



---

## WhatWorks in Log & Event Management: *Maximizing Logging ROI at Premier*

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](http://www.sans.org/whatworks)

About Fred Rickabaugh

CISO for Premier Inc. for the past seven years. Prior to Premier, served as an information security consultant with a major accounting firm as their HIPAA SME and as CISO for the North American operations of a major international manufacturer. Has held the CISSP certification for over ten years. Holds a Bachelors Degree in Engineering, a Masters Degree in Operation Analysis and an MBA.

Jean Wilson

Jean has over 25 years of experience in various information technology leadership positions. She is currently Corporate Information Security Manager at Premier and responsible for risk monitoring, risk management and employee security training and awareness. Jean holds the Certified Information Security Professional (CISSP) certification and is active in the Charlotte ISSA chapter. She holds a Bachelors Degree in Economics.

Dave Gratton

David holds the Certified Information Systems Security Professional (CISSP-ISSMP) with thirteen plus years of management and technical experience. Prior to joining Premier, he worked in various security roles at leading financial and educational institutions. In his current role as a senior risk management analyst, he is responsible for identifying and recommending mitigations for critical systems. He uses SenSage daily to monitor servers, firewalls and databases for anomalies and other events that might indicate problems. He is Premier's representative to InfraGuard.

Ron McGinnis

Ron has over 25 years of progressively responsible experience in hardware and software maintenance, systems and network administration, and information security in government and corporate business environments. He currently focuses on providing risk analysis of, and remediation strategies for, varied information technology projects and the monitoring of corporate system and device logs for attack signatures and deviations from normal operational behavior. He holds the Certified Information Systems Security Professional (CISSP) and GIAC Certified UNIX Security Administrator (GCUX) certifications.

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

**About Premier, 2006 Malcolm Baldrige National Quality Award recipient**

Serving 1,700 hospitals and more than 46,500 other healthcare sites, Premier is the largest healthcare alliance in the United States dedicated to improving patient outcomes while safely reducing the cost of care. Owned by not-for-profit hospitals, Premier operates the nation's largest healthcare purchasing network, the most comprehensive repository of hospital clinical and financial information and one of the largest policy-holder owned, hospital professional liability risk-retention groups in healthcare. Headquartered in San Diego, Premier has offices in Charlotte, N.C., Philadelphia and Washington. For more information, visit [www.premierinc.com](http://www.premierinc.com).

SANS Summary

The security team at Premier needed to quickly review log data in detail and store it for a prolonged period of time—something their current solution did not allow. Though compliance was not a factor, the product they purchased helped with audits and pleased their board of directors with the voluntary move to comply with regulations. They also found a vendor that extended itself far beyond its own product to meet the larger customer need.

~~~~~

Interview

Q. What was going on, what drove you to even look for a tool? Why wasn't what you were already doing quite enough?

A. I guess that the general answer was that the problem of looking at log activity. All operating systems, databases, applications have the capability of keeping logs but you run into a lot of problems from the operations standpoint of not having time to go in and review logs in detail. Also, you usually have the restrictions of both performance and storage for storing the logs for extended amount of times so you lose some history and we were looking for a solution that would allow us to do that. Our goal was to pull an aggregate and very effectively and productively capture logs from a variety of servers and environments and technologies then be able to look at them for untoward activities. We also wanted to be able to check to make sure that internal processes were being followed and things of that nature.

Q. That makes a lot of sense. Let me see if I can summarize back. One is that people didn't have enough storage space to store all the logs. Two is they didn't have time to look at all the logs that they had because they had a lot of other stuff on their plate and three there was no capability to aggregate and four is there was no way to quickly handle all of that aggregated data.

A. Right.

Q. Why do you care? And this has to do with security versus compliance. Some people care because they figured out this could be an early warning system for bad stuff from a security perspective. And the other people care because they've got different laws and regulations and really auditors who are saying, where are the logs? So which one drove this, either or both?

A. The simple answer is both.

Q. What is Premier? What do you do?

A. We're a private company owned by a consortium of not-for-profit hospitals with three main businesses units. First we're the largest group purchasing organization in the United States. We're owned by a consortium of 194 not-for-profit hospitals. We act as a negotiator for products and services used by our members leveraging their combined buying power. The second business unit is our Informatics unit and they're a data aggregator collecting outcomes data, etc. from our participating customers and providing them the ability to compare their performance both over time and as well as against other hospitals in the same area or of similar size and nature, etc. In fact we're involved in a multi-year Pay for Performance quality initiative with CMS (the HQID Project). CMS looks at the performance of the participating hospitals and they actually pay a premium for those hospitals that perform in terms of quality in the upper 80% or 90%. So they actually get an increased Medicaid reimbursement as a result. Our third business helps owner and affiliate organizations manage insurance costs while improving risk management capabilities.

**"We were very pleased with the support that they provided us throughout the installation process. And we were even more pleased with the maintenance and support they've provided us since we went live in June of 2005."**

Q. So it's real money that you can create for your members?

A. Right. Those hospitals participating in this project actually are getting a premium paid through Medicaid. And we collect patient level data from the participants that's used to provide the reports through customized software that Premier developed.

Q. That was the second one? The first was cumulative or aggregate purchasing then this wonderful quality thing, what is the third?

A. We're a re-insurer for our member hospitals. Premier Insurance Management Services seeks to provide broader coverage options than standard markets. Premier's insurance programs, including sponsored and risk-bearing insurance companies, provide stability and predictability for our members.

Q. So you have regulations like GLBA, HIPAA and you probably have PCI right?

A. Actually we don't write the insurance ourselves, we act more of a broker in that area. So Gramm-Leach-Bliley really doesn't apply in that respect. We are not a financial institution. HIPAA doesn't apply to us directly because we're not a covered entity. We're a private company so Sarbanes-Oxley doesn't apply to us. We're not in the financial sector from the standpoint that we don't sell insurance. And last but not least, we're not a health care provider or insurer or payer, so HIPAA doesn't apply to us directly.

Q. So it wasn't an immediate regulatory shove that got you over the hump, it was more of a general need to improve security?

A. However, our board of directors has directed us to work towards complying with Sarbanes-Oxley as if we were a public company. So we also decided to voluntarily comply with the HIPAA info security standards. All these are just good business practices anyway.

Q. Yes, absolutely. Some of them are onerous in terms of paperwork but they make it totally worthwhile.

A. Oh yes.

Q. So you decided both for security purposes and for compliance reasons that you were going to improve the situation of monitoring logs and using them for whatever security benefit they could get both forensically after the fact and maybe an early warning system. How did you go about choosing? What did you use as your criteria and process for picking something?

A. We approached this in a pretty disciplined manner. We established a project and wrote a charter and found a Champion. Our project manager also filled the role of security architect. We started out with an extensive search of system products in the marketplace. We included teams not only from security but from the operations side as well.

Q. Because your operations people thought of this as a tool they might use or just because you wanted to make sure that they were happy with it?

A. Both. We rely on them to react to things we find and it's much better if they're involved in the selection of the tool so they understand what the tool does and can better respond to issues when we bring them up based on the information we collect.

**"We've been completely impressed with SenSage tech support. They've been the best of anybody we've dealt with."**

Q. Did that work pretty well? Did that help them get engaged and keep them as part of the family?

A. I think so. That's very typical of our approach to projects in our IT department.

Q. It's not very characteristic of most security approaches so I wanted to bring it out as part of the discussion and the fact that it worked pretty well, I mean other

people might follow. What we hope people get out of these interviews are little nuggets of things they can go do that they wouldn't have thought of otherwise and that's an example of something you do, that people ought to do but they might not have thought of.

A. Sure. It really helps with the implementation too.

Q. Absolutely because they were in on it from the beginning. So okay, you have a big long list, now how about the criteria for differentiating the list.

A. We had to be able to pull from all the different sources we were wanting to get logs from, network devices, firewalls, all the servers, the applications, the databases and we have some systems that are not really common. Each vendor we looked at had to be able to pull from all of those sources. Another driver was we wanted a solution that wasn't agent based. Our operations teams were pushing to not add more agents on the machines.

Q. Every agent had to be maintained and managed?

A. Yeah, we couldn't find a solution for Windows systems that was agentless, but for the Unix servers there were a couple that we could use without deploying agents.

Q. Anything else that they wanted? Was there anything with reporting or speed or anything like that or were those secondary? They were important but they weren't primary?

A. Well those were factors to differentiate between the different products. It wasn't so much that we had a specification that they had to meet but rather comparing the logging solutions against each other to evaluate which one measured and met our needs better.

Q. Did you get down to a short list and then have them come in?

A. We had some other things we looked at. I think you mentioned them already, such as reporting. We were looking for something that could alert and we were even toying with the idea of real time alerting. At the time, SenSage had a beta version of real time recording. We wanted something that had standard canned

reports and also that we could do ad hoc reporting. We wanted to be able to trend reports across different environments and we wanted to be able to customize the reports as well.

Q. So, compare the changes over time across various systems?

A. Initially we spent months examining the logs and we found configuration errors across the environment, where we saw them on several different systems. They were showing up on several different logs and once we aggregated the logs we were able to see it was a common trend.

**"We wanted something that was customizable from the alerting standpoint so we wouldn't just get an alert every time there was a failed log in."**

Q. Anything else on your list?

A. We wanted something that was customizable from the alerting standpoint so we wouldn't just get an alert every time there was a failed log in. We wanted to be able to configure some parameters around that. If there were five failed logins within 30 minutes or something of that nature. And we also wanted reporting capabilities that were fairly standardized across all of the feeds so that we didn't have to interpret every individual report coming from all the different sources. So that they actually looked somewhat standardized so that you didn't have to interpret every one of them.

And we spent a good deal of time with our operations colleagues both on the Unix side and Windows side understanding the events that were capable of being logged. So we ended up with a list, a fairly short list, of things that were most important to us. We had done a good bit of pre-work so that we knew what we wanted to log.

Q. Sounds like you had this really well thought out.

A. Yes, we actually looked for something, too, that in the future might be able to take some of the feeds from the firewall and the external routers that we might be able to use as an early warning system similar to intrusion detection.

Q. Okay, so a sophisticated and intelligent monitoring capability.

A. Right. And it had to be scalable as well.

Q. And then how did you find out whether each of those people on your long list met those needs, did you have them in? How did you decide?

**"We've not encountered a lot of vendors [before SenSage] that would extend themselves way beyond their product to see the bigger need that the customer had."**

A. We sent some preliminary information to them. Our security architect was very thorough and had in depth conversations with each of the vendors to really understand their products. We ended up with a list of six products that we reviewed and then we short listed to three. For the three that we short listed we had WebEx demos and sales presentations followed by Q&A sessions and customer reference checks.

Q. So it was a manageable subset of the big, long list?

A. Yes.

Q. And how did one of them, what were the one or two among those criteria, or four or five, that separated the winner from the others?

A. One of them was the agent, agent based. Several products had to have agents on all equipment but there were, let's see, I think there were actually only two that we looked at that did not require an agent on the Unix machine, they used Syslog. That's a big plus. So that was the one our Unix team was really pushing so they could stay away from an agent.

Q. Sensible people, yeah. So that makes sense. Anything else get you down to one?

A. You know I think that you pick up a lot when you talk to vendors, particularly when you get past the marketing folks and get into the technical support folks who start to have discussions about what they've done and start to begin to look at how you can put this product in place for your environment. We were just overall impressed with the SenSage folks. They were a new company, very interested in doing whatever they could to meet our needs.

Q. That is the way people tend to separate themselves. Did they follow through on all of that? Because sometimes you see that in the marketing process but then it doesn't stay there when you actually do business with them.

A. You know we were very pleased with the support that they provided us throughout the installation process. And we were even more pleased with the maintenance and support they've provided us since we went live in June of 2005.

Q. How about getting the implementation done? Meaning what did it take to get this thing in, in terms of time and let's talk a little about what it took to get all of the different devices appropriately reporting.

A. Well we had a fairly small scope. We were focusing on servers that had been identified as transporting, storing, or processing electronic patient level data. We're a small shop with fewer than 500 servers in all; we were looking at about 50 or 60 of those servers that fell into that category. So it was a fairly manageable number. I would say that our installation after we made our choice and signed the contracts was probably four to five weeks. We had a couple of weeks where we had an onsite consultant from SenSage. I think two weeks. The consultant was here for a week and then he was gone for a week and then he came back for a week and we all did the training in that week.

Q. The big problem that most people have in that time line is getting all of the different servers to provide the data.

A. Right.

Q. Was that the bulk of the technical time or did that turn out to be because you had a constrained scope, or did that turn out to be kind of okay?

**"We wanted to be able to trend reports across different, environments and we wanted to be able to customize the reports as well."**

A. By the time SenSage technical support was here they were surprised at what we had done ahead of time. We already knew the events that we wanted to log, which I think was a big time saver that probably saved us a week in terms of implementation. We already knew specifically what servers we wanted to log. So really a lot of the consultant's time was spent tweaking applications, the APIs and building the servers. We did have an issue with the hardware because we had 64 bit hardware and their application had never run on 64 bit before it was a 32 bit application.

Q. What was the hardware you chose?

A. It's Red Hat. So there was some time that was lost, two or three days in trying to figure out how to get the application working. They ended up reinstalling it several times.

One of the other things that really helped smooth the bumps out of our implementation was we had a wonderful Unix team here who was very familiar with the native logging within the system as well as the BSM product which is kind of an add on for logging. So they knew how to produce the logs we wanted and it was just a matter of feeding them, of either pushing them or pulling them into the product itself.

Q. Did your selection of what you wanted to look at change? Meaning you decided what you wanted to look at and then after looking at it did you decide, oh, we want to look at other things?

A. We wanted to contain our scope to what we started out with but we've expanded our use of SenSage to add servers and increase what we're looking for since implementation. So the initial things we wanted to look for we still look for. But we always had every intention of expanding our use of it.

Q. Can you point to anything it did that actually improved security? Not that it gave you more confidence, not that it helped you meet the regulatory issues, the regulatory requirements that your board has set, but did it actually help improve security or help operations or both?

A. Absolutely. I can give you an example on the security side. One of the hardest nuts to crack on the security side is the use of generic accounts. Auditors don't like them for

**"We were just overall impressed with the SenSage folks."**

obvious reasons and, from a security perspective, you have a problem with accountability, etc. With SenSage monitoring activity and logons to these accounts we could then implement processes to establish accountability and use SenSage to ensure that process was being following. If it's not being followed SenSage allows us to go back to the

supervisors or management involved and get an explanation. So therefore we were able to demonstrate both from a security standpoint, audit standpoint, etc. that we in fact have established accountability for those shared accounts so it's no longer an issue.

Q. How do you know that it's a shared account?

A. Root, for example. Root is a shared account on all Unix systems. SenSage can monitor shared account on databases. Our financial system has a shared administrator account, runs on a UNIX platform and uses an Oracle database. These shared accounts obviously have an impact on our financial statements. It's important to be able to prove to the internal and external auditors that we can demonstrate accountability for use of these accounts.

Q. If one doctor left his machine on and he said, just use mine, don't bother about logging out, logging in, you can't really know that from the log, right?

A. You're correct. Well we have the ability at this point to look at what the source of the log is so if someone is sharing an account and it's being used from a couple of different terminals we have the ability to see that account being logged on from a varied number of different terminals.

Q. That's true.

A. There's no way to prevent somebody from sharing their use of their account with someone else.

Q. I didn't think there was.

A. That's an issue outside of technology.

Q. Exactly.

A. One of the other ways to generically identify an account is that we have a standard naming convention for our human bodies here so any variance from that gets flagged and we know that it's generic or shared account because it's not named after an individual.

Q. Did it turn out to also help on the operations side? Did it give any benefits to the operations people independent of security?

A. Sure, and we can give you a couple of examples. When we put SenSage in and started to get information about the environment that we've never seen before, we saw things that we really couldn't

explain. And then when we would look at it in an aggregated way it identified some misconfigurations on our servers that were adding to network traffic problems and that allowed us to provide very specific information back to our operations teams and get those things corrected. Our operations teams have also had things happen that have been unexplained and they've contacted us and said, you know is there anything you can find in

**"Each vendor we looked at had to be able to pull from network devices, firewalls, all the servers, the applications, the databases and we some systems that are not really common."**

the SenSage logs that might help explain this. And we have been successful in providing that type of information in the past. And finally our user administration provisioning group is using this tool to find and identify accounts that are added that don't go through their process. So again it's a security issue but it's a group that's outside of our security department using the tool.

Q. What about the physical implementation? Is it a box, is it a piece of hardware, is it software on the servers? I know the answer is on the Red Hat server. But is it just a piece of software or is there a physical piece to do it as well?

A. There's three or four servers, four servers and software so there's both hardware and software involved. I believe they have an appliance they sell now.

**"I noticed that implementing SenSage standardized our logging on each individual system, and we've enabled logging where we didn't have it before. By implementing, we actually got operations to address the logging issues universally."**

Q. Has the maintenance and operation of the Red Hat server been a big pain and therefore maybe the appliance would have been better? I don't know that to be true.

A. Not at all. I think the only issues we had early on with the first release were all application

related. It had a few bugs in it but since we went through the first upgrade it's been very stable. I will tell you that our configuration, our physical configuration was different than anything SenSage had ever done before.

Q. Why was that?

A. It was a scaled down hardware implementation. Most implementations at that time had a single collector server and four logging servers for a total of five hardware devices. And we had a smaller configuration. We had a collector analyzer server and three logging servers.

We own the hardware and our Unix team keeps it up to date so, as you know in the security industry, patching is always an issue. We have several other appliances within our organization and because we have to rely on the vendor for patching, we don't always know what patch level they're at.

I think we have a better confidence level. Sometimes the patches break things but at least we know that our systems are as up to date as we can keep them. You don't know that with an appliance, you just kind of completely rely on the vendor to keep you up to date.

Q. And we have some embarrassing data about security appliances that weren't. So you're exactly right. Did you have any other little surprises? So one surprise was that there were some bugs in the application but ever since the first major update those have gone away. Any other surprises on the negative side of things?

A. Yeah, the reporting. Within SenSage you can schedule the report to run and have it emailed to various individuals. What we wanted it to do and thought it would do was email us when it found something to report on. In other words it ran a report it found two failed logins and it would email that to us. What actually happened was that it emailed us even if the report found nothing. From SenSage's perspective, it alerted us so we would know if it ran successfully. However, we got an email every time, even when there's nothing to look at.

Q. Have you talked to them about that?

A. We have.

Q. Anything else that was a surprise?

A. Not really. I mean from a negative standpoint I think we were not quite as happy with the GUI to begin with; but, they've made significant improvements in the last few releases.

**"We looked for something that in the future might be able to take some of the feeds from the firewall and the external routers that we might be able to use as an early warning system similar to intrusion detection."**

We have had several instances when we expanded SenSage to begin to collect our firewall logs. We have a Checkpoint firewall and their log adapter requires that things come over using LEA which is a protocol that Checkpoint uses. We'd never done this before. We didn't know anything about how to configure our firewalls to push this data. Our firewall administrators didn't know anything about this. The SenSage folks were as knowledgeable about our Checkpoint firewall, more knowledgeable than our teams and they made it work. That was a surprise to us. We've not encountered that with a lot of vendors that we do business with--that they would extend themselves way beyond their product and see the bigger need that the customer had.

Q. It brings up another concept which is shared report ideas. Have you gotten any benefit from being in the SenSage family of very useful reporting that you might not have thought of yourself, either from SenSage or from other customers?

A. That's a great question. One of the things that Premier believes in is knowledge transfer and we don't want to have to reinvent the wheel when somebody has a very good solution out there that we can customize for us. We have been pushing SenSage to set up connections and really put together a user group of people in the Southeast and North and

South Carolina. And we had our first user group meeting in June. We had participants from Tennessee and North and South Carolina and we did learn some things that other clients are doing with this tool and we were able to share some of the things that we're doing with the tool for their benefit as well. And SenSage was very good about putting together that forum and encouraging that type of dialogue.

They also have an online forum which we've used, where you can ask questions and other people will jump in and tell you what they've done. We know of one user who has received some queries from a hospital in Tennessee. So we're in the beginning stages of it, of sharing.

**"Auditors don't like generic accounts for obvious reasons and, from a security perspective, you have a problem with accountability. With SenSage monitoring activity we could establish accountability and ensure that process was being followed."**

When we did business in 2005, SenSage had less than 100 clients or customers. Through some strategic partnerships and third party agreements with resellers, their base is expanding. And I think they're more interested in providing those kinds of linkages than they were in the past. They're in Europe and Australia now.

Q. Any other benefits?

A. I will say one more benefit that I noticed was that implementing this thing changed things across the environment, standardized our logging on each individual system, and we've actually enabled logging where we didn't have it before on some things like the databases. So by implementing this we actually got operations to address the logging issues universally.

Q. How was tech support?

A. We've been completely impressed with their support. When you call them they actually answer the phone and give you a technician who provides support almost instantaneously. If that person isn't available, they actually do call you back, which is pretty rare. Yeah, so I would say I've been pretty impressed with that. They've been the best of anybody we've dealt with.

Q. How do you feel overall about SenSage? Any general bottom line, happy we bought it, it paid off, it did what we needed it to do?

A. We had a four tiered approach to our log management implementation process. We initially wanted to pick up OS logs from our high value and confidential servers. We completed that phase. Then we expanded it to log and analyze our firewall logs. We've done that. Now we're in the third phase and working with our databases to understand

more about activity on them. Our final frontier is to start to look at some of our applications themselves. And that will be something we work on in 2008 and 2009.

Q. But for each of those phases you feel good that SenSage has been right there with you and able to help you and doesn't fall over a cliff on any of them, right?

A. Absolutely.

Q. No capacity problems?

A. No, it's impressive.

Q. How about the speed of query, are you happy with that?

A. Yes. We're all looking forward to the new GUI which is coming out with the 4X release. We got a little preview of it at our June user group meeting but we think that adds a lot of value to the product. There's a pretty neat dashboard that's included in that and we continue to look for a dashboard type application that we can aggregate lots of security information and make it available to our business centers and this may be an extension that allows us to do that.

Q. That would be wonderful because that would really help you to help everybody in the organization.

A. Right.

SANS Bottom Line on SenSage at Premier:

1. Aids in audit and compliance by collecting data over time;
2. Standardizes logging on individual systems and makes universal logging possible;
3. Establishes accountability for shared accounts;
4. Allows extended storage without performance loss;
5. Excellent, adaptable tech support.

**For more information on SenSage:**

**Go to: [www.sensage.com](http://www.sensage.com)**

**E-mail: [megan.webster@sensage.com](mailto:megan.webster@sensage.com)**

**Phone: 415.808.5961**