



FAQs

MARKET OPPORTUNITY

Q1. How large is the market opportunity for security information management software and related products and services? How fast is this market growing?

A. The following independent assessments indicate both the substantial size and growth of this market and are certainly consistent with the triple-digit growth that TriGeo has experienced for the past two years:

Worldwide SMB security related technology spend estimated at \$11.4 billion in 2006, a 23% increase from 2005 with double digit increases anticipated for the forward three years (AMI-Partners).

SMBs are aware of network security threat but lack sufficient controls (Small Business Technology Institute)

- 70% of surveyed SMBs placed information security as a very high priority
- 18% of email systems and 60% of wireless networks unsecured
- Lack of spending on IDS and patch management solutions

Security and Vulnerability Management (SVM), will grow from \$1.6 billion in 2005 to \$3.1 billion in 2009, a CAGR of 17.8% (IDC)

- SIEM will be largest component by 2009

SIEM market is expected to grow from \$254.1 million in 2005 to \$1,394.4 million in 2012, a compound annual growth rate (CAGR) of 27.5% (Frost & Sullivan)

Many vendors foresee the security management market following a path similar to the evolution of the systems and network management market (Current Analysis)

Q2. What current trends are driving the growth of security information management?

A. Today's organizations are swallowing security technology faster than they can digest it. Several trends are fueling the appetite for security technology. The first is the enormous technical challenge presented by the volume of raw log data being generated by security devices – firewalls, routers, IDS, VPN and operating systems. It is extremely difficult to analyze this data, and impossible to do in real-time, without automation. As a result, many organizations are forced to ignore it until it's clear a breach has occurred – the best they can hope for is to learn enough to prevent future attacks. The second is tremendous pressure of Federal and State regulations. Whether its customer or patient privacy, the risks associated with security violations are enormous. While the fines can be substantial, the liability and business interruption issues can be even larger.

Q3. Who are TriGeo’s target customers?

A. TriGeo’s core target market includes small to medium sized enterprises (SME) with employee sizes ranging anywhere from 50 to 10,000. The early adopters of TriGeo were primarily financial and healthcare organizations dealing with sensitive information and facing regulatory pressure. While these customers are still a significant portion of TriGeo’s customer base, we find that TriGeo has tremendous appeal to a variety of markets and organizations that are focused on network security as a critical component of business continuity.

Q4. Which TriGeo products and services are targeted for which types of customers? How does TriGeo benefit each group?

A. The TriGeo SIM solution is focused on solving problems for small to medium enterprises such as these that do not have dedicated security expertise in place, but still desire “enterprise-class” security coverage. Therefore, TriGeo SIM is designed for IT professionals who are responsible for monitoring all of the disparate security devices across the enterprise. Unlike traditional, passive security information management products, TriGeo takes an active role in defending your network. It is the only product on the market today providing automated remediation through intelligent correlation to the small to medium sized enterprises.

Q5. TriGeo SIM is used to provide enhanced security, productivity gains, and ultimate peace-of-mind to businesses. What are some examples of such applications?

A. Security is enhanced by providing real-time analysis, notification and **response**. Even if you had the staff, it’s simply not possible to manually monitor all aspects of network security on a 24/7 basis. The volume of data generated, from even a fairly small organization, is simply overwhelming. Much greater efficiency is achieved by using automation to identify only those events that require investigation, immediate attention, or even warrant an automated response. SIM solutions, such as TriGeo, are in a position to gather all alerts, and make determinations about whether traffic is malicious based on multiple pieces of data, rather than a single point – without requiring trained security specialists or gurus to analyze the incoming information. Bottom line: The peace of mind is achieved through the knowledge that the system is functioning continuously – performing the tasks that you would perform, following the rules that you established and automatically defending the network.

Q6. TriGeo SIM utilizes Active Response and Notification. What are the advantages of these technologies for busy security professionals?

A. When a worm can traverse the entire Internet in less than 10 minutes, we’ve reached the point where automation is not only desirable, it’s essential. Firewalls actively block undesirable traffic and anti-virus software actively opens, cleans or quarantines infected email. It is a natural extension that SIMs communicate with these, and other tools, to coordinate their actions and empower them to actively defend the entire network.

This communication and coordination is precisely what TriGeo enables via its Active Response and Notification policies. The goal is simple, to empower the IT staff with a tool for rapid incident identification and remediation. We make this possible with a sophisticated event analysis and correlation process that incorporates critical assets and company policy.

When an AV product can’t correct the virus, TriGeo can step in to isolate the machine from the network. When the firewall passes “apparently” harmless traffic the IDS can spot it, and TriGeo can step in to drop the connection. When a workstation is being used to explore unauthorized areas of a system, TriGeo can shut it down.

Q7. There seems to be a glut of competitors vying to deliver “centralized security event management tools” to businesses. How is TriGeo differentiating itself in order to gain the attention of SMEs?

A. Several factors contribute to our success in this arena:

- Our Automated Remediation through Intelligent Correlation™ is the feature most often stated as driving the purchase decision. This market isn't interested in another console. They need a product that can actively defend their network.
- Our appliance-based approach is ideal for organizations with minimal IT staff simply because it's not an additional drain on their already stretched resources. We can literally be installed in minutes, and they can be fully trained the same day. All with zero downtime.
- TriGeo SIM is completely self-contained so it does not require an associated management or database server, saving both the cost and the time associated with server and database configuration.
- TriGeo SIM's interface is designed for IT teams so they can quickly configure and monitor those aspects of the network security that they consider most critical. It does not require dedicated, security professionals to use or maintain.
- TriGeo SIM comes bundled with one of the leading IDS products. This product, while quite powerful, has traditionally been daunting to configure and deploy. By bundling with TriGeo SIM, these organizations are able to employ IDS within their networks with no additional IT staff burden or cost.
- Our pricing model is an ideal fit for this market segment. TriGeo provides full coverage without complex equations for events per second, or costs per type of monitored device.

Q8. Who does TriGeo consider to be its closest competitors and how does it compare/contrast to those vendors?

A. **Network Intelligence**, like TriGeo, is an appliance based solution. However, that's where the similarity ends. Our correlation engine, graphical rule builder, event-centric design and active response model provide a much more robust solution.

ArcSight targets the Fortune 500, so we rarely compete directly, but they're noteworthy for sharing a similar philosophical focus on event taxonomy. ArcSight normalizes the thousands of events down to approximately 150, while our core event model is approximately 350, and we ship with over 500 pre-defined rules. This is critical in an active response system where you need the additional granularity to have the certainty to act.

netForensics has been in this field the longest, but its age shows in its approach to event management. As its name implies, they focus on forensic analysis. Their attempts to shift into a real-time mode are seriously hampered by their current architecture, design philosophy and publicly stated objectives.

Cisco MARS, formerly Protego MARS, is now considered a viable option in the SIM appliance market simply because the Cisco name carries so much weight. The product however is still immature when compared to others in this space, and especially with regard to TriGeo. Correlation construction, the heart of any SIM product, is extremely complex yet limited and among the product's shortcomings is one we view as fatal – it's not real-time. Its dependence on Netflow data, collected at 15 minute polling frequencies, renders the system virtually unusable for real-time analysis and response.

Q9. What are the key market drivers that are fueling SMEs interest in TriGeo SIM's approach to taking raw data and transforming it into security intelligence?

A. Regulatory pressures remain one of the driving forces for the acquisition of SIM technology. While these organizations are smaller they face precisely the same threats, utilize the same tools and must satisfy the same auditors as their much larger counterparts. Of course, their situation is compounded by smaller staffs and budgets. Many SMEs have budget for IDS, and the smart ones realize that bringing in an IDS might appease an auditor, but it will only make their lives more difficult. We show them a way to have it all – IDS coverage, true event management, and a satisfied auditor.

TECHNOLOGY

Q10. You say that TriGeo SIM facilitates simplified audits and reporting, and automates the review and analysis of log files in real-time. How does it accomplish this?

A. TriGeo SIM's architecture is focused on real-time processing. The policy engine is the first thing to process any event, the console is second, and the database is last. This approach means that we're able to bring the full power of the appliance's memory and processor to identifying, notifying and responding to threats.

Traditional auditing and reporting requires a painstaking process of manual log aggregation. Logs are generated by virtually every device in the typical data center, but no two devices log precisely the same way, and in many cases they "speak" entirely different languages. The challenge goes beyond simply getting all the logs in one place, but making sense of all the data. It requires serious effort and expertise.

We like to say that TriGeo SIM is your "security guy in a box". We package the expertise to read, interpret, filter and, most important, highlight those events that require attention. Further, by normalizing the data, translating it to a common language, we're able to generate reports that provide a system-wide view of network security. It's this complete picture that assures auditors you have your security issues under control.

From a technical perspective, TriGeo SIM uses a hybrid agent model. Where appropriate, we deploy an agent to remotely gather and securely forward the relevant events to our central repository. Alternatively, many devices and operating systems can route directly to our manager appliance. The advantage of using TriGeo's agent is that it also serves as a front-line soldier. It can be employed in numerous defense scenarios, such as isolating a compromised or infected workstation.

Q11. It's crucial for companies to make sense of critical security information pouring in from their various security systems. How does TriGeo enable them to do this?

A. A significant percentage of TriGeo's engineering effort is focused on event normalization. This is a critical, and often underestimated, first step in security event management. It's during this process that we tune the Signal to Noise ratio. The reality is that 10,000 events might contain only a few dozen that should be monitored, and those need to be seen in context with information from multiple sources to truly evaluate. Our event-centric normalization facilitates this analysis, and distinguishes us from systems that are limited by device-centric aggregation.

Once normalized, this data can be monitored in real-time, and mapped to specific policies. Policies that answer questions such as: At what threshold does an audit event become a

security event? How should we respond when an attack is focused on a critical asset? Who should we notify of inappropriate web or network access attempts? The answers to these and dozens of other questions can be modeled in TriGeo SIM's policies. This is the key to turning the raw data into actionable information.

Q12. How does TriGeo SIM work? Is it different from the traditional event-correlation technologies? If so, how? What are the advantages of each?

- A. TriGeo SIM's architecture is focused on real-time processing. The policy engine is the first thing to process any event, the console is second, and the database is last. This approach means that TriGeo is able to bring the full power of the appliances' memory and processor to identifying, notifying and responding to threats.

Traditional event management and correlation processes are database-centric, which worked well for forensic analysis where real-time response was not a factor. These systems first write to the database, query this information for their consoles, and lastly apply appropriate notification policy. At best, policy can be applied before the console, but they are still bound by database insertion speed – requiring more powerful and expensive database servers to gain any boost in performance. It should be noted that these systems are ill-equipped to provide active response, and some limit their “responses” to various notification methods (email, pager, etc.)

Q13. What are the key benefits of TriGeo SIM?

- A. With its patent-pending technology, real-time log analysis, automatic alerts and policy-based active response mechanism, TriGeo provides a security information management solution that:
- **Identifies** security threats to your network by analyzing real-time data from the security products you already own
 - **Notifies** you and your team of important events instantly
 - **Responds** to threats with Automated Remediation technology

The key benefits of TriGeo SIM are:

- Log Filtering, Aggregation and Normalization
- Real-Time Event Analysis and Correlation
- Coverage from the perimeter to the desktop
- Automated Remediation and Notification
- Bundled IDS
- Rapid Deployment, with zero downtime.
- Affordable
- Regulatory Compliance and Audit assistance
- True 24/7 network security coverage, with limited staff and minimal budget.

Q14. What is required for TriGeo SIM to gather all the relevant security-related information from across operating systems, applications and the network?

- A. First and foremost, the products to be monitored must be integrated with the TriGeo SIM. The integration allows TriGeo to map the security related events to our proprietary event taxonomy for analysis, correlation and policy enforcement. This process is crucial to truly utilize TriGeo, especially our active response capabilities. While others provide generic “agents” to gather raw data, this is of little value if the data isn't normalized and mapped to the appropriate

policies. TriGeo supports an extensive list of leading network security products, in virtually every major category, with more being added every month.

Q15. Is there a maximum data storage requirement for capturing information from specific security devices? How does TriGeo extend the scalability of such applications?

A. Indeed, data storage can be a serious issue -- more so with pure log aggregation products. TriGeo SIM's model is aided by focusing on the normalized data, which reduces the data storage requirements.

Data can be archived to a secondary machine for pickup by the company's standard backup mechanisms and purged at regularly scheduled intervals.

Larger facilities can employ a data warehouse model using Microsoft SQL Server or Oracle. The warehouse configuration and database licensing is the responsibility of the customer, but we automate the replication of the data and provide reporting and analysis tools.

Q16. What operating systems does TriGeo SIM work with?

A. The TriGeo SIM Manager appliance is self-contained, and runs on a hardened version of Linux. The TriGeo SIM Management Console runs on both Windows and Linux; however, the TriGeo SIM Reports are based on Crystal Reports and are restricted to Windows. Our agent technology runs on a growing number of platforms, including: Windows, Linux, Solaris, AIX, HP-UX, OS400. When the agent is used, we're able to create a compressed and encrypted communications channel that's both secure and bandwidth-friendly.

COMPETITIVE LANDSCAPE

Q17. Are any other companies offering event correlation from the perimeter to the desktop? How does TriGeo compare with these companies and offerings?

A. While others claim "support" for the desktop, TriGeo SIM is the only product actively pursuing this critical security hole. TriGeo believes the competitors' apparent hesitation or lack of deployment in this area is based on two factors: First, their technology relies on communications protocols that are too fat and insecure for desktop usage. Second, their pricing models would make desktop coverage prohibitive.

Q18. What are the advantages of the real-time aspect of the Active Response TriGeo SIM technology?

A. It is real-time analysis, combined with multi-dimensional event correlation that makes Active Response practical. If you're going to empower a system to automatically defend your network, the accuracy of its analysis and the speed with which it can act are the two most critical factors. This is where TriGeo's patent-pending technology enables IT teams to fully utilize the systems and products they already own.

Q19. What advantages does TriGeo SIM deliver over Intrusion Detection Systems (IDS) systems?

A. IDS systems, like many other security tools, are point solutions. They're one element of a rational "defense in depth" model. While TriGeo SIM bundles an IDS, it should not be confused with one.

TriGeo SIM is a Security Information Management product. As such, it works with all of the tools, IDS included, that are at its disposal. Utilizing a unique two-way integration model, TriGeo SIM communicates with all of these devices, correlates their disparate events and can instruct them to work together to defend the network.

TriGeo firmly believes that every organization should deploy an IDS. However, an IDS without a SIM product, simply becomes part of the data glut and management problem. An IDS can be a huge drain on resources and the volume of information generated can easily overwhelm an IT team.

COMPANY

Q20. The ability to shorten product development cycles is critical in the software space. What engineering resources does TriGeo have that enables it to be competitive from a time-to-market standpoint?

A. TriGeo's engineering team is led by a CTO with over 25 years of software application development and management experience. He has organized the team around a highly iterative, rapid application development model, which provides TriGeo with a quick time-to-market stance. TriGeo's development methodology allows it to be extremely responsive to customer requirements and market direction.

Q21. What is TriGeo's business model?

A. To sell a quickly deployable appliance to mid-sized organizations that typically have 5000 nodes or fewer. Most sales presentations are done via a web-based presentation coupled with a live demonstration of the TriGeo SIM. The deployment, configuration and training are currently handled via the internet. This model results in significant savings in the cost of sales as compared to competing technologies that were designed and priced for Fortune 500 organizations

Q22. What is TriGeo's sales and distribution strategy?

A. TriGeo utilizes both regional value added channel partners and an inside sales team who often work in conjunction with each other. TriGeo has a very selective process for selecting channel partners based on their security expertise and ability to truly deliver value added services and complimentary products.

Q23. How are TriGeo's products and services priced?

A. The most important thing about our pricing is that it's simple. There are no hidden costs associated with additional hardware, licenses or professional services. The product's base price is \$19,840 and that includes the appliance, licenses for 50 nodes (data sources), unlimited console licenses, training and the first year of support. Coverage for additional nodes is based simply on volume, with substantial volume discounts, and no distinction for the type of node - Firewalls, Routers, Switches, IDS/IPS, Servers, Workstations – they're all the same price.

Q24. Who are TriGeo's strategic partners?

- A. We have sought technology partners in every major area of network security, and continually work to expand these relationships. A few are listed below:
3Com/TippingPoint, Checkpoint, Cisco, HP, IBM, Juniper, Microsoft, NetScreen, Nortel, Novell, Patchlink, SUN, Symantec, Watchguard, Websense.

Q26. Who are TriGeo's funding partners?

- A. TriGeo is completely privately funded by a group of angel investors comprised of very successful local business people. Their backgrounds range from being the CEO of a 20,000 employee company headquartered in Switzerland to an ex-CFO of one of the country's largest chemical companies. All have substantial business experience and many sit on the TriGeo Board of Directors.

TriGeo Network Security, Inc.
510 Clearwater Loop, Suite 1
Post Falls, ID
83854

Sales: 866-664-9292
Office: 208-664-7000
Fax: 208-666-9710

www.trigeo.com