



WhatWorks in Log Management

EventTracker at San Bernardino County Superior Court

WhatWorks is a user-to-user program in which security managers who have implemented effective internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know.
www.sans.org/whatworks

About San Bernardino County Superior Court

San Bernardino County in California is the largest county in the contiguous U.S. Its court system covers 20,105 square miles and nearly 100 cities and towns. The IT department supports over 15 court locations with over 800 employees across the county.

About Kevin Arden

Kevin Arden is a supervising analyst in the IT department for the Superior Court of California, County of San Bernardino. He manages approximately 1,200 desktops and 35 Windows and UNIX servers. He has been with the Courts for nearly 9 years. His daily responsibilities are to oversee the servers, desktops, printers and the Court's network infrastructure, as well as provide some Internet and intranet support.

SANS Summary

Correlating and searching logs manually for information on security events was tiresome and time consuming. A supervising IT analyst in San Bernardino Superior Court had enough and began searching for an event management solution that would streamline the reporting process. He found a solution that provided so many additional services that he reevaluated his original criteria.

~~~~~

## ***Interview***

### **Q. What prompted you to look for an event management solution?**

A. Primarily it was security events on the Windows network. I was being asked some questions about certain security events: when they were happening, where they were happening, etc. I would go through each server and extract the log files and correlate and search them manually to try to find a particular event. That was a long and tedious process and it became very difficult to respond in a timely manner. I was doing that and trying to do all my other tasks as well so I started looking around for a solution, something that would centralize all the events and that I could search on one interface, one database, and find what I was looking for.

*\* To hear Kevin Arden expand on the answers, view his presentation slides, and listen to his answers to many more detailed questions asked by other users from around the world, go to <http://www.sans.org/webcasts/archive.php>.*

**Q. Just to clarify, you didn't have any sort of product in place before? It was a completely manual process?**

A. It was completely manual. I was following some Microsoft-recommended best practices, without an automated solution in place.

**Q. What process did you use to look for a solution?**

A. I turned to Google, did some searches, and couldn't really find anything. I talked to some people and turned up nothing. At a bookstore, I happened to find an article in Windows IT Pro on various products. One really stood out for both the options and the price.

**Q. What did you buy?**

A. EventTracker. I downloaded the demo and tried it out. After a couple of hours of working with it, I knew it was what I wanted. It was everything I was looking for and a whole lot more.

***"EventTracker saves the company time and money."***

**Q. When you began your search for a product, what criteria were most important?**

A. EventTracker is capable of complete event management, so my concept of criteria has changed, but going back to how I originally thought about it, I wanted something that was centralized and supported security events, application events, and system events. Also, something that was in a database format that I could run reports against and produce reports--particularly ad hoc reporting. If management came to me and wanted to know something, I could produce a report on that particular security event. Now that I've been able to use the product a whole lot more, I've been able to take advantage of many other features that I think are key, such as the ability to e-mail, page, and to run actions based on certain events. So if an event comes up I can run a script or do some other things that normally I would have to be in front of the computer to do.

**Q. When you looked at the article and it compared the different products, what set EventTracker apart from the others?**

A. Primarily the value. Comparing the price and the feature set was really it. The two main features that I find are most useful are the way it categorizes events in real-time, and how I can search for a particular event based on computer id, event id or any criteria in the log event.

**Q. How did you go about getting senior management's approval?**

A. I talked to them and said, "Hey this is what it can do, this is what we can get out of it, and it has all this other functionality too." Management was a little skeptical about it until I demonstrated the power of what it could do, like being able to find a security event for a given machine, or a given user, quickly. I was able to just type it in, do a search, then print

or e-mail a report. I proved to my manager that this was an effective solution that addressed a specific need.

**Q. Was there a specific strategy you used with them?**

A. My strategy was I was able to produce professional-looking, clear reports. Before when I had to do it manually, there was a little bit of guesswork in there. Because I was pulling logs files from multiple machines, sometimes there would be some inconsistencies in the reports. But EventTracker produced solid reports, which was key.

**Q. How do you know that it works? You see the alerts, but how do you know it's not missing things?**

A. We watch it in real time. When I first got the product, I was a little skeptical. I would compare what I was actually seeing on the screen to the events on the server and made sure that it was accurate. I'm now to a point where I don't need to do that because I know the product is working. I have never had any trouble going in and running reports. The reports are accurate and the real time events happen like they should. I have specific events set up to e-mail or alert, particularly if certain services on a server fail.

**Q. What was the deployment process like?**

A. Straightforward. It took maybe 20 or 30 minutes. Basically, you install the console and push out the agents to the servers. If you accept the default policy settings, just a couple of mouse clicks and it starts working right away.

**Q. What level of manpower does it require to manage?**

A. Minimal. I have it set up on a computer where I can look at the display in real time if I want to, but I don't normally do that anymore. The monitor is usually off. I got it where I like it and I just leave it there and it does its stuff, and when I need it, I go back and look at it and am able to get results.

***" EventTracker has been a really stable, solid product for us."***

**Q. How much training did you or your staff need to manage it?**

A. We have gone through a couple of hours of phone training, talking to the reps. I've had it for a little over a year and I believe I've only had two calls in to technical support.

**Q. How is technical support?**

A. Technical support wasn't bad. One of the earlier versions of EventTracker had an Access issue, which is actually a Microsoft problem. Microsoft Access has a file size limitation, and the techs were familiar with the issue were able to help me get past it so it's no longer a problem. That probably took 45 minutes to work through.

**Q. Are there any features that you would like to see added?**

A. I would like the interface to be a little friendlier. Some of the screens are not all that intuitive. I know them now because I've worked with it, but at first it was a learning curve because the screens didn't have an intuitive feel to them. Some of the fields on the screens were a little cryptic, but I worked through it.

**Q. What types of event data does it collect?**

A. All the Windows events and events from our UNIX servers. Right now I'm starting to expand its capability by looking at SNMP events. I haven't really got that down yet but I'm looking at and collecting events from some of our switches and network devices. It collects everything I need and I haven't had any compatibility issues at all.

**Q. In terms of storing log data, what are its capabilities? Have you put it to the test for anything?**

A. It offers the option of storing log data either in an ODBC database or the EventVault. From there, you can generate reports. Although EventTracker's defaults are sufficient for our needs, I can see how features that we use lightly may be critical in other situations.

**Q. Does it have any capabilities that really stand out?**

A. Real-time alerting--I've set it up to send an alert to my cell phone if a server goes down. It's happened on the weekend and we've been able to bring the server back up before Monday.

**Q. Is there a particular type of report that you use most often?**

A. I most commonly use security reports. When a virus exploiting Windows shares was circulating I was able to run a report on accounts trying to exploit shares on other computers and where they were coming from because it would collect the computer's name. I was able to go back to those computers--they actually belonged to another department on the same county LAN--and tell them I think their computers are infected. So they were able to run their tools and remove the virus. It made me look really good. They were impressed and wanted to know how I did it. I told them it was Prism Microsystems' EventTracker. It's a great product.

***"After a couple of hours of working with it, I knew it was what I wanted. It was everything I was looking for and a whole lot more."***

**Q. You talked about it being inexpensive in comparison to some other products. Does it actually save you money, maybe in terms of saving you time?**

A. It saves us a lot of down time when it can alert us about a server down. And it saves me a lot of time, so it saves the company time and money. I haven't actually computed how much time it saves, or money, but it's been there.

**Q. How does EventTracker benefit security?**

A. It can alert on just about any security event if it's tuned right and properly configured.

For example, you can configure it to alert you if particular administrator accounts sign on to the domain or to a computer. It will capture that event and e-mail you or alert you or do whatever you want it to do. It can run a batch file or some sort of script. And it works not

***"EventTracker produced solid, professional looking reports, which was key."***

only in a Windows environment but also in a UNIX environment. If someone logs on as root or is trying to exploit an administrative account in either environment, it can tell you so you can be proactive. If you don't have those sorts of tools, you may not know that's happening. This tool will capture that information and help you be proactive.

**Q. What type of data moves through your network?**

A. We're a court, so we have confidential data going across the wire.

**Q. Is there a particular place that you need to deploy EventTracker on your network? How does it come together with all your other security?**

A. It has an agent piece and a console piece. I wanted the console to be in a different location than where all our servers are, in case something happened there. When I found out it had alerting--it does pings to see if a server is up or down--I didn't want it to be in the same segment as our servers in case that segment went down. I put it on a remote site so it could look in rather than being on the same LAN segment.

**Q. What are your thoughts overall on EventTracker?**

A. I think it's great. Bottom line, it's been a really stable, solid product for us, and I'm expanding its use. I continue to buy additional licenses when I can get them, and if I'm going to install a new server I try to budget for that.

***SANS Bottom Line on EventTracker at San Bernardino County Superior Court:***

1. Simple, mouse-click deployment;
2. Requires little training and supervision;
3. Categorizes events in real-time, and makes them searchable by any criteria in the log event;
4. Can e-mail, page and run actions based on events.

**For more information on EventTracker:  
Visit: [www.eventlogmanager.com](http://www.eventlogmanager.com)  
E-mail: [sales@prismmicrosys.com](mailto:sales@prismmicrosys.com)  
Phone: 877-333-1433**