EventTracker
Actionable Security Intelligence

Sarbanes-Oxley Act Solution Brief

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

Sarbanes-Oxley Act

About EventTracker

EventTracker delivers business critical software and services that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in IT audit and event log files. EventTracker's award winning solutions provide capabilities to implement Security Information and Event Management (SIEM), Log Management, and real-time Threat Intelligence to help optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates.

EventTracker software is designed to be implemented for organizations with 25 to 25,000 assets such as servers, firewalls, other network and security devices, workstations, applications. SIEMphonic managed services are right-sized to assist you with system administration, incident analysis and compliance activities through "self- half- or full-service" options.

Sarbanes Oxley (SOX) Compliance

http://www.soxlaw.com

This document provides a brief overview of the Sarbanes-Oxley Act, (Sections 302 and 404), the impact of SOX on IT departments, and the EventTracker solution for critical portions of the Sarbanes-Oxley Act of 2002.

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002, and commonly called "SOX" or "Sarbox", is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals. Intended to protect shareholders and the general public, the bill consists of eleven sections which detail the responsibilities of a public corporation's board of directors, and imposes criminal penalties for misconduct. The Securities and Exchange Commission was required to define and create regulations for how public corporations complied with the law, and administers the act.

As of 2006, all public companies are required to submit an annual assessment of the effectiveness of their internal financial auditing controls to the U.S. Securities and Exchange Commission (SEC). Additionally, each company's external auditors are required to audit and report on the internal control reports of management, in addition to the company's financial statements.

A key component of the Sarbanes-Oxley Act is how IT departments must comply with the regulations regarding the company's electronic records. Though SOX does not define how records should be stored or what best practices should be observed, it does regulate *which* records must be stored and for how long. Noncompliance can lead to the imposition of fines and prison terms.

Part of SOX compliance requires that all business records, including electronic records and electronic messages, must be saved for "not less than five years."

As a result, SOX can be a challenge for IT departments because they must institute and manage an archive that retains the required corporate records, yet is also cost effective.

Ease of SOX Reporting and Alerting

EventTracker offers specific reports, rules and dashboards to help meet the requirements detailed within SOX 404 and 302. These reports, rules and dashboards can be easily and intuitively customized for specific environments. Audits usually are stressful, expensive and time consuming. However, you should also consider that audits serve to confirm that your SOX compliance activities are both understood and practiced by your organization on a regular basis. Auditors have wide discretion to determine what constitutes compliance or non-compliance and the relative severity/intent therein. By demonstrating that your organization is aware of the requirements and is serious about your operational commitment by being "audit-ready all the time," you are more likely to receive corrective guidance as opposed to punitive action in the audit.

EventTracker streamlines both the real-time security incident detection and the compliance report review processes. By providing "single-click" issue flagging and report annotation on-the-fly, SOX audit-ready summaries are available on demand in EventTracker to help minimize the stress and time needed to prepare for SOX audits.

Real-time Monitoring

You must monitor and review logs and access reports for this covered information and information exchange in real-time, or as soon thereafter as is practicable to avoid privacy breaches and placing your organization at risk of failing a SOX audit. You must also document your policies, identify and train responsible personnel and provide evidence of incident and log review procedures on an on-going basis.

Protect Data and Information

EventTracker safeguards cardholder's data by ensuring stringent rules against unknown authentication and authorization. EventTracker monitors access to file and database servers. It also monitors configuration changes on critical file and database servers, and alerts the responsible entity to take further action. EventTracker SIEM also has an optimized, high performance event warehouse that is designed for efficient storage and retrieval of event logs. It reliably and efficiently archives event logs from across the SIEM without the need for any DBMS licenses or other overhead costs. These logs are compressed and sealed with a SHA-1 signature to prevent potential tampering.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker improves security, helps organizations demonstrate compliance, and increases operational efficiencies. EventTracker enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

SIEMphonic is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, SOX audit reports annotation, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security and SOX compliance.

EventTracker provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMWAre ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Open and Extensible with Strong Access Control Measures

EventTracker SIEM enables automatic, unattended consolidation of millions of events in a secure environment along with incrementally scalable to meet the needs of any size organization. It also supports an infinite number of collection points, with each collection point able to process over 100,000 events per second. All this data is identified by the product based Knowledge Base, which contains detailed information on over 20,000 types of events, and automatically determines which logs are alerts, which are incidents, and which can be ignored.

Log Collection includes a flexible, agent-optional architecture providing managed real-time and batch aggregation of all system, event and audit logs. EventTracker SIEM supports UDP and TCP (guaranteed delivery) log transport and is FIPS 140-2 compliant for transmission of events from agent/collection point to console.

EventTracker monitors all administrators and users activities for all file and folder access on all servers. It monitors successful and failed logon attempts to all servers. Each EventTracker user has specific user credentials and permissions. With the authentication and authorization mechanism implemented by EventTracker, access privileges are controlled.

EventTracker SIEM also provides enhanced end-point monitoring and security, generating an event when USB/DVD/CD removable media is inserted including the username and device serial number; all file transfers to USB/DVD/CD devices are recorded including the time/date stamp; USB devices can be automatically disabled based on serial number. EventTracker monitors changes on the file system and in the system registry of a Windows system and substantially improves corporate security and availability. Strong authentication and authorization mechanism is implemented by EventTracker, hence access privileges are controlled.

Ease of Deployment and Scalability

EventTracker is available on premise or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

For more information on EventTracker and SIEMphonic visit www.eventtracker.com

Statement of Compliance – SOX 302 and 404

SOX Requirements	Description	EventTracker Reports & Alerts	EventTracker Capability
SOX Sections 302 and 404 COSO Components: • Risk assessment • Control activities • Information and communication	Section 302 & 404 outline that a company's CEO and CFO are directly responsible for the accuracy, documentation and submission of all financial reports as well as the internal control structure to the SEC. In order for an organization to confidently attest to this it must have a clear understanding of where data is stored, who owns it, who is responsible for it and who is authorized to use it.	Yes	EventTracker monitors and stores in a searchable format, all aspects of data use for information stored on file servers and Network Attached Storage (NAS) devices. EventTracker provides a detailed record of files server contents and how they are used including: filenames, folders, access privileges to files and folders (i.e. a user's or groups NTFS permissions), data use by username of group name (i.e. create, open, delete, rename), a list of the likely business owners of data. This latter is based on EventTracker analysis of legitimate user activity on a given data set.
SOX Sections 302 and 404 COSO Components: • Risk assessment • Control activities • Information and communication	SOX requires an Internal Control Report stating that management is responsible for an ''adequate'' internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. To accomplish this COBIT recommends security officers report directly to high level management and that the following duties be segregated: data entry, computer operation, network management, system administration, systems development and maintenance, change management, security administration, security	Yes	EventTracker helps meet the objectives of these requirements in a number of ways. • EventTracker recommends the revocation of permissions to data for those users who do not have a business need to the data this ensures that user access to data is always warranted and driven by least privilege. • EventTracker generates reports showing the history of permission revocations and the percentages by which overly permissive access was reduced. Via these capabilities, entities can demonstrate a historical and sustained enforcement of least privilege access and its effects.
SOX Sections 302 and 404 COSO Components: • Risk assessment • Control activities • Information and communication	Formal security policies, communication of policies and consistent enforcement of policies are critical to running a secure operation. COBIT recommends organizations develop a ''framework policy which establishes the organization's overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems.''	Yes	EventTracker helps organizations not only define the policies that govern who can access, and who can grant access to unstructured data, but it also enforces the workflow and the desired action to be taken (i.e. allow, deny, allow for a certain time period). This has a two-fold effect on the consistent and broad communication of the access policy: • It unites all of the parties responsible including data owners, SOX compliance officers, auditors, data users AND IT around the same set of information. • It allows organizations to continually monitor the access framework in order to make changes and optimize both for SOX compliance and for continuous enforcement of warranted access.

SOX Requirements	Description	EventTracker Reports & Alerts	EventTracker Capability
SOX Sections 302 and 404 COSO Components: • Risk assessment • Control activities • Information and communication	SOX require that organizations be able to provide evidence that they are compliant. This requires an ongoing effort to document and measure compliance continuously.	Yes	EventTracker provides highly detailed reports including: data use (i.e. every user's every file-touch), user activity on sensitive data, changes including security and permissions changes which affect the access privileges to a given file or folder, a detailed record of permissions revocations including the names of users and the data sets for which permissions were revoked. In fact, because EventTracker allows any query or complex query of data use within the application to be saved and generated as a report, the amount and types of information that can be furnished for SOX compliance documentation are nearly infinite.
SOX Sections 302 and 404 COSO Components: • Risk assessment • Control activities • Information and communication	Accounting for access (particularly administrative access) to critical systems is an important aspect of SOX compliance. Systems must be configured to capture both administrative and user access, to store the logs for later review and to protect the logs from unauthorized access.	Yes	EventTracker maintains a detailed history of all objects managed by the EventTracker application including users, user groups and by extension administrative accounts within user directories. At any given time users of EventTracker can generate reports that show which administrators changed security settings and access permissions to file servers and their contents. The same level of detail is provided for users of data, showing their access history as well as any changes made to security and access control setting of files and folders. Further, alerts and reports are automatically generated for anomalous or overly rigorous activity on important data sets. All of this ensures that access to data in continuously monitored for appropriate use and that organizations have all of the information they need to conduct forensic analysis and process improvement.

References

http://www.soxlaw.com/