

October 14, 2005

# The Forrester Wave™: Security Information Management, Q4 2005

by Paul Stamp

TECH CHOICES

FORRESTER®

Helping Business Thrive On Technology Change



October 14, 2005

## The Forrester Wave™: Security Information Management, Q4 2005

Evaluation Of Top Security Information Management Vendors Across 114 Criteria

by **Paul Stamp**

with Laura Koetzle, Natalie Lambert, and Benjamin Gray

### EXECUTIVE SUMMARY

Security information management (SIM) is one of firms' most versatile weapons for handling security threats. Vendors' SIM products help customers detect threatening activities on the network, understand the importance or impact of the threats, and launch remediation plans. There are three common uses of the technology: centralized security operations centers, distributed incident response teams, and compliance management. Consul Risk Management, netForensics, and Network Intelligence each stood out as vendors that will satisfy all three areas, with ArcSight following close behind.

### TABLE OF CONTENTS

- 2 **Making Sense Of Security Information Is Harder Than Ever . . .**
- 2 **Users Need SIM To Stem The Deluge**
- 2 **Product Architecture Matters Most**
- 3 **There Are Three Effective Modes For SIM**
- 5 **SIM Evaluation Overview**
- 8 **Consul, netForensics, And Network Intelligence Lead The Charge**
- 9 **Vendor Profiles**
- 11 **Other Notable Vendors**
- 13 **Supplemental Material**

### NOTES & RESOURCES

Forrester conducted evaluations in June 2005 and interviewed six vendor companies, including: ArcSight, Consul Risk Management, GuardedNet, netForensics, Network Intelligence, and Symantec.

#### **Related Research Documents**

"Security Event Management Cures Data Deluge"  
March 31, 2004, Tech Choices

## MAKING SENSE OF SECURITY INFORMATION IS HARDER THAN EVER . . .

Security information comes from many sources. Customers have to integrate alerts from intelligence services like iDEFENSE (now VeriSign), Cybertrust, and Symantec's DeepSight, reports from vulnerability scanners like eEye Digital Security's Retina and McAfee's Foundstone Enterprise, patches from OS vendors like Microsoft and device makers like Cisco, plus the results of their own internal risk assessments.

### . . . And It's Only Getting Worse

Because there's so much security information clamoring for administrators' attention, data that's hard to collect — like event logs from application servers, Web servers, and network devices — often gets lost in the shuffle. Furthermore, adding physical security events — such as employees badging into restricted areas of buildings — to this mix makes security event analysis even more difficult.<sup>1</sup>

## USERS NEED SIM TO STEM THE DELUGE

Forrester's original TechRankings® evaluation focused on Security Event Management (SEM) products. SEM products focused on correlating multiple events from multiple sources to find dangerous or anomalous combinations, such as a port scan, followed by access attempts on a network share, which may indicate a worm attack.<sup>2</sup>

Now, the space has evolved into SIM, where products look beyond event data to analyze feeds from vulnerability management, threat intelligence services, intrusion detection system (IDS) sensors, firewalls, applications, and other sources.

## PRODUCT ARCHITECTURE MATTERS MOST

SIM users feel most strongly about how their products generate reports and retrieve events, and about the look and feel of their products' dashboards. Other criteria that customers emphasize include the operating systems and hardware that the SIM products support, how the vendor updates and patches the product, and how the product stores the data that it collects. However, no element of product architecture is more misunderstood and divisive than the use of agents. What's an agent? A small piece of software that users must distribute around their networks to collect events.

### Which Is Better: Agents Or Agentless?

Agentless operation remains the Holy Grail, because users are tired of maintaining multiple agents on each of their managed devices. Thus, vendors go through all sorts of contortions to avoid the A-word; they refer to their distributed elements as "collectors," "listeners," or "aggregators." But an agent by any other name is still an agent: Users must either install these collectors, listeners, and aggregators on existing servers and devices — like antivirus gateways or firewalls — or run them on separate boxes nearby. Also, SIM vendors claiming to be entirely agentless still offer "modules" that

perform local data collection or normalization. The main real distinction seems to be whether the distributed element runs on a separate standalone box or on one of the customer's existing devices.

When Forrester created the TechRankings evaluation criteria for SEM, we were careful not to give preference to agent-based or agentless approaches. However, this is the first question that many clients ask about these products. Many distributed incident response teams prefer the agentless approach. Why? Because the team members don't have administration rights on each other's boxes.<sup>3</sup>

- **Agents aren't so bad — really.** Scalability is the most obvious advantage of agents. Most of the SIM products that we evaluated deploy their agents with simple wizards or installation tools. Once installed, the agents gather certain types of relevant events locally and begin the process of cleaning, parsing, and storing interesting ones, easing the burden imposed by geographic distances and network latencies. For example, if the network goes down, the local collector still does its job — it merely forwards the relevant events when connectivity is restored. Agents also make it easier for customers to divide streams of events from particular systems among widely distributed members of incident response teams.
- **But keep those agents off my mission-critical boxes.** While having a dedicated agent on a server or security device buys you a modest increase in control and potentially in information detail, many customers think they're not worth the increased system load. Typically, security operations teams have lots of responsibility for — but little ownership of or authority over — the very systems they are charged with protecting and monitoring. Thus, server operations teams' tactical concerns about agent compatibility and performance take precedence. This is the same argument that has kept host-based intrusion detection systems away from the very places in which you really want them — on servers running critical applications.
- **Freedom from agents is a popular sentiment, but not an ultimate deal breaker.** Of course users prefer agentless event management, because more agents mean more man-hours of maintenance. Freedom from agents also just makes sense in light of the rapidly expanding world of security and network-based appliances. Appliances are coming out fast and furious in all product categories and argue for an agentless approach to data gathering, especially because these vendors are not anxious to support third-party agents on their respective products. However, the brisk sales of agent-based products from vendors like ArcSight and Symantec indicate that, despite their grumbling, customers see value in agents.

### THERE ARE THREE EFFECTIVE MODES FOR SIM

Originally, most customers used SIM tools either to correlate security events from many sources or as auditing tools. Nowadays, though, there are three main functions for SIM:

- **Security operations center.** Centrally located security analysts sitting in a security operations center (SOC) or command center need special capabilities from their SIM products to facilitate

their monitoring of many distributed event sources. SOC users care most about reliability and scalability. They must also consider the products' database query and indexing structures, plus its ability to drill down into events for more information.

- **Incident response.** Many companies manage security incidents with a loosely knit team of folks in many IT and business departments, like network operations, desktop operations, and eCommerce. Because their members are not all sitting together, distributed incident response teams need extra knowledge resources and trouble ticketing features to aid them in responding to events. Leading incident response SIM products scored highest on administration, reporting, and problem resolution management.
- **Compliance management.** Some customers are primarily interested in measurement and reporting on the current state of the security environment and violations of policy — they're usually concerned with regulations like PCI or standards like ISO 17799.<sup>4</sup> In that case, SIM products with compliance-oriented reporting make the grade. These products also possess the ability to manage historical data and to track trends over time. Thus, top compliance vendors scored highest on configuration and flexibility, and special reporting capabilities related to policy or regulatory compliance.

### A Good SIM Product Will Do All Three . . .

Once you take into account all the different requirements for gathering data from all the different systems and presenting it in the right format for all users, SIM becomes a complicated business. SIM involves integrating different types of devices, re-engineering incident response processes, and developing a wide array of report templates for diverse audiences. Thus, although base product license fees aren't astronomical, most packages start between \$50,000 and \$80,000. SIM is still expensive to implement — meaning that most customers who deploy a SIM product will require that it do all three of the described functions.

In the early days of SIM, customers were most interested in making sense of copious amounts of IDS data. Thus, strong correlation technologies were considered most important. However, more and more customers are looking to their SIM products to help them measure the effectiveness of their security programs — which makes compliance management the most important driver.

### . . . And Service Providers Will Be SIM's Biggest Route To Market

Because fully implementing a SIM system can be a long and painful process, only larger enterprises will have the resources available to implement full SIM solutions on their own. Medium-sized businesses, therefore, will turn to service providers like Counterpane Internet Security, LURHQ, Solutionary, and VeriSign to provide them with SIM functionality as a service. Managed security service providers (MSSPs) have always liked SIM products for their ability to correlate events and minimize the number of incidents to which they must respond. Today, MSSPs are now making

much more than just simple information about security events available to customers. MSSPs provide complex, customizable security information specific to the customer's environment via their portals. MSSPs that build their offerings around commercial SIM products will be an important channel for SIM vendors. However, SIM vendors will have to compete both with each other and with the MSSPs' homegrown solutions for the service providers' business.

## SIM EVALUATION OVERVIEW

To assess the state of the SIM market and to see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top SIM vendors.

### Evaluation Criteria

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria (see Figure 1). We evaluated vendors against 114 criteria, which we grouped into three high-level sections:

- **Current offering.** Forrester evaluated each SIM offerings' current capabilities using four groups of criteria: 1) architecture and integration; 2) reliability and scalability; 3) configuration and flexibility; and 4) administration and reporting.
- **Strategy.** To assess the vendors' strategy, Forrester considered the pricing model for the product, the vendor's product direction, and the strength of the vendor's technology partnerships.
- **Market presence.** Forrester aggregated information about each vendor's installed base, the number and reach of its systems integrator (SI) partners, and its own services capabilities, as well as its call center and other support options.

### Evaluation Methodology

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution:

- **Hands-on lab evaluations.** Vendors spent one day with a team of analysts who performed a hands-on evaluation of the product using a scenario-based testing methodology from the original TechRankings, on which we based this Wave. We evaluated each product using the same scenario(s), creating a level playing field by evaluating every product according to the same criteria.
- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria, both for the original TechRankings and the incremental updates during the last year. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

**Figure 1** Evaluation Criteria

| CURRENT OFFERING              |  |
|-------------------------------|--|
| Architecture and integration  | How is the product deployed, what are its components, how does it collect current and stored data, and from what sources?  |
| Reliability and scalability   | How does the product handle changing performance loads? How well does it work in geographically distributed environments? What capabilities does the platform have for ensuring that applications remain available, processing transactions successfully, and responding to system problems? |
| Configuration and flexibility | How extensive is the product's ability to aggregate, normalize, and correlate event data?  |
| Administration and reporting  | How easy, straightforward, intuitive, and functional is the administration console? How complete are the reporting capabilities?   |
| STRATEGY                      |  |
| Cost                          | What is the cost of this product?  |
| Product direction             | How strong is the vendor's overall product direction and ability to execute from a functional, technical, and vendor risk perspective?   |
| Technology partners           | How strongly do technology partners support this product?  |
| MARKET PRESENCE               |  |
| Installed base                | How large is the vendor's installed base of customers for this product and for all products?   |
| Systems integrators           | How strongly do systems integrator partners support this product?  |
| Contact center                | How strong is the vendor's customer service contact center?  |
| Services                      | How strong are the vendor's implementation and training services?  |
| Employees                     | How many engineers does the vendor have dedicated to this product? How big is the vendor's sales presence?   |
| Revenue                       | How strong is the vendor's financial position?   |
| Revenue growth                | What is the vendor's year-over-year quarterly revenue growth?  |

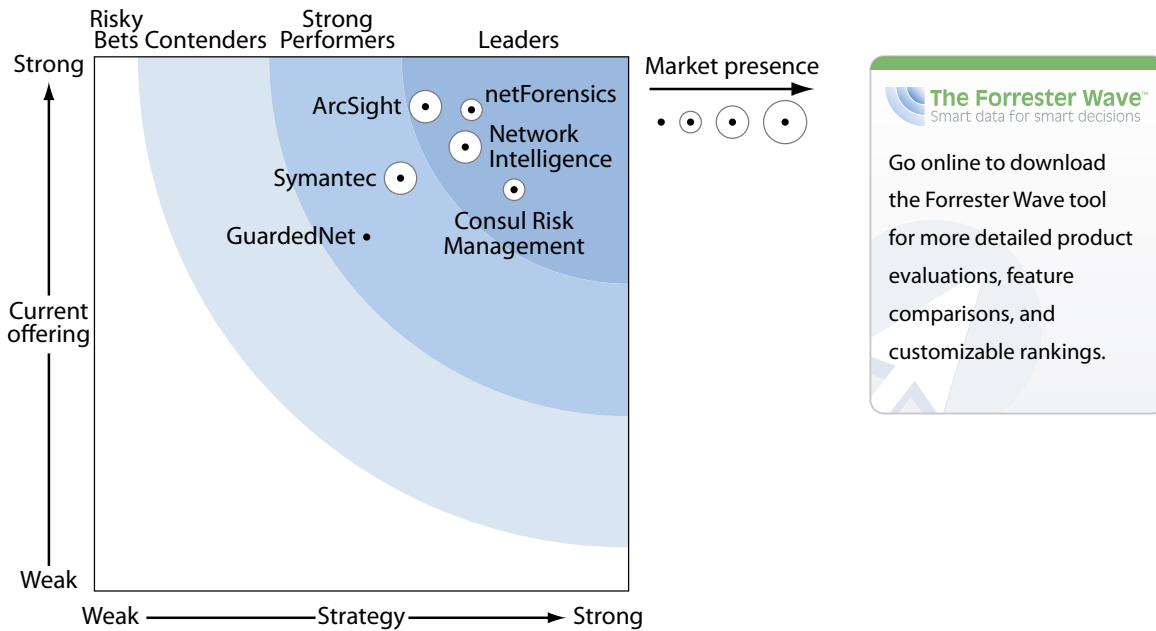
Source: Forrester Research, Inc.

- **Product demos.** We asked vendors to conduct demonstrations of their product’s functionality. We used findings from these product demos to validate details of each vendor’s product capabilities.

**Evaluated Vendors**

Forrester included six vendors in the assessment: ArcSight, Consul Risk Management, GuardedNet, netForensics, Network Intelligence, and Symantec (see Figure 2). Each of these vendors took part in the SEM TechRankings evaluation, and provided updates to their current offering to be included in the evaluation analysis for this Wave. At the time of the TechRankings, several vendors, including Computer Associates (CA), e-Security, and Intellitactics, declined an invitation to participate.

**Figure 2** Forrester Wave™: Security Information Management, Q4 '05



Source: Forrester Research, Inc.

**Figure 2** Forrester Wave™: Security Information Management, Q4 '05 (Cont.)

|                               | Forrester's Weighting | ArcSight | Consul Risk Management | GuardedNet | netForensics | Network Intelligence | Symantec |
|-------------------------------|-----------------------|----------|------------------------|------------|--------------|----------------------|----------|
| <b>CURRENT OFFERING</b>       | 50%                   | 4.51     | 3.73                   | 3.29       | 4.48         | 4.13                 | 3.84     |
| Architecture and integration  | 35%                   | 4.63     | 3.54                   | 3.19       | 4.20         | 4.08                 | 4.02     |
| Reliability and scalability   | 20%                   | 4.86     | 3.60                   | 3.41       | 4.80         | 4.48                 | 4.27     |
| Configuration and flexibility | 20%                   | 4.06     | 3.90                   | 2.36       | 4.72         | 4.06                 | 3.64     |
| Administration and reporting  | 25%                   | 4.45     | 3.98                   | 4.09       | 4.43         | 4.00                 | 3.39     |
| <b>STRATEGY</b>               | 50%                   | 3.06     | 3.89                   | 2.51       | 3.49         | 3.47                 | 2.87     |
| Cost                          | 20%                   | 2.50     | 3.25                   | 3.75       | 3.25         | 4.75                 | 3.75     |
| Product direction             | 40%                   | 3.90     | 4.10                   | 2.90       | 3.60         | 3.80                 | 3.30     |
| Technology partners           | 40%                   | 2.50     | 4.00                   | 1.50       | 3.50         | 2.50                 | 2.00     |
| <b>MARKET PRESENCE</b>        | 0%                    | 3.10     | 2.82                   | 1.56       | 2.79         | 3.12                 | 3.83     |
| Installed base                | 33%                   | 2.45     | 2.30                   | 1.40       | 2.80         | 4.30                 | 3.81     |
| Systems integrators           | 17%                   | 3.20     | 3.80                   | 2.20       | 2.60         | 2.90                 | 2.00     |
| Contact center                | 17%                   | 4.00     | 4.75                   | 2.00       | 2.75         | 4.00                 | 5.00     |
| Services                      | 11%                   | 2.40     | 3.10                   | 1.80       | 2.40         | 2.30                 | 4.40     |
| Employees                     | 11%                   | 2.80     | 2.40                   | 1.70       | 2.80         | 2.50                 | 4.70     |
| Revenue                       | 0%                    | 1.00     | 0.00                   | 0.00       | 0.00         | 0.00                 | 4.00     |
| Revenue growth                | 11%                   | 4.50     | 0.00                   | 0.00       | 3.50         | 0.00                 | 3.50     |

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

### CONSUL, netFORENSICS, AND NETWORK INTELLIGENCE LEAD THE CHARGE

Since Forrester published the first version of the SIM criteria last year, most vendors have developed substantial capability in each evaluation area. Consequently, the evaluation revealed no egregious gaps in vendors' offerings, but leaders have demonstrated both superior execution and solid plans for future product direction:

- **Consul, netForensics, and Network Intelligence take top honors.** netForensics' flexibility earns it a high score in both current offering and strategy. Its Quick Connect technology allows customers to add new unsupported devices quickly and easily, and its built-in workflow engine gives incident response teams the ability to resolve problems promptly. Network Intelligence's homegrown database, LogSmart, allows it to wade through large amounts of online data at high speeds, and its appliance architecture makes deployment easy. Consul has added to its traditional base in the compliance management marketplace with a solid SIM offering, although true integration with the wider InSight suite will come later.

- **ArcSight has a great current offering, but remains more SOC-focused.** ArcSight's wide deployment and scalability give it the best current offering score. However, ArcSight appears more focused on better collection and correlation of information, and visibility into events, rather than concentrating on audit-related activities. Forrester believes this will hinder ArcSight's future progress.
- **GuardedNet and Symantec remain solid offerings but lack the complete picture.** GuardedNet has a smaller, but loyal, customer base that values its workflow and ticketing functionality for incident resolution. Symantec's new appliance-based solution is a big improvement on its previous offering, but relies on other Symantec products for features like compliance management.

## VENDOR PROFILES

The scoring methodology gave better scores in the current offering section to vendors that best serve the needs of one or more of the SOC, incident response, and compliance management teams. Those that demonstrated superior ways to meet the future requirements of SIM customers by offering an overall solution that concentrated more on measurement than monitoring scored highest in the strategy section.

### Leaders

- **netForensics.** The SOC staff and the incident response team will love nFX Open Security Platform. It includes real-time event views, top problem resolution capabilities, and its own workflow engine, so that each member of the team can discover what is happening and who is involved with a glance. A hierarchy of authorized user roles allows team members to report on or display every imaginable slice of the event logs. Efficient agents collect the events, and tag, normalize, aggregate, compress, and forward the logs to the central correlation server.<sup>5</sup>

netForensics has an established relationship with Cisco that has stuttered a little with Cisco's Protego Networks acquisition, but Cisco nevertheless remains a valuable channel. Its new partnership with HP OpenView shows promise. netForensics has a well-defined strategy for adapting to the changing needs of the SIM customer, expanding its reach from event management into incident response and compliance management.<sup>6</sup>

- **Consul Risk Management.** Consul concentrates on business impact, not on infrastructure health. Its InSight Suite product places a higher priority on the way security events impact business policies than on how those events affect the network. The product logs activity by machines and people, on application servers and on the network, and tries to associate that activity with policies. For auditing events, Consul uses the very helpful W7 formula, which asks: Who did it? What did it do? When did it happen? Which application was used? Where from —

which host or connection? Where to? And on what system? This gives Consul a great foothold in the compliance management sector.

Consul's acquisition of NetMon2 also gives it a respectable offering for the SOC, and for the distributed incident response team.<sup>7</sup> However, the integration of NetMon2 with the rest of the InSight Suite is still in its early stages.<sup>8</sup>

- **Network Intelligence.** Easy to install, easy to manage, and extremely efficient — this appliance-based information management product gives any incident response team a real edge.<sup>9</sup> The latest version to LogSmart adds regulatory compliance templates for correlation and reporting, which go beyond just SOX and HIPAA, and include some of the federal reporting standards, like FISMA, NIST-800-26, DCID, and NISPOM.<sup>10</sup>

Its appliance form factor, its starting price tag of \$19,900, and its scalability will make it an attractive proposition for service providers looking to offer a co-managed solution to its customers.<sup>11</sup>

- **ArcSight.** Since Forrester reviewed ArcSight's ESM product, the vendor has released version 3.0, featuring 20:1 data compression in the database. ArcSight has always featured the ability to take a wide variety of actions as a result of its correlation rules "firing." ArcSight ESM 3.0 added to this with interfaces to policy framework systems like Solsoft. ArcSight's integration with Cisco's Network Admission Control (NAC) program will bring information regarding configuration policy compliance into the ArcSight system and — in future releases — quarantining as conditions warrant.<sup>12</sup> For customers interested in finding trends occurring over long periods, ArcSight has introduced its discovery function, which crawls through data archives looking for previously unknown or untracked patterns and then writes new ArcSight correlation rules based on its findings.<sup>13</sup>

ArcSight has a large footprint and will continue to play a major role in the SIM marketplace. However, the company differs from its competitors in that it still sees more future demand for its product in processing real-time security information rather than compliance reporting and long-term trending analysis.<sup>14</sup>

### Strong Performers

- **GuardedNet.** Since our TechRankings evaluation last summer, GuardedNet has added many technical capabilities in neuSECURE version 2.5. The enhanced ticketing makes it easier for team members to communicate with one another and close problems fast. Improved data compression cuts costs associated with storage. neuSECURE version 2.5 has policy and regulatory compliance support, plus a new reporting system, which includes specific packaged SOX reports. However, the product lacks some of the management and configuration tools that its competitors offer. Moreover, the product normalizes all event data, which limits its forensic capabilities.<sup>15</sup>

GuardedNet has struggled to maintain its momentum in the marketplace in the last year. Thus, GuardedNet's acquisition by Micromuse will give the product a much needed shot in the arm marketing-wise, plus opportunities for greater integration with Micromuse's own Netcool systems management suite.<sup>16</sup>

- **Symantec.** Symantec Security Information Manager's strength is in its integration with other elements of the Symantec product suite, like Enterprise Security Manager and DeepSight Threat Management System. Multiple Symantec products can use the versatile agents, which eases implementation and maintenance. The agents also handle basic filtering and correlation and then forward only the most interesting events to the incident response team.<sup>17</sup> Although there have been many improvements to the product since its last release, its reliance on other Symantec products for compliance management will put off customers who don't necessarily want to buy into Symantec's wider portfolio.

However, Symantec continues to be a strong player in managed services and enterprise and consumer security, and Security Information Manager fits well into its overall strategy. Its strong market presence will be an attractive proposition for many prospective SIM buyers.<sup>18</sup>

## OTHER NOTABLE VENDORS

Several other vendors have solid offerings in the SIM space but were not included in the Wave. Among these:

- **OpenService calculates risk and produces metrics.** OpenService's Security Threat Manager version 3 includes attractive features such as risk modeling and performance metrics. The risk calculation starts with a profile of the customer's organization, and then prioritizes security events relative to that profile. Because a local database stays updated with the latest information from eEye Digital Security, ISS X-Force, and other security intelligence services, the product can calculate how vulnerable the target is to that particular set of events. The resulting risk score is useful for prioritizing correlation rules and alerts. The product also provides metrics on threat activity and operational performance by lines of business. In other words, OpenService allows a customer to measure the effectiveness and efficiency of its incident response team, auditors, and administrators in areas like problem resolution and change management.
- **NetIQ offers Security Policy Management and Vulnerability Manager.** NetIQ has a two-pronged security portfolio: vulnerability management and incident management. The two are actually combinations of three years' worth of products developed in-house, acquired from PentaSafe, Marshall Software, and WebTrends, plus an OEM version of Cybertrust's IntelliShield. The event management product accepts IntelliShield alerts, and converts them into custom rules automatically, saving several management steps over competitors.

- **e-Security's design is ideal for large, complex environments.** Its product architecture is supremely scalable and flexible. Using a “messaging bus,” it allows all components, such as the correlation engine, statistics servers, graphical displays, and reporting tools, to work with events without making calls to the database. That saves a lot of time and keeps customers from spending a mint on Oracle licenses to house historical SIM data. The graphical tools, the dashboard, the product's overall ease of use, and its bidirectional communication with problem management products from vendors like Remedy optimize e-Security's product for SOC customers and MSSPs.
- **CA paints a complete picture.** CA's eTrust Security Command Center suite, its eTrust Identity and Access Management products, plus its Unicenter systems management suite give CA the most complete single vendor offering in the marketplace. The eTrust Security Command Center also stands out from the crowd of SEM products because it handles events from physical security systems, such as building entry systems and door controls, as well as IT security events.<sup>19</sup>
- **Intellitactics offers great flexibility . . . at the price of complexity.** The combination of Intellitactics' Security Manager, Security Reporter, and Advanced Analytics combined offer a complete and integrated view of each of the different flavors of SIM. However, by separating the components, this allows organizations to take a bite-sized approach to a complex problem.
- **SenSage expands from log data archive into SIM space.** SenSage — formerly Addamark Technologies — allows its users to search archived security events without the bother of mounting database partitions, making it ideal for environments in which analysts routinely need to mine many terabytes of data for security incident information. Today, SenSage is trying to break into the SIM space with a functional console for managing the collection and correlation of events as they are packed away in the archive.
- **LogLogic addresses the log management problem.** LogLogic LX offers robust appliance-based technology that collects and analyzes security and system log event data for unusual activity and policy breaches. Then, LogLogic ST takes over and archives the logs, streamlining the records management process while making the data available for later interrogation. Forrester believes that log management will be a big driver for SIM and LogLogic is well positioned for this.

## SUPPLEMENTAL MATERIAL

### Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

### Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we narrow our final list to those presented here. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in this document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weighting to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

## ENDNOTES

- <sup>1</sup> Monitoring physical security events alongside IT security events can lead to greater operational efficiency and better security. See the January 11, 2005, Trends “Trends 2005: Security Convergence Gets Real” and see the April 15, 2005, Trends “Converged IT And Physical Security: Small But Real.”
- <sup>2</sup> Detecting worms and other technical threats is just one part of the solution. Companies should establish security measures for before, during, and after the attack. See the March 31, 2004, Tech Choices “Security Event Management Cures Data Deluge” and see the September 15, 2004, Best Practices “Technical Threat Management.”
- <sup>3</sup> In fact, GuardedNet is the vendor with the most visible commitment to agentless deployments, supporting many protocols for event forwarding: AVDL (Application Vulnerability Data Language); Check Point OPSEC LEA; Cisco IDS, including RDEP, XML, and Secure POP; eStreamer from Sourcefire; FTP; SMTP; SNMP v1-3; Syslog; SyslogNG; XML.

- <sup>4</sup> The ISO17799 is the Code of Practice for Information Security Management. Source: <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=>. See the June 23, 2005, Trends “Payment Card Security: Self-Assessment Is Not Enough.”
- <sup>5</sup> netForensics has a large, satisfied customer base. See the September 15, 2004, Tech Choices “Scorecard Summary: netForensics 3.1.1.”
- <sup>6</sup> View the scorecard summary for more detailed analysis on how netForensics fared in this evaluation. See the October 14, 2005, Tech Choices “Security Information Management Scorecard Summary: netForensics.”
- <sup>7</sup> Before Consul acquired NetMon2, in many ways Consul’s InSight Security Manager was more a compliance audit and reporting tool than an SEM product. See the September 15, 2004, Tech Choices “Scorecard Summary: Consul’s InSight Security Manager 5.0.”
- <sup>8</sup> View the scorecard summary for more detailed analysis on how Consul Risk Management fared in this evaluation. See the October 14, 2005, Tech Choices “Security Information Management Scorecard Summary: Consul Risk Management.”
- <sup>9</sup> Network Intelligence enVision v.2.003 comes neatly packaged with the best event storage and searching features, making it desirable for organizations that would rather not have an army of engineers and DBAs managing the product. See the September 15, 2004, Tech Choices “Scorecard Summary: Network Intelligence’s Engine Running enVision v.2.003.”
- <sup>10</sup> The Federal Information Security Management Act (FISMA) was passed as part of the e-Government Act of 2002. See the March 30, 2005, Trends “US Federal Agencies Struggle To Get To The Head Of The Security Class.” The National Institute of Standards and Technology (NIST) released revision one of NIST 800-26 “Guide for Information Security Program Assessments and System Reporting Form.” For more information, see <http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf>. The Director of Central Intelligence Directives (DCID) also has a number of standards for security. For more information, see [www.fas.org/irp/offdocs/dcid.htm](http://www.fas.org/irp/offdocs/dcid.htm). The National Industry Security Program Operating Manual (NISPOM) applies to government agencies and private companies dealing with classified information. For more information, see <http://nsi.org/Library/Govt/Nispom.html>.
- <sup>11</sup> View the scorecard summary for more detailed analysis on how Network Intelligence fared in this evaluation. See the October 14, 2005, Tech Choices “Security Information Management Scorecard Summary: Network Intelligence.”
- <sup>12</sup> Cisco NAC is a specific example of a network quarantine solution. See the June 28, 2005, Tech Choices “Choosing The Right Network Quarantine Solution.”
- <sup>13</sup> ArcSight’s current offering is strong in just about every regard. See the September 15, 2004, Tech Choices “Scorecard Summary: ArcSight 2.5.”
- <sup>14</sup> View the scorecard summary for more detailed analysis on how ArcSight fared in this evaluation. See the October 14, 2005, Tech Choices “Security Information Management Scorecard Summary: ArcSight.”
- <sup>15</sup> For forensic purposes, many organizations require that the product: 1) preserves raw event data and 2) maintains chain of custody for evidence purposes.

- <sup>16</sup> View the scorecard summary for more detailed analysis on how GuardedNet fared in this evaluation. See the October 14, 2005, Tech Choices “Security Information Management Scorecard Summary: GuardedNet.”
- <sup>17</sup> Customers of Symantec security products like Symantec Antivirus, Symantec Enterprise Security Manager, or Symantec Early Warning Solutions will find that Incident Manager is a compatible tool for discovering malicious code activity around the network. See the September 15, 2004, Tech Choices “Scorecard Summary: Symantec Incident Manager 3.0.”
- <sup>18</sup> View the scorecard summary for more detailed analysis on how Symantec fared in this evaluation. See the October 14, 2005, Tech Choices “Security Information Management Scorecard Summary: Symantec.”
- <sup>19</sup> CA holds a special leadership position in the market of convergence of IT and physical security. See the January 11, 2005, Trends “Trends 2005: Security Convergence Gets Real.”

# FORRESTER®

Helping Business Thrive On Technology Change

## Headquarters

Forrester Research, Inc.  
400 Technology Square  
Cambridge, MA 02139 USA  
Tel: +1 617/613-6000  
Fax: +1 617/613-5000  
Email: [forrester@forrester.com](mailto:forrester@forrester.com)  
Nasdaq symbol: FORR  
[www.forrester.com](http://www.forrester.com)

## Research and Sales Offices

|           |                 |
|-----------|-----------------|
| Australia | Israel          |
| Brazil    | Japan           |
| Canada    | Korea           |
| Denmark   | The Netherlands |
| France    | Switzerland     |
| Germany   | United Kingdom  |
| Hong Kong | United States   |
| India     |                 |

*For a complete list of worldwide locations,  
visit [www.forrester.com/about](http://www.forrester.com/about).*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or [resourcecenter@forrester.com](mailto:resourcecenter@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, events, and peer-to-peer executive programs. For more information, visit [www.forrester.com](http://www.forrester.com).