



TriGeo InDepth Melds Real-Time SIEM Correlation and Deep Forensic Log Analysis

IT Search Links SIEM Alerts with Underlying Network Activity

POST FALLS, Idaho (October 15, 2007) —TriGeo Network Security, the proactive network defense company, today introduced TriGeo InDepth, the first IT Search appliance designed to blend real-time event correlation, deep forensic analysis and point and click response.

InDepth gives enterprises search functionality and granular forensic analysis for network events – encompassing users, devices and applications. Powered by Splunk, TriGeo’s new IT Search solution aggregates and archives all log data in real time, with proprietary data collection, storage and indexing technology that delivers secure, fast and repeatable searching across terabytes of data.

“The devil is in the details, which is why IT departments and auditors desire the finest level of information available,” said Michelle Dickman, TriGeo’s president and CEO. “Now, companies can capture and review plain-language alerts of corporate policy violations, and dive deep into the underlying logs – to understand the complete picture of network threats.”

TriGeo InDepth integrates completely with TriGeo SIM to provide a single, seamless console for real-time event analysis and forensic exploration. Completing the circle is TriGeo’s unique Point and Click Response capability that empowers IT staff to act immediately on malicious behavior, policy violations or even just network management issues.

Gartner considers this powerful one-two punch – ease of use and strong analysis – extremely important. “Security information and event management functional requirements are rapidly changing as the technology is adopted broadly to solve compliance and security gaps,” noted Gartner analysts Mark Nicolett and Kelly Kavanagh in Gartner’s May 2007 Magic Quadrant for Security Information and Event Management, (SIEM), 1Q07 report. “Ease of deployment and support and the ability to analyze more detail over a longer period have become key.”

An add-on appliance designed to complement TriGeo SIM, InDepth provides important context for all network activity. While data is analyzed and events are correlated by TriGeo SIM, they’re simultaneously indexed and archived by TriGeo InDepth. The InDepth data can be explored at any time, for any reason, across any period, but when events do occur InDepth surfaces the details needed to take forensic analysis to a whole new level.

Splunk IT Search

Splunk has created the IT Search market for logs and IT data, giving enterprises new visibility into network activity. In the past 21 months, Splunk has added 450 enterprise, service provider and government agency customers, along with 35 OEM partners. The company has won several awards for innovating availability, security, compliance and IT functions, and saving hundreds of staff hours by eliminating manual log searching and filtering, and helping users identify the most important events.

###

About TriGeo Network Security

TriGeo Network Security delivers enterprise security information and event management (SIEM) designed specifically for the needs of the mid-market. TriGeo SIM is the only real-time SIEM appliance that automatically identifies and responds to network attacks, suspicious behavior and policy violations. This award-winning product combines real-time log analysis, event correlation, USB detection and prevention with powerful active response technology. TriGeo SIM is both a unique network defense technology and an "Audit-Proven" compliance solution that meets the security monitoring and log management requirements imposed by PCI, GLBA, NCUA, FDIC, HIPAA, SOX and more.

TriGeo has hundreds of customers across key vertical markets including financial services, health care, government, utility, retail and media/entertainment. TriGeo SIM has won numerous awards including the 2007 SC Magazine Reader Trust Award, the 2007 Gartner Best Execution of a Midmarket IT Solution, and the SC Magazine Best Buy of 2006 award for Event Management. The Company is headquartered in Idaho and is represented by partners nationwide.

For additional information about TriGeo and its products, services and partners, please contact TriGeo at 1 (866) 664-9292 or at www.TriGeo.com.

About Splunk

Splunk is a Silicon Valley company inventing large-scale, high-speed indexing and search technology for IT infrastructures. The company's software indexes and makes it possible to search and navigate data from any application, server or network device in real time. Logs, configurations, messages, traps and alerts, scripts and metrics. If a machine can generate it -- Splunk can eat it. It's easy to download, install and use and very powerful. More than 450 enterprises, service providers and government agencies and more than 125,000 users are achieving higher availability, investigating security incidents in record time, and meeting compliance requirements at lower costs with Splunk. Download a free copy at www.splunk.com.

About the Magic Quadrant

The Magic Quadrant is copyrighted 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Media contacts:

Adam Parken

Dan Brennan

Corporate Ink Public Relations

(617) 969-9192

aparken@corporateink.com

dbrennan@corporateink.com