing maintenance, updates, and redundant architecture to ensure availability.

*... monitoring is a mission-critical function that cannot be allowed to go offline because of hardware or network failures.*

## HARDWARE COSTS

### Nagios

“Hefty” server (not including additional redundant backup).

**\$3-5k+** every 3 years

### LogicMonitor

Lightweight collector on any server, no added infrastructure.

**\$0** (SaaS-based)

# 4. Initial Configuration

The biggest difference between Nagios and LogicMonitor is in the area of configuring the tools to work with systems and applications in the data center.

Configuring **Nagios** to work with a system involves creating a text file that:

1. Defines the system or application.
2. Specifies what services to monitor.
3. Sets up alerts and thresholds for alerting.

**Figure 1** shows an example of a text file configuring a Windows® server running a web server.

The configuration file in Figure 1 is relatively simple; some can be much more complex. One of the managers mentioned that configuring monitoring for a SQL Server database could involve up to 16 services.

Templates are available for common devices and applications, although these must be tweaked and tested to ensure that they are up to date, and functional.

However, monitoring more complicated devices and applications often requires scripts, which have to be reviewed, adjusted and tested by someone with programming skills, as well as knowledge of the device or application.

## Additional steps are required to set up alerts and escalations.

The data center managers commented that although it is not hard to work with these configuration files, it is very easy to overlook services that should be monitored, especially if the administrator does not have a detailed knowledge of the device or application.

```
define host{
  host_name      Elive
  alias          Elive Desktop
  address       192.168.1.10
  check_command check-host-alive
  max_check_attempts 5
  check_period  24x7
  process_perf_data 0
  retain_nonstatus_information 0
  notification_interval 30
  notification_period 24x7
  notification_options d,u,r
}

define service{
  use          generic-service
  host_name   Elive
  service_description  Disk Space
  check_command  check_all_disks!20%!10%
}

define service{
  use          generic-service
  active_checks_enabled 1
  passive_checks_enabled 1
  parallelize_check 1
  obsess_over_service 1
  check_freshness 1
  notifications_enabled 1
  event_handler_enabled 1
  flap_detection_enabled 1
  process_perf_data 1
  retain_status_information 1
  retain_nonstatus_information 1
  register 0
}

define service {
  use          generic-service
  hostgroup_name  http-servers
  service_description  HTTP
  is_volatile 0
  check_period 24x7
  max_check_attempts 3
  normal_check_interval 3
  retry_check_interval 1
  contact_groups admins
  notification_interval 30
  notification_period 24x7
  notification_options w,u,c,r
  check_command check_http
}
```

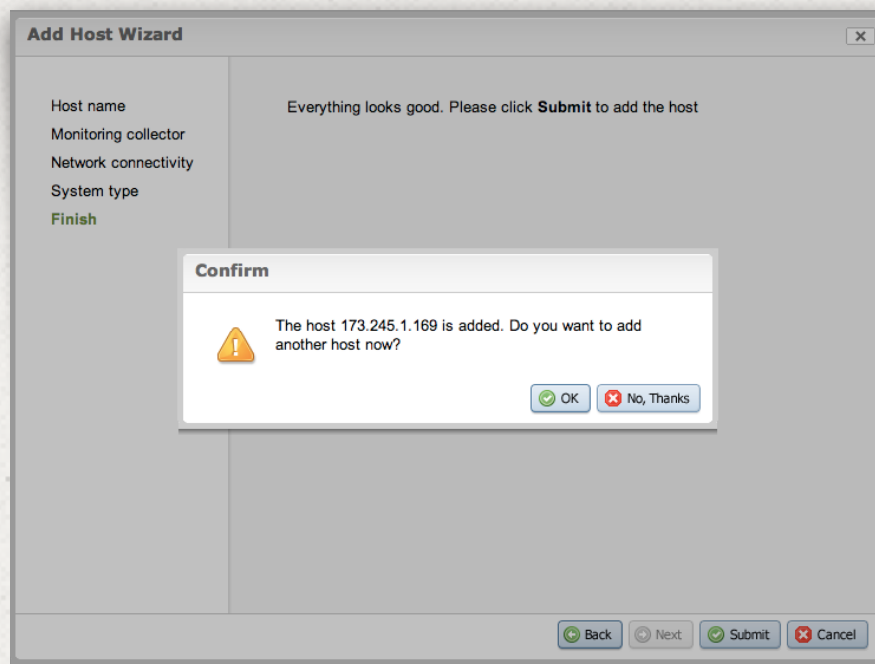
**Figure 1:** Example of a Nagios configuration file.

(Source: Jack Wallen, Installing Nagios: An Enterprise-Worthy Network Monitor)

**LogicMonitor**, in contrast, includes an auto-discovery feature that detects devices and applications on the networks and automatically sets up monitoring on all of the services that can be observed.

In addition, LogicMonitor features a UI that make it easy to add new devices, as shown in **Figure 2**.

*Several of the data center managers mentioned being surprised by how quickly LogicMonitor detected and began monitoring new devices, and also that it monitored services the administrator would not have thought to monitor.*



**Figure 2:** LogicMonitor auto-discovers devices by IP and provides graphical configuration screens.



# 5. Ongoing Configuration

The data center managers describe ongoing configuration as another area where the auto-discovery feature of LogicMonitor provided an advantage.

LogicMonitor was able to detect new equipment brought online, upgrades to hardware and software, and even subtle changes in configurations such as adding a card to a server.

Administrators using Nagios would have to put effort into collecting information from colleagues in other groups in order to maintain an inventory of equipment being monitored and changes in those systems. This reliance on manual updates from colleagues can lead to inventory inaccuracies and lack of a holistic understanding of an IT infrastructure.

A second consideration related to ongoing management was that LogicMonitor made it easy to change a setting for a group of systems in one step. Nagios required administrators to change configuration files for systems one at a time, or else to write and test scripts to make multiple changes.

Finally, one manager commented on the fact that administrators continually need to tweak alert settings and thresholds to avoid being inundated with low-priority messages, and that this was far easier with LogicMonitor than with Nagios.

**“ Nagios is built around the idea that you have someone who’s willing to waste time every day in a constant tuning and changing mode. I’m not paying someone for that. ”**

“ If you really want to make Nagios useful you have to do a bit of work. Some might see this work as too time consuming and or challenging. I can understand that on a large network. Because Nagios can not do auto-discovery, it is up to the admin to configure any device to be monitored...Now, if you are interested in monitoring every single device, on a larger network, you will either need to get clever with some scripting to search out your devices (and track down their associated addresses) or you will need to move on to a different solution. ”

**Jack Wallen**, *Easily extend Nagios' functionality*

**Figure 3:** Expert comment on configuring Nagios.

# 6. Graphing

The data center managers were unanimous in stressing the importance of graphing monitoring data. Alerts and individual data points are simply not satisfactory for managing systems.

For example, an alert about an out-of-boundary condition could be the result of:

- A **spike in activity** caused by a one-time event.
- A **peak load** that repeats itself at the same time every day.
- A long-term **trend of increasing activity**.

The remedy would be very different depending on the cause. A graph or trend-line is essential to determine which of these causes (or another) is most likely.

**Nagios** does not include a graphing module. According to our data center managers, the common practice is to interface a graphics program like Cacti to Nagios. But this has two major downsides:

1. For every graph, an administrator needs to write a script to move data from Nagios to the graphing program, and then to create the desired graph.
2. The administrator then needs to implement and manage two software packages, Nagios and the graphing program.

**LogicMonitor** automatically creates graphs and reports by default with no additional effort, as well as the ability to easily create custom graphs.

# 7. The User Interface

All of the data center managers emphasized the value of having a single UI for all monitoring. That is, one product that can provide unified reporting for all types of systems and applications.

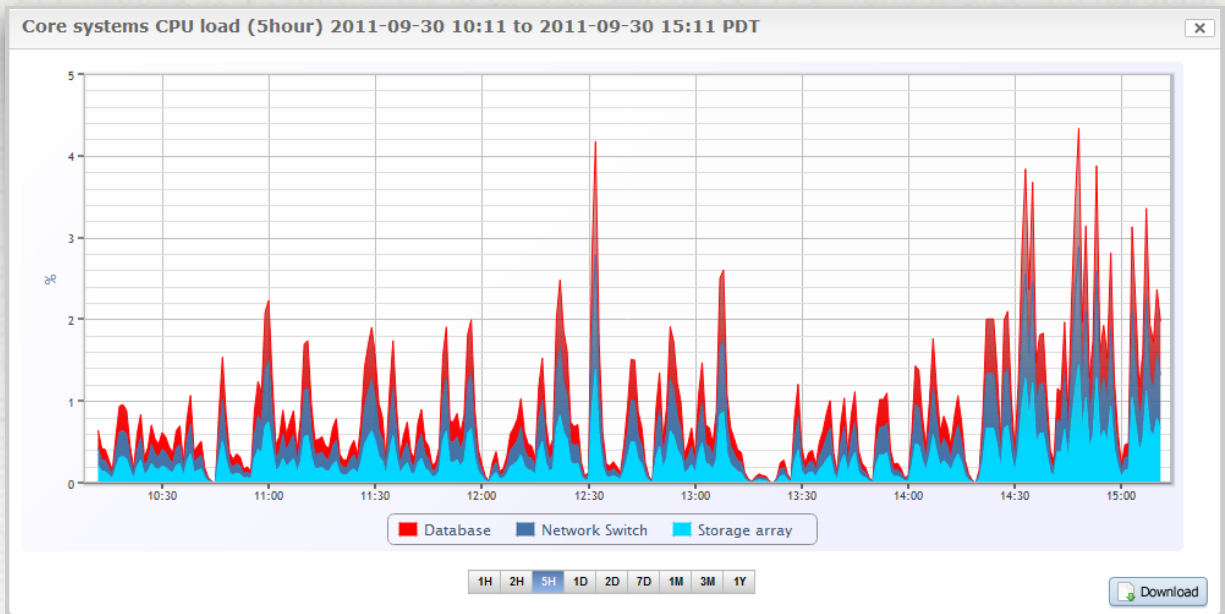
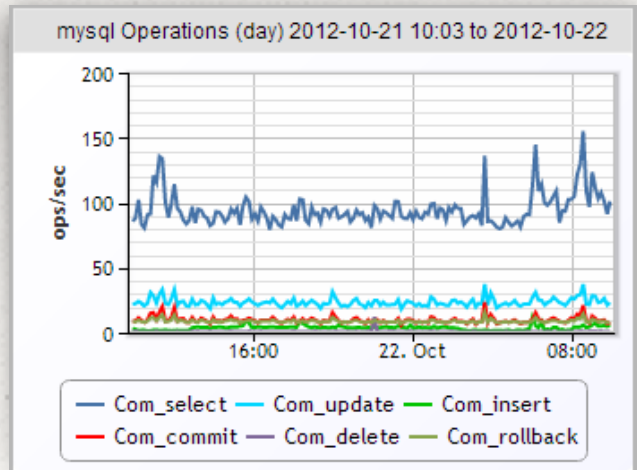
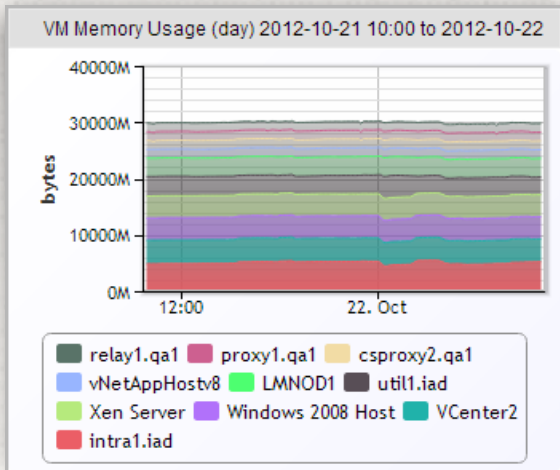
They described the typical environment as containing between three and five monitoring and graphing applications, often with separate software packages for:

- Network equipment
- Load balancers
- Web, file and application servers
- Storage networks
- Enterprise applications
- Virtual machines
- Graphing monitor results

This separation of duties has several negative consequences:

- Extra costs to acquire, install and manage multiple applications (specialized monitoring tools for load balancers can cost tens of thousands of dollars).
- The inability of different IT groups (network, server room, storage, database) to see the same data and work together.
- The inability to detect underlying causes.
- Interdependencies between systems in the same infrastructure.

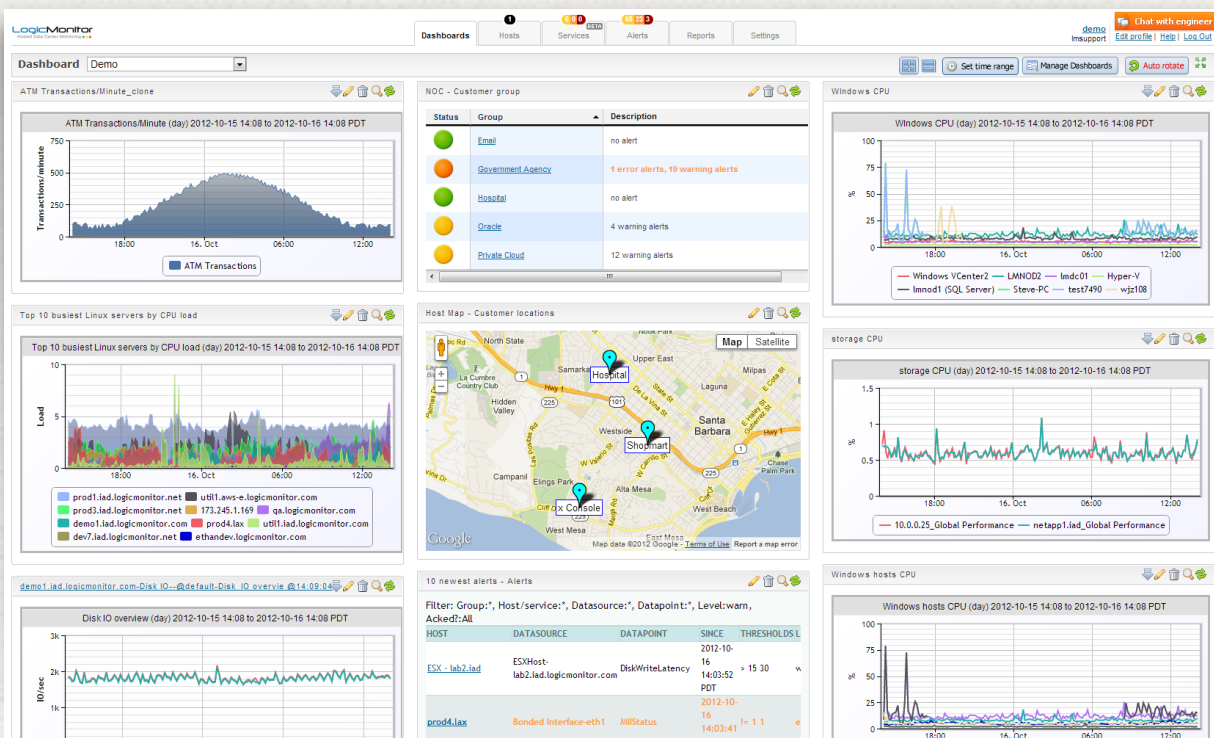
The data center managers were unanimous in highlighting the ability of LogicMonitor to capture and correlate data from an extremely wide range of devices and applications. **Figure 4, 5, and 6** provide an excellent example: tracking results from database, network switch and storage array devices, all on one chart, makes it much easier to tease out the underlying cause of performance problems.



**Figures 4, 5, and 6:** With LogicMonitor, data from many types of devices, applications, and databases can be compared on one graph.

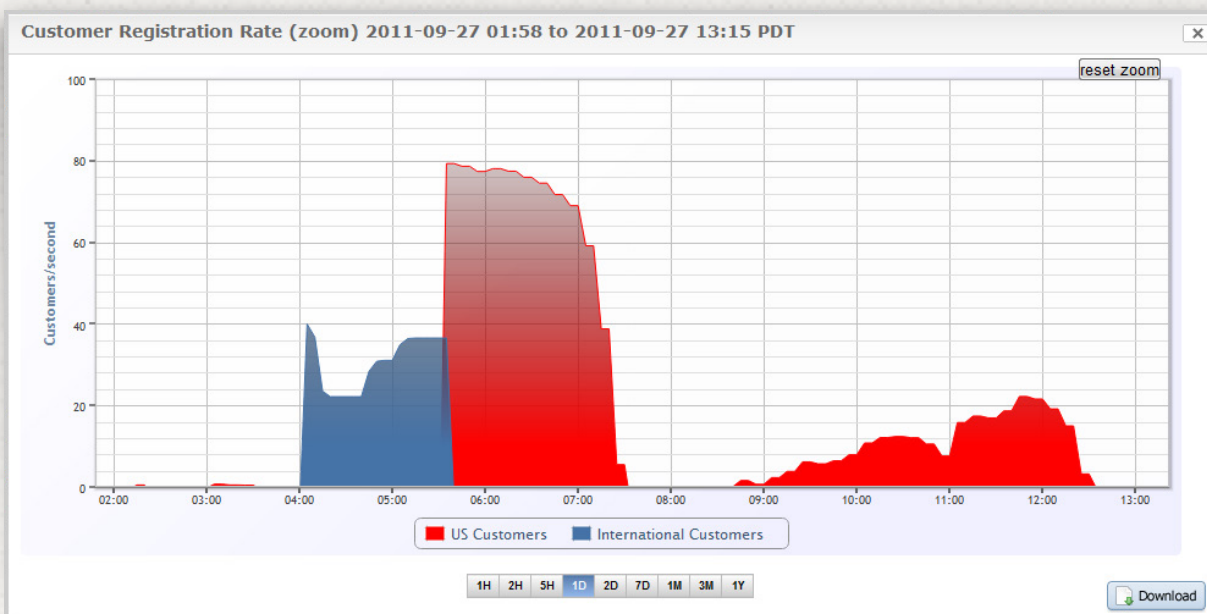
# 8. Customizing for Business Managers

Some of the data center managers described how dashboards could provide value to more than just IT Ops. They described how dashboards showing key technical indicators could reassure business managers that the technical infrastructure was under control.



**Figure 7:** Besides showing key data to administrators, LogicMonitor dashboards can reassure business managers that the infrastructure is under control.

In addition to providing IT metrics, two managers discussed creating custom dashboard panels showing key business parameters like web site hits, transactions, and customer registrations (**Figure 8**). Having this data presented in easy-to-read charts gave business managers visibility into their business that they did not have before.



**Figure 8:** A LogicMonitor custom chart giving executives insight into a key business metric.

*LogicMonitor has excellent tools for creating and customizing dashboards. Nagios has none, and in fact none of the data center administrators had even tried to use Nagios plus a graphing program to create dashboards, believing that it would be too difficult.*

## 9. Device Updates and Support

The managers noted that updates and support were somewhat haphazard in the open source world.

Specifically, when a new storage network or load balancing device was introduced, a configuration template or integration plugin might or might not be available, and support information might or might not be available on bulletin boards or in user forums.

*In contrast, LogicMonitor typically had configurations for the new devices available in customer portals almost immediately, without the customer having to do any manual updates. Customer support through email, chat and telephone was extremely responsive, and included in the cost of the service.*



# 10. Costs and Pricing

## DEDICATED SERVER PRICE

Average server replaced every 3 years, not including redundancy.

**\$4500**

Average price of dedicated server.

**\$0**

Collector installed on any existing Linux or Windows server.

## DEDICATED EMPLOYEE COST

Dedicated monitoring employee salary at \$120k per year.

**\$10K**

Monthly

**Not Required**

## SUPPORT CONTRACT

Nagios support based on number of hosts and limited by incidents.

**\$1295**

1-50 hosts and 3 incidents.

**Included**

No additional cost, no limitations.

## SOLUTION

Pricing for LogicMonitor is based on the number of hosts monitored.

**\$0**

Free to download.

**\$20** per host

Price per host drops with volume.

The data center managers were extremely mindful of financial considerations in choosing a monitoring solution, and a few areas really stood out.

Nagios is a free to download, open source software product, and from a user's perspective that may present an advantage.

However, this was usually more than offset by the hardware costs, additional setup time needed, and high labor costs to install Nagios and configure it for all devices and applications in the data center. For example, one manager estimated an extra day's work with Nagios for every new device, and two hours for every new MySQL instance.<sup>i</sup>

Most of the managers also emphasized the difference in time to construct custom graphs. One administrator estimated that creating a detailed graph would take 6 hours with Nagios and Cacti but only 20 minutes with LogicMonitor, and another estimated 2 hours with Nagios and a graphing program compared with 10 minutes with LogicMonitor. Finally, one administrator said that LogicMonitor had saved his organization the equivalent of one full-time systems administrator at a rate of \$120,000 each year.<sup>ii</sup>

***Several of the administrators agreed that the ability of LogicMonitor to collect and correlate data from many sources had improved uptime for the organization as a whole, based on higher productivity and higher revenue.***

<sup>i</sup> See How LogicMonitor saves Estalea time and money, <http://www.logicmonitor.com/learn-more/case-studies/how-logicmonitor-saves-estalea-time-and-money/>

<sup>ii</sup> Appfolio saves \$120,000 per year with LogicMonitor, <http://www.logicmonitor.com/learn-more/case-studies/appfolio-saves-120000-per-year-with-logicmonitor/>