

Security information management tools should help consolidate information, provide an audit trail and reporting facilities, as well as give clear overall picture. By Jon Tullett

Organizations need a tool that can consolidate information from various sources and provide a coherent overall perspective, together with intuitive report generation and logging facilities.

Such tools do exist, often under the banner of "security information management" (SIM), "security event management" (SEM), "inci-

dent monitoring," "log management," or other such terms.

What we hoped to find were capabilities that helped us provide a coherent view of the network and its activities, together with the ability to present such information quickly and in an intuitive manner.

We also looked for tools that provide an audit trail and reporting fa-

cilities, and could also interface with existing tools where applicable.

We found them all quite capable. Being able to see your IT infrastructure, its potential vulnerabilities and events intuitively from a central location undoubtedly enables a deeper understanding as well as the ability to respond to threats in a timely manner.

TriGeo Security Information Manager



Supplier TriGeo Network Security
Price from \$19,840 for 50 nodes
Contact www.trigeo.com

This product is based upon a substantial rack-mount hardware appliance running Linux, and a Windows-based console and reporting capability with which to administer the system. Agents are then placed on target machines across the network and acknowledged at the console.

TriGeo is targeting this product at small and medium-sized enterprises. Such organizations do not always have the luxury of full-time information security staff to analyze developments as reported by conventional SIM tools. So the TriGeo approach is to perform real-time monitoring coupled to automated

remediation, based upon a comprehensive set of rules.

In this way, organizations can be protected with a minimum of human intervention.

One should not presume that this product is a plug-and-play device that magically secures your organization from all possible ills. Like any such tool, it will require careful configuration in order to align it to your particular situation and get the best from it.

However, TriGeo make this an easier process than is sometimes the case, with an array of well-considered preconfigured rules and an innovative approach to training. When coupled to comprehensive third-party product support for operating systems, firewalls, routers, anti-virus and intrusion detection systems, you have the basis for a very powerful information management capability.

The appliance supplied for

review was based upon a very substantial Dell rack mount server running a version of Debian Linux. This fired up reliably and reassuringly. The Windows-based console installed without a hitch, is attractive and intuitive, and uses the Crystal Reports run-time for reporting duties.

Agent installation was similarly reliable and one quickly gains the impression that the folks at TriGeo have thought things through pretty well in order to ease the implementation of what is, after all, a potentially complex, yet vitally important capability.

SC MAGAZINE RATING	
Features	★★★★☆
Ease of use	★★★★☆
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★
For Straightforward implementation, automated remediation potential, good third-party product support.	
Against Will still require learning curve on the part of the user.	
Verdict A sturdy appliance-based tool; potentially comprehensive capabilities.	



Our Best Buy is the TriGeo Security Information Manager, a highly capable and comprehensive tool that is nonetheless straightforward in its implementation and well supported by the supplier.

Jon Tullett



TriGeo Network Security, Inc.
 510 Clearwater Loop, Suite 1
 Post Falls ID 83854
 Toll Free: 866.664.9292
 Direct: 208.664.7000
www.trigeo.com