EventTracker

Security Center v7.6

DETAILS

Vendor EventTracker

Price Starts at $5,995 (depends on options and log source count).

Contact eventtracker.com

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

Strengths Depth of support from both fee-based and no-cost support options.

Weaknesses None found.

Verdict Easy installation, quick configuration and in-depth security coverage elevates EventTracker as one of our top-rated SIEM solutions.

The EventTracker Security Center v7.6 is a great solution for enterprise security information and event management (SIEM). EventTracker does not offer a preconfigured hardware appliance, but the product is available for deployment either as a preconfigured VM or a standalone installer for custom installation. Virtual appliances are available for both Hyper-V and VMWare. The solution has shown significant growth since its v7.5 release, as it now includes full integration of external threat intelligence with internal threat analysis. The comprehensive functionality of this software allows for a security team to properly and effectively develop risk management strategies and policies to help mitigate network incidents.

The tool was easy to set up. It was sent to us on a USB stick containing all necessary documentation and installation wizards to get the installation going. We installed and configured the software using the provided installers on Windows Server 2008R2 in under an hour. The installation and configuration guides were streamlined and extremely easy to follow. Once the installers finished we were easily able to integrate the full functionality of EventTracker with our network and start the testing.

Although we decided to completely set up and configure Security Center v7.6 with our network, EventTracker provides free initial configuration and tuning for all customers. Once installed, it compresses and stores logs on flat files with a 92 percent ratio compression rate that allows for easy retrieval. The use of a flat file database, consequently eliminates the need for a database administrator and allows non-experts to easily take advantage of the software's storage functionality. The product integrates with both external threat intelligence (SANS Top 20 Attackers, Spamhaus, MalcOde, etc.) and internal threat intelligence (behavior anomalies, process whitelisting, IP internal whitelisting, internal blacklisting) to provide real-time threat dashboard, alerts and analytics. This allows for an unknown process that occurs internally to correlate with real-world data, such as communication with known malicious addresses.

All guides are easy to read and provide clear screen shots for most of the steps necessary.

Clients are offered either a basic no-cost or a fee-based support option. The basic includes access to 8/6 phone and 24/7 email support, as well as a knowledge base on the website. The fee-based option provides the option of a partial weekly or full daily managed service.

Overall, the EventTracker Security Center v7.6 is an efficient product and a must-see when searching for a trusted SIEM solution. Once EventTracker is properly installed and integrated, it significantly improves security while simultaneously demonstrating compliance, saving time and maintaining the standards for best practices. – *JV*