

[www.prismmicrosys.com](http://www.prismmicrosys.com)

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

## OVERVIEW

An IT infrastructure today can consist of hundreds or even thousands of devices such as servers, routers, and domain controllers. These devices generate large quantities of valuable information in the form of event logs. Without an automated solution in place to help; managing and making effective use of this valuable information is enormously difficult. To be successful, you need a solution that first automates the collection of all the events, and then stores, correlates, and enables in-depth analysis of the event data. That solution is EventTracker.

EventTracker is a software-only, agent-optional framework that centrally monitors and manages events generated by Windows (2008/VISTA/2003/XP/2K/NT), Solaris BSM, UNIX (syslog), syslog-ng and SNMP devices. Real-time EventTracker Agents go well beyond just monitoring the event log and monitor file and registry integrity, USB device activity, CPU/memory/disk utilization, any flat file log, device changes, application start/stop, software install/de-install and runaway processes.

Event data is voluminous. EventTracker stores events in a compressed (greater than 90% compression) and secure event repository that requires no relational database. This frees you from additional hidden costs in the form of databases licenses and expensive and time-consuming database administrator tasks.

EventTracker is both highly scalable and cost effective and includes a comprehensive automated compliance solution. EventTracker is quick to implement and despite its advanced functionality is both easy to use and maintain.

## Improve Security

Security management is all about protecting your data and business intelligence. While most attacks come from outside the firewall, many of the most serious attacks are internal, and the best way to ensure success is through defense in depth. EventTracker monitors and protects both the perimeter as well as the servers where data resides. EventTracker provides security event correlation, host based intrusion detection and security that goes far beyond the capability of standalone firewall and intrusion detection systems.

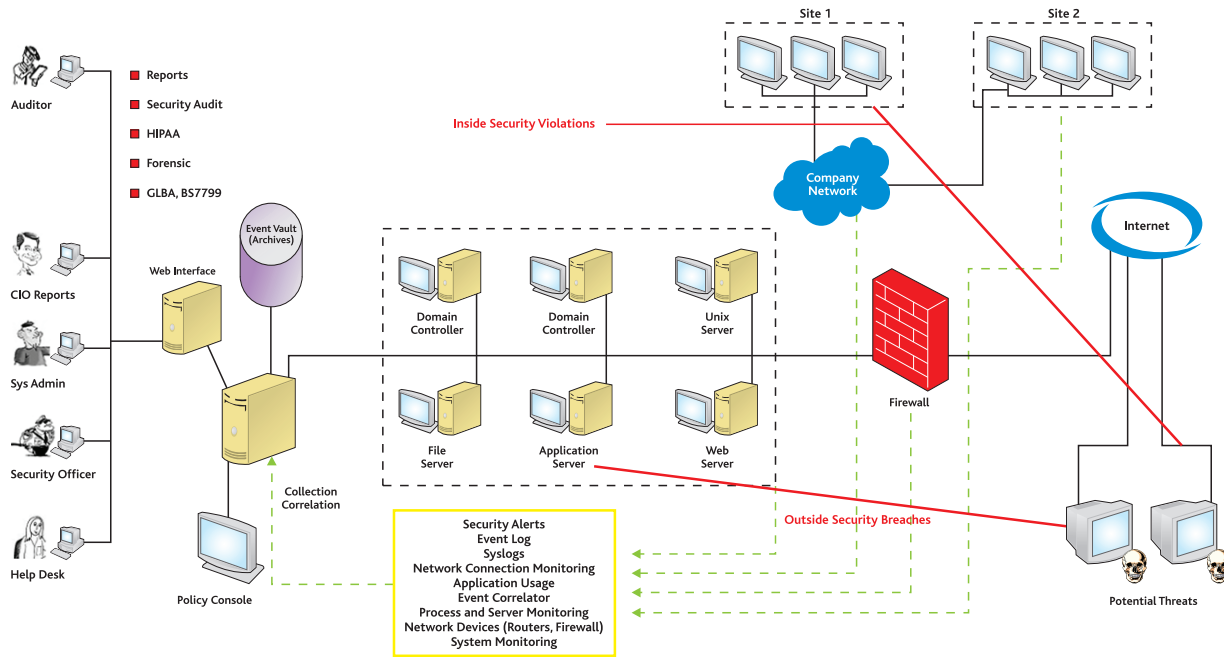
## Achieve Compliance

EventTracker is a cost effective solution designed to automate your compliance process. Automation helps your IT team maintain regulatory compliance without taking staff and resources away from other projects that are important to your organization's bottom line. With capability to store event data securely in a highly compressed form, years of event data can be maintained online for analysis without requiring significant investment in storage devices.

## Reduce Cost

EventTracker pays for itself by increasing the availability of critical IT resources. With automated event log management you can proactively avoid security breaches and system disruptions, and decrease incident response and resolution time. The amount of time IT personnel spend monitoring logs is also significantly reduced. Finally, with an automated compliance process in place, the cost of preparing for audits and remaining in compliance is substantially reduced. Customer studies have found that using EventTracker results in savings to IT operations alone at \$100 per server each month. And when you add in the savings to the overall business through increased productivity, EventTracker returns a positive ROI in a matter of a few months.





## EventTracker Framework

- Support for Windows domain-based and domain-less Network configurations
- Agent optional – Both agent-based and agent-less options available
- Event Warehousing – Ability to archive events for unlimited years in a compressed (>90% compression), tamper-proof archive
- Multi-tier Architecture – Enterprise view, Business unit view, Departmental view
- Active Directory (AD) – Organizational Units (OUs) Administrator Console
- Optional encrypted, compressed and guaranteed delivery of events
- Automatically backs up and clears the Windows event logs when needed
- Full support for all SNMP devices with included MIB compiler
- Monitoring of any SYSLOG or SYSLOG NG compliant log.
- Extensive detailed knowledgebase of over 20,000 Event IDs
- Powerful reporting and analytics framework for event analysis
- Role-based Web Event Console

## Minimum System Requirements

### EventTracker Manager

- 2.8GHz Pentium-based machine, >1GB RAM
- Windows 2003 Server
- Approximately 120GB disk space per 50 systems per year

## Features

### Complete Event Collection

EventTracker enables automated collection of events from Windows Server 2008/Vista/XP/2003/2K/NT, syslog and syslog-ng, Solaris BSM, z/OS, SNMP and any flat file log. Optional Windows Agents support advanced file and registry integrity monitoring, USB device activity and monitoring of critical system metrics such as CPU, memory and disk utilization.

### Complete Event Log Monitoring

EventTracker enables automatic, unattended consolidation of millions of events in a secure environment. EventTracker supports multiple collection points with each collection point able to process over 10,000 events per second in realtime.

### Event Correlation

Events from multiple servers and domains can be analyzed and correlated using a powerful regular expression-based rules engine to provide faster decision making and greater security. EventTracker includes over 800 predefined rules.

### Historical Event Analysis & Forensics

Reporting engine allows powerful custom querying of the event repository. Predefined reports can be generated on a scheduled basis and distributed in PDF, DOC or html formats.

### Regulatory Compliance Support

EventTracker helps regulatory compliance efforts by providing efficient, secure and tamper-proof storage of unlimited years of event data. Over 2000 predefined report templates support multiple compliance standards such as Sarbanes-Oxley, HIPAA, GLBA and PCI-DSS.

