



EventTracker Architecture Handling Millions of Events Each Day

The importance of consolidation, correlation, and detection
Enterprise Security Series

White Paper

6990 Columbia Gateway Drive, Suite 250

Columbia MD 21046

877.333.1433

EventTracker 
www.eventLogManager.com

Publication Date: Jan 15, 2007

Abstract

The purpose of this paper is to highlight the major advantages of employing EventTracker to consolidate, correlate, and manage event log data. The paper introduces at a high level the major design concepts that enable EventTracker to process, store and allow users to gain actionable intelligence from the millions of events that the devices in an organization's IT infrastructure generate each day.

Event data contains a wealth of valuable information for IT controls and compliance, and in many cases, company directives require event information be kept for multiple years. Collecting and storing event logs offers significant challenges however. Each device type has unique events and event Logs are voluminous. A single Windows server can generate over 100,000 events per day. When the auditing feature is in use, Windows servers, like UNIX systems, firewalls and Solaris BSM can generate over a million events per day. As a result even a relatively modest-sized organization can easily generate well over 20 million events each day. EventTracker was designed to automate the efficient collection, storage and analysis of these events.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2007 Prism Microsystems Incorporated. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Handling Millions of Events Each Day

The term *event management* sometimes seems like an oxymoron. By the time you combine the sheer quantity of arcane event data generated by network systems and complex IT infrastructures with the requirement to meet complex compliance regulations and then add the always pressing mandate to further guarantee information security, the ability to successfully manage events seems a very distant and, often, a very lofty goal.

Insuring IT compliance and enforcing security policies is no longer optional for companies today. Windows, UNIX, network devices and database systems, as well as critical applications, record a substantial number of security and error events into local logs. At a bare minimum these logs must be collected and archived to meet compliance. Most companies are undertaking this task manually and the collection of log data for even as few as 10 systems is immensely time consuming while in many businesses the reality is the number of event logs that need to be collected and archived is often in the hundreds or thousands.

These logs contain valuable information that, if accessible, can detect serious impending system problems and security violations before they impact users. It is a challenge to view event logs one system at a time and make sense of them. Message formats vary widely from system to system, and many of the conditions that indicate issues can only be detected when events are correlated or associated with events happening on other systems and devices. Overall, the process of reviewing event logs is so expensive, inefficient and time consuming that most companies do so only after something has gone wrong, despite the fact the information that could have enabled them to prevent the problem to begin with was usually there well in advance.

Storing event log data is a challenge. Event log data contains a wealth of information and the logs are voluminous. Normally, a single Windows server can generate over 100,000 events every day without using the auditing feature. With the audit feature in operation, Windows servers, like many UNIX systems, SNMP devices and firewalls, can produce over one million events per day. It is not unusual for even a small organization to generate well over 20 million events every day. This information needs to be securely archived for IT controls and compliance. Most companies' directives, not to mention federal regulations like Sarbanes/Oxley and HIPAA, require event log information be kept for years. One hundred Windows servers with an average number of 100,000 events each, means a total of 10 million events per day – and that is without auditing! If these events are kept for 90 days, it is necessary to manage and store 900 million events. Kept for three years, the archive would contain over 10 billion separate event records.

It is no wonder that even IT managers and administrators who grasp the importance of the event log data still find the entire task of event log management a difficult challenge. Also security and compliance auditors also want to see reports that tell them that it not only is being done, but that the data is secure and that security policies are operational.

Even if a company takes the approach that most logged events are useless and adopts aggressive filtering prior to collection and maintains only an event subset; this is often unsuccessful for a number of reasons. First, it is very difficult to know in advance which events are important, and with hundreds of servers, the filtering scheme may be appropriate for one server, but inappropriate for another. Second, relying on expert knowledge is usually impossible, because tens of thousands of different event IDs and types exist and no one expert can have complete knowledge. The Prism Microsystems online Knowledge Base (<http://kb.prismmicrosys.com>) contains detailed information for more than

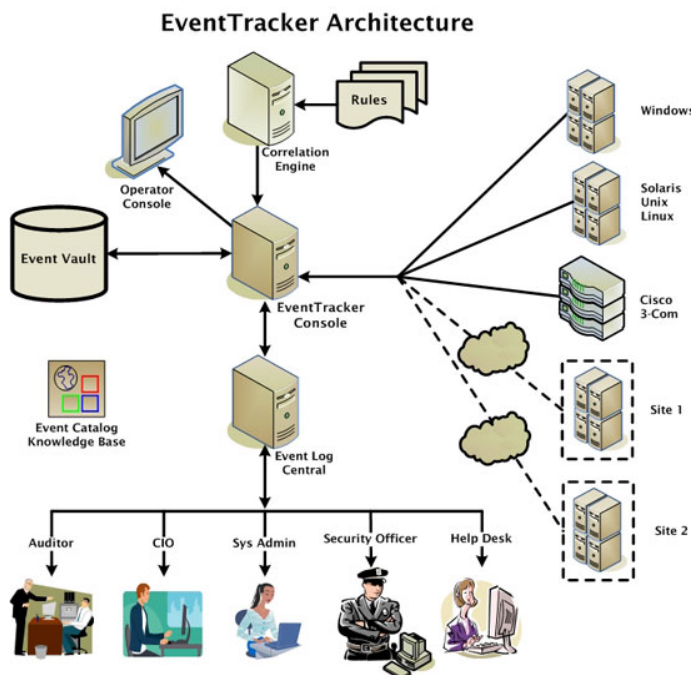
20,000 events, and this is still a subset of the total events that devices generate today. Thirdly, aggressive filtering of the event data will never produce a complete picture for security analysis, and with the stringent regulatory environment it is highly advisable to err on the side of caution and collect more rather than less. Finally even if you can reduce event collection by 50%, using the example above, after 3 years that is still over 5 billion events and even with the logs reduced in size, they still must be collected from all those systems. An efficient automated collection and archival method is absolutely critical regardless of whether robust event suppression is undertaken.

IT Professionals must ask themselves the following questions:

- What is the easiest way to automate the collection of events?
- How can I store all that data securely and efficiently so it is still accessible?
- How can I gain actionable intelligence from all that data in real-time?
- How do I generate reports out of consolidated data?
- Can the solution handle my unique requirements without expensive customization?
- How long will it take me to get a solution up and running, and what are my ongoing costs?

EventTracker (www.eventLogManager.com) is the answer

EventTracker automates the secure collection and consolidation of all enterprise events to a central point and makes them readily available to IT personnel for analysis. The EventTracker technical architecture is designed with scalability in mind and is highly configurable while still being easy to install and quick to implement. EventTracker features an extremely efficient, secure, tamper-proof event archive for reporting and compliance requirements, a powerful real-time correlation engine that operates on the event stream, and a Windows or web-based reporting engine for ad-hoc and scheduled querying.



EventTracker Agents

To initiate the collection process, EventTracker provides optional EventTracker Agents. EventTracker Agents go well beyond simple log monitoring with the capability to monitor, for example, system thresholds such as CPU, disk usage and memory, or the introduction of memory devices such as Flash drives. The EventTracker Agents are centrally configured, managed and distributed from the EventTracker Manager. The Agent then monitors the event log and processes and forwards events as they occur to up to five EventTracker Managers. In addition, EventTracker can monitor logs from additional sources such as applications like IIS and Exchange or databases like Oracle. EventTracker agents can perform sophisticated filtering of the event logs prior to transmission to the central collection point, so if reduction of the event stream is possible, it can be easily accomplished. In Agent-less mode, data is simply periodically collected from the host systems and brought to the EventTracker Manager for processing.

EventTracker Manager

Although EventTracker supports multiple, distributed Managers for scalability, a single Manager instance can process up to 40,000 events per minute. Each logical Manager is hosted on Microsoft Windows and contains a Receiver component that listens for and processes events from EventTracker Agents, SNMP-enabled devices, SysLog or Solaris BSM; a Windows-based event console UI for administration, configuration and event viewing; and the EventVault® event archiver.

Optional components consist of a real-time correlation engine and Event Log Central, a role-based web interface. The correlation engine and Event Log Central can be deployed on a single machine with the rest of the Manager, or over multiple machines to maximize performance.

EventVault®

EventTracker archives events in a compressed and secured event warehouse for reporting and compliance purposes. The records are all sealed with a tamper-proof MD-5 checksum. With EventTracker, no separate database licenses are required. With millions of events generated daily, a database can be an expensive and slow medium for archiving data. One million events can easily consume over 5 GB of storage, and storing even a small time period of event data can require a huge database, a big database server machine and additional expensive database licenses. Databases are also not guaranteed secured storage and event log data can be tampered with.

By default, EventTracker does not store event log data in a traditional database; instead, it is stored in EventVault®, which is Prism's proprietary event storage mechanism. EventVault is optimized for the write-once/read many times nature of event log information. In EventVault log data is compressed to less than 10% of the original size, sealed with an MD-5 checksum and stored in CAB files. If 100 million events are archived, a traditional database can grow to 400 GB while EventVault would require just 10 GB. When a report is generated, EventTracker automatically selects the required archived data, decompresses and unseals it, and then generates the necessary report. Despite the decompression step, reports via EventVault are still generated faster than using a standard RDBMS, and sophisticated caching of the event data, once opened, enables subsequent report generation to be very fast. The EventVault archives can be stored on any storage device that can be accessed from the EventTracker Manager.

Though EventVault provides great benefits, some organizations still prefer to archive collected events in traditional databases. As a result, EventTracker supports SQL Server, Oracle and Microsoft Access for storing events. The database can be installed on the same server or a separate dedicated database server.

EventTracker Correlation Engine

An EventTracker correlation engine can be configured to correlate events coming into an EventTracker Manager. The correlation engine enables powerful real-time monitoring and rules-based alerting on the event stream. Rules can watch for seemingly minor unrelated events occurring on multiple systems across time that together represent clear indications of an impending system problem or security breach. Detecting these problems early prevents or minimizes costly impact on operations. IT staff can be notified of triggered alerts through the EventTracker Console or Event Log Central; or, alternately, an email notification, SNMP trap, or pager alert can be generated. With the EventTracker correlation engine the entire contents of the event can be examined and, EventTracker comes packaged with over 500 predefined rules of the most common conditions. Custom rules can be configured through a Rules wizard. Full PCRE syntax (Perl Compatible Regular Expressions) is also supported

EventTracker Reporting Engine

EventTracker contains a powerful report generator for custom ad-hoc and scheduled based reporting on the data. Reports can be generated in Html, Microsoft Word or PDF formats. The product also comes with over 1000 predefined report templates that enable a business to quickly comply with the regulatory standards applicable to them.

Event Log Central

Event Log Central is EventTracker's secure web-based user interface to view event log data collected by EventTracker. Event Log Central comes with multiple pre-defined roles such as Help Desk, System Administrator or IT Manager, and custom roles can also be created by the Administrator. User authentication is integrated with Active Directory for single sign-on support and https is used as a secure transport between browser client and server. Reports can be configured through a reporting wizard on either the Windows UI or Event Log Central. Event Log Central also provides an optional report scheduling package called Event Log Reporter that enables users to schedule reports that are regularly generated on the off-hours and distributed to subscriber lists, or published to users in Event Log Central.

Collection Points

The Collection Point model is designed for large organizations that have multiple sites or are organized into multiple units within the same site. In many cases, the event log data must all be consolidated and archived in a single place for compliance purposes, but the real-time correlation and day to day management is the responsibility of a distinct IT organization. In these instances, real-time roll-up of the events is not necessary, and the Collection Point model allows an organization to collect and stage event logs in EventVault archives at a location or business unit level, and then automatically transmit these compressed and secure archives to a central enterprise-wide report server on a periodic basis. The business units can access either their local archives for analysis or access the enterprise store. An added advantage with the Collection Point architecture is that data is transmitted via TCP, and delivery is guaranteed. The Event Data is also encrypted prior to transmission and the combination of the two enables a company with multiple locales to use the internet for transmission without resorting to VPN tunneling.

EventTracker Knowledgebase

In order that EventTracker can support the thousands of event types Prism has developed the EventTracker Knowledgebase which is updated constantly as new events are defined. The Knowledgebase is hosted by Prism Microsystems and provides detailed descriptions of event meanings. These definitions can be used to configure rules or as a convenient look-up for unknown event types. In the case where a new event is not already cataloged in the Knowledgebase, or if the event is a custom type (for example, an event from a custom application), rules can still be configured easily by the user.

Summary

EventTracker represents an investment of over 100 man years of development and is the most advanced, scalable and flexible event log management solution available on the market.

Sophisticated Agents, flexible event routing and event collection enables EventTracker to successfully meet the requirements of customers ranging in size from 50 to thousands of managed devices. With EventTracker manual collection and slow and tedious analysis of individual event logs are things of the past. With the component architecture, event processing can be split over multiple machines for the highest degree of scalability, and customers can define consolidation, roll-ups and management views based around their business structure and requirements.

Once collected, the events are securely and efficiently stored to ensure complete regulatory compliance while still remaining available for sophisticated analysis using the EventTracker Reporting Engine. Real-time event correlation represents a powerful tool to prevent system failures and security breaches.

With EventTracker you can meet compliance requirements with ease, improve information security and improve service levels by reducing infrastructure downtime. Studies by our customers show that using EventTracker saves \$100 per server per month in maintenance costs, and EventTracker returns positive ROI in a matter of months.

About Prism Microsystems

Prism Microsystems, Inc. delivers business-critical solutions to consolidate, correlate and detect changes that could impact the performance, availability and security of your IT infrastructure. With a proven history of innovation and leadership, Prism provides easy-to-deploy products and solutions for integrated Security Management, Change Management and Intrusion Detection. EventTracker, Prism's market leading enterprise log management solution, enables commercial enterprises, educational institutions and government organizations to increase the security of their environments and reduce risk to their enterprise. Customers span multiple sectors including financial, communications, scientific, healthcare, banking and consulting.

Prism Microsystems was formed in 1999 and is a privately held corporation with corporate headquarters in the Baltimore-Washington high tech corridor. Research and development facilities are located in both Maryland and India. These facilities have been independently appraised in accordance with the Software Engineering Institute's Appraisal Framework, and were deemed to meet the goals of SEI Level 3 for CMM.

For additional information, please visit <http://www.prismmicrosys.com/>.