5 WAYS

To Keep Your

IT MANAGEMENT SOFTWARE

From Becoming

SHELFWARE

April 2015

An Industry Perspective

netreo

84%

of companies are paying for

SHELFWARE

A leading industry analyst recently estimated that 84% of companies were paying for software licenses that were either not fully deployed or had been neglected and marginalized to the point of becoming 'shelfware'. This boneyard of shelfware products, idle and irrelevant, sits in the back gathering dust and gobbling up budgets with its outdated lifecycle footprint before it's finally put to pasture. This process can go on for years.

It's all too common to see Management software at the top of the heap for shelfware. We've been able to identify some of the leading causes that prompt companies to abandon these (often significant) software investments.

Here are 5 key pointers you can use to keep your IT management software investment producing positive returns.

We've been able to identify some of the leading causes

1. Too Many Alerts Are Worse Than Not Enough

Many companies, excited by the possibilities inherent in their new management software, are eager to configure every possible monitor, alert, and threshold so that they can get maximum visibility into their environment. When they do this, the resulting flood of alerts tends to cause 'alert overload' among the IT staff, and very quickly the alerts get ignored or filtered out. If 90% of the alerts are 'not actionable' - meaning that the person receiving the alert is not expected to do anything about it - the natural instinct is to overlook them. The real challenge here is that when a critical issue occurs, it is very often lost in the noise and chaos of all the false alarms that are being generated. It can also cause a false sense of security, with users thinking that every possible occurrence will be detected and reacted to. In reality, we've seen many companies with this kind of configuration still relying on the users calling the help desk as their first sign that something is really, seriously wrong.

The key thing to remember when configuring alerts is to make sure that they are "actionable" alerts - that the person receiving them is intended to take immediate action to correct the problem. Everything else can be handled via automated reports to send the information out on a daily, weekly, or even monthly basis. The ultimate goal is to be proactive in addressing the conditions that cause them.

2. Don't Make People Go To Multiple Places To Gather Information

We often find companies have allowed each department to select and purchase their own tool. This makes perfect sense in some cases, like allowing the DBA team to implement something very specialized for their specific database monitoring needs. Debugging tools for an in-house software development team might be another example. But if left unchecked, multiple departments using their own tools can lead to lots of finger pointing. Often when a problem occurs, none of the individual 'silo' tools have spotted the issue, and the departments each run around checking their own areas of responsibility looking for something that went wrong. This wastes a lot of time and resources, and puts you in the position where you're still relying on users as your primary failure detection system.

In order to achieve real proactive management and stay ahead of the curve, you need an holistic view into all the different aspects of IT - from the applications themselves, to the servers delivering them, the middleware and database systems that support them, and the infrastructure they run across, including routers, switches, load balancers, firewalls, WAN optimizers, and even the UPS and environmental systems they depend on.

3. Keep The Interface Simple And Fast

Many network management platforms fall victim to the 'show them everything' fallacy. It's common knowledge that putting an overwhelming amount of information in front of someone causes them to miss important data-points, because they stop actually interpreting the material and start merely skimming it instead. Any software that defaults users to a screen where there is a huge list of log data to go through, or multiple sets of unrelated information, is going to be harder to use and slower to resolve problems than one that presents a clean, uncluttered overview of everything that's going on. Requiring an engineer to navigate 10 levels of folders to find out what's turning that light red is just making their job more difficult and increasing the chances that it will impact the users before it's resolved.

In addition, a simple to use interface will tend to perform better, especially on mobile platforms or when trying to access the system remotely. Often engineers are on-site trying to help resolve a problem and forcing them to download and install new software on a remote computer that they're using is a pain.

Simpler and easier means reduced training requirements, which means faster deployment and less time bringing the team up to speed, which translates into quicker problem solving. It can also help to provide 'self-service' views for non-technical stakeholders into the state of the environment, allowing managers and executives to see that "Yes, the website is OK" without having to understand the individual naming conventions for all the servers, databases, load balancers, and firewalls that go into making that work. That means they're not interrupting engineers to ask about the status of things.

4. Minimize Administration

It's important to consider the ongoing service burden that implementing a management system is going to create. The less daily care-and-feeding a system requires, the more likely it is to stay relevant to the business and to actually solve problems for you. In spite of this, most management platforms seem to operate on the assumption that you have several full time employees dedicated to constantly keeping the thing running and configured.

Look for systems that don't require you to manually configure every change, as that leads to rapidly out-of-date configurations. Good management platforms should integrate automatic discovery, synchronize with other platforms (like your virtualization system to detect new virtual servers, for example), and provide an easy way to import new devices without relying on your staff to decode obscure SNMP MIB files in order to add support into the platform. Ideally, you want a system where patching and updating the software is automatic, so it doesn't add additional operating overhead for your staff.

Schedule a periodic configuration review for your management platform, at least twice a year (more often in very dynamic environments) to make sure that as you add new applications and systems, and the environment changes, that it is still monitoring the things you want in the way you need them to be - and that it's not generating excessive alerts in doing so.

Another important thing to look for is the ability to automate reporting, and to quickly generate new reports as needed. If the software requires someone to learn a new scripting language, or for a network engineer to learn SQL in order to generate reports, it's not likely to be used much. Standardize on systems that allow quick ad-hoc reporting to fix problems as they come up and to address the concerns of management or executives as needed, but that also then allow those reports to be automatically sent out. Busy engineers will often forget to go look at reports, sometimes waiting on alerts or even users to inform them of problems that could easily have been prevented by getting an email once a week of 'servers with lowest free drive space,' for example. Time spent manually creating reports every month is time that could be easily saved and dedicated to more pressing tasks - allowing a smaller staff to handle a larger environment.

5. Don't Buy Software

Buying software is putting a capital investment into something that may not fit your business, or your needs, a year from now.. or ten years from now. Sure, initially buying the software might seem to let you front-load your costs, but don't forget what happens when you buy a 1,000 device license and then downsize a few locations or push applications out to the cloud a year or two from now and only need half of that. And you also usually have to budget for a paid upgrade every year or two, plus the labor costs required to implement it. If the software you select is not appliance-based (but instead runs on a general purpose operating system) you also need to carefully calculate the full price of the software you're buying - remember most software has a lot of hidden deployment costs in the form of OS licensing, hardware requirements, database licenses (often from a third-party vendor), backup software, and anti-virus licensing. It will also add to the operating overhead of your IT team, adding additional systems to patch and maintain. Often companies will discount your initial purchase, but base the recurring maintenance price on the non-discounted price, which can be as high as 25% per year.

Subscription-based software insures that you're not paying for any more licenses than you need, and that you always have the most current version. And the lower annual cost can help you stay in-budget, without 'first year spikes' in pricing, so it's easier to migrate your legacy systems.

The OmniCenter Solution

Netreo has been helping customers successfully deploy, implement, and manage our OmniCenter network management appliance in their environments for 15 years, and we've managed to retain more than 90% of those customers. A large part of the reason why is that OmniCenter avoids becoming shelfware by addressing each of these items in an elegant, affordable way.

OmniCenter Automatically Minimizes Alerts

OmniCenter includes extensive tools to minimize false and redundant alerts, including the automatic detection of dependencies and root cause, alert suppression, planned maintenance windows, and advanced rule-based incident management. These tools work together to make sure that when you get an alert, it's already been verified as a real problem and that it's the root cause you should be addressing. It can even provide advanced information as part of the alert, like a list of the users who are using the most bandwidth at that location, or customized alerts to tell you if a redundant device has prevented user impact.

You can configure the sensitivity of the alerts, including tuning the number of times to re-check a service and the intervals to check at, as well as setting time frames for thresholds (so that small spikes in the CPU of a SQL server don't generate alerts, for example). OmniCenter also lets you filter alerts by time-of-day and day-of-week, so if you want to avoid getting alarms during your recurring maintenance and backup windows, that's easy to do. And OmniCenter is one of the only monitoring systems that is time-zone aware, so all alerts and reports can be automatically adjusted based on the location of the server or devices you're monitoring, insuring that "Working hours" means the right thing even for your systems in New York, or Dubai, or Chennai.

One Pane-of-glass That's Easy To Use And Understand

OmniCenter includes many pre-configured dashboard views into every aspect of your IT environment, including applications, voice, email, cloud services, and virtualization, and you can customize your own views as well. Users can be assigned to partitions to insure they only see the devices they are responsible for, further de-cluttering the interface, and important problems are right where they should be - right at the top and never more than 1 click away from detailed information about what's causing any alert. OmniCenter can even show you potential problems before they happen, with failure prediction and long-term trend analysis.

Designed from the ground up for ease-of-use, OmniCenter's user interface ensures that even with minimal training users are able to quickly identify problems and get detailed information about what's going on from anywhere in the extended enterprise. Even from mobile devices or tablets. Different types of devices are presented in a consistent format, making multiple-platform management easy. And the entire interface is web-based so there's never any clients or applets to download or install. OmniCenter is designed to let you spend less time 'managing the management platform' and more time focusing on your customers.

Near-zero Administration

By automating most repetitive maintenance tasks, OmniCenter reduces the routine maintenance tasks required to near-zero, freeing up engineering time. Intuitive design and default settings allow for minimal administration and quick deployment. OmniCenter also simplifies user and permissions administration by integrating with Active Directory, LDAP, or SAML authentication systems. OmniCenter can even open a secure VPN connection from your network to Netreo, allowing Netreo engineers to provide remote configuration support, upgrades, patches, and even new device definition or custom coding with minimal time requirements for your team.

Reports can be created through the web interface in seconds, and then saved as favorites to return to with a single click, or automated and scheduled to go out automatically.

Hundreds of built-in reports and simple-to-define custom reports can be linked together into report templates to address even complex reporting needs, all without scripting or writing SQL, and without the need for any additional reporting software or client programs.

For the ultimate in easy administration, Netreo provides managed services for OmniCenter, allowing Netreo engineers to provide 'cloud level' support for the platform, even hosted at your site. This guarantees the management system will stay in perfect sync with your environment, including periodic configuration reviews, alert tuning, and incident analysis. Managed services free your staff to concentrate on improving your core business service levels, without worrying about their management platform.

Hassle-free Purchasing And Deployment

Using our appliance-based architecture, rollouts are a snap. You've got your choice of a VMWare-based Virtual Appliance (VA), one of our robust and redundant hardware appliances, or a cloud-based appliance. All of these options include all of the inherent advantages of an appliance-based architecture: there is no general-purpose underlying OS to administer, no databases to license or upgrade, no anti-virus licenses to deal with, no extra hardware to purchase or spec out. There are also no clients, agents, or probes. Regardless of appliance format, scaling is easy and seamless whether you need to monitor 5 devices or 50,000.

A simple, self-contained solution with one low monthly or annual cost that covers the full OmniCenter license and includes free revision updates. There are no terms, commitment periods or contracts. Devices licensing can change month-to-month with no penalties - you pay only for what you need, so you're never stuck with licenses you paid for but aren't using.

OmniCenter is used by hundreds of leading universities, government agencies, and public and private enterprises of all sizes to monitor and manage complex, mixed-vendor networks with stringent uptime and performance requirements. For more information or to start a free trial today, please contact **Netreo** at **866-Netreo1** or online at **www.netreo.com**.