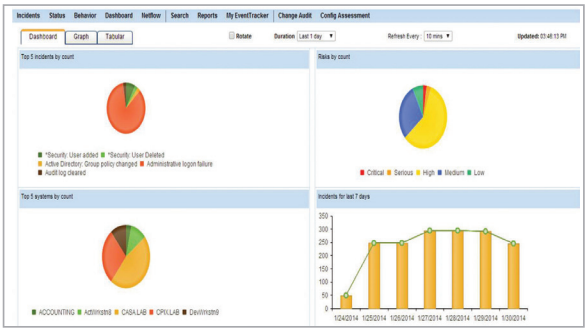
EventTracker Enterprise v7.5



EventTracker Enterprise v7.5 is a remarkable product. This feature-rich tool is designed to meet the needs of organizations of all sizes. It hits all the marks for an enterprise SIEM.

EventTracker can be deployed in a manner that is highly scalable enabling multiple collection points and central consoles (physical or virtual). Its risk-based prioritization of incident identification and automatic or manual remediation solutions are provided out of the box. Too, it provides a large attack signature information source of 2,000 log sources to enhance log parsing and escalation. Threat Intelligence Feeds display IP addresses, URLs, malware, etc. that can be managed for use in alerting, reporting and automated remedial actions. Scripted scheduling provides scripts that can be scheduled with output that are presented in the reports console or other location. This feature is often used to generate reports on Active Directory accounts with expiring passwords, update threat intelligence feeds, geo-locate top/new IP addresses to country of origin, etc.

The EventTracker installation resources came in a USB device. Provided were a virtual machine, an install guide, application installer, license certificate and a user guide. The product requires Win 7 Pro SP1 or higher, Server 2003/2008/2008R2/2012 (Standard or Enterprise, 32- or 64-bit), SQL Express (2008R2) or SQL Enterprise IIS Express 7.5 or higher or IIS 6 or higher and ASP.Net 3.5 SP1.

From start to finish, it took us a half-hour to prepare the server to be used (Windows Server 2008R2) using the documents provided. The actual installation took 10 minutes, including setting up the configuration items. Enrollment of agents took a few minutes from within the EventTracker v7.5 server. Tools were enabled that were used to perform remediation tasks. Syslog network devices, Ubuntu and Linux servers were enrolled. Adding users to the system was easy by putting user IDs in an Active Directory group. Admin rights were initially set up in a separate group. The system had an enormous set of reports and alerts and was a playground of features and functions, including scripted and prepared tools.

Navigating the system was a refreshing treat. The graphic interface was intuitive, with anything we wanted to do completed in a short time. User-defined dashboards were easy to set up. We took only minutes to create a number of ad-hoc alerts. Basically, if you can imagine it, you can create it.

Support options were plain. The annual license renewal includes the technical support, new releases, updates and product enhancements. The company defined three fee structures, including: EventTracker Log Manager, 50 log sources at $1,999/year; EventTracker Security Center, 250 log sources at $12,500/year; and EventTracker Security Center, unlimited log sources, single console at $29,995/year. Further, while the company indicates it provides a call-in support service, it did not indicate hours available.

On top of the maintenance fees, EventTracker provides an excellent knowledge base and FAQ list. The value for the money spent is excellent.

– Peter Stephenson, technology editor

DETAILS

Vendor EventTracker

Price Starts at $1,999 (EventTracker Log Manager, 50 log sources).

Contact eventtracker.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths The attention to quality and the company's creativity.

Weaknesses No weaknesses found.

Verdict EventTracker has hit a homerun with this product. We make it our Best Buy