

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

About The Customer

Equity Methods is a global market leader in complex accounting reporting solutions. From financial data engineering to valuation consulting and forecasting, Equity Methods provides the technology, industry expertise, and customer support an organization needs to implement smarter compliance. Equity Methods launched its first valuation consulting services in 1998. Since then, it has assembled a world-class team of professionals that set the industry standard for FAS 123R experience and expertise. The company's comprehensive portfolio of solutions, developed by renowned experts in accounting and finance, has helped hundreds of the Fortune 1000 solve compliance issues in the most simple, efficient and effective ways.

Business Requirements

With a number of public customers subject to the Sarbanes-Oxley Compliance requirements, Equity Methods has made a conscious decision to implement strict IT controls to demonstrate due diligence as part of its value proposition. This includes adherence to the SAS 70 compliance program that requires service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. To qualify for the certification, organizations must demonstrate that they have adequate safeguards and controls in place when they process or host data belonging to their customers.

The EventTracker Solution

Scott Cummins, senior systems engineer at Equity Methods, considered two other solutions before finally selecting EventTracker. The decision was driven by EventTracker's ability to store log data from disparate devices for extended periods of time to facilitate security audits.



Business Drivers:

- Demonstrate presence of safeguards for SAS 70 compliance
- Ensure integrity and confidentiality of critical data

Cummins was also impressed with EventTracker's central web-based console that provides convenient role-based access to all log data, as well as the ease of using the solution.

"Everything is available on one window. Not only can I get a birds-eye view of all activity on the servers, I can also delve deeper to pinpoint a particular server, date, time or user" says Cummins.

EventTracker helps Equity Methods on both the security and audit fronts. By consolidating and correlating millions of events from various sources in real-time, EventTracker helps Cummins find and resolve problems before it's too late. Drill-down capabilities allow him to pinpoint the exact location of a compromise on his network, and respond immediately with automatic policy-based action and real-time notification. For instance, when the anti-virus was removed from a few servers, EventTracker immediately sent out an alert on activity that looked viral in nature. After a quick investigation, Cummins was able to fix the issue before a larger security problem developed.

"I would not have known of this if it hadn't been for EventTracker" he says.

By shortening the gap between threat detection and remediation, EventTracker has helped Equity

Methods take a proactive stance towards security, greatly improving its visibility into vulnerabilities that threaten to harm the company's networks.

In addition, EventTracker provides a powerful analytics module that helps determine at a detailed level the cause of a security incident.

"It allows us to do forensic analysis from a central location without having to visit each system and sift through the log data manually" says Cummins. *"Plus we no longer have to worry about the event log on each machine emptying itself out, and if needed, we can even look at historical data to research the sequence of events that led to an incident,"* he adds. *"It definitely saves us a lot of time – what took several hours previously now takes less than an hour every week."*

On the audit front, EventTracker's integrated reporting engine provides Equity Methods with the ability to assess the effectiveness of internal controls and demonstrate to auditors that safeguards are in place. Over 500 pre-defined reports monitor system access and integrity. These reports facilitate periodic reviews to confirm that internal processes are in tune with security policies. Custom reports based on any sub-set of collected data can also be quickly generated in response to auditor queries and scheduled for automatic generation.

Bottom Line

By implementing EventTracker, Equity Methods has not only been able to meet its initial compliance objectives, but has also gained real-time insight into its security operations, leading to greater efficiency in internal auditing processes and a more proactive security posture.

"I haven't found anything that EventTracker can't do" concludes Cummins.