

Logging In Depth

EventTracker is a Security Information and Event Management (SIEM) solution designed to enhance the security of critical systems, ensure confident compliance and improve overall performance and availability

THE UNIVERSITY OF ARIZONA.

The College of Humanities Administrative Computing Support Team

Overview

Business benefits:

- Vulnerabilities pinpointed in a few minutes instead of a few hours.
- High-level of network availability maintained with proactive detection of potential issues.
- Quick, real-time response to issues enabled with real-time alerting.
- Dramatic operational efficiencies gained without additional staff or resources

Platform: Windows

Business Need:

Network optimization and operational efficiency

Industry: Education

Customer Profile

The University of Arizona, College of Humanities Administrative Computing Support Team provides network access to its users for academic and administrative purposes. Their goal is to maintain a safe and secure computing environment for administrators, faculty and staff as well as provide them with access to fast, reliable network servers for storage, network printing and authentication.

Michael Vereshchatsky, the team's senior application analyst, is a 15-year networking veteran and is responsible for ensuring server and network availability. He is a member of a team of 4 IT professionals.

Business Challenge

The College of Humanities network users are constantly collecting, sharing, and analyzing information. In this demanding environment it is essential that around the clock 24/7 server and network availability is maintained. According to Michael, minimizing system downtime by avoiding and quickly recovering from system problems is critical for maintaining such a high level of availability.

Prior to acquiring EventTracker, Michael's team addressed this issue by manually investigating high volumes of log data to identify patterns for potential problems or failures. Whenever a user reported a problem, the IT team had to literally comb through thousands of logs to pinpoint system errors for subsequent resolution.

Not only was this a very time-consuming and cumbersome process that created additional administrative burdens, it was also an inefficient way of successfully managing a network. At times, major network disruptions and system downtimes would go un-noticed until a user called in to report a problem. Even when noticed, the time between issue and resolution would often take a few hours due to lack of information regarding the cause of the breakdown.

The EventTracker Solution

After grappling with homegrown solutions and manual processes, Michael decided that his team needed an easy to maintain, affordable solution that would automate the collection, storage and analysis of log data for complete network visibility and to improve overall server performance and availability.

After looking at other solutions, Michael came across EventTracker, enterprise-level event management software, developed and maintained by Prism Microsystems, Inc.

EventTracker not only offers insightful details into network behavior with real-time collection and analysis of log data, but also provides a centralized console for immediate and convenient access, analysis and reporting.

“We were impressed with EventTracker since it provided us with far better functionalities than other log management solutions at a much more affordable price and also delivered tremendous value in terms of increased efficiency and savings in time” says Vereshchatsky.

Michael was able to readily deploy EventTracker for immediate monitoring of the department’s Windows servers. When he required technical support, he found the EventTracker team to be *“extremely responsive and helpful”* and the level of customer support *“exceptional”*.

Real-time alerting

EventTracker collects in real-time all the log data generated by the IT department’s Windows servers and stores it securely and at 10% of original size in an integrated event repository. Based on thresholds established by the IT team as well as over 500 pre-defined rules for common errors, the software triggers alerts for critical events to instantly notify the team of impending problems either through the central console or with email notifications, SNMP traps, pager alerts or even custom scripts.

“EventTracker’s real-time alerting capability is particularly beneficial since it keeps us abreast of what is happening in our server rooms at all times” adds Vereshchatsky.

Enhanced efficiency without additional staff or resources

Automated log collection and analysis has driven dramatic efficiency gains for the Computing Support Team at the College of Humanities. The log review process is now

automated with little or no staff interference and no requirement for additional resources. As a software only solution that comes packaged with its own database, EventTracker does not require any extra hardware, licensing, administrators or lengthy service agreements.

With EventTracker, Michael’s team has been able to move out of a reactive posture into a more proactive role in which they are never caught off-guard.

The software’s advanced analysis allows them to identify flare-ups before they occur by matching patterns of events across multiple servers for seemingly minor inconsistencies that might suggest an impending problem.

When the unavoidable system breakdown or downtime does occur, the team makes use of intuitive prepackaged reporting templates to pinpoint system errors and vulnerabilities. The process takes a few minutes rather than the several hours it took prior to EventTracker, and significantly improves the time it takes to resolve an issue.

EventTracker KnowledgeBase

Windows event logs contain more than 25,000 unique event definitions and each event is structured differently. In many cases, event messages are undocumented and cryptic providing little information on the event in question. Although, having centralized event collection is essential to analysis, having the knowledge to interpret these events and detect critical system errors is crucial.

Using EventTracker, Michael’s team does not need event management expertise to detect issues and make sense of log data. The software comes fully integrated with a KnowledgeBase that contains descriptions and cause-resolution information for thousands of events in a searchable vendor-neutral collection offering a *“convenient look-up for unknown event types.”*

“We were impressed with EventTracker since it provided us with far better functionalities than other log management solutions at a much more affordable price and also delivered tremendous value in terms of increased efficiency and savings in time.”

- Michel Vereshchatsky
(Senior Application Analyst)