TECH CHOICES

December 5, 2006

The Forrester Wave™: Enterprise Security Information Management, Q4 2006

by Paul Stamp

FORRESTER® Helping Business Thrive On Technology Change

December 5, 2006

The Forrester Wave™: Enterprise Security Information Management, Q4 2006

ArcSight And Symantec Lead, With Network Intelligence And Consul Risk Management Not Far Behind

by Paul Stamp
with Laura Koetzle and Sarah Bernhardt

EXECUTIVE SUMMARY

Forrester evaluated leading enterprise security information management (SIM) vendors across 62 criteria and found that both ArcSight and Symantec had a solid current offering, especially for analysts in the security operations center (SOC), plus a strong vision for where their SIM solutions should fit within the IT ecosystem. Network Intelligence and Consul risk management also offer excellent solutions, especially for those overseeing the security program. Intellitactics, Novell, and netForensics are strong offerings but exhibit certain weaknesses around product vision and cost. CA, eIQnetworks, and NetIQ have solid feature functionality in some areas of SIM but are lacking in others. Finally, Cisco Systems lacks the breadth required by a SIM but is nevertheless a top-class network monitoring tool.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester conducted product evaluations in September 2006 and interviewed 36 vendor and user companies, including ArcSight, CA, Cisco Systems, Consul risk management, eIQnetworks, Intellitactics, netForensics, NetIQ, Novell, Network Intelligence, and Symantec.

Related Research Documents

"Security Information Management Is Much More Than Just A Fancy IDS"
March 24, 2006, Trends

"The Forrester Wave™: Security Information Management, Q4 2005"
October 14, 2005, Tech Choices

TARGET AUDIENCE

Security and risk professional

SIM TOOLS LET SECURITY TEAMS GET AN ENTERPRISE VIEW

Security people thrive on information. But, more complex security infrastructure means that security teams have reams of data to plow through to get to the nuggets of information that they need, whether that be information to identify a threat, investigate an incident, respond to an audit request, or to just demonstrate to management that they're doing a good job. In a survey in January 2006, Forrester found that security teams bought security information management to:[1]

- **Identify the most serious issues that needed a response.** Security analysts in the SOC rely on SIM tools to help them correlate threats and policy violations across disparate systems, prioritize those incidents, and make sure that staff members take the right actions to respond to them.

- **Investigate policy violations and security breaches.** SIM tools help security teams identify the source of incidents and give them the right information to take action against the culprit. Although most security teams with full-blown investigative processes usually use specialized forensics tools, they find SIM solutions especially useful for preliminary investigation. They then use forensics tools for deeper dives.[2] On the other hand, companies without advanced investigative capability use SIM tools as the main weapons in their arsenal.

- **Get a view into the organization's IT compliance posture.** CISOs need a high-level view into where their IT environments are lacking relative to legislative or regulatory mandates, contractual obligations, or internal policies. SIM tools increasingly provide valuable inputs into identifying the areas where the organization needs to improve.

- **Demonstrate the effectiveness of the security program.** Upper management teams are increasingly asking CISOs to prove their value through metrics. In turn, CISOs are requiring that their direct reports demonstrate how well they're doing their jobs. The security team is again calling on SIM tools to help report on operational and business performance indicators.

To help security people achieve these goals, SIM tools generally collect, analyze, and report the following types of data:

- **Events that tell users what's actually happening.** Log data from security devices, network devices, and hosts tell users what happened, when, and by whom. They alert users to threats and policy violations and allow them to investigate issues retrospectively.

- **Vulnerabilities that help users decide the impact of an occurrence.** Vulnerability data about an organization helps to identify problem areas that need attention. Also, vulnerability data helps prioritize issues, for example, when the system sees a hacker attacking a vulnerable host.

- **Configurations that give users a closed-loop view of policy compliance.** System configuration knowledge helps to identify when users misuse privileges to make unauthorized changes. Also, this knowledge allows analysts to track the status of issues that need remediation or changes.

SIM tools still focus largely on event data, but, increasingly, security teams want to incorporate vulnerability and configuration data to get a more comprehensive view of the enterprise security posture.

SIM Output Moves Up The Management Chain

SIM tools used to be purely the domain of the security analyst working on operational issues. These days, the information that a SIM tool provides often ends up on the CISO's, or even the CIO's, desk. Vendors need to adapt and modify the outputs to suit this new audience better. To respond to these new requirements, vendors are starting to incorporate more advanced features in several areas.

- **Identity information ties actions back to a specific person.** Security teams are looking to integrate more information about the identity of IT users, so security teams can 1) map issues back to specific users rather than just devices and 2) get alerted to policy violations by users that cannot be prevented easily by access control.

- **Business metrics help increase the visibility and credibility of the security team.** More and more security teams are looking to metrics gathered by SIM tools to help them measure the value of security, both to get a better idea internally of how effectively they're doing their job and to demonstrate to upper management the business value of the security program.[3]

- **IT policy compliance features map issues to business goals and constraints.** Security managers often need to comply with a slew of regulatory mandates, contractual obligations, and internal IT policies. A SIM tool helps security teams make sense of how a security issue can affect compliance or business goals by mapping issues to best practices frameworks, such as ISO 17799 or COBIT, specific regulations, or custom internal policies.[4]

Fragmented Marketplace Makes Selection A Difficult Task

The security information management marketplace is a confusing beast, with dozens of vendor offerings. Companies in this space, from the smallest to the largest, all claim to cure the security team's information management woes. A vendor's focus generally differs in the following ways:

- **Dedicated SIM versus overall infrastructure focus.** Infrastructure management vendors like CA, NetIQ, and Symantec have long included security information management in their portfolios. Other vendors, including EMC and Novell, have followed suit and have made acquisitions in this space.

- **Midmarket versus enterprise focus.** Two years ago, the vast majority of SIM customers were large enterprises that had the time and resources to invest in complex, flexible solutions. However, in the past two years, a number of solutions from the likes of TriGeo Network Security and High Tower Software have emerged that are more popular with the smaller organization. These solutions have simpler interfaces but fewer options that need to be configured.

- **Operational versus oversight focus.** Some SIM vendors like ArcSight and Cisco have traditionally aimed straight for the operational teams, which need to identify, prioritize, and respond quickly to incidents. Other vendors like Consul and EMC, meanwhile, have aimed their solutions more at providing the tools for those overseeing the IT environment, including tools for measuring policy compliance and managing log data.

Complexity And Politics Are Still SIM's Biggest Enemies

Customers tell us that SIM tools are still difficult to deploy, but usability enhancements aren't likely to change that. SIM, like identity and access management, is by its very nature a heterogeneous problem, and, thus, SIM rollouts involve complex technical integrations and political negotiations. Getting the SIM tool up and running is usually not the critical path in a SIM implementation project — change management processes for monitored devices usually take far longer and drag out the implementation process.

The architecture of the SIM tool doesn't seem to make a whole lot of difference either. Even if a solution doesn't require an installed agent to get information from a system, it still usually requires a configuration change or privileged account to get the data it needs — and system owners aren't likely to let that happen without good reason.

SECURITY INFORMATION MANAGEMENT EVALUATION OVERVIEW

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

Evaluation Criteria Focus On Enterprise Class Deployments

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria to best reflect the needs of the large enterprise (see Figure 1). We evaluated vendors against approximately 62 criteria, which we grouped into three high-level buckets:

Figure 1 Evaluation Criteria

CURRENT OFFERING	
Compatibility and integration	How well does the solution integrate with other security and IT components?
Security operations center	How well can the solution identify threats in real time and facilitate a response?
Digital investigation	How well can the solution aid a security analyst in identifying, prioritizing, and investigating security incidents?
Compliance and reporting	How well can the solution aid in identifying policy violations and gaps in compliance? How well can the solution produce the operational and business reports needed by an organization?
STRATEGY	
Product strategy	What is the overall product strategy and vision for security information management?
Financial resources to support strategy	Is the vendor profitable? What is the vendor's cash flow? Does the company have sufficient revenues, profits, and cash flow to support its strategies?
Cost	What is the cost of this product?
MARKET PRESENCE	
Installed base	How large is the vendor's installed base of customers for this product and for all products?
Revenue	What is the vendor's revenue over the past four quarters?
Revenue growth	What is the vendor's year-over-year revenue growth over the past four quarters?
Systems integrators	How many integrator partners have completed three or more deployments of any version of this product in the past 18 months?
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?
Technology partners	How strongly do technology partners support this product?

Source: Forrester Research, Inc.

- **Current offering.** To evaluate vendors' current offerings, we examined how well they integrate with the devices that they need to monitor and with the tools that facilitate response to a security incident. We also looked at how well the solutions serve the audience in the SOC, those performing digital investigations, and those needing to monitor IT compliance.

- **Strategy.** We looked at upcoming new features in the product offerings and how the companies see their solutions fitting into the IT ecosystem. We also evaluated the financial health of the vendors and the cost of their products.

- **Market presence.** Finally, we examined the customer install base, the vendors' revenues and growth rates, and the number of employees. We also analyzed the companies' key technology and reseller partnerships.

Evaluated Vendors Have Demonstrable SIM Expertise With Enterprise Customers

Forrester identified more than 20 vendors with at least some SIM functionality and evaluated solutions that could demonstrate actual large-scale enterprise deployments. Forrester thus included 11 vendors in the assessment: ArcSight, CA, Cisco Systems, Consul risk management, eIQnetworks, Intellitactics, netForensics, NetIQ, Novell, Network Intelligence, and Symantec. Each of these vendors was able to supply three customer references that were (see Figure 2):

- **Directly monitoring at least 500 data sources using the product.** Each of the references had to be using the solution to capture data from at least 500 devices, including servers, network devices, security solutions, and applications.

- **Using the solution for both real-time monitoring and historical analysis of captured data.** Each of the references had to be using captured data for both real-time alerting to threats and policy violations, as well as for historical query of captured data for audit or investigative purposes.

- **Capturing activity as well as exceptions for at least 25% of the monitored devices.** Each of the references had to be capturing user activity, like successful logon or logoff and file access, as well as exception data, like failed accesses or intrusion events.

- **Keeping online data available for 30 days and archived data for at least six months.** Each of the references had to be keeping data available for online query for 30 days or longer and archived in long-term storage for at least six months.

Furthermore, at least one of the references needed to have annual revenues of greater than $1 billion or be an equivalently sized government department.

Figure 2 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated	Product version evaluated	Version release date
ArcSight	Enterprise Security Manager	3.5	October 2005
CA	eTrust Security Command Center	8.0	October 2005
Cisco Systems	Monitoring, Analysis and Response System	4.2.2	September 2006
Consul risk management	InSight Suite	7.0	May 2006
eIQnetworks	Enterprise Security Analyzer	2.5	July 2006
Intellitactics	Security Manager	5.5	July 2006
netForensics	nFX Open Security Platform	3.4	June 2006
NetIQ	Security Manager	5.5	March 2006
Network Intelligence	enVision	3.3	July 2006
Novell	Sentinel	5.1.3	August 2006
Symantec	Security Information Manager	4.0.3	July 2006

Vendor selection criteria*
Directly monitor at least 500 data sources using the product.
Use the solution for both real-time monitoring and historical analysis of captured data.
Capture activity as well as exceptions for at least 25% of the monitored devices.
Keep online data available for 30 days and archived data for at least six months.
Annual revenues of greater than $1 billion or be an equivalently-sized government department.

*Forrester identified more than 20 vendors with at least some SIM functionality and evaluated solutions that could demonstrate actual large-scale enterprise deployments. Forrester thus selected vendors whose reference customers could demonstrate these attributes.

Source: Forrester Research, Inc.

Other Notable Vendors

Forrester did not include a number of vendors in the evaluation, but some other interesting players in the space include:

- **LogLogic and SenSage, which provide enterprise log management.** Many SIM vendors are taking a leaf out of LogLogic and SenSage's book, providing much richer tools for analyzing log data to look for suspicious activity and finding the root cause of operational problems. However, neither vendor competes directly in the SIM space, and thus we excluded them from the evaluation.

- **Q1 Labs and NitroSecurity, which provide network incident analysis.** Like Cisco, both Q1 Labs and NitroSecurity focus on providing network-focused data to aid the security analyst and network analyst alike. However, neither has a focus on gathering host data, and thus we excluded them from the evaluation.

LEADING VENDORS BALANCE OPERATIONAL AND OVERSIGHT NEEDS

The evaluation uncovered a market in which (see Figure 3):

- **Symantec and ArcSight lead the SOC-focused offerings.** Both Symantec and ArcSight have best-in-class offerings for identifying and alerting to threats and policy violations. What's more, they both have a strong vision for improving their weaker reporting functionality and firm plans for integrations with other security and systems management technologies.

- **Network Intelligence and Consul offer best-in-class auditing with log management features.** The solutions from both Network Intelligence and Consul risk management have moved way beyond simple reporting. The solutions now include much better tools for real-time analysis of threats and policy violations and users are deploying them in some heavy duty environments. Both companies now face the challenge of working out their next moves. Network Intelligence has some large integration efforts ahead, and Consul needs to build on its existing partnerships.

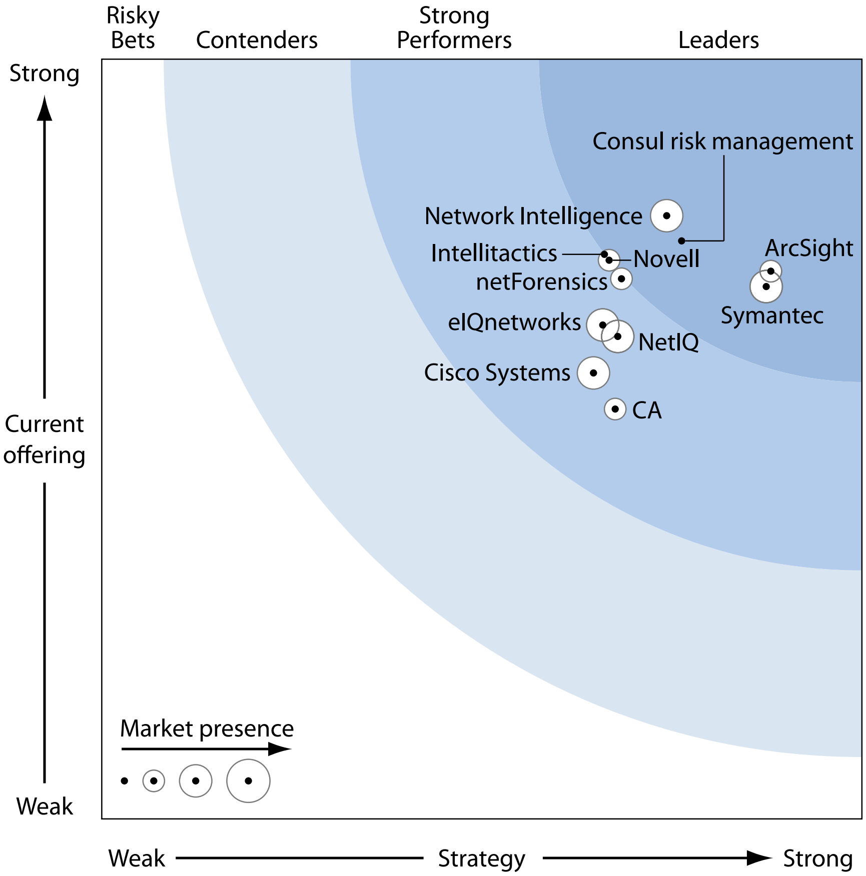
- **Intellitactics, Novell, and netForensics are strong offerings but exhibit some weaknesses.** Intellitactics has vastly improved its reporting and metrics functionality, netForensics still has impressive features for SOC analysts, and Novell is one of the leading solutions for facilitating digital investigations. However, each has its strategic challenges ahead. As standalone SIM vendors, Intellitactics and netForensics need to sharpen their product vision and partner strategy, while others might be put off by Novell's hefty price tag.

- **CA, eIQnetworks, and NetIQ have solid feature functionality but lack broad appeal.** Both CA and NetIQ have a strong story when combined with other security systems management tools from the same vendor, but the SIM tools alone lack some of the wider functionality of their counterparts. A strong up-and-comer, eIQnetworks is making better headway in the larger environments than its traditional install base but still needs to demonstrate true enterprise class functionality to be a leader.

- **Cisco Systems lacks breadth but offers a top class network monitoring tool.** Cisco Systems was the odd man out in this evaluation. The Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) is a great tool for the network-focused security analyst, monitoring suspicious activity on the network and providing great visibility into network events. However, this isn't the right tool for those looking for a more end-to-end view of applications and host activity.

This evaluation of the security information management market is intended to be a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 3 Forrester Wave™: Enterprise Security Information Management, Q4 '06



The Forrester Wave™
Smart data for smart decisions

Go online to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Enterprise Security Information Management, Q4 ’06 (Cont.)

	Forrester’s Weighting	ArcSight	CA	Cisco Systems	Consul	eIQnetworks	Intellitactics	netForensics	NetIQ	Network Intelligence	Novell	Symantec
CURRENT OFFERING	50%	3.60	2.69	2.94	3.81	3.26	3.72	3.55	3.18	3.99	3.67	3.49
Compatibility and integration	15%	4.15	3.10	2.80	3.55	3.50	3.15	3.00	2.65	3.85	4.10	3.90
Security operations center	35%	4.00	3.10	3.65	3.15	2.90	3.15	4.10	3.95	3.40	3.65	4.00
Digital investigation	20%	3.30	1.95	2.85	4.50	4.15	4.05	3.20	3.60	4.60	3.85	3.55
Compliance and reporting	30%	3.05	2.50	2.25	4.25	2.95	4.45	3.40	2.25	4.35	3.35	2.65
STRATEGY	50%	4.40	3.38	3.24	3.82	3.30	3.31	3.53	3.40	3.71	3.40	4.38
Product strategy	50%	4.80	4.00	1.80	4.00	3.00	3.40	3.00	4.00	4.00	4.00	4.20
Financial resources	35%	4.00	3.00	5.00	4.00	3.00	3.00	4.00	3.00	3.00	3.00	5.00
Cost	15%	4.00	2.20	3.90	2.80	5.00	3.70	4.20	2.30	4.40	2.30	3.50
MARKET PRESENCE	0%	2.86	2.20	3.55	1.57	3.31	1.64	2.70	3.10	3.68	2.09	3.25
Installed base	30%	2.40	1.00	5.00	2.20	3.50	2.70	3.10	4.80	4.10	1.80	2.80
Revenue	15%	2.00	5.00	5.00	0.00	1.00	0.00	1.00	3.00	5.00	5.00	5.00
Revenue growth	15%	3.00	1.00	2.00	0.00	5.00	0.00	3.00	0.00	4.00	1.00	2.00
Systems integrators	5%	3.00	3.00	0.00	1.00	5.00	2.00	2.00	2.00	4.00	1.00	2.00
Services	10%	3.60	4.40	1.50	3.60	2.20	3.60	2.20	4.30	2.20	1.50	4.40
Employees	10%	3.40	3.00	1.00	2.40	1.40	1.60	2.80	4.20	3.60	1.00	5.00
Technology partners	15%	3.60	0.70	5.00	1.70	5.00	1.40	3.80	1.70	2.10	2.30	2.10

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

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders

- **ArcSight leads the evaluation of enterprise security information management solutions.** ArcSight leads with its feature-rich security operations functionality and much-improved reporting interface. Since the evaluation, they have also released enhancements to address its shortcomings in trend reporting and log management. Its flexibility and reliability make ArcSight a favorite with many enterprise customers, especially in the security operations center.[5]

- **Consul risk management is solidly among the leaders in the enterprise SIM space.** Consul has expanded its traditional focus on audit and IT compliance with many useful features for the analyst in the security operations center as well as those conducting digital investigations. Moreover, its database audit module makes it a very useful tool for organizations that need to keep very specific information on who has access to sensitive data.[6]

- **Network Intelligence enVision exhibits all-around competence across different SIM functions.** This all-around functionality earns the company the best marks for a current offering among the evaluated vendors. The Network Intelligence solution started life as little more than a reporting tool, and it still has excellent features for capturing data for later retrieval and analysis. However, with improvements to its event correlation and real-time processing capabilities, it's now a lot more useful to SOC analysts.[7]

- **Symantec Security Information Manager 4.0.3 includes many features that SOC analysts love.** It is also much easier to deploy and configure than previous incarnations. Its data management capabilities make it much more suited than previous versions for historical analysis, although buyers must shop elsewhere in Symantec's portfolio for advanced reporting capabilities.[8]

Strong Performers

- **CA.** CA's SIM offering, a combination of its eTrust Security Command Center and eTrust Audit products, forms the core of CA's eTrust security portfolio. As a standalone SIM, the solution lacks some of the functionality and demonstrated scalability of competing SIMs; but, it's still a strong offering, especially for big CA customers and for companies that prefer a framework approach to SIM to generic out-of-the-box functionality.[9]

- **Cisco Systems.** Cisco Security MARS is an excellent, low-cost solution for a network operations or network security team looking to pinpoint and respond to security and availability problems. However, MARS lacks many of the features for monitoring and reporting on threats and policy violations on hosts and in applications that many cross-functional enterprise security teams require.[10]

- **eIQnetworks.** Until about 18 months ago, eIQnetworks played primarily in the small and medium-size business (SMB) market but now boasts a bevy of enterprise customers and large-scale deployments. The Enterprise Security Analyzer solution is quick to deploy, easy to use, and unlikely to induce sticker shock in a potential buyer. Customers with more complex compliance or integration needs might find that the tool is not as flexible as its competitors, but it nevertheless suits the needs of an enterprise with a cost-conscious CISO and a more vanilla IT environment.[11]

- **Intellitactics.** Intellitactics Security Manager has an excellent reporting interface and a data warehouse that provides organizations with a useful tool for investigating security incidents. Its main differentiator, though, is its Security Assurance Metrics module, which provides an excellent business-centric view into the effectiveness of the organization's security posture. Its deployment model and pricing model make it highly flexible, but users tell us that getting full value from the solution is still difficult despite usability improvements.[12]

- **netForensics.** Of the 11 SIM products that Forrester evaluated, netForensics' Open Security Platform (OSP) best supported the goals of the SOC. While OSP provides some of the best out-of-the-box rules and threat identification features, netForensics needs to sharpen its product vision and work on its partner strategy. The company's upcoming release aims to address some of the product's tactical shortcomings, particularly in reporting.[13]

- **NetIQ.** NetIQ's Security Manager is flexible and scalable for large environments. The product excels at culling information from host platforms, especially in Microsoft-centric environments. When used in combination with other NetIQ systems management tools, Security Manager provides solid SIM functionality. As a standalone product, however, Security Manager lacks some of the reporting features of its competitors.[14]

- **Novell.** Novell is a strong all-around performer in the security information management space and, with several large-scale deployments, has a strong track record. Its main strength is the quality of its tools for customizing data sources, rules, and reports, as well as its internal incident and case management capabilities. Novell also has strong plans for incorporating the product into its overall security strategy. However, some customers might find its price tag a little steep.[15]

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

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

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

- **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.

- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with two or three of each vendor's current customers, plus more informal conversations with other customers during inquiry calls.

The 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 then narrow our final list. 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 the Forrester Wave 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 weightings 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

[1] In January 2006, Forrester surveyed 149 technology decision-makers at North American SMBs and enterprises about their approaches to IT security. Thirty percent of respondents said that they were likely to purchase or implement a SIM solution this year. However, almost two-thirds of respondents want SIM for reasons other than detecting and alerting them to attacks on their infrastructure. Rather, they state a primary interest in SIM to help with a variety of issues, including incident response, compliance, and measuring security effectiveness. See the March 24, 2006, Trends "Security Information Management Is Much More Than Just A Fancy IDS."

[2] A digital investigation is the search of computers and other electronic devices for evidence or specific information. Investigations require planning and preparation, but how do you plan for the unknown? Sadly, IT security's culture of secrecy and shame makes it harder for you to learn how to prepare for and conduct successful digital investigations than it is for attackers to learn new attacks and how to cover their tracks. But don't despair — products designed for specific types of investigations, information sharing groups, and partnerships between industry and law enforcement agencies are all making digital investigations less of a

black art. The digital investigations market is entering its adolescent growth spurt. So, what should you do next? Create and train your incident response and digital investigations teams, and form relationships with experts from law enforcement and consultancies, so that they'll be ready to help you when you need them. See the January 3, 2006, Market Overview "CSI: Cyberspace."

[3] Information security managers around the globe are frustrated. They are struggling to make sense of the reams of data being churned out in today's enterprise environment. The real challenge for them is not only to identify what is important but also to be able to tie this information from disparate tools into business-centric metrics so that the senior executives can understand them, take action, and be confident that the enterprise is secure. Security managers must differentiate between sustainable operational metrics that help them manage and business-centric metrics that are meaningful to top management. To craft the right metrics, information security managers need to subdivide the initiative into three discrete phases. See the March 31, 2006, Best Practices "Are We Secure Yet?"

[4] Regulatory compliance is driving many IT organizations to adopt frameworks to manage compliance and accompanying controls. Sarbanes-Oxley (SOX), along with a host of other regulations, has created increased awareness and interest in control frameworks from the business perspective down into IT and information security. The most common frameworks being adopted for IT compliance operate at the levels of IT governance, operations, and security. See the February 24, 2005, Best Practices "IT Frameworks For Control And Compliance."

[5] ArcSight leads the evaluation of enterprise security information management solutions with its feature-rich security operations functionality, its much-improved reporting interface, and its planned enhancements to address its shortcomings in trend reporting and log management. Its flexibility and reliability make ArcSight a favorite with many enterprise customers, especially in the security operations center. See the December 5, 2006, Tech Choices "ArcSight Leads Enterprise SIM Solutions."

[6] Consul risk management is solidly among the leaders in the enterprise security information management space. Consul has expanded its traditional focus on audit and IT compliance with many useful features for the analyst in the security operations center as well as those conducting digital investigations. Moreover, its database audit module makes it a very useful tool for organizations that need to keep very specific information on who has access to sensitive data. See the December 5, 2006, Tech Choices "Consul Risk Management Scores High Marks Among Enterprise SIM Solutions."

[7] Network Intelligence enVision's all-around competence across different SIM functions earns it the best marks for current offering among the evaluated vendors. The Network Intelligence solution started life as little more than a reporting tool, and it still has excellent features for capturing data for later retrieval and analysis. However, with improvements to its event correlation and real-time processing capabilities, it's now a lot more useful to analysts in the SOC. See the December 5, 2006, Tech Choices "Network Intelligence Has The Best Functionality Among Enterprise SIM Solutions."

[8] Symantec Security Information Manager 4.0.3 is much easier to deploy and configure than in previous incarnations, and it includes many features that analysts in the security operations center love. Its data management capabilities make it much more suited than previous versions for historical analysis, although

buyers must shop elsewhere in Symantec's portfolio for advanced reporting capabilities. See the December 5, 2006, Tech Choices "Symantec's Much Improved Offering Is A Leading Enterprise SIM Solution."

[9] CA's SIM offering, a combination of its eTrust Security Command Center and eTrust Audit products, forms the core of CA's eTrust security portfolio. As a standalone SIM, the solution lacks some of the functionality and demonstrated scalability of competing SIMs; but, it's still a strong offering, especially for big CA customers and for companies that prefer a framework approach to SIM to generic out-of-the-box functionality. See the December 5, 2006, Tech Choices "CA Is A Strong Performer But Lags Other Enterprise SIM Solutions."

[10] The Cisco Security Monitoring, Analysis and Response System (MARS) is an excellent, low-cost solution for a network operations or network security team looking to pinpoint and respond to security and availability problems. However, MARS lacks many of the features for monitoring and reporting on threats and policy violations on hosts and in applications that many cross-functional enterprise security teams require. See the December 5, 2006, Tech Choices "Cisco Systems Provides A Network-Focused Enterprise SIM Solution."

[11] Until about 18 months ago, eIQnetworks played primarily in the SMB market but now boasts a bevy of enterprise customers and large-scale deployments. The Enterprise Security Analyzer solution is quick to deploy, easy to use, and unlikely to induce sticker shock in a potential buyer. Customers with more complex compliance or integration needs might find that the tool is not as flexible as its competitors, but it nevertheless suits the needs of an enterprise with a cost-conscious CISO and a more vanilla IT environment. See the December 5, 2006, Tech Choices "eIQnetworks Provides Easy-To-Use, Low-Cost Enterprise SIM Solutions."

[12] Intellitactics Security Manager has an excellent reporting interface and a data warehouse that provides organizations with a useful tool for investigating security incidents. Its main differentiator, though, is its Security Assurance Metrics module, which provides an excellent business-centric view into the effectiveness of the organization's security posture. Its deployment and pricing models make it highly flexible, but users tell us that getting full value from the solution is still difficult despite usability improvements. See the December 5, 2006, Tech Choices "Intellitactics Offers Metrics Reporting Through Its Enterprise SIM Solution."

[13] Of the 11 SIM products that Forrester evaluated, netForensics' Open Security Platform (OSP) best supported the goals of the SOC. While OSP provides among the best out-of-the-box rules and threat identification features, netForensics needs to sharpen its product vision and work on its partner strategy. The company's upcoming release aims to address some of the product's tactical shortcomings, particularly in reporting. See the December 5, 2006, Tech Choices "NetForensics Has The Best SOC Focus In The Enterprise SIM Market."

[14] NetIQ's Security Manager is flexible and scalable for large environments. The product excels at culling information from OS security logs, especially in Microsoft-centric environments. When used in combination with other NetIQ systems management tools, Security Manager provides solid SIM functionality. As a standalone product, however, Security Manager lacks some of the reporting features of its competitors. See the December 5, 2006, Tech Choices "NetIQ Integrates Enterprise SIM Into An Overall Systems Management Strategy."

[15] Novell is a strong all-around performer in the security information management space and, with several large-scale deployments, has a strong track record. Its main strength is the quality of its tools for customizing data sources, rules, and reports, as well as its internal incident and case management capabilities. Novell also has strong plans for incorporating the product into its overall security strategy. However, some customers might find its price tag a little steep. See the December 5, 2006, Tech Choices "Novell Provides A Strong All-Around Enterprise SIM Solution."

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
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

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

For a complete list of worldwide locations, visit 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. 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.

FORRESTER®