

EventTracker Capabilities Overview

EventTracker is a security, compliance, and operations solution that provides a 360 degree view of your organization's IT infrastructure. It is a comprehensive Security Incident Event Management (SIEM) solution that combines log management, log monitoring, log search, file integrity monitoring, system monitoring, reporting, analytics, and visualization for continuous monitoring of system logs, users, file changes, servers and desktops, all the way to USB and writeable media. EventTracker is designed to meet the security, compliance and operational needs of organizations with 100 to 10,000 devices in their infrastructure, protecting against inside and outside threats. Offering incremental scalability, EventTracker is a cost-effective and efficient solution providing all the functionality and usability demanded by today's IT security professionals.

Network Infrastructure and Log Sources

Whatever the device in your IT infrastructure, EventTracker can collect the logs generated from these devices, and provide actionable intelligence in real-time. The sources of these logs include users and Admins, applications and databases, USB and writeable media, routers and switches, IDS/IPS, antivirus, VM Ware, mobile devices - even physical security systems and biometric systems. The simplicity of the integration capabilities of EventTracker make it possible to collect the logs from the widest variety of sources available on the market - Knowledge Packs for devices can be created very quickly and easily by either Prism or the your organization, expanding EventTracker's reach and value in your IT infrastructure.

These source types include (but are not limited to) Windows, UNIX/Linux, z/OS, Solaris BSM Syslog and Syslog NG, SNMP devices, and can process any flat file, making EventTracker highly extensible.

Event Log Collection/Archival

EventTracker provides automatic, unattended consolidation of millions of events in a secure environment in real-time from a comprehensive collection of sources that can be set-up utilizing agent, agent-less, or combination configurations. With a highly scalable collection-point architecture, EventTracker supports multiple virtual collection points on a single machine as well as collection points on multiple machines. EventTracker prioritizes events, and transmits the FIPS-140 compliant encrypted data for archival in multi-terabyte local or SAN storage for an unlimited period of time.

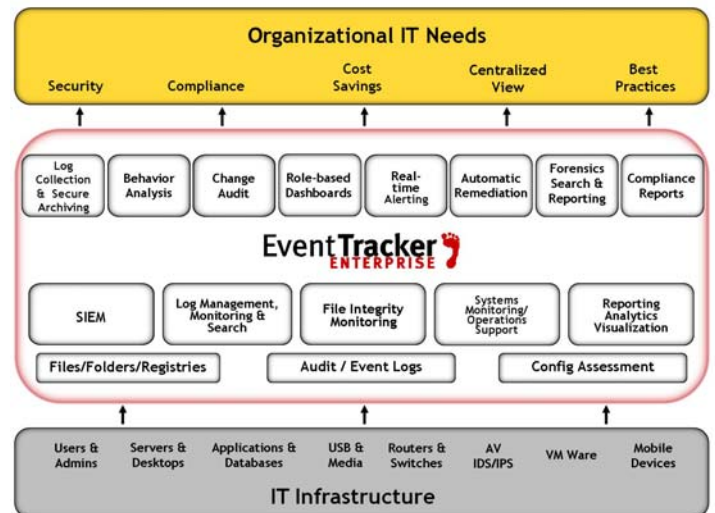
EventTracker archives all collected event logs in EventVault, an optimized and high performance event warehouse that is designed for efficient storage and retrieval of event logs. These event logs are compressed (over 90% compression ratio), sealed with a SHA-1 signature to prevent tampering, written to standard CAB files, and efficiently archived without the need for any DBMS licenses or the overhead costs of Database Administrators.

Behavior Analysis/Event Correlation

EventTracker's unique Behavior Analysis uses automatic statistical analysis to monitor the event stream for any new, different or unusual occurrences. EventTracker learns the normal activity of the network, systems, applications and users, and detects and alerts on any new, unseen behavior or any deviations from the norm. If a user normally logs in 50 times a day and suddenly logs in 200 times in a day this pattern is detected. Is this a problem? Perhaps not, but it is certainly unusual and worth investigating. Similarly anything new -- a new user, application, process, is recorded and can be easily reviewed. This automatic monitoring augments and improves the manual review of logs, resulting in quicker detection and less time spent correcting the issue. Conditions that are detected by EventTracker include abnormally high or low administrator activity, user activity, process or IP activity, new IP addresses, and sudden changes in event volumes.

EventTracker's Event Correlation collects security information from perimeter devices, systems and applications, and applies rules on events from multiple servers and domains to detect patterns of behavior indicating a breach of security. Because evidence of an ongoing attack or IT problem is scattered across multiple systems and devices, it makes it nearly impossible to detect these subtle signs manually in real-time. Once collected, the log data can be processed by EventTracker's Event Correlation Engine, presenting information on statistical anomalies -- unusual behavioral patterns for users, systems, network traffic, applications and more. This powerful capability enables insight into potential conditions for which a formal rule has not been written. EventTracker helps you identify unauthorized logon activity, monitor unauthorized network port usage, monitor logon/logoff activity, manage Active Directory OU delegation and detect new IP addresses, new destinations, and other "first-time events".

The Event Correlation Engine provides "out-of-box" correlation rules to detect the most common and critical security conditions in real-time, the ability to create custom correlation rules and actions, support for Heuristic, Vector, Threshold, Comparison and Redirecting Correlation scenarios, and both Statistical and Behavioral Correlation.



Change Audit

The file system and registry of every Windows system is ever-changing. This change may be voluntary or involuntary and happens quickly and often without the user's knowledge. Under the current Windows OS architecture there is no easy way for the user to understand change, identify change and recover from change.

Change Management is a concept by which all system changes are intelligently tracked and reported on demand for the user to analyze, understand, and if needed, recover from change. The advantage of change management is that it provides the user insurance against change that could be harmful. During the course of a day there are thousands of changes happening on your Windows systems. By using an effective change management solution, you can view changes with only the critical ones being highlighted, while having the non-critical folders and registry hives filtered out.

Role-Based Dashboards

EventTracker provides customizable, role-based dashboards that allow organizations to control the information visible to a user based on their role in the organization. It also allows users to remove the information they do not want to see, and rearrange the location of the information on the dashboard. For example, a system administrator may only have access to the information on the ten servers they are responsible for maintaining, while the director of security will see the relevant information concerning the entire infrastructure. It is from this interface that all searches are performed, and detailed information on an event can be accessed. EventTracker is designed to make the user experience as easy and efficient as possible.

Real-Time Alerting

All incidents are logs, but not all logs are incidents. It is vital that the proper person is alerted when trouble does arrive, and EventTracker provides user-configurable alert weighting algorithm that enables alerts to be prioritized on the criticality of the event, importance of the affected resource, and through integration with leading vulnerability scanners, the vulnerability score of the resource as well. These alerts are displayed in the EventTracker Alerts View for action. EventTracker also allows configurable automated notification such as via e-mail or a pager, automatic remediation, or forwarding of the alert to a variety of other IT systems such as enterprise trouble ticketing systems or NOC software

EventTracker is pre-programmed with alerts for the most common predefined alert conditions, but allows you to customize and prioritize the event criteria as it pertains to your organization.

Automatic Remediation

There are times and instances, where immediate action must be taken to prevent harm to your IT infrastructure or the data it

contains. EventTracker has been designed to provide you with the ability to have you allow EventTracker to initiate action if certain actions occur in the infrastructure. Whether it is a brute force attack, detection of a vulnerability, or insertion of an unauthorized USB or writeable media, you can have EventTracker initiate a number of actions including restarting a device or operation, disable services, disable a user, kill unapproved processes, or prevent file types that are not on your black list or white list. By taking these actions in real-time, using user-defined policies, EventTracker responds to threats against your organization.

Forensics, Search & Reporting

After an incident, it is vital to uncover what happened, when it happened, what was affected, and if possible, who was responsible. EventTracker greatly reduces the time, effort, and costs associated with an incident. This is accomplished using the powerful forensics capabilities of EventTracker including a "Google-like" search that allows you to quickly and easily search through terabytes of log data to pinpoint critical events behind security and operational incidents. Searches can be performed using single and multiple strings within an event description, freeform keywords, phrases, operators, and wildcard characters.

When it comes time to collate and report the data, EventTracker has over 2000 summary and detail templates for security and operations. EventTracker also provides the ability to generate customized reports so you can construct the data in the way you need to see it.

Compliance Reporting

EventTracker enables companies to maintain their compliance, and provide the necessary pre-defined reports for FFIEC, FDCC, FISMA, GLBA, HIPAA, NISPOM, PCI-DSS, and SOX 404. Because the common theme in all compliance standards is auditing user activities, particularly with regard to access to confidential customer data, EventTracker automates the compliance procedures of securing the environment, establishing the baseline, monitoring and recording user activity, alerting on potential breaches of policy, and generating audit-ready reports.

About Prism Microsystems

Prism Microsystems delivers business critical solutions 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 log files. Prism's leading solutions offer Security Information and Event Management (SIEM), real-time Log Management, and powerful Change and Configuration Management to optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates. Visit www.prismmicrosys.com for more information.