

Comparing Appliance vs. Software Frequently Asked Questions

© Prism Microsystems, Inc. September 2009

Is EventTracker an appliance or a software-only solution?

EventTracker is a software-only Log Management solution. It runs on an industry standard Windows Server 2008 operating system (also on 2003, 2000 and XP). The program can manage logs from Unix/Linux, Windows, Cisco, z/OS, iSeries and a number of other platforms and applications.

Prism Microsystems is a Microsoft Gold Certified Partner.

Aren't appliances easier to configure and manage?

Maybe for routers or self-learning switches but certainly not in this case. In order for the appliance or software to be useful, you must configure it with your site-information to be meaningful.

Configuring which data sources to monitor, what filters to have on data, what patterns constitute an alert, where to send them, what reports to generate, how long to retain data etc. are the same regardless of whether your solution is an appliance or software only.

Appliance vendors are usually silent about agent installation (or source configuration) for the simple reason that they leave it up to you to manage. By contrast, EventTracker offers a full featured System Manager application that lets you install, remove, configure and upgrade agents from a central location.

The appliance vendor I am talking to says they are “up & running in 10 minutes”.

Sure, but with no alert rules, no reports, no retention schemes, no optimization. Turning on a box and assigning an IP address is a 10 min task but that is hardly “Log Management”.

Think end-to-end i.e., what is the time to install and configure all components so as to satisfy your business objective. This means alerts, reports, retention, access rules, the works...

With EventTracker you need to provision a system and install the software. In virtual environments it is even quicker. The install program for EventTracker has been carefully developed to be remarkably easy to use. Almost all settings can be left at default in most installations and takes a matter of minutes. And with EventTracker it is quicker and easier to do the real configuration work described above than any other solution available.

Isn't an appliance inherently a safer place to store archives?

Appliances tend to be standalone boxes not sharing drives or passwords or login credentials with other machines in the network.

All of this is easily accomplished with a software based/server solution as well. In addition, you control the hardening of the OS to adhere to your security requirements.

One advantage of Server solutions are they can reside within your domain and inherit your security policies such as authentication. This makes single sign-on very possible. Appliances (usually Linux based) are usually hard pressed to integrate and require separate provisioning.

Moving archive data to an offline or near line storage location is far simpler with a software-only solution as well.

Don't appliance approaches scale better?

Not hardly! Appliance vendors will have you believe they provide some magic built-in scalability. In reality with appliances, scalability is simply unused and excess capacity. Appliances force you to predict your log volume and then live within it because it is used to size the appliance. If you predict your volume too high, you have lots of scalability as you bought more than you need. If you predict too low you are quickly going to find yourself buying another expensive appliance.

When you outgrow the appliance, growth is usually chunky – it requires another appliance. Log Management appliances are not \$59 routers, or even another Windows machine – buying another \$30-50K appliance is going to hurt.

By contrast, EventTracker's software only approach permits very granular scaling – one monitored device at a time. Upgrades don't need to break your budget. If you need to move the installation, you can decide how and where to move the archives and software.

Isn't sparing easier with an appliance?

What is your recourse if the appliance fails on a Friday? How can you spare 1 for N with a specialty appliance? What is the vendor's ability to get a spare out to you? In the interim what happens to data? Who do you call and when will they respond? How much of this problem is outside your hands?

With EventTracker, you maintain the same hardware relationships you have for all your other mission critical servers. Sparing 1 for N is the same as your other machines. You have full control of how to migrate a failed box and you are not dependent on any outside vendor to get back online. In addition, EventTracker can be easily depolyed in a virtual environment and will run in both VMware of Microsoft Hyper-V making sparing even simpler.

As you charge on a per device basis don't I end up paying more in the end, rather than an appliance that charges a single price regardless of number of devices?

Perhaps...but...it's not as simple as that. It depends entirely on your environment. Let's look closer at how the two pricing models work.

The number of devices an appliance can manage depends on the log volume generated from the various devices you are monitoring in your enterprise. If you have a lot of quiet devices, an appliance can handle a large number. The reality is, however, that heavily used resources like firewalls and domain controllers generate heavy log volume that must be processed and stored and they quickly eat up capacity on an appliance. Servers with auditing on generate lots of events. Often how many devices an appliance vendor claims they can manage is a highly optimistic model of low per device volumes.

Can you predict your log volume accurately? If you predict lower than actual, you'll have to buy more appliances. If you predict higher than actual, you paid for capacity you won't use.

Assuming you right sized your appliance, if your device count or log volume grows, you'll need another appliance. Not free. Big chunk.

In contrast, EventTracker is priced on a per-device basis. With EventTracker you pay a modest fee for the additional devices. It is predictable and you can plan in advance for device growth. Being software, there are a great number of parameters that you can tweak to minimize spend on hardware to run the software. If you need to add additional long term log archival and want it online you simply add more disk in your current server, or allocate space on another server, you do not need to buy another storage appliance.

Appliance vendors often claim that they provide free and virtually limitless scalability – in reality their scalability is simply a result of their inflexibility, you had to buy a bigger box than you really needed (limited configurations available in the appliance).

So, can an appliance be cheaper than the EventTracker per device model? Only if you are managing large numbers of mostly quiet machines