



Skytide Analytical Platform for Security & Compliance Management

There is such an avalanche of data from numerous security and IT systems that companies are finding it nearly impossible to get a clear picture of how well they're managing security and compliance. The Skytide Analytical Platform analyzes all data—structured, unstructured, and extensible—from all data sources to provide insight that security and compliance professionals need to meet their objectives. Only by analyzing data from log files, security systems, transaction systems, and other data sources can companies ensure they're in compliance and protected against security attacks.

Increasing Volumes of Data Is Forcing Changes to Data Management and Analysis

To comply with evolving federal and industry regulations such as Sarbanes-Oxley and HIPAA, enterprises are spending billions of dollars annually on new and expanded systems, information storage, time-consuming audits, and the people to manage it all. At the same time, sophisticated attacks by external parties and internal policy violations by employees result in substantial risk of downtime, remediation, liability, litigation, and damage to corporate reputation.

This presents a very real data management dilemma for organizations regardless of vertical industry—it puts enormous pressure on those responsible for the operational health of the organization. In particular, Security and Compliance officers and their staffs are faced with the challenge of sorting through an exponentially growing volume of event data and log files from the ever-increasing reliance on pervasive information technology.

For example, a bank needs to analyze data from numerous sources to get a complete picture of how secure their systems are, including card-swipers, web logs, intrusion detection system (IDS) logs, firewall logs, surveillance video, application logs, network access logs, call transcripts collected by call centers, and banking transactions.

In order to do their jobs more effectively, security and compliance professionals need to juggle an often conflicting set of business requirements:

- Provide high-quality IT services to customers, partners, and fellow employees
- Achieve maximum system availability while lowering IT costs
- Comply with all industry and government regulatory requirements
- Defend against, identify, and respond to security threats and various Cyber-crime issues
- Improve operational efficiencies required by the business

The task is made all the more difficult as security and compliance requirements become larger, more complex, and more demanding, putting severe pressure on IT's ability to continue to provide high quality service. Achieving all of these business requirements is dependent upon and highly reliant on the analysis of

A Customer Example: Trade Latency

Trade latency is an example of how the sequence of events, more than the events themselves, indicate whether there's a compliance breach or not.

Trade latency is when a stock, bond, or commodity trader executes a trade outside of the allowed time window trying to gain an additional benefit from the changed price. This creates a liability issue in that the broker rather than the customer benefits from the trade, and a business performance issue, because if the price moves in the wrong direction the company will be liable for the difference.

Analyzing transaction files will never identify this problem. Only through more sophisticated analysis available from Skytide, such as Path Analysis, will companies ensure such practices are identified and minimized.

Challenges to SIM Solution Adoption

Market acceptance of Security Information Management (SIM) solutions has been slow, and the barriers to a higher level of adoption by the marketplace are formidable.

- 1. Too much log data**—Companies can have hundreds to thousands of devices generating millions or even billions of events per day. This equates to multiple gigabytes of data daily for most organizations. Downstreaming and analyzing such a high volume of information is both costly and time-consuming.
- 2. Lack of an industry-standard log format**—Computers, firewalls, routers, switches, servers and various applications each use a different, often proprietary, format. This is true of protocols and formats as well, such as syslog, snmp, XML, odbc, and Cisco POP.
- 3. No standardization across vendors**—Most vendors support unique data repositories and data management technologies. Many rely on a RDBMS data storage model, whose characteristics create additional overhead on the system.
- 4. High cost of initial implementation and maintenance**—After initial system costs ranging up to seven figures, it is estimated that companies spend an additional \$200,000 per year maintaining a log management system (SANS Study).
- 5. Log file-only orientation**—Existing SIM solutions focus on individual log files when what is really needed is to correlate information across multiple log files as well as with other sources of data such as ERP systems.

(Continued on next page.)

numerous data sources. One can only be confident of the company's security and compliance performance if all the available data from all parts of the business are being analyzed. There is no such thing as 100% security but rather a constant move toward a more secure environment by continuously monitoring and analyzing all data and by continually introducing new analytical models in response to ever-changing security threats. Security and compliance is like anti-virus software. Just like one has to upgrade the virus definition file all the time to stay on top of the recent attack threats, one needs to be constantly adding new data sources and changing existing analytical models assessing the threats.

Analyze Large Volumes of Diverse Data to Gain Critical Insights

The Skytide Analytical Platform is the industry's first solution specifically designed to apply the knowledge gained from traditional business intelligence solutions to log files and event-based information sources. With Skytide, companies can gain insight into all the elements of a security solution—availability, authentication, accountability, confidentiality and integrity—by correlating data within and across diverse systems, and doing so in a fraction of the time and cost of today's conventional solutions.

With the Skytide Analytical Platform, companies can:

- Analyze patterns from multiple events to provide insight into attacks, breaches, faults and systemic problems
- Perform event correlation among varied sources with respect to unusual activity monitoring, forensic investigations and event reconstruction, with the goal of identifying patterns to expose insider abuse, policy violations or operational anomalies
- Look beyond simple volume data or compliance metrics to analyze a series of events and identify risks associated with action or inaction
- Reduce risks through early identification of the sequences of events that may adversely effect business performance and create a liability
- Identify the drivers behind key performance indicators (KPI), enabling companies to address the root cause and improve business performance while maintaining high levels of security and compliance

Skytide's unique solution features sophisticated yet easy-to-use technology that delivers insight into security and compliance management issues, which is not possible with traditional software vendors in this space.

The software vendor community has responded to the log file and event management analysis problem with security information management (SIM) solutions, but the market acceptance of those solutions is still in its adolescence. Several factors have contributed to this slow adoption, including the high volume of data, the lack of industry standards, and long delays from events to analysis (see Challenges to SIM Solution Adoption sidebar).

The Skytide Analytical Platform enables organizations to address these shortcomings by providing a sophisticated way of analyzing network, security, and application log data without having to store it in an external repository.

Skytide Analytical Platform—Technology Overview

The Skytide Analytical Platform uses multi-dimensional analysis to answer the who, what, what if, and why questions companies ultimately need to know in order to ensure compliance and security.

Skytide technology utilizes the concepts of *dimensions* and *measures*. Dimensions represent the objects of analysis. For example, in a network intrusion log, *dimensions* could be the source IP address or attack signature and time.

Challenges to SIM Solution Adoption

(Continued from previous page.)

- 6. Rudimentary analysis**—The tools provided by the vendors are focused on trends and alerts, and usually provide a set of pre-defined rules and reports that are mapped to common security monitoring guidelines and compliance standards. This limits the flexibility to do ad hoc analysis and is limited to just the data that is indexed and referenceable within each vendor reporting tool.
- 7. Analysis Latency**—Standard BI solutions require restructuring of the data and moving it from where it naturally resides into a datamart or data warehouse, causing significant delays in gaining insights into log data. Analysis latency becomes a significant risk factor when dealing with time-sensitive data governance and security issues.

The unique capabilities of the Skytide Analytical Platform enable it to overcome all of these obstacles, providing timely, cost-effective, and insightful analysis across all data sources.

Skytide, Inc.

1820 Gateway Drive,
Suite 300
San Mateo, CA 94404

Phone:
1.650.292.1900

Fax:
1.650.312.1400

E-mail:
info@skytide.com

Internet:
www.skytide.com

© 2006 Skytide, Inc. All rights reserved. Skytide and the Skytide logo are registered trademarks of Skytide, Inc. All other trademarks are the property of their respective owners.

Measures represent the numeric data that you analyze across *dimensions*. For example, in the same network intrusion log example, the number of instances of connections between a particular pair of IP addresses would be a *measure*.

In this way, Skytide enables you to answer such questions as, "How many instances of a particular attack are originating from a particular IP address?" And, "Which particular IP addresses are attractive to attackers over time?"

Dimensions are also hierarchical. For example, attack signatures can be grouped into categories, such as Denial of Service. *Measures* can then be calculated according for each group within the hierarchy.

Solution Benefits

The Skytide Analytical Platform provides the following benefits:

- **Streamline Your Analysis**—You can focus on only the important data you need to satisfy your analytical requirements, significantly lowering the bandwidth and storage requirements.
- **Fast Time To Analysis**—Since Skytide does not require that data be normalized and imported into a proprietary repository, datamart or data warehouse, analytics can be performed in near-real time or at the customer's discretion.
- **High Value; Low Cost**—Skytide delivers high-value, low-cost solutions. For example, you don't need to license a data warehouse or datamart, which can be cost-prohibitive. Also, the system is designed for business users without IT assistance, lower ongoing maintenance costs.
- **Flexible, Customized Reports**—Skytide allows the user to slice and dice the data as needed. It is not limited by pre-defined reports and a fixed view of the data because Skytide brings the data in at the time that the analysis is needed.

Using the Skytide Analytical Platform, you will achieve these key insights at a low cost and with a minimum of training. Our unique patented technology is based on industry standards, such as Java, SOA and XML, so it can be implemented quickly and without disruption to your current systems. Skytide technology was designed with ease-of-use in mind while providing the capability to meet complex analytical needs.

Please take a test drive of the technology at our website, www.skytide.com, or contact us at info@skytide.com for more information.

About Skytide

Skytide is a leading provider of next-generation analytical solutions that provide an unprecedented view into what is driving business performance. Skytide's breakthrough technology uses XML as a common layer to dramatically reduce system complexity while offering advanced functionality that cannot be achieved by traditional BI technology. Application areas for Skytide technology include contact centers, risk and security management, compliance, and other areas of business that generate significant volumes of mission-critical unstructured and semi-structured data. Skytide partners include IBM, Sun Microsystems and Inxight. Based in San Mateo, CA, Skytide is a privately held company funded by Granite Ventures and El Dorado Ventures.

For more information about Skytide, please visit www.skytide.com.

