

How Proactive Security Organizations Use Advanced Data Practices To Make Decisions

August 5, 2011

Introduction

Both security information management (SIM) and business intelligence (BI) tools were created to make sense of data. SIM tools were created to make sense of security; data and BI tools were created, traditionally, to make sense of business and operational data. Today, there is movement toward an intersection of these tool sets to filter larger and more complex data sets, support more effective and efficient security decisions, and give users greater controls to mine security data for suspicious events and threats. This profile examines synergies between SIM and BI technology adoption trends in enterprises of 5,000 employees or more and reveals expanding user demand for security data filtering, analysis, correlation, distribution, and retention. This market demand is pushing SIM products beyond basic reporting toward a more sophisticated analysis to meet business demands that require deeper IT and business data analytics.

Expanding SIM Use Helps Organizations Make Business Decisions

According to Forrester Research's Forrsights Security Survey, Q3 2010, 41% of North American enterprises have already adopted SIM technologies or have plans to adopt SIM in the next 12 months. The key drivers for implementation are compliance and reporting and incidence investigation (see Figure 1). The adoption of SIM tools for compliance and reporting purposes shows that users intuitively understand that these tools provide the foundation for security dashboards and have re-engineered the products to meet their reporting and visualization needs. SIM tools are good at collecting and correlating data generated by the technologies used in IT organizations, so users naturally gravitated to their SIM to build out their IT data analytics capabilities, embedding SIM as a reporting and analytics tool, helping IT professionals of all types make business decisions.

Beyond those top drivers, a surprising number of organizations (61%) report adopting SIM to demonstrate security program effectiveness to outside groups. Like any other analysis, knowing and proving effectiveness can highlight areas where more work is needed and offer a benchmark for other groups to gauge their progress.

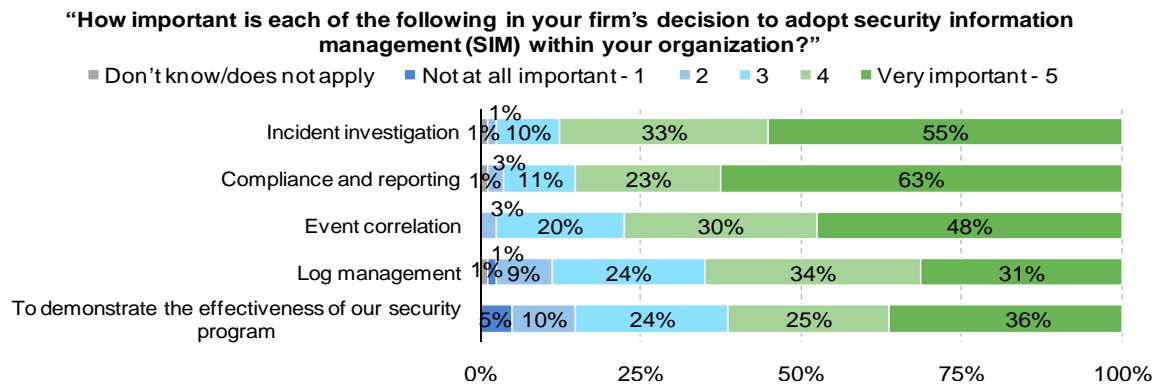


Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

Figure 1

SIM Adoption Decision Drivers



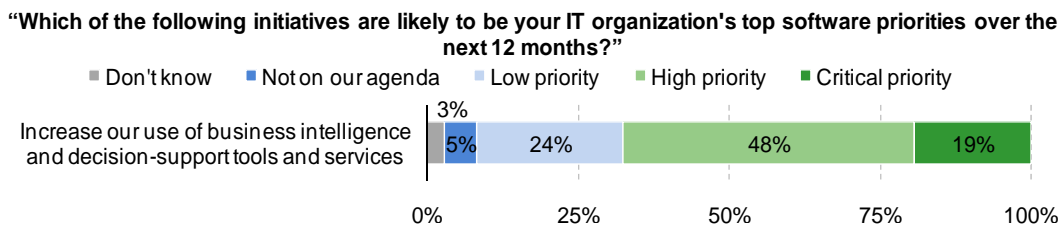
Base: 80 North American enterprises with 5,000-plus employees who have adopted or plan to adopt SIM technologies in the next 12 months

Source: Forrsights Security Survey, Q3 2010

Enterprises are also giving priority to business intelligence activities across the organization. In fact, according to Forrsights Software Survey, Q4 2010, 67% of North American enterprises consider increasing the use of business intelligence and decision support tools and services as a high or critical software priority this year (see Figure 2). This may be a result of IT organizations that are becoming more business-focused but have more and more data — inside and beyond their organization — that they need to understand in order to make effective decisions.

Figure 2

Top Enterprise Software Priorities



Base: 434 North American enterprises with 5,000-plus employees

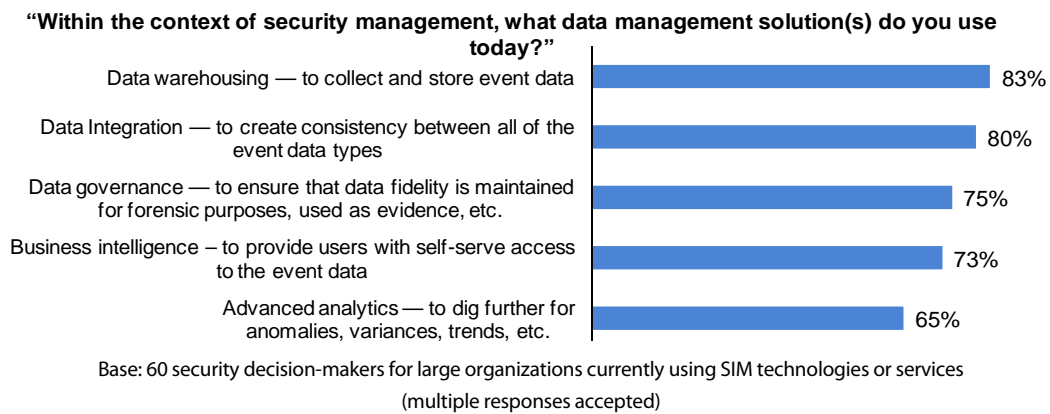
Source: Forrsights Software Survey, Q4 2010

Proactive Data-Driven Organizations Are Getting Even More Value From SIM

In June 2011, Sensage commissioned Forrester Consulting to look closer at enterprises that have already taken charge of security information management by implementing SIM technologies and uncover how these organizations use data and business intelligence as part of their security management processes. The resulting survey of 60 North American enterprise security professionals shows that a full range of data management and analysis use cases are active within existing security management practices (see Figure 3). These use cases indicate notably proactive approaches, not just for the storage of data for basic compliance purposes, but also for the active management of data fidelity, data provisioning for self-service by various role players, and advanced analytics necessary to pursue a deeper understanding of security operations.

Figure 3

Proactive SIM Organizations Have Implemented Data Management Across A Wide Array Of Uses



Source: A commissioned study conducted by Forrester Consulting on behalf of Sensage, June 2011

The intersection of SIM, data warehousing, and business intelligence resonates throughout the IT organization and is driven by three powerful forces: vast amounts of data being generated by IT systems; sophisticated and difficult to discover new threats; and the added complexity from mobile device proliferation, IT consumerization, and cloud computing requirements. This combination creates a perfect storm for even the most advanced IT organization.

The research shows that security organizations using SIM tools are also using data management solutions to support business processes outside IT. When we asked security decision-makers to compare their original SIM implementation with current use, they reported getting much more value from SIM tools today than their original purchase might have predicted (see Figure 4). Not surprisingly, the most popular original uses were compliance, security, and incident response, but today, these tools are used as often for real-time monitoring, risk management, and policy validation. In fact, policy validation and threat correlation have seen the greatest increases in support, compared with original implementation. The increased use of SIM allows organizations to access and analyze IT data to show how security systems, people, and processes are performing — and clearly, they see the value of this intelligence and want more.

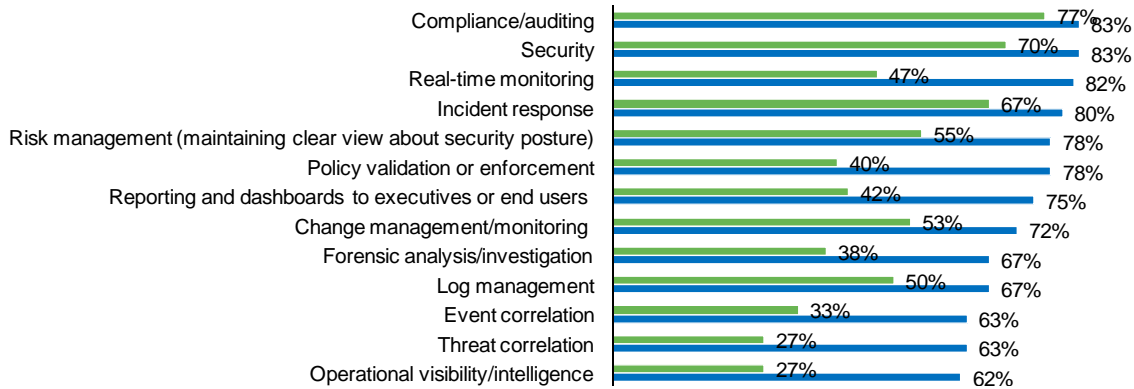
Figure 4

Cross-Organizational Uses Of Data Management Have Dramatically Increased Since Original Implementations

“When your organization originally adopted your data management solution, which processes were you using the solution to support? Which processes do you use data management solutions to support TODAY?”

(Select all that apply)

■ Original implementation ■ Today



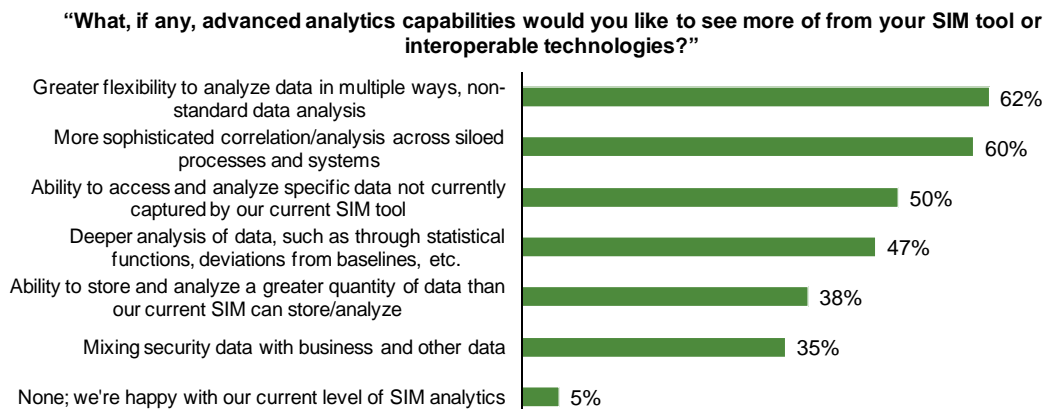
Base: 60 security decision-makers for large organizations currently using SIM technologies or services (multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of Sensage, June 2011

Future SIM Tools Should Focus On Better Data Integration To Meet Market Demands

The increase in use cases across the proactive security organization may just be one step toward the ultimate goals for using next-generation SIM tools in decision-making. When asked about their lingering desires for additional analytics, 95% pointed to one or more areas where they’d like to see more from their tool (see Figure 5). Greater flexibility to pursue nonstandard analysis and a more sophisticated approach across siloed processes were seen as the greatest areas for improvement in analytics. For example, data generated by routers, switches, and applications can be correlated to help track latency, manage bandwidth, and ultimately improve user experiences. By combining security event data with BI best practices, organizations are able to identify long-range attacks more effectively, understanding anomalies and variances in patterns that point to where and when threats are occurring.

Security data retention policies are also putting pressure on SIM tools for incident response and forensic analysis and investigation. Requirement 10.7 of the PCI DSS — requiring log data be retained for at least a year — has become the standard for security data retention. That means new use cases may require security teams to retain and analyze a larger amount of data in order to meet compliance and forensic requirements. Traditional SIM alone can’t grapple with large volume exercises, driving the need for more robust event data warehousing and sophisticated analysis tools, which are capable — purpose-built — to deal with nonstandard, complex correlation and query requirements across a massive data set.

Figure 5**Proactive SIM Organizations Are Still Looking For More Analytics From Their SIM Tools**

Base: 60 security decision-makers for large organizations currently using SIM technologies or services
(multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of Sensage, June 2011

The Future Of SIM Rests In Advanced Data Analytics To Drive Better Security Decisions

IT departments are often faced with more data than they can effectively store, access, and analyze. It's no surprise that mature, data-driven organizations see the need for advanced use of data management to reduce risk and drive cross-functional efficiency and decision-making. This is particularly critical as incidents like insider threats, advanced persistent threats, and data breaches are no longer isolated to one or two areas of IT. New and ever-changing threats and increased compliance pressures, coupled with inherent budget pressures, have created a real need to offer the business deeper analytics of all types of IT-generated data to ensure a secure, compliant, and efficient organization.

Methodology

This Technology Adoption Profile was commissioned by Sensage. To create this profile, Forrester leveraged its Forrsights Security Survey, Q3 2010, and Forrsights Software Survey, Q4 2010. Forrester Consulting supplemented this data with custom survey questions asked of 60 North American security decision-makers at enterprises with 5,000 or more employees that have already adopted SIM technologies or services. Survey questions were related to current and future use and goals for SIM/data management tools. The auxiliary survey was conducted in June 2011. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

About Forrester Consulting

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.

© 2011 Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, RoleView, Technographics, TechRankings, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective owners. Reproduction or sharing of this content in any form without prior written permission is strictly prohibited. For additional reproduction and usage information, see Forrester's Citation Policy located at www.forrester.com. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. [1-IM70YI]