

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



Reinsurance Ltd. (Bermuda)

Business Drivers:

- Enable fast, efficient demonstration of Sarbanes-Oxley Compliance
- Provide in-depth network insight for security surveillance and risk mitigation.

Infrastructure

- 50 servers
- 100 workstations
- Windows-centric

Overview

Arch Reinsurance Ltd. (Bermuda) was formed in Hamilton, Bermuda, in 2001 to provide a much-needed infusion of highly rated capacity to the specialty property and casualty reinsurance marketplace. With an experienced management team, industry-leading underwriting talent, and substantial capacity, Arch Reinsurance Ltd. (Bermuda) provides sound, flexible products for "large lines" on selected property, casualty, nontraditional and multi-line reinsurance contracts.

As an insurance company that deals with sensitive financial data, security is a top priority for Arch Reinsurance. The company realizes the importance of protecting the interest and privacy of its customers with best-practice security processes and best-of-breed technology solutions. In addition, as a publicly-traded company, it is critical for Arch Reinsurance to comply with the Sarbanes-Oxley (SOX) Act of 2002 that describes specific requirements and controls for financial reporting.

Robert Sheridan K. Smith, Information Technology Manager at Arch Reinsurance knows that staying abreast of the latest practices is crucial for demonstrating due diligence to external auditors. "It was clear that we needed a log management solution like EventTracker to monitor access to critical systems and to detect suspicious and unauthorized activities in compliance with Sarbanes-Oxley" says Robert. After conducting an internal needs assessment and evaluating the log management market, Robert put together a shortlist of potential vendors. "A few things that convinced me of EventTracker's value over the other two vendors that I evaluated were its user-friendliness, reporting capabilities and the role-based central console."

Within 3 days of purchasing the software, Robert had implemented EventTracker across the company's 150 devices, and configured all relevant reports, alerts and thresholds. "Implementation was pretty straightforward and quick, and I required minimal support" he confirms.

The EventTracker impact

With EventTracker, Arch Reinsurance has been able to effectively meet SOX regulatory compliance requirements by collecting, storing, monitoring and reporting on Sarbanes-Oxley relevant log data. This log data provides an immutable fingerprint of all network, system and user activity and provides auditors with the assurance that financial data has not been tampered with. In addition, since EventTracker compresses the entire audit trail data and applies an MD-5 checksum to it, auditors gain another level of security knowing that the data has not been corrupted. “I was impressed with the amount of compression delivered on EventTracker’s data repository” adds Robert.

Robert conducts both routine and ad-hoc queries to ensure compliance. Pre-defined audit-ready reports allow him to automatically schedule reports for generation. All he has to do is select the relevant systems and users and decide when he wants the reports to run. The following reports are automatically generated on a daily basis:

- Log-on Failure report by users/systems
- Software Install report
- Software Uninstall report
- File-access report by users/systems
- Active directory changes - user added/deleted, computers added/deleted, groups added/deleted

Custom reports can also be quickly generated in response to auditor requests. Additionally, EventTracker’s ability to store log data in its raw

format for several years ensures that reports can always be re-run on historical data. “EventTracker really helped us with our Sarbanes-Oxley compliance. The auditors loved the reports and the fact that we were able to demonstrate a proper review process” says Robert.

In addition to helping with compliance auditing, the reports also provide Robert with the ability to quickly detect vulnerabilities. “Our log-on failure report generally runs 10 pages. One day it ran to over 3,000 pages. This quickly alerted me to an issue with our passwords, and helped me prevent potential security threats. I would never have caught this, if it hadn’t been for EventTracker.”

Although the primary driver for purchasing EventTracker was to simplify Sarbanes-Oxley compliance by automating requirements pertaining to IT controls, Robert soon realized the depth of functionalities that EventTracker offered. “It immediately opened up visibility into all corners of our network. Apart from being able to monitor systems and servers in real-time, I can also track users’ IT behavior to note any unusual activity. With this kind of visibility, we are confident that all employees only have access to information that’s appropriate to their roles” says Robert.

EventTracker’s powerful alerting capabilities deliver another layer of continuous security insight by providing early warning of insider misuse or unusual behavior. “The real-time alerts are terrific. They keep me updated 24/7 and ensure that nothing can happen on the network without me knowing” he adds.

Bottom Line

EventTracker has provided Arch Reinsurance with the ability to effectively and efficiently demonstrate due diligence with Sarbanes-Oxley compliance. With greater visibility into Active directory issues and a ‘window’ into all network, system and user activity, the solution has also helped the company improve its security posture and provided it with the ability to discover security and policy issues before larger problems occur.