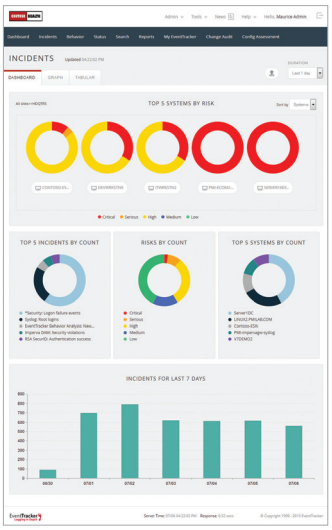

EventTracker
Security Center

DETAILS

Vendor EventTracker

Price Starts from $5,795 to $12,995.

Contact eventtracker.com

Features	★★★★¾
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Excellent value and wide-ranging capabilities in a modestly priced package.

Weaknesses A strong evolution toward full next-gen functionality. While by no means a show-stopper, look for this one to evolve considerably in the near future.

Verdict If you are a SMB, this product is a no-brainer. With a strong feature set for a modest price it is an excellent choice. If you are a larger organization, by no means should you discount this one.

EventTracker is what the company refers to as "co-managed." The software installs on-premises and communicates with EventTracker support. You may select minimal up to daily support. The system is built around industry-standard tools, such as Snort and OpenVAS. EventTracker has done an excellent job of integrating these tools into a coherent user-friendly package. For example, the Snort UI is all right for security techies, but for a quick analysis, such as one might want in a SOC, the UI has been spiffed up considerably using EventTracker's Snorby UI.

We watched a demo of the tool's new features in v8.1 and then deployed the product in the SC Lab. It took very little time to load the software in our test bed, connect to our network and begin testing. The deployment is straightforward and when we looked at the various service bundles available it became clear that this is one of those products with a foot in each of the SIEM and UTM camps. For example, it can be integrated with any of several anti-malware products including client-side tools.

With Snorby it becomes its own IDS/IPS and with OpenVAS it becomes a vulnerability assessment tool that can be run by EventTracker personnel on whatever schedule you choose. Using NTOP NG it also collects flow data. For all of that, EventTracker has impressive support for over 2,000 manufacturers with differing log sources, including standard Windows-based log sources, making it a solid SIEM as well as a very good UTM.

Once the system was up and collecting data, we were able to see threat sources displayed on a geo-location map. Drilling down on one of these sources we got a quick picture of the level and nature of the threat. The tool derives this information based on reputation. Because it integrates with any of several threat intelligence sources, further drill-down reveals known details about the threat, including, among other things, the full whois record for the IP.

Drilling further, we see the processes that are associated with the connection to the threat IP. If malware is involved, you get an MD5 hash which goes to VirusTotal for analysis. Another feature allows a view across the enterprise based on the details of the threat. This helps identify lateral movement within the network, an important aspect of threat hunting. A detailed log of the entire threat process is available enabling a quick analysis of the threat, its current status within the enterprise, and how it got to the point where you discovered it.

Support is excellent and we were well satisfied with the documentation. Reporting is excellent and the vendor even provides a schedule for testing and report generation for a very good mix of regulatory compliance and real security.

– Peter Stephenson, technology editor