EVENTSENTRY

East Alabama Medical Center Stays Healthy with EventSentry

East Alabama Medical Center (EAMC) is a general medical and surgical hospital located in Opelika, Alabama. It's the only hospital in Alabama to be ranked among the top 5 percent in the nation for Outstanding Patient Satisfaction 3 years in a row. The 334-bed facility has won numerous awards, including Becker's Hospital Review 100 Great Community Hospitals and ASCEND Peak Performance awards in 2014.

eamc
east alabama medical center

Michael Wegner, security administrator at EAMC, is a CISSP, MCSE, CNE, and PowerShell devotee. In his spare time, he balances the challenges of his position with woodworking, gardening, reading, and dabbling in ham radio. But at work, Wegner is faced with the daily challenge of managing the security of the hospital, where a constant influx of patients rely on his systems' integrity for their health care and privacy. "We depend more and more on computers for health care," Wegner says.

"We would have had to piece together a solution and hope something didn't break in the middle," he remembers. "With EventSentry, we don't have to worry about that."

As a security administrator, Wegner's most pressing need was a solution that would alert him to unauthorized or unexpected changes in the system. "I need to completely depend on getting an alert if something potentially dangerous happens, such as an admin group change," he explains.

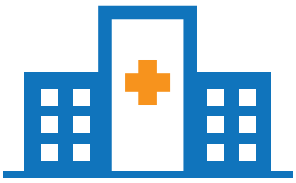
After testing several commercial products, Wegner selected EventSentry since no other product could match EventSentry's integrated capabilities. "We would have had to piece together a solution and hope something didn't break in the middle," he remembers. "With EventSentry, we don't have to worry about that."

EAMC uses EventSentry to monitor more than 200 servers. The product tracks such items as disk space warnings, password resets that might suggest fraud, locked-out credentials that possibly indicate hacking attempts, newly created shared folders that might be a security risk, and a host of other items. "I sleep better at night knowing I don't have to check these kinds of things manually," says Wegner, "or worry that I might have missed something I should have checked."

Wegner uses the product to log and alert on all kinds of network activity: server reboots, Group Policy changes, admin-type group membership changes, administrator logons, and any changes to admin credentials (which trigger an immediate alert). "All of those security alerts together are probably worth at least one security person," Wegner estimates.

For more information call 312.624.7698
www.eventsentry.com

EVENTSENTRY



EventSentry has been a particular life-saver when it comes to drive space monitoring. The hospital has a lively virtual environment, and its engineers like to keep the system drives on virtual machines (VMs) as small as possible. Occasionally, however, the system drives fill up with temporary work files, and if the drive fills up completely, the OS crashes. "We set EventSentry to alert us if those drives have less than 1GB of disk space remaining," Wegner says, "and that allows the engineers time to get to work during off hours (or to remote in) and get the drive resized before it comes crashing down."

Wegner is confident that EventSentry's monitoring and reporting capabilities have prevented many interruptions and outages at the hospital. Once, the product tracked down a virus-infected workstation when it noticed that the machine was repeatedly attempting to log on using a certain set of credentials—and locking out those credentials in the process. And Wegner places particular value on EventSentry's daily report of newly shared folders: "This helped us to prevent a vendor from giving all users full access to protected data!" Real-time notification of critical events, such as a person being added to or removed from the Domain Administrator group, is essential in the EAMC IT environment.

A daily report of newly shared folders helped prevent a vendor from giving all users full access to protected data.

Although Wegner uses EventSentry mostly for security-related issues, the product has been indispensable for other reasons. "EventSentry also solved a website problem involving a library of code that our programmers couldn't edit," he recalls. "The problem caused an occasional error that would require a reboot of a back-end server to resolve. I was able to set EventSentry to watch for that error and send a reboot command to the back-end server when it occurred, which saved the web guys from having to come in at night or on the weekends to reboot the server. Needless to say, I was popular with the web guys!"

In Wegner's previous position as an engineer, he used EventSentry for hardware monitoring and SQL Server database error reporting. "When I was on call for the weekend, I would spend much of Friday looking at the Health Matrix page and fixing things proactively so I wouldn't get called over the weekend," he remembers.

Wegner admires EventSentry's reliability and return on investment (ROI). "It wouldn't take much downtime in a hospital to make up the cost of EventSentry!" he proclaims. On the rare occasion that product support becomes necessary, he has nothing but kind words for the NETIKUS.NET support group. "It's nothing short of fantastic. This level of support is what all companies should aspire to, and I'm very serious when I say that."

For more information call 312.624.7698
www.eventsentry.com