



## TriGeo Unveils Fifth Generation SIEM Solution

### ***Increased Performance, Scalability, Functionality and Usability Makes TriGeo SIM the Best Security Information and Event Management Solution for Midmarket Organizations***

**POST FALLS, ID (Feb. 16, 2010)** — [TriGeo Network Security](#), the leading provider of [security information and event management \(SIEM\)](#) technology for midmarket enterprises, just launched TriGeo SIM Version 5.0, the most powerful SIEM solution designed specifically for midmarket organizations in [financial services](#), [healthcare](#), government, [utility](#), [retail](#) and media/entertainment.

TriGeo SIM Version 5.0 is the only SIEM solution that combines sophisticated behavioral analysis rules, real-time database monitoring and the automated responses that empower midmarket organizations to proactively defend their networks and protect critical data.

"Effective and comprehensive security solutions are needed by companies of all sizes. However, many companies do not have the resources required to actively monitor and control multiple security solutions," said Charles Kolodgy, research director for security products at IDC. "TriGeo gives midmarket companies visibility into their networks with SIEM, but also incorporates additional security capabilities into its next generation solution. These components simplify management and enhance the ability of smaller IT departments to secure their networks."

Input from industry experts and customers in key vertical markets was combined with leading edge technology and TriGeo's domain expertise to deliver a true fifth generation solution to the challenge of real-time event analysis and proactive network defense.

"TriGeo SIM helps me take a proactive approach to network security with a variety of features, including end-point security through its USB-Defender solution," said Laura Briscoe, VP of information security at Stillwater National Bank. "You can't be passive in IT security, especially when you're working in a highly regulated and highly targeted industry – which is why we selected TriGeo."

TriGeo SIM Version 5.0 delivers:

- **Unmatched anomalous behavior detection enterprise wide.** TriGeo's patented, in-memory correlation engine now has an event analysis capacity that exceeds 10 million simultaneous events providing real-time response to suspicious or malicious activity.
- **Up to 300 times faster performance.** TriGeo's new, high performance, high compression database substantially accelerates data analysis and report performance, providing near-instant insight into network activity.
- **Powerful application layer monitoring and integrated threat management.** TriGeo captures and correlates events from every layer providing complete visibility and proactive network defense. Its powerful rule builder comes stocked with more than 650 pre-configured correlation rules and dozens of

active responses that empower IT teams to immediately address unique security concerns and daily headaches like account lockouts or unauthorized installation or use of third-party applications.

- **Two to five years worth of data in seconds.** TriGeo's live data storage capacity eliminates the need for external storage arrays, and enables customers to quickly pull data to meet any regulatory requirement.
- **Real-time monitoring and enforcement of USB devices.** TriGeo's advanced [USB-Defender](#) provides endpoint detection and protection capabilities with local policy enforcement that prevents the use of unauthorized USB devices on all connected, mobile and even disconnected systems.
- **A state-of-the-art user interface.** TriGeo's new interface includes an "operation center" dashboard with dozens of out-of-the-box widgets designed to provide immediate visual insight into key network security and operation metrics. The new console simplifies workflow with drag-and-drop capabilities and the power to instantly refine real-time views to display only high priority items that help uncover security needles in network haystacks.
- **Enhanced database activity monitoring (DAM).** TriGeo's real-time monitoring of critical databases provides detection and prevention of rogue admin access, SQL injection and many new and emerging data integrity threats.
- **300+ pre-defined reports.** TriGeo's enhanced reporting console includes (at no additional charge) coverage for [every major compliance initiative](#), including the Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and the Health Insurance Portability and Accountability Act (HIPAA).

"We created the market for real-time log analysis to proactively defend the network, and we continue to lead that market by delivering the most innovative SIEM technology available," said Michelle Dickman, president and CEO of TriGeo Network Security. "While other security vendors are focused on cutting costs in a tough economy, we never stop investing in the future to keep our customers out ahead of emerging security threats."

TriGeo SIM Version 5.0 represents more than a year of focused research and development. The solutions' interface is one of the largest commercial Adobe Flex and AIR applications on the market and sets a new standard for real-time network monitoring and security management. Deployed on Dell's latest generation R610 server platform, TriGeo's multi-threaded architecture maximizes the appliance's dual, quad-core processors and multi-channel memory to deliver unparalleled real-time event correlation.

To see a live demonstration of TriGeo SIM Version 5, please visit <http://www.trigeo.com/demo/> or stop by TriGeo's booth at the RSA Conference (booth #817) or Interop Las Vegas (booth #715).

For more information please visit: <http://www.trigeo.com/> or follow us on Twitter at <http://twitter.com/trigeotweets>.

###

**About TriGeo Network Security**

TriGeo Network Security delivers enterprise security information and event management (SIEM) designed specifically for the needs of the midmarket. 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 management, 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, NERC CIP, FDIC, HIPAA, SOX and more.

TriGeo has hundreds of customers across key vertical markets including financial services, healthcare, government, utility, retail and media/entertainment. TriGeo SIM has won numerous awards including three *SC Magazine Awards*, the 2007 Frost & Sullivan North American Technology Innovation of the Year Award, the *Bank Technology News* #1 ranking in the 2008 FutureNow List, and the *SC Magazine Best Buy* of 2006 award for Event Management. The Company is a member of the PCI Security Standards Council and PCI Security Vendor Alliance and is represented by partners worldwide.

**TriGeo Media contact:**

Dan Brennan  
Corporate Ink Public Relations  
(617) 969-9192  
[dbrennan@corporateink.com](mailto:dbrennan@corporateink.com)