Reference Code: TA001820SEC
Publication Date: December 2009
Author: Alan Rodger, Karthik Balakrishnan, and Somak Roy

TECHNOLOGY AUDIT

EventTracker 6.4

Prism Microsystems

OVUM BUTLER GROUP VIEW

ABSTRACT

EventTracker, from Prism Microsystems, is a software solution that combines log, change, and event management in a single product that provides log collection, event analysis, some remediation, archival, and reporting covering server and network elements, as well as some desktop activity monitoring. Its data correlation engine enables real-time monitoring and rule-based alerting of events to IT administrators and users. Ovum is particularly impressed with the reporting features, which include pre-built, compliance-oriented report packages that match a number of industry regulations and legal requirements. An informative knowledge base provides users with detailed descriptions of many common events, and facilitates the rule configuration and analysis process. The solution has a mid-sized market focus, a segment where management of log information can be a major headache, and where a number of the out-of-the-box features will be particularly valuable. EventTracker would be of interest to any company with numbers of systems in the order of thousands, particularly to those in regulated industries.

KEY FINDINGS

- A real-time correlation engine combines both defined rules and statistical techniques to detect anomalous behaviour
- Provides out-of-the-box reports for prevalent compliance requirements
- Graphical, intuitive reporting and query interface
- Flexibility and scalability excellently suitable across mid- and large-sized organisations.
- EventTracker supports monitoring VMware and Hyper-V environments
- Lacks support for integration with vulnerability assessment tools
- Available in three editions with pricing based on the number of devices monitored
- Provides Knowledgebase and EventTracker Pulse as free-of-charge services.

Key: Product Strength | Product Weakness | Point of Information

LOOK AHEAD

The next release (in early 2010), will have a new GUI, FDCC compliance, and support for Netflow collectors.

FUNCTIONALITY

IT systems typically generate enormous volumes of log data, only for it to be ignored until there is a problem with systems, devices, or applications. The diagnostic analysis of log data can be difficult, time-consuming, and when undertaken unaided, very challenging. As spreadsheets and custom script dominate mainstream approaches to log reporting and analysis, insight is also inflexible. In addition, regulations such as Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standards (PCI DSS), and Basel Capital Accord (Basel II) compel organisations in affected industries to implement processes to ensure that log information is managed consistently and is easily retrievable. Consequently, solutions that encompass log and event management, and which can handle log collection, storage, monitoring, and event generation based on rules, diagnostic and forensic analysis, log mining, and reporting, are directly aligned with enterprise business requirements.

Product Analysis

EventTracker is a software solution that collects log data from various log sources such as commercial or custom IT systems, devices, and applications, and integrates the information with log reporting, compliance-oriented reporting, and event management capabilities. The range of technical platforms from which EventTracker can collect logs generated includes Windows systems, Syslog and Syslog NG (typically from Unix systems, and various networking devices), Simple Network Monitoring Protocol (SNMP) v1 and v2, legacy systems, applications, and databases. Across the infrastructure, its coverage extends from servers to workstations, operating systems to applications, network devices to hosts, and physical assets (including USB devices, racks, and server hardware) to hypervisors (i.e. those from VMware, Microsoft's Hyper-V, and management applications such as Dell OpenManage, VSphere, and System Center). The solution classifies, archives, and enriches log data for use by forensic analysis, log data mining, infrastructure management tools, and compliance-oriented reporting. EventTracker is also capable of real-time log monitoring and near-real-time event reporting through a system of rules. Events are anomalies in the log data that could potentially represent a security, performance, compliance, or availability issue. The solution generates alarms and notifications for critical events.

The key components of EventTracker are a management console, a real-time correlation engine, a change management module, and Event Log Central, a central Web server offering that provides controlled access via a role-based, secure Web interface. The user interface design allows the IT user to view all events and to drill down to the detail showing not only the event logged, but also the context in which it was logged. For example, for an application failure the report identifies when the application failed, and allows users to drill down into the context by viewing log entries preceding or following the application failure, affording a better chance to work out what might have caused the failure and what happened after the failure.

EventTracker has two distinct sets of capabilities that help administrators recognise the difference between normal and abnormal behavioural patterns. The first is a rule-based event detection system, which can be used to define pattern-based rules across multiple systems. For example, a rule can be defined to look for a threshold number of failed logins across all systems in the enterprise from a single IP address. If EventTracker detects this condition, an alert can be generated via e-mail, pager, or directly to a system management tool. Early warnings like this are particularly useful for identifying security-related incidents, and by grouping log sources into a logical set it is possible to monitor specific business systems, such as the accounting system or corporate e-mail service.

The Enterprise Activity Monitoring (EAM) feature set is the second set of capabilities that enables the detection of anomalous and therefore potentially high-risk behaviour. It provides a dashboard that enables identification of any new or out-of-the-ordinary activity by users, administrators, systems, processes, or IP addresses, based on statistical and behavioural correlation. This complements the correlation engine, which depends on rules.

Among EventTracker's many additional capabilities and components, the following are of particular note:

- EventTracker provides a comprehensive, powerful reporting interface that enables users to manage reporting of all event data. It enables reports to be configured through a reporting Wizard, and rules to be defined to manage scheduled report generation and individual distribution. Reports can be generated in several formats including printer, screen, Word document, HTML, ASCII text, PDF, and CSV, and can also be viewed in the EventTracker console or within Event Log Central. Users may be notified of reports via RSS feed. EventTracker is shipped with over 2,000 predefined report templates that can be used to monitor compliance with regulatory standards such as SOX 404, GLBA, FISMA, HIPAA, NISPOM, Basel II, FFEIC, and PCI DSS. EventTracker stores all data items associated with an event (such as the events preceding its occurrence, and how it was resolved), and the reporting engine enables users to query complete event descriptions either with the Boolean AND and OR operators, or by using full Perl Compatible Regular Expressions (PCRE) syntax.
- EventTracker Knowledgebase, which is hosted by Prism Microsystems, and which supports users in configuring rules by providing detailed descriptions of all events generated by common infrastructure elements and systems, such as Windows, Unix, and Cisco systems; anti-virus tools; and products from third-party vendors such as Symantec, OpenManage, and VMware. It holds descriptions and suggestions for problem causes and resolutions, which are distilled from information on over 22,000 event logs. Searches can be made using combinations of key parameters such as description, Windows event ID, or source. This is a free service that is updated regularly, as new events are defined.
- EventTracker provides a change auditing capability called EventTracker Change, suitable for Windows servers and workstations. This makes a periodic snapshot of a system's state for comparison against either a 'Gold' master configuration or a previously retained snapshot, enabling administrators to capture and analyse all changes that have occurred on a Windows file system and registry, over a period of time. Changes are also logged on EventVault, which can enable further analysis. EventTracker Change is also integrated with other EventTracker modules, and any policy violation identified, such as a change that violates a policy, triggers an event to be sent to the EventTracker console.
- Ovum believes that monitoring of devices' USB activity particularly differentiates EventTracker. It monitors insertion into and removal from USB ports, and records all activity including writes, deletes, and modifications made to files inside the USB-connected device. It can also instantly disable the USB capability based on violation of predefined policy stipulations. Removable storage devices have become a key weakness in the fight against malicious insider activity and inadvertent introduction of malware or data loss, and comprehensive USB event detection is a noteworthy aspect of EventTracker.

- The incorporation of automated remediation capabilities also differentiates this solution from other log and event management tools. Based on user-defined conditions, EventTracker provides automatic execution of commands or actions such as disabling USB facilities, restarting a service, shutting down a system, stopping a service, terminating a process, or executing custom scripts.
- EventTracker Pulse is a free service provided by Prism Microsystems that enables searching of log data through a simple, Google-like interface. Pulse collects and archives log data from Windows and Syslog sources and provides a personal log search service to assist system and network administrators to detect anomalies and take precautionary measures. This facility fits well with the SME market focus of Prism Microsystems, and has already been downloaded over 10,000 times.

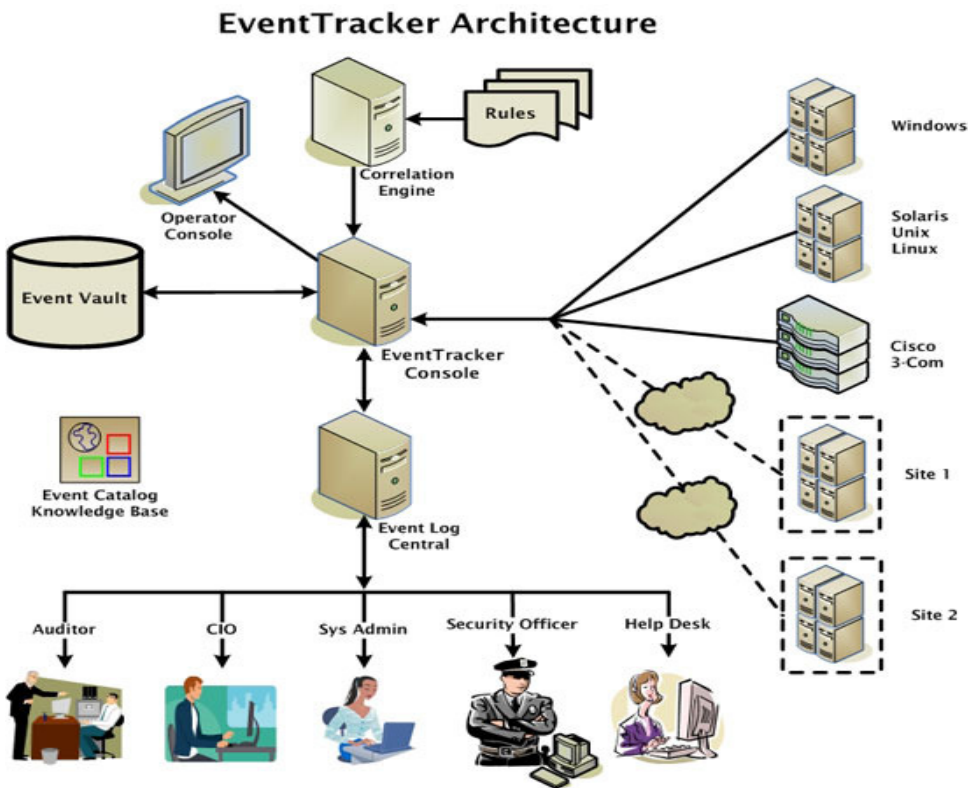
EventTracker does not support integration with vulnerability assessment tools, a facility that some competitor solutions have incorporated for extra value. However, in Ovum's opinion, EventTracker is a well-rounded offering, and is suited to any organisation that manages a number of servers and systems in the order of thousands, and that generates large amounts of log data. This is especially true for organisations in industries that are heavily regulated, and Ovum believes that the need for compliance is a key driver of adoption of log and event management solutions. The reporting capability that is readily available with EventTracker's report templates is of great value in the context of such requirements.

Product Operation

EventTracker incorporates extensive capabilities within its collection layer, which enables agent-based or agentless integration with log environments, as appropriate to the target technology. For example, agents are typically used in Microsoft environments, where log export and real-time event forwarding is not well supported, but elsewhere direct integration with Syslog, Syslog ng, and SNMP is facilitated. Where agent-based monitoring is used, it can enable the monitoring of system thresholds such as CPU, disk usage, and memory. Agents can be remotely installed and configured through the EventTracker console, and are capable of filtering events before these are transmitted to the console based on organisation- or user-specific filtering rules, an approach that helps to reduce the volume of the event stream.

Figure 1 provides a schematic illustration of the EventTracker architecture, showing EventTracker Console as the focal point. The console is installed on a Microsoft Windows server, and is responsible for the configuration and management of agents and the collection of log data. The console is also used for managing customised, organisation-specific rules to those that are pre-defined. The rules are used by Correlation Engine to analyse log data and generate events. This provides a distilled focus of varied log data in the form of a discrete entity representing the high-level occurrence (as determined by Correlation Engine) that should be the target of remediation. Event streams are also captured by EventTracker Console, and users can employ its Event Log Central component to handle administration, configuration, and event viewing, reporting, and analysis. EventTracker Console routes events and all relevant log data to the Event Vault for archival.

Figure:1 EventTracker Architecture



Source: Prism Microsystems

OVUM BUTLER GROUP

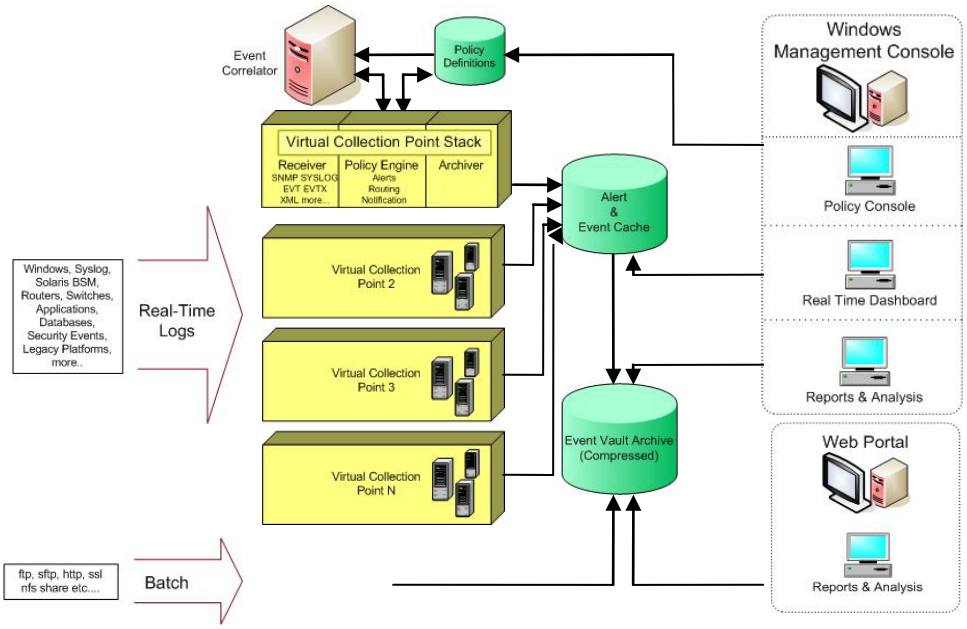
Multiple collection points or consoles can be configured if necessary to provide flexible options to support log collection and temporary storage to support real-time and near real-time reporting, or so that the collection point can be used as a distributed element of the overall organisational log data. Examples of this approach are to enable analysis of events for a specific location or business unit, or to process specific events differently, perhaps by defining rules that filter non-essential events and directly archive them. All event data can be encrypted prior to transmission, and guaranteed delivery mechanisms can be incorporated. Multiple collection points can be useful for organisations that are geographically dispersed and required to locally manage all activities that they are responsible for, while at the same time being able to satisfy enterprise-level compliance requirements.

EventTracker provides Virtual Collection Points (VCPs) in each console that enable collection of event logs on multiple ports at the same time, helping to increase the capacity of EventTracker. Each VCP has a virtualised event processing stack, receiver components, policy engine, and archive component to store events in the Event Vault (see Figure 2). Any number of VCPs can be used, helping to address the requirements of large-scale environments by distributing workloads while incorporating efficiencies with regard to the use of infrastructure. EventTracker supports configuration of multiple, distributed consoles, with each console capable of processing over 20,000 events per second (steady state) in real time using a low-specification Windows server. Incorporating VCPs enables EventTracker to take advantage of multi-CPU or multi-core hardware, and 64-bit operating systems.

Below is a summary of the capabilities of the remaining, foundational elements of the EventTracker architecture:

- Correlation Engine correlates events from the log data transmitted to any VCP or console, implementing real-time monitoring and user-defined rule-based alerting to users or IT administrators via the Web-based user interface, email notification, SNMP traps, or pager alerts. EventTracker is shipped with over 500 predefined rules of the most common conditions. The definition of customised rules is aided by rule Wizards, making a complex rule relatively easy to establish, such as to alert specified users about failed login attempts (over a defined occurrence limit) by a single user or IP address, over a certain period of time, across all machines in the enterprise.
- Event Log Central is a Web portal capable of generating, scheduling, and also viewing log reports within EventTracker. Event Log Central provides secure, Web-based access to log and event date from a standard browser via https. The user view is based on role, with six pre-defined variants (EventTracker Admin, IT Manager, System Administrator, Security Analyst, Auditor, and Help Desk) to which custom roles can be added.
- EventVault manages the storage of archived log data, events, and changes in a compressed, secured event warehouse that can be utilised later for reporting and compliance purposes. It uses a write-once/read-many mode of archiving event log information, and compresses original EventVault log data to less than 10% of its original size, as well as implementing SHA-1 checksum encryption. Storage is within 'cabinet' (.cab) files that can further consolidate many compressed files. Archived data is automatically decrypted and decompressed if it is subsequently needed for reporting. Archives can be stored on any type of storage device, and can only be accessed directly through the EventTracker Console

Figure:2 EventTracker Virtual Collection Point Architecture



Source: Prism Microsystems

OVUM BUTLER GROUP

Product Emphasis

EventTracker enables organisations to deal with log capture, analysis, and archival in environments with thousands of systems. It provides event generation (and some automated remediation) from the underlying individual log entries, change auditing, compliance reporting, and performance- and security-oriented reporting across many and varied event types (user login and logoff, password reset, account lock-out, security profile changes, and system performance problems including CPU, disk, memory, and service performance). Ovum believes EventTracker to be very well suited for its target market, encompassing characteristics such as installation on low-cost servers, consolidation of broad scope into one solution, rapid deployment, the availability of predefined reporting, along with scalability spanning needs ranging from economising to efficiently accommodating extra growth.

DEPLOYMENT

Prism Microsystems claims that configuring EventTracker is relatively straightforward, although one person from Prism Microsystems is usually involved initially, via a Web link or in person. Only one Windows system administrator from the customer's organisation would typically be required. A pilot project usually involves Prism Microsystems personnel assisting installation via a Web link, while a 30-user departmental-scale implementation also requires a knowledge transfer session in addition to the technical deployment. Pilot and departmental-scale implementations are normally completed within a day, while enterprise-wide deployments take up to two days.

The following levels of support are available:

- An online support portal with training videos, product documentation, FAQs, with guidance on feature usage and how-to topics at http://www.prismmicrosys.com/Support/index.php, which can be accessed without registration.
- Provision of upgrades and unlimited e-mail and telephone support 24x5, from both the US and India offices, the cost of which is included in the first-year licensing, and payable additionally subsequently at 20% of the license cost.

Currently, EventTracker can only be deployed on customer premises and equipment. All components of EventTracker are software modules with install Wizards that help organisations deploy the solution. It is available in three editions: Small Business edition (for small office deployments), Medium Enterprise edition, and Large Enterprise edition.

EventTracker can be deployed on Microsoft Windows platforms (Windows 2008/2003 Server), and is able to monitor Microsoft environments (desktops or servers running Windows Vista, XP, 2000, or NT, or Server 2008/2003), Linux environments (via monitoring of Syslog, or Syslog NG), Solaris (via a Solaris BSM agent), and all versions of AIX, HP/UX, z/OS, and Mac OS.

PRODUCT STRATEGY

EventTracker is primarily targeted at mid-sized enterprises with less than US$1 billion in annual revenue and between 500 and 5,000 devices. With compliance-related issues being the primary driver for adoption, the focus is on heavily regulated industries such as finance, healthcare, and government. However, EventTracker is also aimed at companies looking to utilise log management technologies to address issues beyond compliance.

The route to market is via direct sales to customers across North America, and in other parts of the world except EMEA and Asia-Pacific, where sales are via resellers. Direct sales account for 85% of the company's revenues. Prism Microsystems' implementation and distribution partners include COCC, Jacadis, Statworks, JC Hanlon, Finally Software, Abraxax BV, Evercom Networks, Arabesque Group, Paramount, Technology Effect, and Soft Solutions. The company's technology partnerships include Microsoft (where the company is a Gold partner), Sun (Advantage partner), Check Point (OPSEC partner), Type80, Patrick Townsend and Associates, Imperva, and Rapid7.

EventTracker is offered via a perpetual licensing model and is licensed on a per-managed-node basis. The pricing includes all modules and there are no extra charges for optional add-ons such as compliance packs. Prism Microsystems states that the size of a typical entry-level deal is US$8,000, while the average size of a deal is US$30,000, and the largest of the company's deals (involving customised, multi-site licensing) was priced at about US$200,000. An entry-level implementation would normally not require any services support, while an average-sized deal would involve services to the tune of about 10% of the total implementation cost, and that proportion would be about 20% for large deals.

Prism Microsystems typically releases one public release of EventTracker every four months, with interim patches. The next release, version 7, which is planned for early 2010, will include a completely remodelled GUI with many new features, also incorporating Federal Desktop Core Configuration (FDCC) compliance capability, and support for Netflow collectors.

COMPANY PROFILE

Founded in 1999, Prism Microsystems provides solutions for integrated compliance, security, and change management. The company is privately held and funded, and has been profitable since 2002. It is headquartered in Columbia, Maryland US, with research and development facilities at its head office and a facility in Bangalore, India. The company has over 75 employees worldwide and more than 750 global customers spanning sectors including government, finance, retail, healthcare, and technology. Referencable clients may be viewed at http://www.prismmicrosys.com/customers.php.

SUMMARY

The log management technology segment, and the broader Security Information and Event Management (SIEM) market, are areas of high growth and competition, with participating vendors including server platform providers, and software companies that focus on security, IT infrastructure, networking, or SIEM as their major capability. These companies and the solutions provided by them vary in terms of the extent of their solutions' focus on security event management, compliance reporting, and operational performance, as well as the scope of their coverage of data centre, networking, and security infrastructure elements, integration with other solutions vendors' portfolios, and market segment focus (whether oriented to mid-sized or large customers).

EventTracker stands out in several ways as a differentiated offering. Its focus is on the mid-market, although its impressive scalability at multiple points in the solution would be far from limiting in terms of catering for larger customers. In consolidating log management, event management and resolution, and compliance management features, and in covering technical aspects such as remediation and USB-related functions, EventTracker is broad in scope compared with many of its competitors. Overall, this solution, from a growing company that has a large installed base, certainly merits a closer look.

Table 1: Contact Details

Corporate Headquarters
8815 Centre Park Drive
Columbia MD 21045
USA
Tel: (Toll Free from US) 877 333 1433
Tel: +1 (410) 953 6776
Fax: +1 (410) 953 6780
www.prismmicrosys.com

Source: Prism Microsystems

OVUM BUTLER GROUP

Headquarters
Shirethorn House,
37/43 Prospect Street,
Kingston upon Hull,
HU2 8PX, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Australian Sales Office
Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

End-user Sales Office (USA)
245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684