Gartner

Research

Publication Date: 13 May 2005 **ID Number: G00126563**

Selection Requirements for Business Activity Monitoring Tools

Bill Gassman

When evaluating business activity monitoring product alternatives, focus on the features that distribute alerts and display business indicators, the analytic engine that generates the information and the mechanisms to collect business events.

WHAT YOU NEED TO KNOW

Business activity monitoring requires a basic set of functionality, but competition is driving providers to offer advanced features. When comparing products, use this decision framework to break down the alternatives by architectural level and evaluate the need and availability of basic vs. advanced features.

ANALYSIS

Along with the increased availability of products for business activity monitoring (BAM) come many features from which to choose. Although the purpose of BAM technology is to provide business users with real-time access to, and analysis about, important business indicators, the level of sophistication in the solution can widely vary. The output of a BAM application may be a simple e-mail message, or BAM may be the underlying technology for a complex operational decision support system. The analysis underlying a BAM application may use simple threshold comparisons, or it may incorporate standard deviation monitoring, complex event processing and pattern matching.

The requirements for sophistication are driven by how complicated the business indicators are to obtain and monitor, what analysis is involved in delivering the information, and the decisions and actions that will be driven by the insight delivered. As with many software projects, budget, skills and motivation also determine what is selected.

BAM functionality is based on a relatively simple architecture. Alerts and frequently updated displays are driven by a processing and analytic engine that is supplied with a stream of events that is received or collected from a variety of sources working in real time. When evaluating products, it is easier to use an architectural approach to understand the value of available alternatives.

Use the architectural breakdown and description of basic and advanced criteria in this research as evaluation guidelines. They do not include every feature on the market. The evaluation criteria are based on:

- Gartner's view of how BAM capabilities will develop
- Discussions with BAM technology providers
- Client requirements

Depending on its target market, a BAM solution does not have to support every feature listed here, but it must address the general requirements and each the basic features of four architectural categories:

- Delivery and display
- Processing and analysis
- Operational databases
- Event collection, filtering and transformation

General Requirements

A system to monitor business activity will likely:

- Require continuous operation
- Support mission-critical business functions
- Operate in a fault-tolerant mode
- Make configuration changes during operation
- Retain context during restarts
- Have enough instrumentation so that its health can be monitored with self-contained operations and maintenance tools, or managed with an IT operations framework

In addition, security requirements, ideally through integration with an enterprisewide security model, are applicable at each architectural layer. Vendor requirements for viability and support are dependent on how long the solution will be deployed and the urgency and complexity of the business problem being addressed.

Delivery and Display

Although the degree of sophistication in a BAM system lies in its ability to process and analyze events, the value is exhibited in the timeliness, accuracy and context of alerts. To get the most value out of a BAM product, users need a degree of visual delight, usability, perception of performance and at least task-level integration with other applications. Most BAM systems offer a console with a thick, thin or rich Web client to show key business indicators and manage alerts. A separate mechanism to deliver alerts is commonly included. Alerts can be consumed by people, drive scripted actions or be sent to other event-driven applications.

Basic features to look for:

- A visually intuitive dashboard that updates in real time and can be personalized
- Delivery of alerts in multiple formats — e-mail, instant message, icon-tray, Short Message Service (SMS) or pager — with support of Extensible Markup Language (XML) formatting
- User-controlled filtering and reporting of alerts, and setting the scope of what is monitored
- Scripting tool to accomplish simple actions based on the context of an alert

Advanced features to look for:

- Web links in alerts that point to detailed drill-down information (internal or external to the BAM system)
- Guided decision support with suggested actions and resolutions
- Support for links to unstructured information, such as policies, contracts and manuals
- Embedded business intelligence functions for historical reporting and analytic tasks
- Collaboration tools to share views of situations and discuss actions
- Knowledge-capture features to record situations, actions taken and results
- Search capability through events, captured knowledge and rules

- Incident life cycle management system to prioritize, assign, forward, escalate and close alerts
- A rule editor and activation utility that is easy to use by a broad user base, such as drag-and-drop definition and wizard-driven actions
- A design utility to build custom dashboards with standards-based portal support
- Dashboards and reports tailored to vertical-industry-specific jargon, tasks and best practices
- Delivery of alerts to integration brokers, with transformation to specified event formats

Processing and Analysis

Processing and analysis are the core of a BAM system. They determine the system's sophistication, and these capabilities are important to establishing trust with users that the critical business indicators are being monitored correctly. Scope and scale are the key issues. Scope is determined by the type of rules that are supported and the ability to obtain and maintain historical context. Scale is important, because processing and analysis must keep up with a rapid stream of events with little latency between significant incidents and emergence of results.

Basic features to look for:

- Continuous-flow rule engine that processes each event that has successfully passed through the event-filtering and transformation layer
- Library of analytic functions, such as static and dynamic thresholds, absolute values, duration, coincidence, frequency, statistical balance and rate of change

Advanced features to look for:

- Discrete and aggregated metric analysis
- Complex event processing — rules can be nested and based on a sequence of events
- Support of forecast analytic models and rules that trigger on forecast changes
- Packages of metrics and rules that are tailored for a vertical-industry solution
- Use of scripting tools to verify situations before issuing alerts and add external data context before delivery
- Captured event replay to enable analysis and debugging; detect correlations; and model, simulate and optimize rules
- Compliance features to examine metadata for rules, including source, modification log (who, what and when), times activated and deactivated, how often invoked and how often triggered
- Complex event-processing rule development environment
- Integration with external rule engines
- Security to restrict access to sensitive data and rules based on profiles

Operational Databases

Several databases may be required in a BAM system. A real-time operational database is used to maintain the state of metrics and business indicators, and as temporary storage for intermediary results of complex rules. Additional historical databases may be present for auditing purposes.

Basic features to look for:

- High performance, which may be delivered through in-memory databases
- Persistence to maintain context across application restarts
- Derived, abstracted and aggregated metrics support, with immediate update as root metrics are changed — analogous to spreadsheet function
- Maintenance functions to age and archive data that is no longer required

Advanced features to look for:

- The ability to easily implement changes to the schema of the event-driven operational database
- Federated query support to enable a single query by a scripted action to obtain data from multiple sources
- Historical storage of basic and derived metrics — state changes and values — to provide context for rules and alert drill-down

Event Collection, Filtering and Transformation

The analytic engine is fed by a stream of raw events. The source of events can be passive or active. Passive collection is accomplished through integration broker subscriptions, listening daemons or Web services, and provides the least latency with the lowest overhead. Active collection uses scripts or remote software agents that are associated with the BAM system to poll for information and look for changes, then generate an event that represents the change.

Basic features to look for:

- Validation and augmentation of incoming events to ensure data quality and add contextual information, such as the source and a time stamp
- Event cleansing, such as sequencing and consolidating duplicates
- High-performance design that queues event streams until they can be processed
- Library of adapters to event sources, such as message brokers
- Change data capture agents for databases and event logs
- Polling engines for data acquisition

Advanced features to look for:

- Configuration of collection agents to acquire what is needed and filter what is not
- Screen scrapers to gather information from applications
- Web page data capture of unstructured information
- Development tools to build adapters as required

- Event-profiling utility to aid in building transformations
- Transformation functions, such as data type conversion, string manipulation, calculations, lookup and replace, and aggregations
- Prepackaged adapters and transformation routines for specific vertical applications, such as retail point of sale or healthcare diagnostic systems

Key Issues

What evaluation criteria should IT managers consider for business activity monitoring systems?

Acronym Key

BAM	business activity monitoring
SMS	Short Message Service
XML	Extensible Markup Language

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner